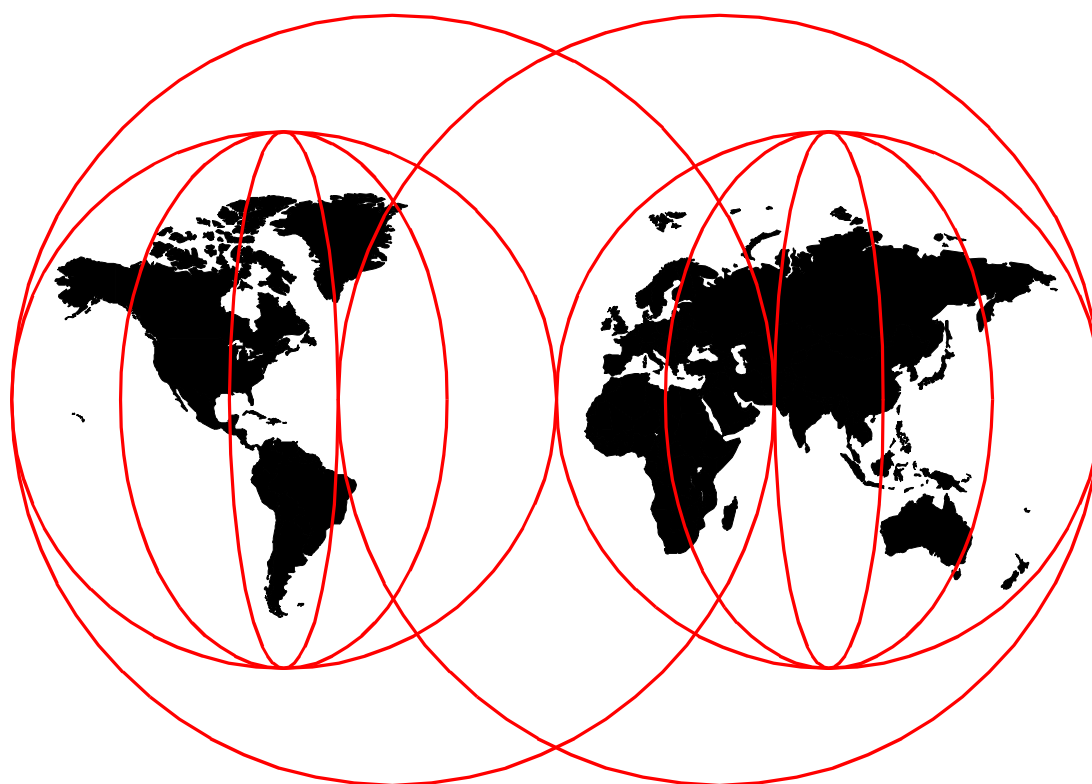


AS/400 Internet Security: Implementing AS/400 Virtual Private Networks

*Marcela Adan, Thomas Barlen, Weng Wai Chia, Andrew Grant,
Darrell Grundy, Peter Hey, Stephan Imhof, Linda Kinnunen, Eric Zeier*



International Technical Support Organization

www.redbooks.ibm.com



International Technical Support Organization

SG24-5404-00

**AS/400 Internet Security: Implementing
AS/400 Virtual Private Networks**

December 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix A, "Special notices" on page 877.

First Edition (December 1999)

This edition applies to Version 4 Release 4 Modification 0 of OS/400 (5768-SS1), Version 4 Release 4 Modification 0 of IBM Cryptographic Access Provider (5769-AC2 and 5769-AC3), and Version 4 Release 4 Modification 0 of IBM Client Access Express for Windows (5769-XE1).

Comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. JLU Building 107-2
3605 Highway 52N
Rochester, Minnesota 55901-7829

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1999. All rights reserved.

Note to U.S Government Users - Documentation related to restricted rights - Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Preface	xv
The team that wrote this redbook	xv
Comments welcomexvii

Part 1. VPN concepts and overview 1

Chapter 1. Virtual Private Network (VPN) overview	3
1.1 Private networks	3
1.1.1 Traditional private network	3
1.1.2 Modern private networks	4
1.1.3 Virtual Private Networks (VPN)	6
1.2 VPN customer scenarios	7
1.2.1 Branch office connection scenario	7
1.2.2 Business partner and supplier scenario	8
1.2.3 Remote access scenario	9
1.3 VPN requirements	9
1.4 VPN protocols	10
1.4.1 IP Security (IPSec) protocols	11
1.4.2 Summarizing the main VPN protocols	12
1.4.3 VPN versus SSL	13
1.5 Authentication Header (AH)	14
1.5.1 AH packet format	14
1.5.2 AH transport and tunnel modes	16
1.5.3 AH transforms	17
1.6 Encapsulating Security Payload (ESP)	18
1.6.1 ESP packet format	18
1.6.2 ESP transport and tunnel modes	20
1.6.3 ESP in tunnel mode	20
1.6.4 ESP transforms	21
1.6.5 Why the need for two authentication protocols (AH and ESP)?	22
1.7 Combining AH and ESP	23
1.7.1 Transport adjacency	23
1.7.2 Iterated tunnels	23
1.8 Key management objectives	25
1.8.1 Internet Key Exchange (IKE)	26
1.8.2 The two phases of IKE	26
1.8.3 IKE main and aggressive modes	28
1.9 IPSec configuration concepts	29
1.9.1 SA combinations	30
1.9.2 Security Parameters Index (SPI)	31
1.9.3 IPSec policy databases	31
Chapter 2. Introduction to Layer 2 Tunneling Protocol (L2TP)	33
2.1 Remote access overview	33
2.2 The evolution of dial-up networks	34
2.2.1 Traditional dial-up networks	34
2.2.2 Modern dial-up networks	36
2.3 L2TP overview	37
2.3.1 L2TP Access Concentrator (LAC)	38
2.3.2 L2TP Network Server (LNS)	38

2.3.3	Call establishment	39
2.3.4	Address allocation	39
2.3.5	Authentication	39
2.3.6	Security	40
2.3.7	Tunnel modes	40
2.3.8	L2TP encapsulation	40
2.4	L2TP tunnel modes: Compulsory and voluntary	41
2.4.1	L2TP compulsory tunnel	41
2.4.2	L2TP voluntary tunnel	43
2.4.3	VPN tunnels comparison	45
2.5	L2TP IP address management	45
2.6	L2TP security with IPSec	47
2.7	L2TP characteristics summary	48

Part 2. VPN implementation on the AS/400 system 49

Chapter 3. AS/400 VPN implementation	51
3.1 AS/400 VPN overview	51
3.2 VPN software prerequisites	52
3.3 AS/400 VPN components	53
3.3.1 VPN graphical user interface (GUI)	53
3.3.2 New Connection Wizard	53
3.3.3 CL commands	54
3.3.4 VPN and L2TP server jobs	54
3.3.5 VPN policy database	54
3.3.6 IP packet security	55
3.4 Layer Two Tunneling Protocol (L2TP) VPN support	55
3.5 Virtual Private Network Network Address Translation (VPN NAT)	56
3.6 Planning considerations	57
3.6.1 Verify TCP/IP communications and routing	57
3.6.2 VPN through firewalls and routers	57
3.6.3 Interoperability	58
3.6.4 Basic planning	61
3.6.5 Selecting the VPN connection type	62
3.6.6 New Connection Wizard planning	63
3.6.7 Key policy (IKE phase 1) and data policy (IKE phase 2) lifetime and size limits	65
3.6.8 IP packet security planning	66
3.6.9 Miscellaneous planning considerations	67
3.7 VPN configuration overview	68
3.7.1 VPN configuration GUI: AS/400 Operations Navigator	68
3.7.2 Starting the New Connection Wizard	71
3.7.3 VPN configuration objects created by the wizard	74
3.7.4 VPN configuration object relationships	74
3.7.5 Customizing the VPN configuration objects created by the wizard	75
3.7.6 Changing the Virtual Private Networking GUI default values	76
3.7.7 Configuring manual connections	77
3.7.8 Configuring L2TP connections	78
3.7.9 Deleting a VPN connection	82
3.7.10 Configuring IP filters	84
3.8 VPN operations and management	84
3.8.1 IP packet security operations	84
3.8.2 VPN server operations	87

3.8.3	VPN connections operations	90
3.8.4	Starting L2TP and VPN connections on the AS/400 LNS.	93
3.8.5	Starting L2TP and VPN connections on the AS/400 L2TP initiator.	95
3.8.6	Checking the VPN connections status.	97
3.8.7	Stopping VPN connections	100
3.9	Backup and recovery considerations.	101
Chapter 4. AS/400 IP filtering overview		103
4.1	How IP filtering works	103
4.1.1	IP filter rules examples	107
4.1.2	IPSec-related IP filter rules	111
4.1.3	AS/400 IPSec processing logic	113
4.1.4	Network Address Translation (NAT) considerations.	117
4.2	Configuring IP packet security.	117
4.2.1	Creating a new filter rules file	118
4.2.2	Updating an existing filter rules file	128
4.2.3	Deactivating all active filters: Remove TCP/IP Table.	129
4.3	Refining the traffic for active connections: Connection granularity.	129
4.3.1	Connection initiator and responder	131
4.3.2	Configuring the traffic for active connections parameters	133
4.4	Restricting services in VPN connections	135
4.4.1	Scenarios network configuration	135
4.4.2	Scenario 1: Restricting services to Telnet-only by IPSEC filter	135
4.4.3	Scenario 2: Restricting services to Telnet-only by connection	140
4.4.4	Scenario 3: Allowing Telnet only in both directions	144
4.4.5	Scenario 4: Allowing normal mode FTP in one direction	152
Chapter 5. Getting started: AS/400 host-to-host VPN.		163
5.1	Business partner VPN connection (AS/400 host-to-AS/400 host)	163
5.1.1	Scenario characteristics	163
5.1.2	Scenario objectives.	164
5.1.3	Scenario network configuration	165
5.1.4	Software prerequisites.	165
5.1.5	Task summary.	165
5.2	Verifying IP connectivity	166
5.3	Configuring a host-to-host VPN on the AS/400 system (AS14)	167
5.3.1	Completing the planning worksheets for AS14	167
5.3.2	Changing the default security values.	169
5.3.3	Configuring a host-to-host VPN on AS14.	171
5.3.4	Customizing the VPN configuration created by the wizard on AS14	176
5.3.5	Configuring IP packet security on AS14	179
5.4	Configuring a host-to-host connection on AS20.	187
5.4.1	Completing the planning worksheets for AS20	187
5.5	Configuring a host-to-host VPN on AS20	189
5.5.1	Customizing the VPN configuration created by the wizard on AS20	194
5.5.2	Configuring IP packet security on AS20	194
5.6	Configuration cross-reference table	196
5.7	Starting the VPN connection	196
5.8	Performing verification tests	197
Chapter 6. Gateway-to-gateway VPN		199
6.1	VPN gateways at the network boundaries: No firewall protection	199
6.1.1	Scenario characteristics	200
6.1.2	Scenario objectives.	200

6.2	Implementing the Gateway to gateway: No firewall scenario	201
6.2.1	Scenario network configuration	201
6.2.2	Implementation task: Summary	202
6.2.3	Verifying TCP/IP routing	203
6.3	Configuring the Rochester AS/400 VPN gateway (AS14).	203
6.3.1	Planning worksheets for the the AS14 gateway	204
6.3.2	Configuring the gateway-to-gateway VPN on AS14	206
6.3.3	Configuring IP filters on the AS14	217
6.4	Configuring the Minneapolis AS/400 VPN gateway (AS05)	229
6.4.1	Planning worksheets for the AS05 gateway	229
6.4.2	Configuring the gateway-to-gateway VPN on AS05	231
6.4.3	Configuring IP filters on AS05	232
6.4.4	Starting the gateway-to-gateway VPN connection	233
6.4.5	Verification tests	237
6.5	Adding host-to-gateway and gateway-to-host connection groups.	238
6.5.1	Configuring a host-to-gateway VPN on AS14.	240
6.5.2	Configuring a gateway-to-host VPN on AS14.	246
6.5.3	Adding IPSEC filter rules	248
6.5.4	Configuring host-to-gateway and gateway-to-host VPNs on AS05	252
6.5.5	Starting host-to-gateway and gateway-to-host VPN connections	254
6.5.6	Tracing the VPN tunnels	256
6.6	Additional TCP/IP configuration information.	259
6.6.1	AS14 TCP/IP interfaces and routes configuration	259
6.6.2	AS05 TCP/IP interfaces and routes configuration	260
6.6.3	AS20 TCP/IP interfaces and routes configuration	260
6.6.4	Router configuration	261
6.6.5	PC07 TCP/IP configuration	261
Chapter 7. L2TP host-to-gateway voluntary tunnel		263
7.1	Branch office to main office connection using L2TP voluntary tunnel	263
7.1.1	Scenario characteristics.	264
7.1.2	Scenario objectives	264
7.1.3	Scenario network configuration	265
7.1.4	Implementation tasks: Summary	265
7.2	Configuring the LNS in a voluntary tunnel protected by IPSec (AS05)	266
7.2.1	Configuring IPSec tunnel to the client: Host to Dynamic IP Users	266
7.2.2	Configuring the L2TP terminator profile (AS05)	273
7.2.3	Configuring IP filters in the LNS AS/400 system (AS05).	279
7.3	Configuring the L2TP client in a voluntary tunnel protected with IPSec	286
7.3.1	Configuring the PPP dial-up connection to the ISP (AS25b).	286
7.3.2	Configuring the L2TP VPN connection on the initiator (AS25b)	291
7.3.3	Configuring IP filters in the L2TP client AS/400 system (AS25b)	304
7.3.4	Configuring a virtual PPP connection on the L2TP initiator (AS25b)	311
7.4	Starting the connections in an L2TP voluntary tunnel with IPSec.	315
7.4.1	Starting the LNS in an L2TP voluntary tunnel (AS05).	315
7.4.2	Starting the L2TP initiator in an L2TP voluntary tunnel (AS25b).	317
7.5	Verifying interfaces and routes	317
7.5.1	Verifying interfaces and routes in the LNS (AS05)	317
7.5.2	Verifying interfaces and routes in the L2TP client (AS25b).	320
7.6	Verification tests	322
Chapter 8. L2TP gateway-to-gateway voluntary tunnel		323
8.1	Branch office network to corporate network connection with L2TP.	323

8.1.1	Scenario characteristics	324
8.1.2	Scenario objectives	324
8.1.3	Scenario network configuration	324
8.1.4	Implementation tasks: Summary	325
8.1.5	Planning the networks IP addressing and routing scheme	326
8.2	Configuring the LNS in a voluntary tunnel protected by IPSec (AS05)	327
8.2.1	Configuring IPSec tunnel to the client: Host to Dynamic IP users	327
8.2.2	Configuring the L2TP terminator profile (AS05)	327
8.2.3	Configuring IP filters in the LNS AS/400 system (AS05)	333
8.3	Configuring the L2TP client in a voluntary tunnel protected with IPSec	333
8.3.1	Configuring the PPP dial-up connection to the ISP (AS25b)	333
8.3.2	Configuring the L2TP VPN connection on the L2TP initiator	333
8.3.3	Configuring IP filters in the L2TP client AS/400 system (AS25b)	333
8.3.4	Configuring a virtual PPP connection on the L2TP initiator (AS25b)	333
8.4	Starting the connections in an L2TP voluntary tunnel with IPSec	339
8.4.1	Starting the LNS in an L2TP voluntary tunnel (AS05)	339
8.4.2	Starting the L2TP initiator in an L2TP voluntary tunnel (AS25b)	340
8.4.3	Verifying the VPN connection status	343
8.5	Verifying interfaces and routes	344
8.5.1	Verifying IP interfaces in the L2TP client (AS25b)	344
8.5.2	Verifying routes in the L2TP client (AS25b)	345
8.5.3	Verifying IP interfaces in the LNS (AS05)	346
8.5.4	Verifying routes in the LNS (AS05)	348
Chapter 9.	L2TP compulsory tunnel	351
9.1	Branch office to main office connection using L2TP compulsory tunnel	351
9.1.1	Scenario characteristics	351
9.1.2	Scenario objectives	352
9.1.3	Scenario network configuration	352
9.1.4	Implementation tasks: Summary	354
9.2	Configuring the LNS in a compulsory tunnel protected by IPSec (AS05)	354
9.2.1	Configuring the L2TP terminator profile (AS05)	354
9.2.2	Configuring the IPSec AH tunnel to ISP: Host to Dynamic IP Users	361
9.2.3	Configuring the IPSec ESP tunnel to the client: Gateway to hosts	368
9.2.4	Configuring IP filters in the LNS AS/400 system (AS05)	374
9.3	Configuring the PPP dial-in client in a compulsory tunnel with IPSec	389
9.3.1	Configuring the PPP dial-up connection to the ISP (AS25b)	389
9.3.2	Configuring the IPSec ESP tunnel to the LNS: Host to Gateway	396
9.3.3	Configuring IP filters in the initiator dial-in client (AS25b)	406
9.4	Starting the connections in an L2TP compulsory tunnel with IPSec	411
9.4.1	Starting the LNS in an L2TP compulsory tunnel (AS05)	411
9.4.2	Starting the dial-in client in an L2TP compulsory tunnel (AS25b)	412
9.5	Verifying interfaces and routes	414
9.5.1	Verifying interfaces and routes in the LNS (AS05)	414
9.5.2	Verifying interfaces and routes in the dial-in client (AS25b)	416
Chapter 10.	Secure remote access for PC clients over the Internet	419
10.1	Remote PC clients with IPSec-only support	419
10.1.1	Scenario characteristics	420
10.1.2	Scenario objectives	420
10.1.3	Scenario network configuration	421
10.1.4	Implementation tasks: Summary	421
10.1.5	Verifying end-to-end connectivity	422

10.1.6	Completing the planning worksheet for the VPN PC clients	422
10.1.7	Completing the planning worksheet for the AS/400 system (AS05)	424
10.1.8	Configuring Gateway to Dynamic IP Users VPN on AS05	424
10.1.9	Configuring IP filters on the AS/400 system (AS05)	430
10.1.10	Configuring Windows 95 Dial-Up Networking (DUN)	436
10.1.11	Installing the IRE SafeNet Soft-PK	438
10.1.12	Configuring the IRE SafeNet Soft-PK client on TPA	439
10.1.13	Starting the VPN connection	443
10.2	Remote PC clients with IPsec and L2TP support.	444
10.2.1	Verifying end-to-end connectivity	445
10.2.2	Completing the planning worksheet for the WinVPN client	445
10.2.3	Completing the planning worksheet for the AS/400 system (AS05)	446
10.2.4	Configuring a Host to Dynamic IP Users VPN on AS05	447
10.2.5	Configuring IP filters on the AS/400 system (AS05)	452
10.2.6	Configuring the L2TP terminator profile (AS05)	452
10.2.7	Configuring Windows 95 Dial-Up Networking for WinVPN	453
10.2.8	Installing the WinVPN client	453
10.2.9	Configuring iVasion WinVPN client	453
10.2.10	Configuring the L2TP initiator for the WinVPN client	458
10.2.11	Starting the LNS AS05	460
10.2.12	Starting the L2TP with IPsec PC client (WinVPN)	461
10.2.13	Verifying the status of the connection.	461
10.3	Supporting a mixed client environment	464
10.3.1	Modifying IP filters for IPsec-only and L2TP with IPsec clients . .	464
10.3.2	Verification tests	465
Chapter 11. Secure LAN access for PC clients in the intranet		467
11.1	VPN connections between PC clients and AS/400s in an intranet	467
11.1.1	Scenario characteristics	468
11.1.2	Scenario objectives	468
11.1.3	Implementation tasks: Summary	469
11.1.4	Verifying end-to-end connectivity	469
11.1.5	Completing the planning worksheet for IRE SafeNet Soft-PK	469
11.1.6	Completing the planning worksheet for generic VPN client (PC D)	471
11.1.7	Completing the planning worksheet for RALYAS4A	472
11.1.8	Completing the planning worksheets for RALYAS4C	473
11.1.9	Configuring the AS/400 system RALYAS4A	474
11.1.10	Configuring IP packet security on RALYAS4A	487
11.1.11	Configuring the AS/400 system RALYAS4C	494
11.1.12	Configuring IP packet security on RALYAS4C	496
11.1.13	Installing IRE SafeNet Soft-PK client: ThinkPad C	499
11.1.14	Configuring the IRE SafeNet Soft-PK client on ThinkPad C	499
11.1.15	AS/400 and SafeNet Soft-PK VPN configuration cross-reference	509
11.1.16	Starting the VPN connections	510
11.1.17	Checking the VPN connection status	511
Chapter 12. Don't forget a firewall: Protecting your VPN server		515
12.1	Choosing the VPN gateway platform	515
12.2	Gateway-to-gateway VPN through a firewall	517
12.2.1	Scenario characteristics	517
12.2.2	Scenario objectives	517
12.2.3	Firewall requirements	518
12.2.4	Implementing a gateway-to-gateway VPN through a firewall	518

12.2.5	Subnetting considerations	519
12.2.6	Virtual IP addressing and routing: VPN gateway behind a firewall .	520
12.2.7	Task summary	522
12.2.8	Configuring the firewall to permit IPSec protocols	522
12.2.9	Verifying end-to-end connectivity	526
12.2.10	Configuring the AS/400 VPN server behind the firewall (AS14) .	527
12.2.11	Configuring the AS/400 security gateway at the branch office . .	531
12.2.12	Configuring VPN connection and IP filters on AS05	533
12.2.13	Activating the VPN connection	534
12.2.14	Performing verification tests	535
12.2.15	Additional TCP/IP configuration information	535
12.2.16	AS14 TCP/IP interfaces and routes configuration	536
12.2.17	AS05 TCP/IP interfaces and routes configuration	537
12.2.18	AS20 TCP/IP interfaces and routes configuration	538
12.2.19	Router configuration	538
12.2.20	PC07 TCP/IP configuration	539
12.2.21	Firewall configuration	539
12.3	Remote access to an AS/400 VPN gateway behind a firewall	540
12.3.1	Scenario test network	541
12.3.2	Subnetting considerations	542
12.3.3	Virtual IP and routing: Access to VPN gateway behind a firewall .	542
12.3.4	Firewall configuration summary	543
12.3.5	AS/400 VPN gateway behind a firewall: IP filters summary	546
12.4	L2TP considerations	549
12.4.1	Firewall filters for L2TP voluntary tunnel protected by IPSec	550
12.4.2	Firewall filters for L2TP compulsory tunnel protected by IPSec . .	550
Chapter 13.	VPN Network Address Translation (VPN NAT)	551
13.1	Resolving IP address conflicts in a VPN connection	551
13.1.1	Scenario characteristics	552
13.1.2	Scenario objectives	553
13.2	VPN NAT source inbound implementation (AS14)	553
13.2.1	Scenario network configuration	553
13.2.2	Task summary	554
13.2.3	Verifying TCP/IP routing	555
13.2.4	Completing the planning worksheets for AS14	556
13.2.5	Configuring the gateway-to-gateway VPN on AS14	558
13.2.6	Configuring the VPN NAT source inbound on AS14	558
13.2.7	Configuring IP filtering on AS14	562
13.2.8	Completing the planning worksheets for AS05	563
13.2.9	Configuring the gateway-to-gateway VPN on AS05	564
13.2.10	Configuration changes for VPN NAT source inbound on AS05 .	565
13.2.11	Configuring IP filtering on AS05	570
13.2.12	Starting the VPN connections	570
13.3	VPN NAT source outbound implementation	571
13.3.1	Configuring the gateway-to-gateway VPN on AS05	574
13.3.2	Configuring VPN NAT source outbound on AS05	575
13.3.3	Configuring IP filtering on AS05	580
13.3.4	Configuring the gateway-to-gateway VPN on AS14	581
13.3.5	Configuration changes for VPN NAT source outbound on AS14 .	581
13.3.6	Configuring IP filtering on AS14	583
13.3.7	Starting the VPN connections	583
13.4	Hiding IP addresses from your VPN partner: VPN NAT for servers . . .	584

13.4.1	Scenario characteristics	585
13.4.2	Scenario objectives	586
13.5	VPN NAT for servers implementation	586
13.5.1	Scenario network configuration	586
13.5.2	Task summary	588
13.5.3	Verifying TCP/IP routing	588
13.6	Configuring the manufacturer's AS/400 VPN gateway (AS14)	590
13.6.1	Planning worksheets for the manufacturer AS/400 gateway (AS14)	590
13.6.2	Configuring the gateway-to-gateway VPN on AS14	592
13.6.3	Configuring VPN NAT for servers on AS14	599
13.6.4	Configuring IP filtering on AS14	604
13.7	Configuring the distributor's AS/400 VPN gateway (AS05)	615
13.7.1	Planning worksheets for the distributor AS/400 gateway (AS05)	615
13.7.2	Configuring the gateway-to-gateway VPN (AS05)	617
13.7.3	Making configuration changes for VPN NAT for servers on AS05	617
13.7.4	Configuring IP filtering on AS05	623
13.7.5	Starting the VPN connections	624
Chapter 14.	AS/400 VPN problem determination	627
14.1	AS/400 VPN problem determination tools	628
14.1.1	Active Connections window	628
14.1.2	IP filter journal	630
14.1.3	VPN journal	634
14.1.4	Trace TCP/IP Application (TRCTCPAPP) command	640
14.1.5	Job logs	642
14.1.6	Communications trace	649
14.1.7	Work with Connection Status (NETSTAT) command	651
14.2	Common problems	651
14.2.1	Unable to encrypt keys. QRETSVRSEC must be set to 1	651
14.2.2	All keys are blank	652
14.2.3	CPF9821: Not authorized to program QTFRPRS in QSYS library	652
14.2.4	Unable to communicate with the remote system	652
14.2.5	No remote phase 1 policy	653
14.2.6	No remote phase 2 policy	653
14.2.7	Pre-shared key not found on local system	654
14.2.8	Preshared key not found on remote system	654
14.2.9	Pre-shared key is invalid	655
14.2.10	Filters not loaded correctly on WAN interfaces	655
14.2.11	Invalid filter rule name	655
14.2.12	Active filter rules fail to deactivate	655
14.2.13	3DES not a choice for encryption	656
14.2.14	Key policy not a choice in a Dynamic IP Connection Group	656
14.2.15	Item not found	656
14.2.16	A valid key policy is required	657
14.2.17	Unable to update the object	657
14.2.18	Connection is running after you stopped it	657
14.2.19	Connection not displayed in the Active Connections window	658
14.2.20	Status for a connection in the Active Connection window is blank	658
14.2.21	Unexpected columns display in the Active Connections Monitor	658
14.2.22	Unable to retrieve connection information in the Active Connections window	658
14.2.23	Parameter PINBUF is not valid	658
14.2.24	Connection overlap with existing connection	659

14.3	VPN key manager job messages and reason codes	659
14.3.1	TCP8705 error processing VPN Connection Manager command	659
14.3.2	TCP870C proposal not accepted with remote system &1	664
14.3.3	TCP8709 VPN policy processing error. RC=5	665
14.4	L2TP error messages	666
14.5	Known limitations in AS/400 VPN V4R4	668
14.5.1	IPSec specific notifications	669
14.5.2	Phase 1 SA control	669
14.5.3	Commit Bit and CONNECTED notification	669
14.6	Internet Key Exchange (IKE) protocol overview	670
14.6.1	IKE phases overview	670
14.7	Oakley Mode overview	670
14.7.1	Notation used to describe Oakley mode exchange	670
14.7.2	The Main Mode model	671
14.7.3	The Aggressive Mode model	671
14.7.4	The Quick Mode model	672
14.8	AS/400 communication trace example	673
14.9	AS/400 communication trace example with details	676

Part 3. VPN interoperability scenarios 685

Chapter 15. Host-to-gateway VPN: AS/400 to 2212 router	687
15.1 Branch office VPN connection (AS/400 host to 2212 router gateway)	687
15.1.1 Scenario characteristics	687
15.1.2 Scenario objectives	688
15.1.3 Scenario network configuration	688
15.1.4 2212 router software	688
15.1.5 Implementation tasks: Summary	688
15.1.6 Verifying initial connectivity	689
15.2 2212 router configuration	689
15.2.1 Completing the planning worksheets for the 2212 router	689
15.2.2 Configuring the VPN in the 2212 Router: Configuration summary	693
15.3 AS/400 host-to-gateway VPN configuration	696
15.3.1 Completing the planning worksheets for the AS/400 system	696
15.3.2 Configuring a host-to-gateway VPN on RALYAS4A	698
15.3.3 Matching the 2212 router VPN configuration	705
15.3.4 Configuring IP filtering on the AS/400 system (RALYAS4A)	709
15.4 VPN configuration cross-reference table: AS/400 to 2212 router	717
15.5 Starting the VPN connections and final verification	717
15.5.1 Starting the VPN connection on the AS/400 system	718
15.5.2 Verification tests	721
Chapter 16. Gateway-to-gateway VPN: AS/400 to 2210 router	723
16.1 Branch office VPN connection (AS/400 gateway to 2210 gateway)	723
16.1.1 Scenario characteristics	723
16.1.2 Scenario objectives	724
16.1.3 Scenario network configuration	724
16.1.4 2210 router software	724
16.1.5 Implementation tasks: Summary	724
16.1.6 Verifying initial connectivity	725
16.2 2210 router configuration	725
16.2.1 Completing the planning worksheets for the 2210 router	725
16.2.2 Configuring the VPN in the 2210 router: Configuration summary	729

16.3 AS/400 gateway-to-gateway VPN configuration	742
16.3.1 Completing the planning worksheets for the AS/400 system	742
16.3.2 Configuring a gateway-to-gateway VPN on RALYAS4A	744
16.3.3 Matching the 2210 router VPN configuration	751
16.3.4 Configuring IP filtering on the AS/400 system (RALYAS4A)	754
16.4 VPN configuration cross-reference table: AS/400 to 2210 router	762
16.5 Starting the VPN connections and final verification	762
16.5.1 Starting the VPN connection on the AS/400 system	763
16.5.2 Verification tests	768
Chapter 17. Host-to-host VPN: AS/400 to AIX server	769
17.1 Business partners VPN connection (host-to-host AS/400 to AIX)	769
17.1.1 Scenario characteristics	769
17.1.2 Scenario objectives	770
17.1.3 Scenario network configuration	770
17.1.4 AIX software	771
17.1.5 Implementation tasks: Summary	771
17.1.6 Verifying initial connectivity	771
17.2 AIX VPN configuration	771
17.2.1 Completing the AIX server planning worksheet	771
17.2.2 Configuring a host-to-host VPN in the AIX server	772
17.3 AS/400 host-to-host VPN configuration	778
17.3.1 Completing the AS/400 system planning worksheet	778
17.3.2 Configuring a host-to-host VPN in the AS/400 system	780
17.4 VPN configuration cross-reference table: AS/400 to AIX server	790
17.4.1 Configuring IP filters on the AS/400 system (RALYAS4C)	791
17.4.2 Starting the VPN connection	795
17.4.3 Verification tests	797
Chapter 18. Host-to-host VPN: AS/400 to S/390	799
18.1 Business partner VPN connection (host to host AS/400 to S/390)	799
18.1.1 Scenario characteristics	799
18.1.2 Scenario objectives	800
18.1.3 Scenario network configuration	800
18.2 S/390 software	801
18.2.1 Implementation tasks: Summary	801
18.3 Verifying IP connectivity	802
18.4 S/390 VPN configuration	802
18.4.1 Completing the S/390 system planning worksheet	802
18.4.2 Configuring a host-to-host VPN on the S/390 system	804
18.5 AS/400 host-to-host VPN configuration	821
18.5.1 Completing the AS/400 system planning worksheets	821
18.5.2 Configuring a host-to-host VPN on RALYAS4A	823
18.5.3 Matching the S/390 system VPN configuration	828
18.5.4 Configuring IP packet security on RALYAS4A	832
18.6 VPN configuration cross-reference table: AS/400 to S/390	839
18.7 Starting the VPN connection	840
18.7.1 Starting the VPN connection on the AS/400 system (RALYAS4A)	840
18.7.2 Starting the VPN connection on the S/390 system	841
18.8 Performing verification tests	843
Chapter 19. Manual connection VPN: AS/400 to eNetwork Firewall	845
19.1 Branch office host-to-corporate office gateway VPN	845
19.1.1 Scenario characteristics	845

19.1.2 Scenario objectives	846
19.1.3 Scenario network configuration	846
19.1.4 eNetwork Firewall for Windows NT software	846
19.1.5 Implementation tasks: Summary	847
19.1.6 Verifying initial connectivity	847
19.2 eNetwork Firewall for Windows NT configuration.	847
19.2.1 eNetwork Firewall for Windows NT planning worksheet.	847
19.2.2 Configuring eNetwork Firewall for Windows NT.	849
19.2.3 Exporting the eNetwork Firewall VPN configuration.	851
19.2.4 eNetwork Firewall IP filter configuration	855
19.3 AS/400 manual connection VPN configuration	855
19.3.1 Completing the AS/400 system planning worksheet	856
19.3.2 Configuring a manual VPN connection on the AS/400 system	857
19.3.3 Configuring IP packet security on RALYAS4A	867
19.4 VPN cross-reference configuration table: AS/400 to eNetwork Firewall	873
19.5 Starting the VPN connections and final verification	874
19.5.1 Starting the VPN tunnel on the eNetwork Firewall for Windows NT	874
19.5.2 Starting the VPN connection on the AS/400 system	875
19.5.3 Verification test	875
Appendix A. Special notices	877
Appendix B. Related publications	879
B.1 IBM Redbooks publications.	879
B.2 IBM Redbooks collections.	879
B.3 Other resources.	879
B.4 Referenced Web sites.	880
How to get IBM Redbooks	881
IBM Redbook fax order form.	882
Index	883
IBM Redbooks evaluation	891

Preface

Secure your AS/400 network with Virtual Private Networks (VPN). This redbook explores VPN concepts and describes its implementation using IP security (IPSec) and Layer 2 Tunneling Protocol (L2TP) on the AS/400 operating system. The redbook is designed to meet the needs of network administrators, consultants, and AS/400 specialists who plan to design, implement, and configure VPNs where AS/400 systems are employed. This redbook covers various scenarios some of which may not apply to your environment. However, before implementing any particular AS/400 VPN configuration, we strongly recommend that you read the following chapters in this redbook:

- Chapter 3. AS/400 VPN implementation
- Chapter 4. AS/400 IP filtering overview
- Chapter 5. Getting started: AS/400 host-to-host VPN
- Chapter 6. Gateway-to-gateway VPN
- Chapter 12. Don't forget a firewall: Protecting your VPN server

In this redbook, you can find:

- How to design and implement VPNs where the AS/400 system is either an endpoint host or a gateway to a private network
- A variety of scenarios that show how to securely connect your AS/400 systems to remote PC clients, branch offices, and business partners over the Internet
- How to protect your AS/400 VPN server with a firewall
- VPN cross-platform examples covering all of the IBM products that support virtual private networking
- Discussions of such advanced topics as problem determination, trouble shooting, and VPN NAT

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Rochester Center.

Marcela Adan is a Senior Consultant at the International Technical Support Organization, Rochester Center. She writes extensively and is a frequent speaker in AS/400 technical classes and conferences world wide. Her areas of expertise include AS/400 Internet security, communications, and system management. Ms. Adan has held several positions as a field technical support specialist, network administrator, developer, and consultant.

Thomas Barlen is a Software Service Specialist in Germany working in the AS/400 Second Level Support Center. He has worked for IBM for 17 years, primarily with IBM mid-range systems. His areas of expertise include AS/400 networking and communications as well as LAN and WAN network design and implementation. Currently, Mr. Barlen is on an international assignment with the ITSO in Raleigh, North Carolina.

Weng Wai Chia is an AS/400 Advisory IT Specialist in IBM Global Services, Singapore. He has been working with the AS/400 system since 1989. His areas

of expertise include AS/400 communications, Internet security, e-commerce, and process consultancy. Mr. Chia holds a degree in Electrical and Computer Systems Engineering from Monash University, Australia.

Andrew Grant is a communications specialist working for IBM Managed Operations in New Zealand. He has 10 years of experience with IBM mid-range systems, communications, and client connectivity. His main area of expertise is the design, implementation, and support of large, multi-platform networks.

Darrell Grundy is an Advisory Technical Support Specialist with IBM UK and has been with the company for four years. He holds a Bachelor of Science degree in Computer Studies. Mr. Grundy's areas of expertise include TCP/IP, Internet security, and client/server communication over a variety of platforms.

Peter Hey is a Senior IT Specialist in IBM UK. He joined IBM in 1979, specializing primarily in S/3x and AS/400 communications and networking. His other areas of expertise include AS/400 systems management and performance. Mr. Hey currently works in a technical support role responsible for AS/400 networking in the IBM E/ME/A Northern Region. He has held a variety of jobs in IBM including branch Systems Engineer and services specialist.

Stephan Imhof is a Senior IT Specialist in IBM Switzerland. He has worked for IBM for 26 years focusing on networking during the last 15 years. His expertise includes all areas of AS/400 networking and security as well as IBM routers.

Linda Kinnunen is a software engineer with the User Technologies (UT) Department in IBM Rochester. Linda is currently a team leader for the UT security information team, which designs and creates documentation for AS/400 security products. Since joining IBM in 1997, she has also written Information Center articles about Virtual Private Networking (VPN), AS/400 NetServer, AS/400 Toolbox for Java (GUI Builder), and TCP/IP.

Eric Zeier is a Software Engineer with IBM Global Services and Support in Rochester, MN. He has five years of experience with the AS/400 system earning a degree from The Chubb Institute in Parsippany, NJ. Mr. Zeier's areas of expertise include TCP/IP connectivity, WAN communications, and Internet Security.

Thanks to the following people for their invaluable contributions to this project:

Martin Murhamer
Gail Christensen
Jorge Ferrari
Mike Haley
Tatsuhiko Kakimoto
Tim Kearby
Shawn Walsh
International Technical Support Organization, Raleigh Center

Jerry Engelbert
Tom Gray
Marv Kulas
Kris Peterson
Ryan Rhodes
Jenifer Servais
International Technical Support Organization, Rochester Center

Ed Boden
John Corcoran
Gary Diehl
Paul Gebler
Janet Geoffroy
Frank Gruber
Joe Miller
Mark Melville
Don Palermo
Frank Paxhia
Eric Roscoe
Kurt Streifert
Scott Sylvester
Mark Vallone
Mike Williams
IBM Endicott Development Laboratory

Skip Booth
John Crawbuck
Susanne Vergara
John Walczyk
IBM Research Triangle Park

Mark Davis
IBM Rochester

Orcun Atakan
IBM Turkey

Beomjum Cho
IBM Korea

Giancarlo Rodolfi
IBM Brazil

Titus Peedikayil
Wind River Systems

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in “IBM Redbooks evaluation” on page 891 to the fax number shown on the form.
- Use the online evaluation form found at <http://www.redbooks.ibm.com/>
- Send your comments in an Internet note to redbook@us.ibm.com

Part 1. VPN concepts and overview

A virtual private network (VPN) allows your company to securely extend its private intranet over the existing framework of a public network such as the Internet. With VPN, your company can control network traffic while providing important security features such as authentication and data privacy.

OS/400 VPN support uses the IP Security Architecture (IPSec) open framework. IPSec is unique in that it provides base security functions for the Internet, as well as furnishes flexible building blocks from which robust, secure virtual private networks can be constructed.

OS/400 VPN also supports Layer 2 Tunnel Protocol (L2TP) VPN solutions. L2TP connections, which are also called virtual lines, provide cost-effective access for remote users by allowing the home network server to manage the IP address assigned to the remote user. In addition, L2TP connections provide secure access to your system or network when you use them in conjunction with IPSec.

This part introduces VPN concepts and protocols. It provides the theoretical background that you need to understand the practical examples shown in the following parts of this redbook.

Chapter 1. Virtual Private Network (VPN) overview

With the explosive growth of the Internet, companies are asking: How can we best exploit the Internet for our business? Initially, companies used the Internet to promote their company's image, products, and services by providing World Wide Web access to corporate Web sites. The Internet has also proven itself to be an efficient and resilient communications network for the transportation of electronic mail.

However, today the focus has shifted to e-business. Companies are leveraging the global reach of the Internet for easy access to key business applications and data that reside in their traditional I/T systems. They can now securely and cost-effectively extend the reach of their applications and data across the world through the implementation of secure Virtual Private Network (VPN) solutions.

1.1 Private networks

VPN allows your corporation to make the transition from the traditional private network to the modern private network. It maintains the level of security from the traditional model and uses the global reach and cost savings of the Internet.

1.1.1 Traditional private network

Traditional corporate networks are largely self-contained. All data travels over private facilities. For example, many corporations use dial-up connections, leased lines, or other wide area networks (WAN) technologies (such as frame relay) to communicate with their branch offices and remote users as shown in Figure 1. In this closed, tightly controlled environment, the traditional corporate network is considered to be *secure* because the traffic only flows through private links.

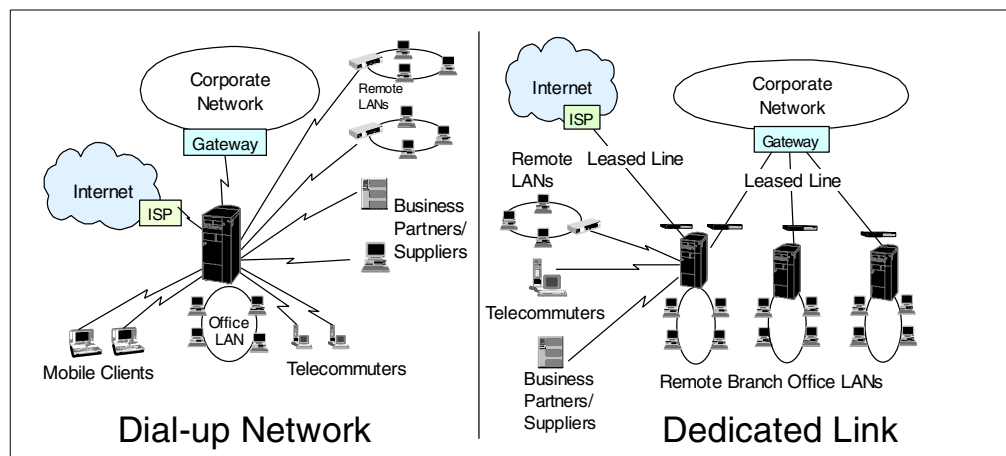


Figure 1. Examples of traditional private networks

However, a new business model is emerging. Not only do corporations need to communicate with their branch offices and remote users, but they also need secure intercompany communication. This new extended corporate network is a collection of physically separated intranets that are connected by the public Internet. The economical, worldwide reach of the Internet makes it an attractive replacement for the traditional intra-business network as well.

Ideally, the modern private network would retain the desirable characteristics of the traditional private network, while incorporating the cost-effective, global reach of the Internet.

1.1.2 Modern private networks

In a modern private network, your corporation can take advantage of the global reach of the Internet to extend its corporate network to almost anywhere in the world. At the same time, the corporate network maintains control over incoming and outgoing traffic as in the traditional private network.

In Figure 2, remote clients make a local connection to the Internet Service Provider (ISP) Point of Presence (PoP), and use the Internet to access the corporate network through the security gateway.

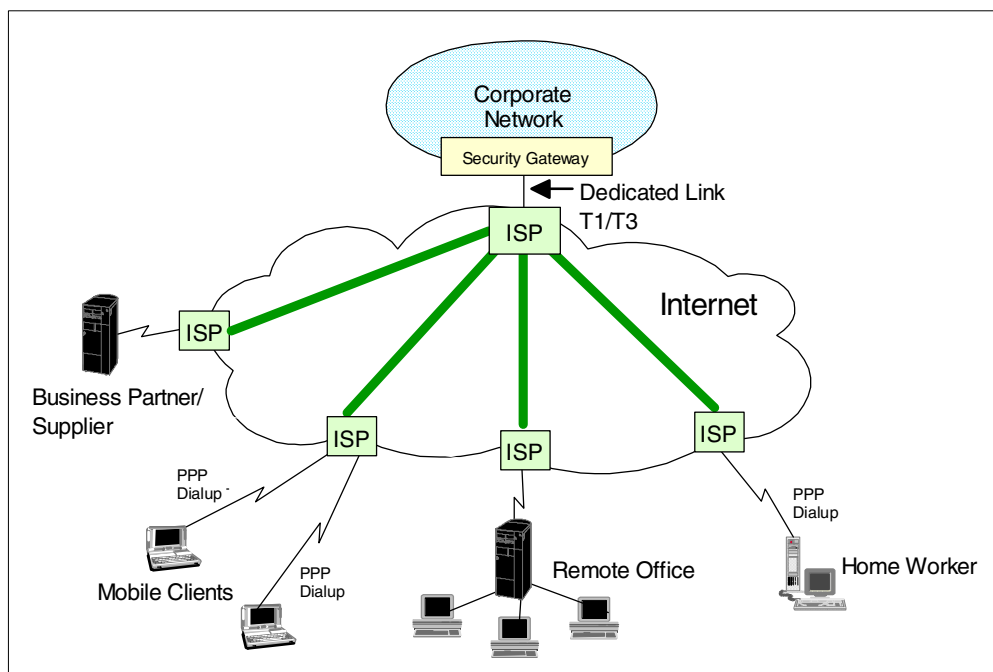


Figure 2. Example of a modern private network

There are several advantages to this configuration:

- **Worldwide reach:** As long as the parties that need to communicate with each other can access the Internet, connectivity is guaranteed. There is no need to set up special and compatible communication equipment to enable end-to-end communications.
- **Outsource of network management to the ISP:** The ISP now provides and maintains the network infrastructure (for example, modem pools or routers). In a traditional network, the corporation manages the entire network. By off-loading some of the administrative requirements to an ISP, your corporation can realize savings in terms of resources and in-house skills.
- **Cost savings in communications links and equipment:** When you connect your corporate network to the Internet via an ISP, you no longer have to pay for expensive leased lines or long distance phone calls. Instead, you pay the ISP fee and local phone call (if applicable).

1.1.2.1 Incoming traffic consolidation

Figure 3 illustrates the variety of remote connections that are possible by using an ISP PoP to connect to a single dedicated link into the corporate network. Hosts within the corporate network connect to the Internet through the same link.

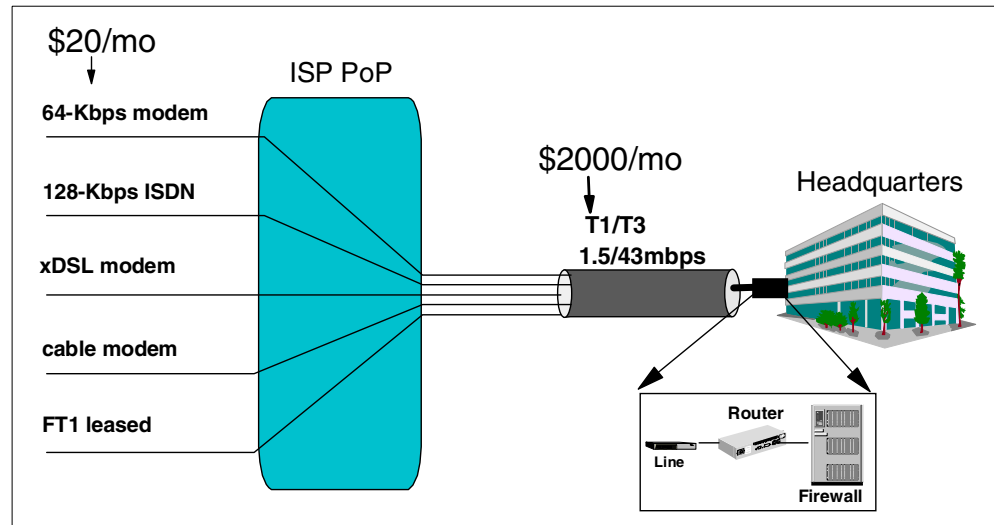


Figure 3. Using the most appropriate network access media and equipment

Note

The monthly cost estimates in Figure 3 are based on the average cost in the US. They serve as a useful comparison. However, remember that local telephone calls are generally free of charge in the US. Your costs may vary depending on your geographical location.

The following points are important to note in Figure 3:

- The client connection media is the most appropriate for the application and use. It is also independent of the headquarters connection media.
- In general, all connections are made to a local ISP.
- Only headquarters may require dedicated high-speed links and, naturally, a firewall.
- The dedicated high-speed link at the headquarters is shared with remote access, as well as general Internet traffic.

The access media shown in Figure 3 is:

- FT1** Fractional T1. A T1 line, in the US, is a 1.54 Mbps digital circuit. A Fractional T1 is a subdivision of this, that is a digital leased line up to 1.54 Mbps.
- T3** US terminology for a 43 Mbps digital leased line. Different line speeds (and terminology) apply in different countries.

Cable modems

Available in some countries to connect to the Internet at high speeds through the optical cable networks owned by the local cable companies.

DSL Digital Subscriber Line. For example, Asymmetric Digital Subscriber Line (ADSL) is a modem technology that transforms ordinary phone lines (also known as "twisted copper pairs") into high-speed digital lines for ultra-fast Internet access. It is asymmetric in that it provides faster speeds in one direction than in the other on the basis that Internet downloads are generally much heavier than traffic sent in the other direction.

1.1.3 Virtual Private Networks (VPN)

A VPN is an extension of your company's private intranet over the existing framework of a public network, such as the Internet. VPN technologies allow you to control network traffic while providing important security features such as authentication and data privacy. This is typically achieved by defining a secure tunnel through which data flows in an encrypted form and is indecipherable to eavesdroppers or hackers.

Figure 4 illustrates that VPNs are a convenient and secure way to communicate with your branch offices, business partners, and remote users over the Internet infrastructure.

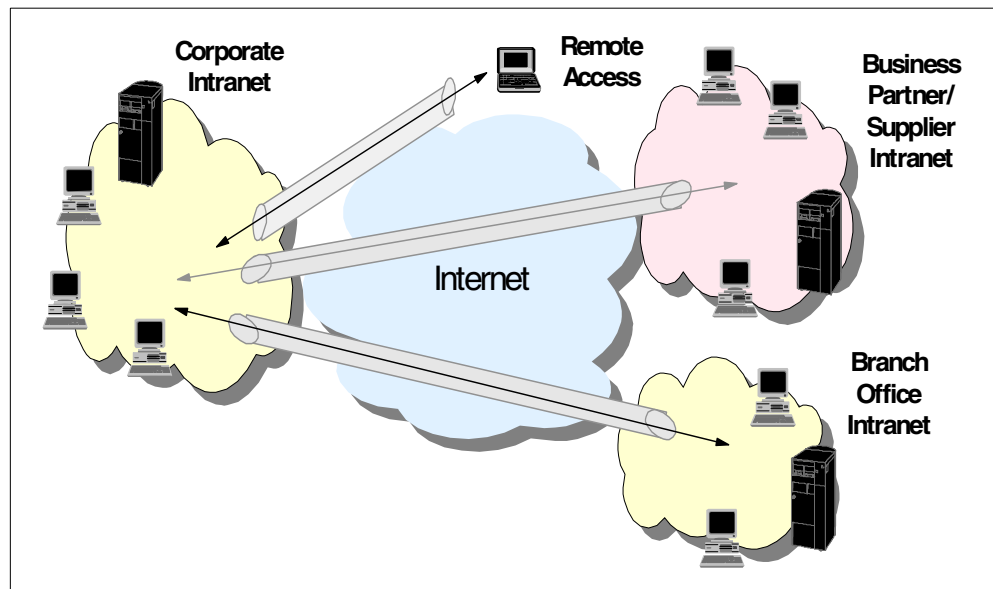


Figure 4. Deployment of multiple Virtual Private Networks

1.1.3.1 VPN customer value

VPN technologies offer customers the following advantages:

- Cost savings
 - Eliminates the need for expensive leased lines, long-distance calls, and toll-free telephone numbers
 - Estimated 20 to 47% savings in WAN costs and 60 to 80% savings in remote access dial-up costs (Infonetics Research, Inc.)
- Easy access to corporate networks and resources
 - Remote users and remote locations access sensitive information whenever they want and from wherever they are.

- Internet access is available worldwide, where other forms of connectivity may be either not available or more expensive.
- e-business
 - Focuses on gaining a competitive advantage
 - Strengthens relationships with business partners, suppliers, and distributors
 - Transforms the way corporations do business

1.2 VPN customer scenarios

In this section, we look at the three most likely business scenarios that are well suited to the implementation of a VPN solution. These are: branch office connections, business partner and supplier connections, and remote user connections.

1.2.1 Branch office connection scenario

Your company has a central, corporate intranet into which you want to connect remote branch offices. These offices may be in the same country, internationally located, or both.

The traditional option is to install an expensive private or managed network using leased lines or a frame relay. An alternative is to use dial-up lines, but these can be equally expensive over long distances and with anything other than short connection times. VPN can provide a cost effective, "permanent" (as opposed to part-time dial up links) solution.

Internet connectivity is available almost anywhere in the world, and the ISPs have to make it easy. Millions of people connect to the Internet with little or no knowledge of networking or communications technology. Compare that with managing your own network, potentially including many different technologies, suppliers, modem pools, and so on.

Figure 5 on page 8 shows that VPNs can significantly reduce your backbone communication costs.

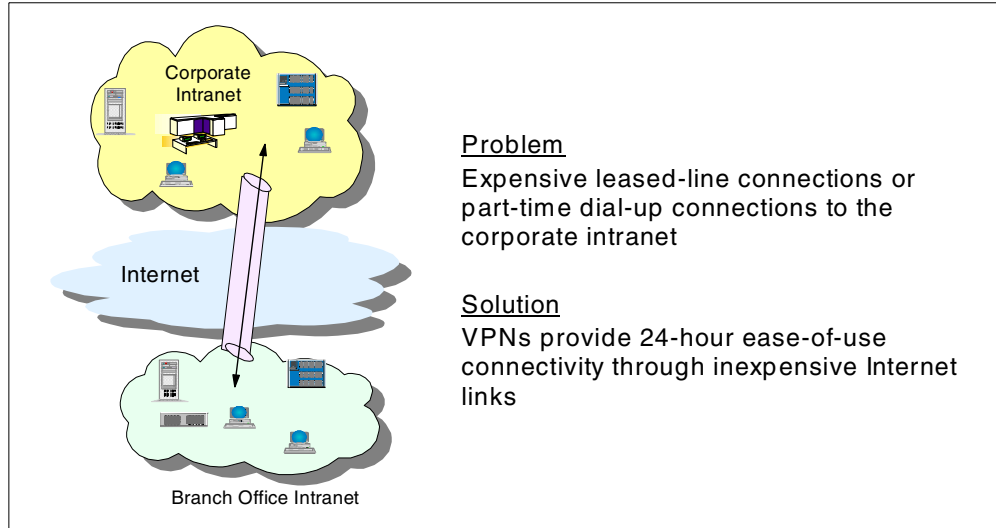


Figure 5. Branch office connection scenario

1.2.2 Business partner and supplier scenario

Similarly, VPN can provide an excellent solution for connecting to your business partners and suppliers almost anywhere in the world. Internet technology makes such connections easy and relatively inexpensive. VPN makes them secure.

This scenario is unlike the previous branch office scenario where you may allow any traffic to flow through the VPN connection between your central, corporate intranet and the branch office networks. With your business partners, you can limit and control the systems and applications they can access.

Figure 6 highlights the point that with VPNs, you can communicate with your business partners without needing additional network links.

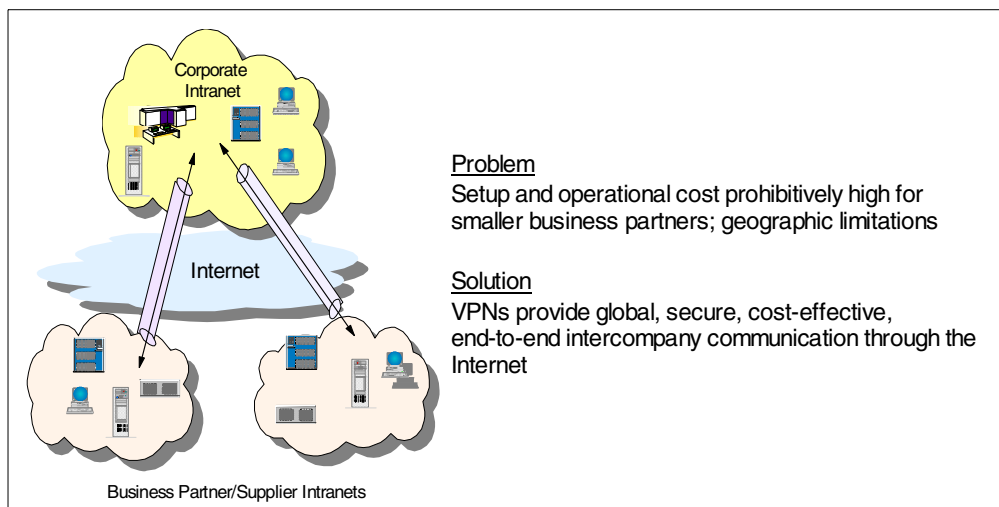


Figure 6. Business partner and supplier network scenario

1.2.3 Remote access scenario

Finally, VPN can provide an excellent solution for connecting remote users, either from their homes or while traveling. Rather than installing and managing modem pools and paying long distance call charges (or financing the calls through toll-free numbers), VPN allows users to dial in to a local ISP as shown in Figure 7. The ISP is responsible for providing the modem pool, and the Internet provides the "long distance" connection to your corporate network. Security of remote dial-in access is always a concern. The authentication and optional encryption of VPN provides a safe and reliable solution to this problem.

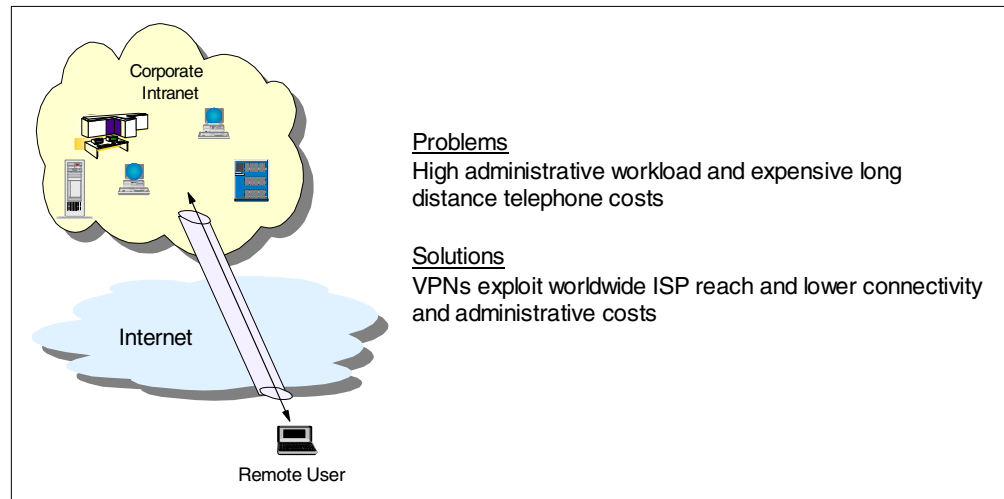


Figure 7. Remote access scenario

1.3 VPN requirements

Implementing a VPN presents your company with many significant challenges. No single entity owns the Internet or sets its policies. Data from many different sources flows through its common backbone infrastructure and through its routers. As the idea of e-business grows, more and more data will flow between companies. As a result, a VPN may potentially present security exposures that were not present in the traditional corporate network model.

There are security exposures everywhere along an end-to-end path: on the dial-up link, in an ISP access box, in the Internet, in the firewall or router, and even in the corporate intranet. Although there is a popular belief that most security threats are present in the public Internet, there have been studies which show that many of the attacks actually occur internally.

Like any form of crime, there are two kinds of attacks that are committed: *random* attacks and *targeted* attacks. Random attacks make the most of any loopholes in your security policy. Targeted attacks analyze and monitor your environment to identify a weak-point.

To be effective, VPNs must address the following basic requirements:

- **Data origin authentication:** To verify that each datagram was originated by the claimed sender.

- **Data integrity:** To verify that the contents of a datagram were not changed in transit, either deliberately or due to random errors.
- **Data confidentiality:** To conceal the clear text of a message by using encryption.
- **Replay protection:** To ensure that an attacker cannot intercept a datagram (containing, for example, an encrypted user ID and password) and play it back at some other time.
- **Key management:** To ensure that your VPN policy can be implemented throughout the extended network with little or no manual configuration.
- **Performance and availability:** To ensure that the VPN does not hinder your business operations, but rather grows as your business grows. Also, ensures that your VPN can accommodate future technologies as they become available. Performance and availability are still a concern in the current VPN implementations. However, there are emerging Internet standards that are working to address these requirements.
- **Interoperability:** To ensure that your VPN uses standard-based technologies to maintain interoperability with other VPN vendors.

IP Security Architecture (IPSec) provides the first definition of a comprehensive, consistent solution to a majority of these requirements. IPSec can provide end-to-end protection, as well as segment-by-segment protection.

1.4 VPN protocols

In Figure 8, the TCP/IP layered protocol stack is shown with the VPN-related protocols associated with each layer.

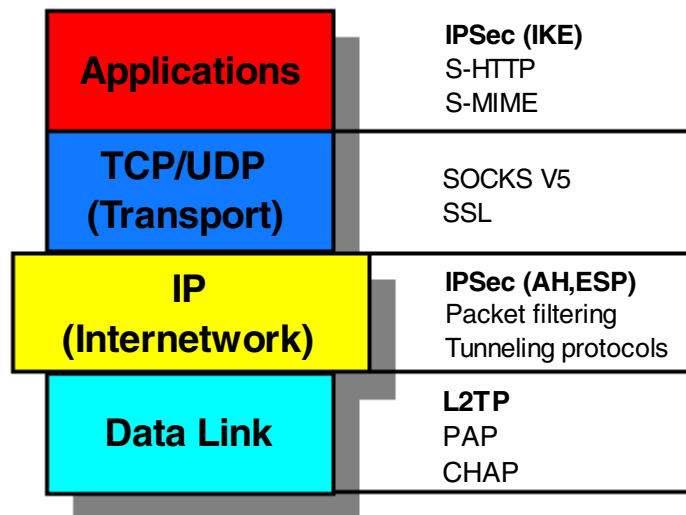


Figure 8. TCP/IP protocol stack with VPN-related protocols

Based on the work of the Internet Engineering Task Force (IETF), IBM chose to use IPSec for its IBM eNetwork VPN solutions for the following reasons:

- Open, standards-based, network layer security technology
- Supports authentication, integrity checking and encryption per packet

- Provides a key management solution by using the Internet Key Exchange (IKE) protocols (incorporates ISAKMP/Oakley)
- IPSec is standard in IPv6 (optional in IPv4)
- Used to secure Layer 2 Tunneling Protocol (L2TP) tunnels

L2TP is a good companion for IPSec because it offers the following advantages:

- Open, standards-based link layer technology
- Transports multiprotocol data over the Internet
- Cost-effective (extends PPP connections to destination network)
- Industry standard defined in RFC 2661
- No inherent security features (uses IPSec for security)

Most VPN offerings can be categorized in several different ways. In our opinion, the most important differentiator is the protocol layer on which the VPN is realized. In the context of this discussion, there are two different approaches to VPN implementation:

- Network layer-based solutions that use IPSec
 - Provides blanket protection for all upper-layer application data carried in the payload of an IP datagram. Does not require a user to modify the applications.
- Data link layer-based solutions that use L2TP
 - Provides cost-effective remote access by extending the span of a Point-to-Point Protocol (PPP) connection. Also provides secure access when used in conjunction with IPSec

There are other methods that operate on upper layers and complement a VPN solution, such as SOCKS, Secure Sockets Layer (SSL), or Secure Multipurpose Internet Mail Extension (S-MIME). Some solutions use only the upper layer protocols to construct a VPN, usually a combination of SOCKS V5 and SSL. While these methods are certainly “players”, in terms of VPN implementation, we focus primarily on IPSec and L2TP technologies in this redbook.

To satisfy the performance and availability requirements, the Internet Engineer Task Force, along with several vendors, are working on developing and implementing new Internet technologies. The new technologies, based on multiprotocol label switching (MPLS) with Quality of Service (QOS), will make the use of service level agreements more viable in the future.

1.4.1 IP Security (IPSec) protocols

Within the layered communications protocol stack model, the network layer (IP in the case of the TCP/IP stack) is the lowest layer that can provide end-to-end security.

IPSec was designed for interoperability. When correctly implemented, it does not affect networks and hosts that do not support it. IPSec is independent of current cryptographic algorithms. However, it supports all of the cryptographic algorithms in use today, and can also accommodate newer, more powerful algorithms as they become available. The specific implementation of an algorithm for use by an IPSec protocol is often referred to as a *transform*. For example, the Data Encryption Standard (DES) algorithm used in an Encapsulated Security Payload (ESP) is called the ESP DES-CBC transform.

The IPSec Working Group has concentrated on defining protocols to address the following VPN requirements:

- Data origin authentication
- Data integrity
- Data confidentiality
- Replay protection
- Key management

The principal IPSec protocols are:

- Authentication Header (AH)

The AH protocol presents the following characteristics:

- Provides data origin authentication, data integrity, and replay protection
- Uses hashed message authentication codes (HMAC) based on shared secrets
- Does not encrypt datagram content

- Encapsulating Security Payload (ESP)

The ESP protocol presents the following characteristics:

- Provides data confidentiality (except for transform NULL)
- Encrypts the payload of an IP packet by using cryptographic keys
- Optionally provides data origin authentication, data integrity, and replay protection

- Internet Key Exchange (IKE) protocol

The IKE protocol presents the following characteristics:

- Dynamically generates and refreshes cryptographic keys
- Rekeying occurs while a VPN connection is running
- Two-phase approach protects keys and data

1.4.2 Summarizing the main VPN protocols

Figure 9 on page 13 summarizes the roles of the main VPN protocols. Note that establishing an L2TP connection is not essential but provides additional functionality.

L2TP provides a virtual PPP tunnel across a network. It extends the corporate address space to the remote client. For more information on L2TP, refer to Chapter 2, “Introduction to Layer 2 Tunneling Protocol (L2TP)” on page 33.

IKE provides a secure mechanism for exchanging keys between VPN servers. These keys can, and should, be changed frequently and automatically.

The IPSec AH and ESP protocols provide authentication and encryption (using keys generated by IKE) for higher level protocols running over IP.

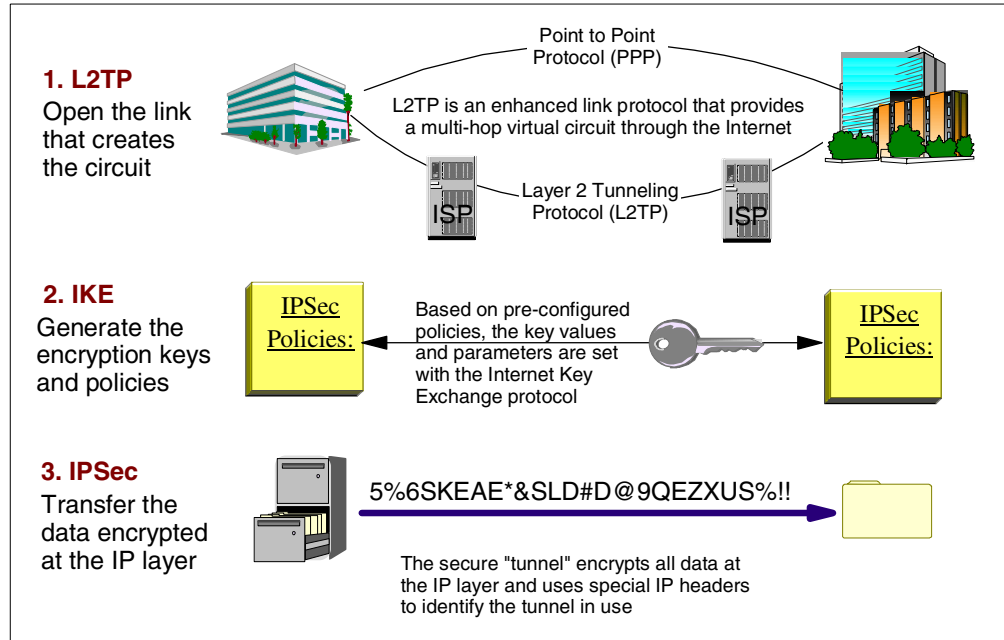


Figure 9. Main VPN protocols - Summary

1.4.3 VPN versus SSL

Figure 8 on page 10 shows that Secure Sockets Layer (SSL) is implemented in the transport layer (TCP/UDP), and requires modification of the applications that use it. Only those TCP/IP server and client applications written to SSL can use this protocol.

In contrast, secure tunneling protocols, such as IPsec, on which AS/400 VPN support is based, are implemented in the network layer (IP) of the TCP/IP stack. Network-layer security protocols provide blanket protection for the upper-layer application without requiring modification of the upper layer applications that use the secure tunnel. Once a host supports IPsec, all TCP/IP applications are protected without any changes to the application. This provides the virtual network view of the interconnected VPN hosts.

It is important to note that, both the server and the client must be SSL-enabled to participate in an SSL session. For example, in V4R4, the AS/400 Telnet server is SSL-enabled, but the Telnet client is not. Therefore, you cannot use a Telnet "green screen" session to access the Telnet server running over SSL. You need to use an SSL-enabled 5250 emulator such as TN5250 from Client Access/400 Express, PCOM 4.3 or later, or Host on-Demand 3.0. Likewise, if the TCP/IP server is not SSL-enabled (for example, the AS/400 FTP server is not SSL-enabled in V4R4), using an SSL-enabled client is *not* sufficient to successfully establish an SSL session.

To participate in a VPN connection, either the host or the intervening security gateway must support compatible VPN protocols.

SSL offers more granularity for authentication which is provided for each application independent of one another. SSL authenticates the user-based on a user digital certificate, while VPN authenticates the hosts.

Note: The application must support client authentication to authenticate users with SSL.

It is also easier to turn SSL on and off as needed to save performance costs of encryption.

1.5 Authentication Header (AH)

The AH protocol provides data origin authentication, data integrity, and replay protection. It may be worth noting here that these three distinct functions are often grouped together and referred to as *authentication*. In the simplest terms, AH ensures that your data has not been tampered with en route to its final destination.

Although AH authenticates as much of the IP datagram as possible, the values of certain fields in the IP header cannot be predicted by the receiver. As an example, consider Time To Live (TTL) field, which changes as it passes over each hop. These fields are called *mutable* and are not protected by AH. However, AH always protects the payload of the IP packet.

In many cases, your data needs only to be authenticated. While the Encapsulating Security Payload (ESP) protocol can perform authentication, AH does not affect your system performance as much as the encryption of ESP affects it. Another advantage of using AH is that it authenticates the entire datagram. ESP, on the other hand, does not authenticate the leading IP header or any other information that comes before the ESP header. Packets that fail authentication are discarded and are never delivered to upper layers. This greatly reduces the chances of successful denial of service attacks, which aim to block the communication of a host or gateway, by flooding it with bogus packets.

In addition, ESP requires strong cryptographic algorithms to be implemented. Strong cryptography is restricted in some countries, while AH is not regulated and can be used freely around the world.

AH is defined in RFC 2042 and is a separate IP protocol, number 51. For clarification, this means it does not use TCP or UDP as an underlying transport protocol.

1.5.1 AH packet format

Figure 10 on page 15 shows the position of the AH header in the IP packet and the header fields.

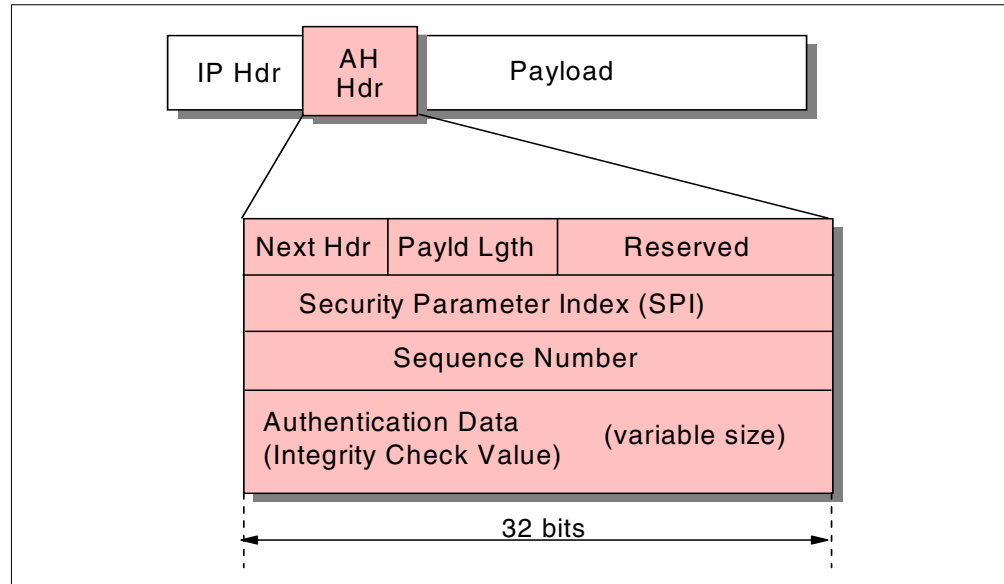


Figure 10. AH packet format

The following list explains the fields within the AH header:

- **Next Header:** The Next Header is an 8-bit field that identifies the type of the next payload after the Authentication Header. The value of this field is chosen from the set of IP protocol numbers defined in the most recent "Assigned Numbers" RFC from the Internet Assigned Numbers Authority (IANA). For example, TCP is assigned protocol number 6, and UDP is assigned protocol number 17.
- **Payload Length:** This field is 8 bits long and contains the length of the AH header expressed in 32-bit words, minus 2. It does not relate to the payload length of the IP packet as a whole. If default options are used, the value is 4 (three 32-bit fixed words plus three 32-bit words of authentication data minus two).
- **Reserved:** This field is reserved for future use. Its length is 16 bits, and it is set to zero.
- **Security Parameter Index (SPI):** This field is 32 bits in length. SPI is discussed in greater detail in 1.9, "IPSec configuration concepts" on page 29.
- **Sequence Number:** This 32-bit field is a monotonically increasing counter, which is used for replay protection. Replay protection is optional. However, this field is mandatory. The sender always includes this field, and it is at the discretion of the receiver to process it. When a security association is established, the sequence number is set to zero. The first packet transmitted using the security association (SA) has a sequence number of 1. Sequence numbers are not allowed to repeat. Thus, the maximum number of IP packets that can be transmitted on any given SA is $2^{32}-1$. After the highest sequence number is used, a new SA and, consequently, a new key is established. Anti-replay is enabled at initiation by default. After the SA has been established, if the receiver chooses not to use it, the sender is no longer concerned with the value in this field.

Note: Manual key management does not typically use the anti-replay mechanism. In addition, older IPSec implementations, such as the one used in

IBM Firewall for AS/400, are based on the original AH specification (RFC 1826), which does not support the concept of sequence numbers.

- **Authentication data:** This is a variable-length field, also called the Integrity Check Value (ICV). The ICV for the packet is calculated by using the algorithm agreed upon when the SA is initialized. The authentication data length is an integral multiple of 32 bits. As its name implies, the receiver uses it to verify the integrity of the incoming packet.

In theory, any MAC algorithm can be used to calculate the ICV. The specification requires that HMAC-MD5-96 and HMAC-SHA-1-96 be supported. The old RFC 1826 requires Keyed MD5. In practice, Keyed SHA-1 is also used. Implementations usually support two to four algorithms.

When doing the ICV calculation, the mutable fields are considered to be filled with zero.

1.5.2 AH transport and tunnel modes

AH can be used in two modes: *transport mode* and *tunnel mode*.

1.5.2.1 AH in transport mode

In transport mode, the IP header of the datagram is the outermost IP header, followed by the AH header and then the payload of the datagram. The entire datagram, except the mutable fields, is authenticated as shown in Figure 11. However, the information contained in the datagram is transported in clear text form and, therefore, is subject to eavesdropping.

The transport mode is used by hosts, not by gateways, which means there is less processing overhead. This also means that the hosts *must* be IPSec enabled.

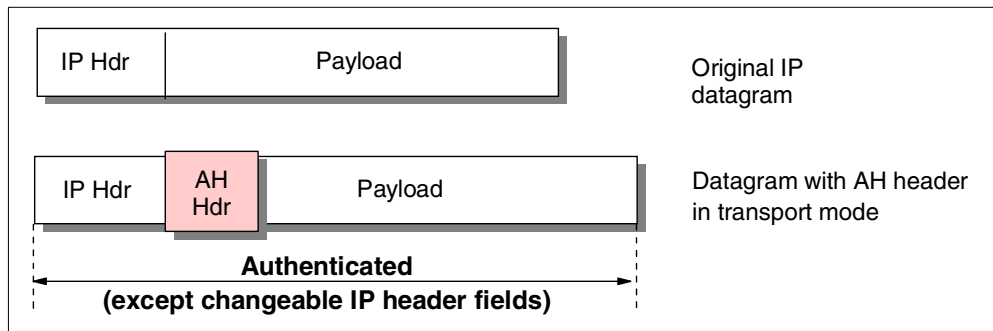


Figure 11. AH in transport mode

1.5.2.2 AH in tunnel mode

Figure 12 on page 17 illustrates how tunnel mode creates a new IP header and uses it as the outermost IP header of the datagram. The AH header follows the new IP header. The original datagram (both the IP header and the original payload) comes last. AH authenticates the entire datagram, which means that the responding system can detect whether changes were made to the datagram in transit.

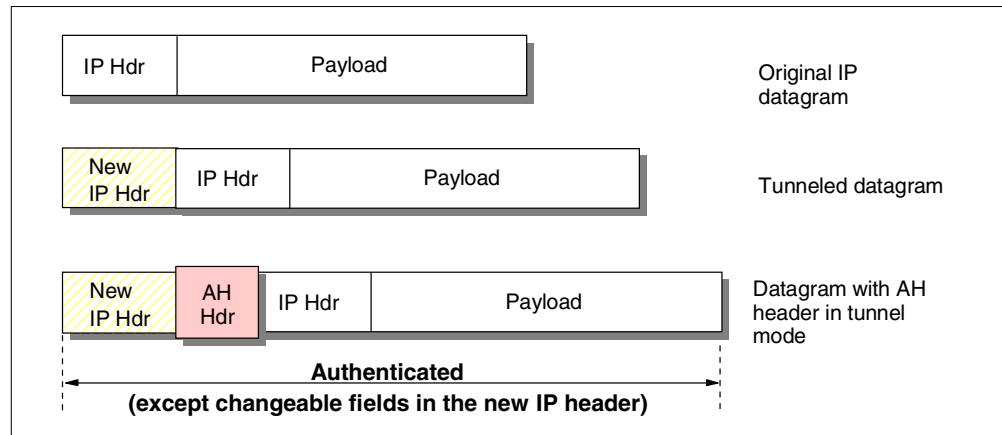


Figure 12. AH in tunnel mode

When either end of a security association is a gateway, you must use the tunnel mode. In tunnel mode, the source and destination addresses in the outermost IP header do not need to be the same as those in the original IP header. For example, two security gateways may operate an AH tunnel to authenticate all traffic between the networks that they connect together. In fact, this is a typical configuration.

One advantage of using tunnel mode is that it totally protects the encapsulated IP datagram. Another significant advantage is that it makes it possible to use private addresses in the original IP header. Thus, original datagrams with private source or destination addresses can be routed across a public network if the outer IP header contains public, routable addresses. Therefore, a tunnel can be created across the Internet between two private networks.

1.5.3 AH transforms

The transforms or protocols supported with AH are:

- Mandatory Authentication Transforms
 - HMAC-MD5-96 (RFC 2403)
 - HMAC-SHA-1-96 (RFC 2404)
- Optional Authentication Transforms
 - DES-MAC (Data Encryption Standard-Message Authentication Code)
- Obsolete Authentication Transforms
 - Keyed-MD5 (RFC 1828)

AH uses algorithms known as Hashed Message Authentication Codes (HMAC). The mandatory AH authentication transforms HMAC-MD5 and HMAC-SHA. Both take variable-length input data and a secret key to produce fixed length output data (called a *hash value*). If the hashes of two messages match, then it is likely that the messages are the same. Both MD5 and SHA (Secure Hash Algorithm) encode the message length in their output, but SHA is regarded as more secure because it produces larger hashes.

DES-MAC is a method that uses DES CBC to encrypt the message blocks and output the final block in the ciphertext as the checksum.

The AS/400 system supports HMAC-MD5 and HMAC-SHA authentication algorithms.

1.6 Encapsulating Security Payload (ESP)

The ESP protocol can provide data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection. The difference between ESP and the Authentication Header (AH) protocol is that only ESP supports encryption, while both protocol types provide authentication, integrity checking, and replay protection. Also, AH authenticates the entire datagram, except the mutable fields of the leading IP header. ESP, on the other hand, does *not* authenticate the leading IP header or any other information that comes before the ESP header. With ESP, both communicating systems use cryptographic keys for encrypting and decrypting the data they exchange.

If you decide to use both encryption and authentication, the responding system first authenticates the packet and then, if the first step was successful, proceeds with decryption. Since decryption is more processor intensive than authentication, this type of configuration reduces processing overhead, as well as reduces your vulnerability to denial of service attacks.

ESP is defined in RFC 2406 and is a separate IP protocol, number 50. For clarification, this means it does not use TCP or UDP as an underlying transport protocol.

1.6.1 ESP packet format

Figure 13 shows the position of the ESP header in the IP packet and the header fields.

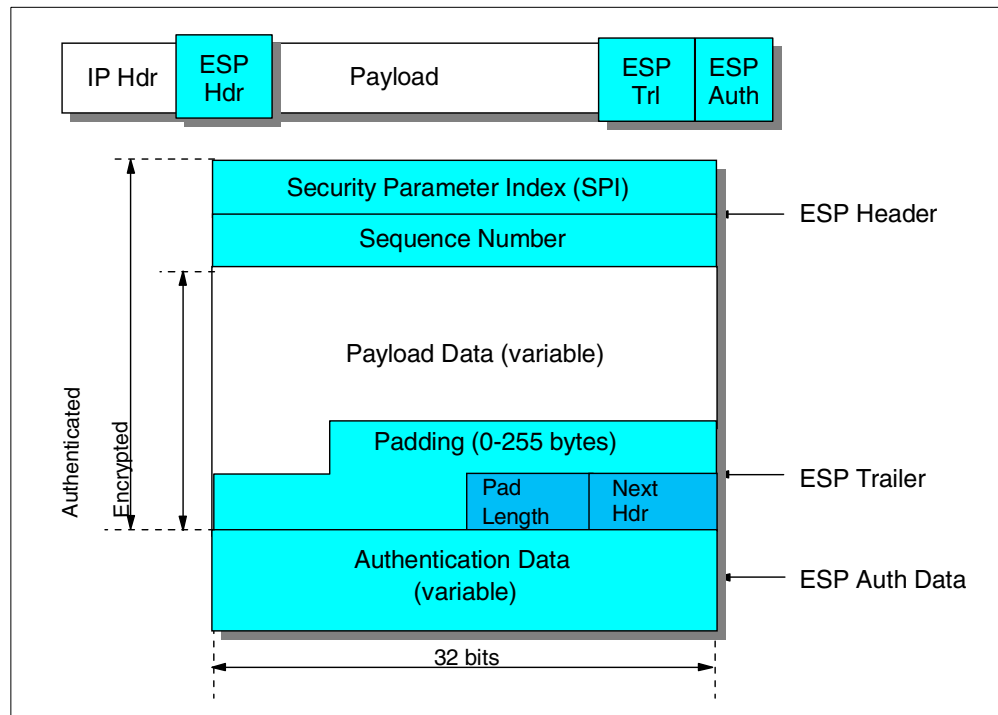


Figure 13. ESP packet format

The format of the ESP packet is more complicated than that of the AH packet. Not only is there an ESP header, but also an ESP trailer and ESP authentication data. The payload is located (encapsulated) between the header and the trailer, which gives the protocol its name. The following fields are part of an ESP packet:

- **Security Parameter Index (SPI):** This field is 32 bits in length. SPI is discussed in greater detail in 1.9, “IPSec configuration concepts” on page 29.
- **Sequence Number:** This 32-bit field is the monotonically increasing counter that we described in the AH header format.

Note: Manual key management does not typically use the anti-replay mechanism. In addition, older IPSec implementations, such as the one used in IBM Firewall for AS/400, are based on the original ESP specification (RFC 1827), which does not support the concept of sequence numbers.

- **Payload Data:** The Payload Data field is mandatory. It consists of a variable number of bytes of data described by the Next Header field. This field is encrypted with the cryptographic algorithm agreed upon when the security association was established. If the algorithm requires initialization vectors, these are also included here.

The ESP specification requires support for the DES algorithm in CBC mode (DES-CBC transform). Often, other encryption algorithms are also supported, such as triple-DES and CDMF.

Note: CDMF = Commercial Data Masking Facility. It is a variation of DES using only 40 bits of a 56-bit key.

- **Padding:** Most encryption algorithms require that the input data be an integral number of blocks. Also, the resulting ciphertext (including the Padding, Pad Length, and Next Header fields) must terminate on a 4-byte boundary, so the Next Header field is right aligned. This is why this variable length field is included. It can be used to hide the length of the original messages too. However, this can adversely impact the effective bandwidth. Padding is an optional field.

Note: Encryption covers the Payload Data, Padding, Pad Length, and Next Header fields.

- **Pad Length:** This 8-bit field contains the number of the preceding padding bytes. It is always present, and the value of 0 indicates no padding.
- **Next Header:** The Next Header is an 8-bit mandatory field that shows the data type carried in the payload, for example, an upper-level protocol identifier such as TCP. The values are chosen from the set of IP protocol numbers defined by the IANA.
- **Authentication Data:** This field is variable in length and contains the ICV calculated for the ESP packet from the SPI to the Next Header field inclusive. The Authentication Data field is optional. It is included only when integrity check and authentication have been selected at SA initialization time.

The ESP specifications require two authentication algorithms to be supported: HMAC with MD5 and HMAC with SHA-1. Often, the simpler keyed versions are also supported by IPSec implementations.

Notes

- The ICV does not cover the IP header.
- The original ESP specification in RFC 1827 discusses the concept of authentication within ESP in conjunction with the encryption transform. That is, there is no Authentication Data field and it is left to the encryption transforms to provide authentication.

1.6.2 ESP transport and tunnel modes

ESP can also be used in two modes: *transport* mode and *tunnel* mode.

1.6.2.1 ESP in transport mode

In transport mode, the ESP header follows the IP header of the original IP datagram. If the datagram already has an IPSec header, then the ESP header goes before it, as shown in Figure 14. The ESP trailer and the optional authentication data are appended to the payload of the original datagram.

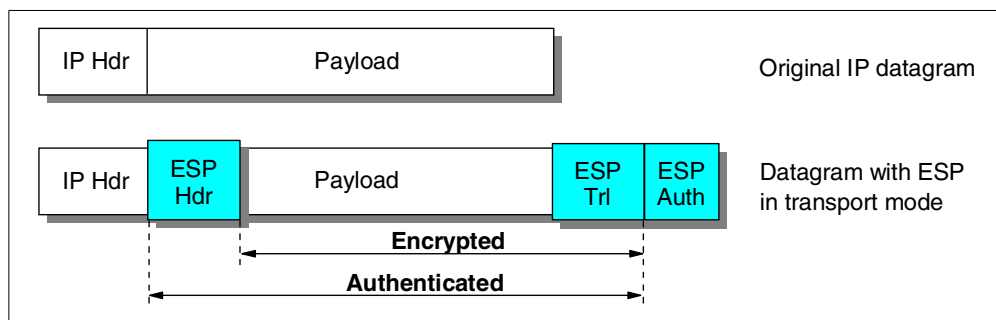


Figure 14. ESP in transport mode

Transport mode does not authenticate or encrypt the IP header, which can expose your addressing information to potential attackers while the datagram is in transit. Transport mode requires less processing overhead than tunnel mode, but does not provide as much security. In most cases, hosts use ESP in transport mode.

1.6.3 ESP in tunnel mode

Tunnel mode creates a new IP header and uses it as the outermost IP header of the datagram. The ESP header follows and then the original datagram (both the IP header and the original payload) as shown in Figure 15 on page 21. The ESP trailer and the optional authentication data are appended to the payload.

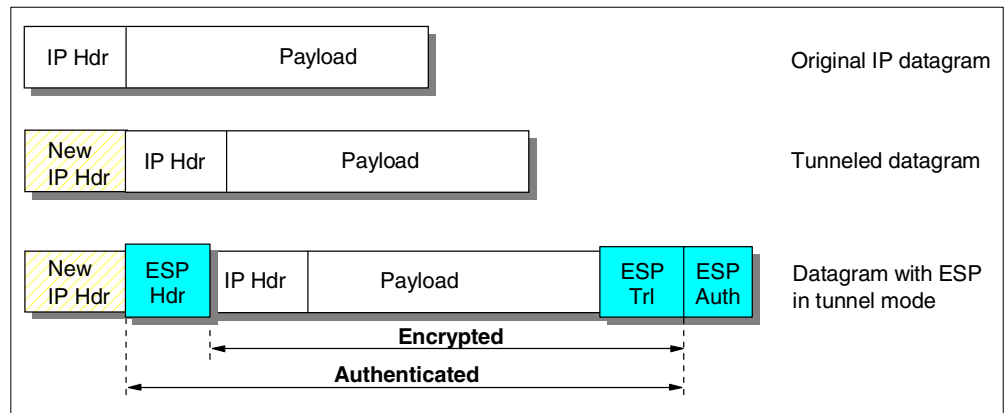


Figure 15. ESP in tunnel mode

If you decide to use both encryption and authentication, ESP completely protects the original datagram because it is now the payload data for the new ESP packet. However, ESP does not protect the new IP header. Gateways must use ESP in tunnel mode.

1.6.4 ESP transforms

Transforms supported with ESP include:

- Mandatory Encryption Transforms
 - DES_CBC (RFC 2405)
 - NULL (RFC 2410)*
- Optional Encryption Transforms
 - CAST-128 (RFC 2451)
 - RC5 (RFC 2451)
 - IDEA (RFC 2451)
 - Blowfish (RFC 2451)
 - 3DES (RFC 2451)
- Mandatory Authentication Transforms
 - HMAC-MD5-96 (RFC 2403)
 - HMAC-SHA-1-96 (RFC 2404)
 - NULL (RFC 2410)*
- Optional Authentication Transforms
 - DES-MAC

Note

NULL cannot be used for authentication and encryption at the same time.

ESP uses a symmetric key that both communicating parties use to encrypt and decrypt the data they exchange. The sender and the receiver must agree on the key before secure communication takes place between them.

For authentication, ESP uses the same HMAC algorithms that AH uses.

The AS/400 system supports the following authentication and encryption algorithms in V4R4:

- Authentication
 - HMAC-MD5
 - HMAC-SHA
 - None
- Encryption
 - DES-CBC
 - 3DES-CBC
 - NULL

DES is an acronym for Data Encryption Standard. DES produces cipher texts of the same length as the clear text, and the decryption algorithm is exactly the same as the encryption, the only difference being the subkey schedule. These properties make it suitable for hardware implementations. Although DES is aging (its origins date back to the early '70s), after more than 20 years of analysis the algorithm itself is still considered secure. The most practical attack against it is *brute-force*: try the decryption with all possible keys and look for a meaningful result. The problem is the key length. Given enough money and time, a brute-force attack against a 56-bit key can be feasible. That's why recently, a new mode of DES, called triple-DES (3DES) has gained popularity. With 3DES, the original DES algorithm is applied in three rounds, with two or three different keys. This encryption is thought to be unbreakable for a long time, even with the foreseeable technological advances taken into account.

Cipher Block Chaining (CBC) mode is where the result of the encryption of the previous block is used in the encryption of the current block. Thus, each ciphertext block is dependent not just on the corresponding plain text block, but on all previous plain text blocks.

1.6.5 Why the need for two authentication protocols (AH and ESP)?

Knowing about the security services of ESP, one may ask if there is really a requirement for AH. Why does ESP authentication not cover the IP header as well? There are no official answers to these questions, but here are some points that justify the existence of two different IPSec authentication protocols:

- ESP requires strong cryptographic algorithms to be implemented, whether it will actually be used. Strong cryptography is an over-hyped and sensitive topic in some countries, with restrictive regulations in place. It may be troublesome to deploy ESP-based solutions in such areas. However, authentication is not regulated, and AH can be used freely around the world.
- Often only authentication is needed. While ESP may have been specified to cover the IP header as well, AH is more efficient compared to ESP with authentication only, because of the simpler format and lower processing overhead. It makes sense to use AH in these cases.
- Having two different protocols means finer-grade control over an IPSec network and more flexible security options. By nesting AH and ESP, for example, one can implement IPSec tunnels that combine the strengths of both protocols.

1.7 Combining AH and ESP

You can apply the AH and ESP protocols alone or in combination. Given the two modes of each protocol, there is quite a number of possible combinations. Luckily, out of the many possibilities, only a few make sense in real-world scenarios. There are two approaches to combining AH and ESP:

- *Transport adjacency* where both security protocols are applied in transport mode to the same IP datagram.
- *Iterated tunneling* (nested) where the security protocols are applied in tunnel mode in sequence. After each application a new IP datagram is created and the next protocol is applied to it. This method has no limit in the nesting levels. However, more than three levels are impractical.

1.7.1 Transport adjacency

Figure 16 illustrates transport adjacency. This method is practical for only one level of combination: host-to-host connections. The idea is to ensure total protection of the datagram, including the IP header. If you recall from our earlier discussion, ESP does not protect the IP header, while AH does protect it.

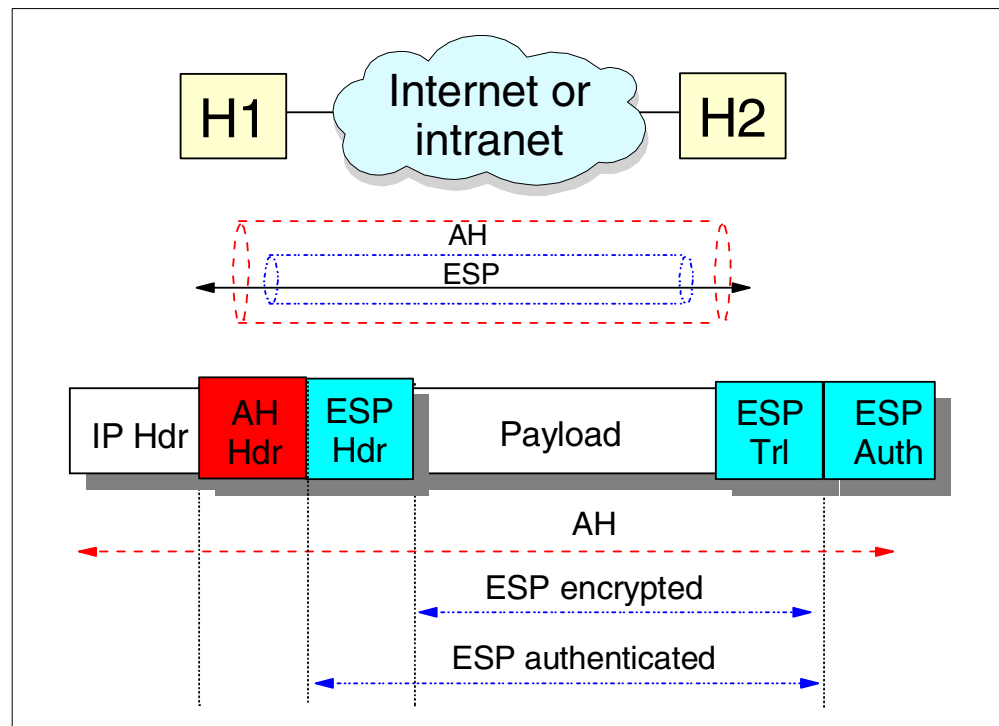


Figure 16. Host-to-host connections with transport adjacency

1.7.2 Iterated tunnels

Figure 17 on page 24 illustrates one of the most common configurations for combining AH and ESP: AH in tunnel mode protecting ESP traffic in transport mode. Combined AH-ESP tunnels between gateways are also common.

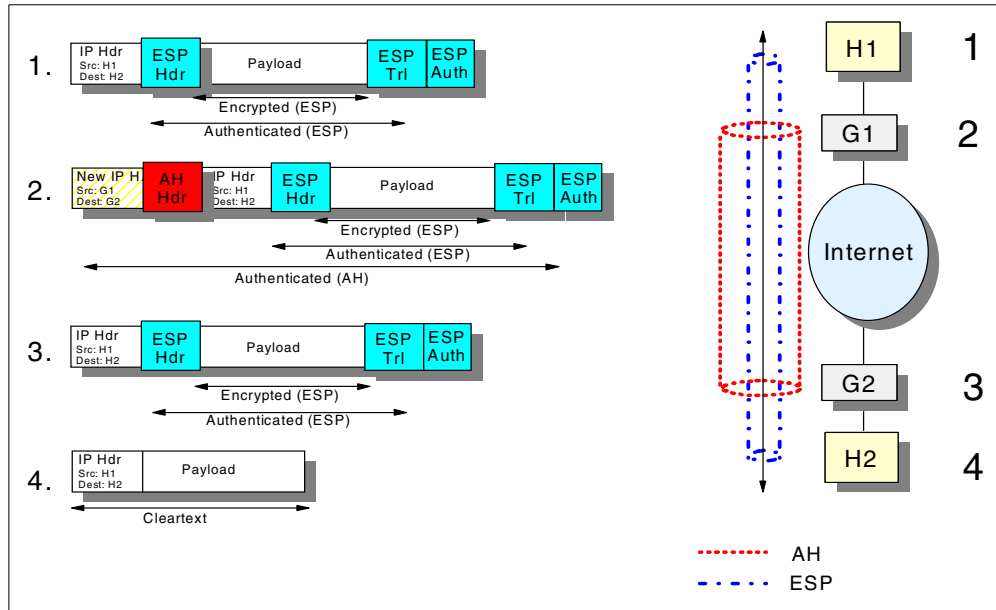


Figure 17. AH and ESP together in an iterated tunnel

To combine AH and ESP when they have different endpoints, at least one level of tunneling must be applied. Transport adjacency does not allow for multiple source/destination addresses, because only one IP header is present. The practical principle of combining AH and ESP is that, upon receiving a packet with both protocol headers, the IPsec processing sequence should be authentication followed by decryption. It is common sense not to bother with decrypting packets of uncertain origin.

Following this principle, the sender first applies ESP and then AH to the outbound traffic. In fact, this sequence is an explicit requirement for transport mode IPsec processing. When using both ESP and AH, a new question arises. Should ESP authentication be turned on since AH authenticates the packet anyway? The answer is simple. Turning ESP authentication on makes sense only when the ESP connection extends beyond the AH connection, as in the case of the supplier scenario. In this case, not only does it make sense to use ESP authentication, but we highly recommend that you do so.

As far as the modes (transport or tunnel) are concerned, the usual way is to use transport mode between the endpoints of a connection and tunnel mode between two machines when at least one of them is a gateway.

In Figure 17 on page 24, the local host (H1) sends an IP packet to the remote host (H2). Here is what happens:

1. Host H1 constructs the IP packet and applies ESP transport to it. H1 then sends the datagram to the local gateway (G1). The destination address is the remote host (H2).
2. The local gateway (G1) realizes that this packet should be routed to the remote gateway (G2). Upon consulting its IPsec databases (SPD and SAD; see 1.9.3, "IPsec policy databases" on page 31, for more information), G1 concludes that AH in tunnel mode must be applied before sending the packet

out. It does the required encapsulation. The IP packet now has the address of G2 as its destination. The ultimate destination, H2, is encapsulated.

3. G2 receives the AH-tunneled packet. It is destined to itself, so it authenticates the datagram and strips off the outer header. G2 sees that the payload is yet another IP packet (the one sent by H1) with destination H2, so it forwards to H2. G2 does not care that this packet has an ESP header.
4. Finally, H2 receives the packet. Since this is the destination, ESP-transport processing is applied, and the original payload is retrieved.

1.8 Key management objectives

Encryption is the transformation of a clear text message into an unreadable form to hide its meaning. The opposite transformation, which retrieves the original clear text, is the *decryption*. The mathematical function used for encryption and decryption is the *cryptographic algorithm* or *cipher*. The security of a cipher may be based entirely on keeping how it works a secret, in which case it is a *restricted* cipher. There are many drawbacks to restricted ciphers. It is difficult to keep in secret an algorithm used by many people. If it is incorporated into a commercial product, then it is only a matter of time and money to get it reverse engineered. For these reasons, the currently used algorithms are *keyed*. That is, the encryption and decryption makes use of a parameter, the key. The key can be chosen from a set of possible values, called the *keyspace*. The keyspace is usually large, the bigger the better. The security of these algorithms relies entirely on the key, not on their internal secrets. In fact, the algorithms themselves are public and are extensively analyzed for possible weaknesses.

DES is an example of a *symmetric* or *secret-key* algorithm. Symmetric algorithms are keyed algorithms where the decryption key is the same as the encryption key (contrast this with the more processor intensive asymmetric or public-key algorithms where different public and private keys are used). Symmetric algorithms are the conventional cryptographic algorithms, where the sender and the receiver must agree on the key before any secured communication can take place between them.

The problem is, how do you securely and reliably communicate the key before you have an encrypted link to send it over (and how do you have an encrypted link without a key)? You could pass it verbally over the phone, but this is potentially subject to eavesdropping and may be unreliable for complex hexadecimal keys. Consider also that you will want to change keys on a regular basis to reduce the time available and hence the chance of them being broken.

A manual connection, or manual tunnel, requires that keys are generated and configured manually. All IPSec implementations should support this, effectively as a lowest common denominator.

Some proprietary mechanisms exist for automatically exchanging keys. For example, IBM IP Security Protocol (IPSP) or IBM Tunnel are both supported by the IBM Firewall for AS/400 at V4R3. However, these are now considered proprietary and nonstandard.

The IETF has proposed a standard that allows for dynamic key management or generation called the Internet Key Exchange (IKE) protocols.

1.8.1 Internet Key Exchange (IKE)

Internet Key Exchange (IKE) framework, previously referred to as ISAKMP/Oakley, is a proposed IETF standard, which supports the automated negotiation of Security Associations, and the automated generation and refresh of cryptographic keys.

Generating your keys securely is the most important factor in establishing a secure and private connection. If your keys are compromised, then your authentication and encryption efforts, no matter how strong, become worthless. The ability to perform this function with little or no manual configuration will become an increasingly critical element as your VPN grows in size.

IKE requires that all information exchanges be both encrypted and authenticated. That way, no one can eavesdrop on your keying material and your keying material is generated only among authenticated parties. IKE procedures deal with initializing the keys, so they must be capable of running over links where no security can be assumed to exist. Therefore, the IKE protocols use the most complex and processor-intensive operations in the IPSec protocol suite.

In addition, the IKE methods have been designed with the explicit goals of providing protection against several well-known exposures:

Denial of Service

Identifies and rejects invalid messages without running processor-intensive cryptographic operations.

Man-in-the-Middle

Prevents common attacks such as deletion of messages, modification of messages, reflecting messages back to the sender, replaying of old messages, and redirection of messages to unintended recipients.

Perfect Forward Secrecy

Compromised keys provide no useful clues for breaking any other key, whether it occurred before or after the compromised key. Each refreshed key is derived without dependence on past keys.

IKE uses the UDP protocol with a source and destination port number of 500 and is defined in RFCs 2408-09 and 2411-12.

1.8.2 The two phases of IKE

IKE uses two distinct phases in its implementation:

- **Phase 1** establishes a shared master secret from which subsequent cryptographic keys are derived to protect user data traffic. This is true even if no security protection yet exists between the two endpoints.
- **Phase 2** exchanges are less complex, since they are used only after the security protection suite negotiated in phase 1 has been activated. In this phase, the subsequent cryptographic keys are negotiated and protected by the security associations generated in phase 1.

Figure 18 on page 27 illustrates the two phases.

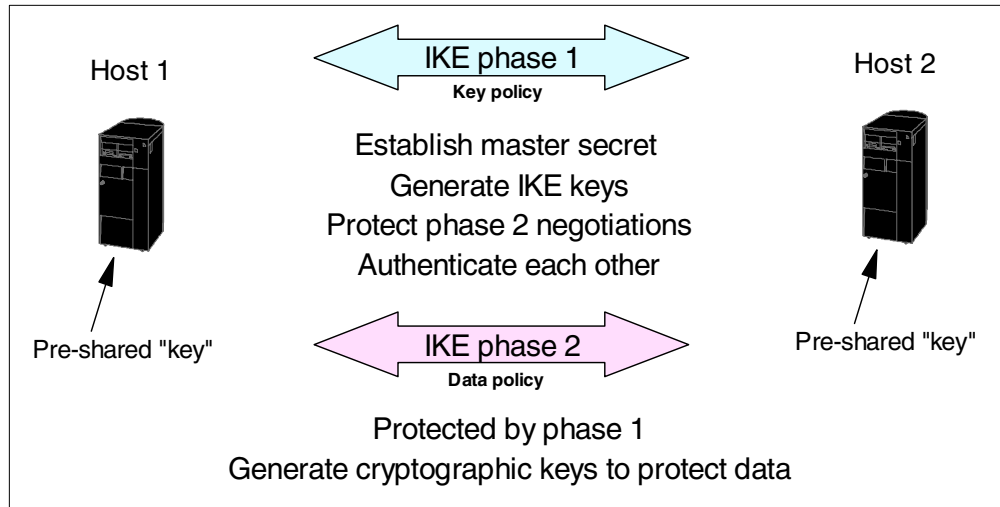


Figure 18. The two phases of IKE

Note: Keys are derived, and *never* transmitted.

1.8.2.1 IKE phase 1

Various authentication methods can be used to authenticate phase 1 negotiations, as well as to establish the keys that protect the IKE messages that flow during the subsequent phase 2 negotiations. These include pre-shared keys, digital signatures, public key encryption, and revised public key encryption. At V4R4, AS/400 VPN only supports pre-shared keys. The advantage of pre-shared keys is their simplicity. The disadvantage is that a shared secret must be distributed out-of-band prior to IKE negotiations.

A pre-shared key is perhaps a misnomer. In fact, a predefined character string is agreed upon and entered manually on both endpoint VPN key servers, but this is not really the key. The actual keys are derived, starting with a *Diffie-Hellman* key exchange.

Using the Diffie-Hellman algorithm, a large random number is generated on each key server and used to exponentiate an agreed integer value. The resulting exponents are exchanged and each key server then exponentiates the received exponent again using its random number. Both key servers now have the same result (the original integer exponentiated by both random numbers), which can be used as an initial shared secret key. The security of the exchange is based on the fact that it is extremely difficult to inverse the exponentiation performed by the two parties (the random numbers used are never transmitted). This shared secret key is then applied to the pre-shared key (and some other exchanged values called *Nonces*) to derive a string of bits called *keying material* from which all other authentication and cryptographic keys are generated.

Note

It is important to understand that keys themselves are never entered or communicated between servers, but derived using agreed inputs and algorithms by each of the key servers.

1.8.2.2 IKE phase 2

Phase 2 negotiates the keys and encryption or authentication algorithms that protect the actual application data exchanges. Remember, up to this point, no application data has actually been sent. Phase 1 protects the phase 2 IKE messages.

Once phase 2 negotiations are complete, your VPN establishes a secure, dynamic connection over your network and between the endpoints that you defined for your connection. All data that flows across the VPN is delivered with the degree of security and efficiency that was agreed upon by the key servers during the phase 1 and phase 2 negotiation processes.

In phase 1, the cryptographic operations are the most processor-intensive, but only need to be done infrequently. A single phase 1 exchange can be used to support multiple subsequent phase 2 exchanges. In general, phase 1 negotiations are implemented less often, while phase 2 negotiations are refreshed as often as in the order of minutes. Higher refresh rates increase your data security, but decrease system performance. Use short key lifetimes to protect your most sensitive data.

Note: AS/400 VPN terminology refers to phase 1 as the *key policy* and phase 2 as the *data policy*.

1.8.3 IKE main and aggressive modes

IKE supports two modes of its phase 1 negotiations: *main* (or *identity protection mode*) and *aggressive mode*. Figure 19 illustrates the differences.

Two IKE phase 1 modes are supported...

"Main" mode

- Also known as "identity protection" mode
- Encrypts identities during phase 1 negotiations

"Aggressive" mode

- Faster
- Does not encrypt identities





Figure 19. The differences between the two IKE modes

Main mode encrypts the identities of the key servers. In the simplest case, these are their IP addresses, but IKE also supports the use of permanent identifiers such as a name or e-mail address.

Aggressive mode is faster than main mode since it uses a three message exchange rather than six, but identifiers flow in clear text. Note that the IP header of the UDP datagrams always contains unencrypted IP addresses or else routing would not be possible. However, in some cases it may be that the key servers use different IP addresses than those used externally.

In phase 1, the initiator offers one proposal with at least one choice of transform combinations to use. In phase 2, the initiator can offer multiple proposals with multiple transform combinations to use. This is required to accommodate the

ability to define iterated tunnels. You may remember that transforms are the authentication and encryption algorithms to be used. Figure 20 shows a simplified diagram of the proposal negotiation.

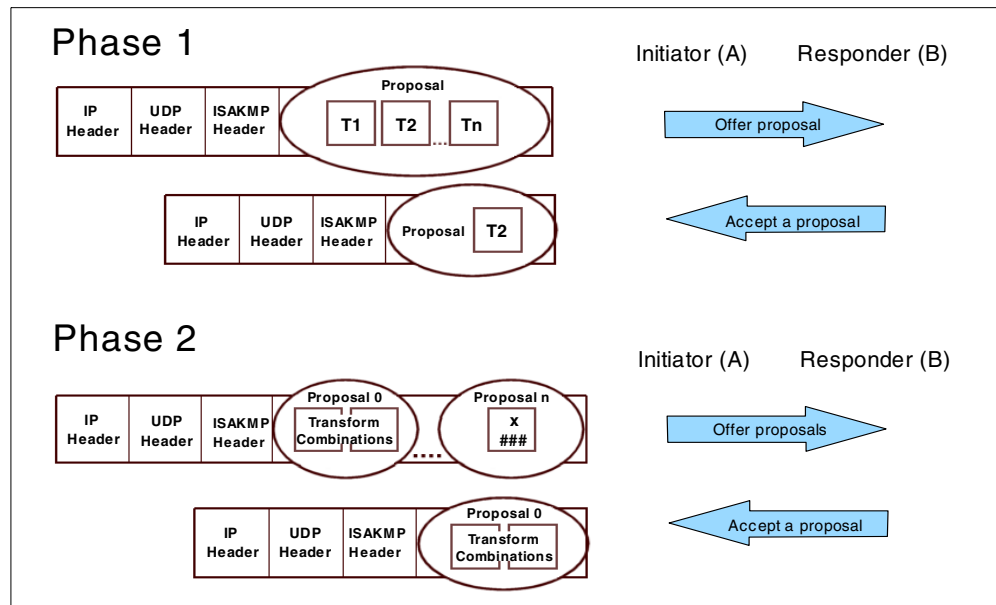


Figure 20. IKE proposal negotiation for phase 1 and phase 2

The responder looks through its own list of proposals and selects the first that matches. The sequence in which proposals are checked is controlled by the initiator. Matches must be exact. For example, 3DES will not match DES. There is one exception: if key expiration times are different, the lower time is accepted.

1.9 IPSec configuration concepts

The concept of a Security Association (SA) is fundamental to IPSec. IKE SAs are bi-directional. Protocol (data) SAs are unidirectional (simplex) logical connections between two IPSec systems, uniquely identified by the following triple:

<Security Parameter Index, IP Destination Address, Security Protocol>

Note the following explanation of the elements:

Security Parameter Index (SPI)

This is a 32-bit value used to identify different SAs with the same destination address and security protocol. The SPI is carried in the header of the security protocol (AH or ESP). The SPI has only local significance, as defined by the creator of the SA. The SPI values in the 1 to 255 range are reserved by the Internet Assigned Numbers Authority (IANA). The SPI value of 0 must be used for local implementation-specific purposes only. Generally, the SPI is selected by the destination system during the SA establishment.

IP Destination Address

This address may be a unicast, broadcast, or multicast address. However, current SA management mechanisms are defined only for unicast addresses.

Security Protocol

This can be either AH or ESP.

Because these SAs are simplex, bi-directional communication between two IPSec systems requires two SAs: one for each direction. An SA gives security services to the traffic it carries by using either AH or ESP, but not both. In other words, for a connection that should be protected by both AH and ESP, two SAs must be defined for each direction. In this case, the set of SAs that define the connection is referred to as an *SA bundle*. The SAs in the bundle do not have to terminate at the same endpoint. For example, a mobile host can use an AH SA between itself and a firewall and a nested ESP SA that extends to a host behind the firewall.

1.9.1 SA combinations

Figure 21 illustrates some of the SA combinations that are possible between hosts and gateways.

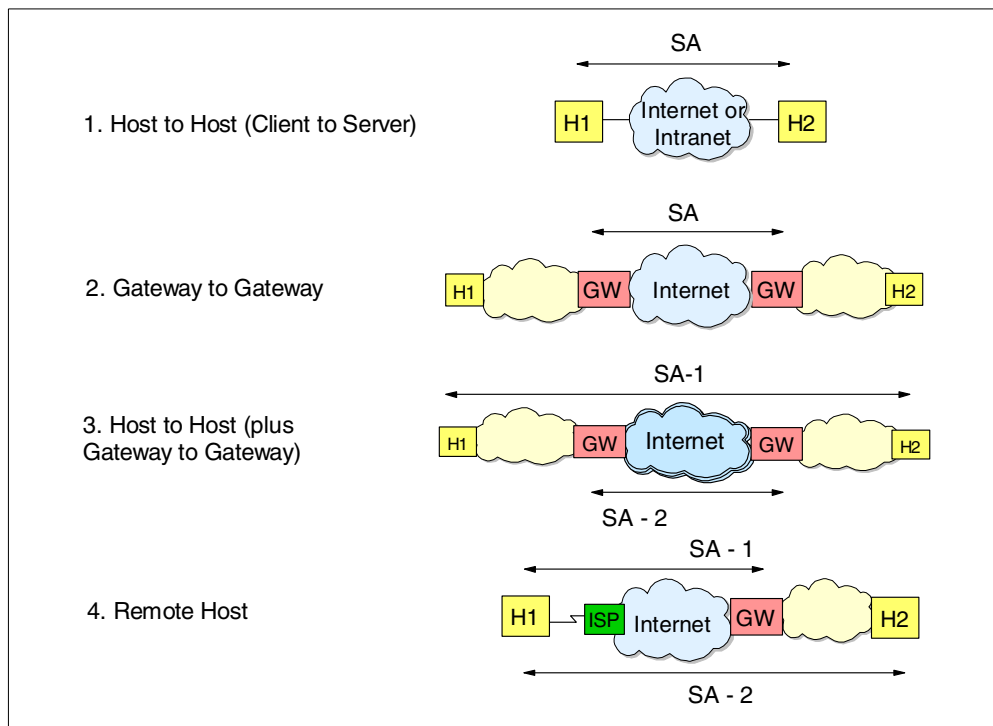


Figure 21. SA combinations - VPN configuration options

Note the following explanation for Figure 21:

1. A simple client server connection between two hosts.
2. A typical gateway-to-gateway connection between, perhaps, a branch office network and a central corporate network.

3. Could be a connection between the networks of business partners or suppliers. AH authentication may be applied between gateways and ESP encryption/authentication between the hosts.
4. Could represent a dial-up connection from a host into a gateway.

1.9.2 Security Parameters Index (SPI)

The Security Parameters Index (SPI) is simply a pointer to the SA to be used to authenticate and decrypt a datagram. When a datagram is received, the receiving system must know what algorithms to use to do this. Therefore, the SPI is sent as clear text in the IPsec header as shown in Figure 22. If the SPI was encrypted, the receiver would not know how to decrypt it. The SPI value in itself is a meaningless number.

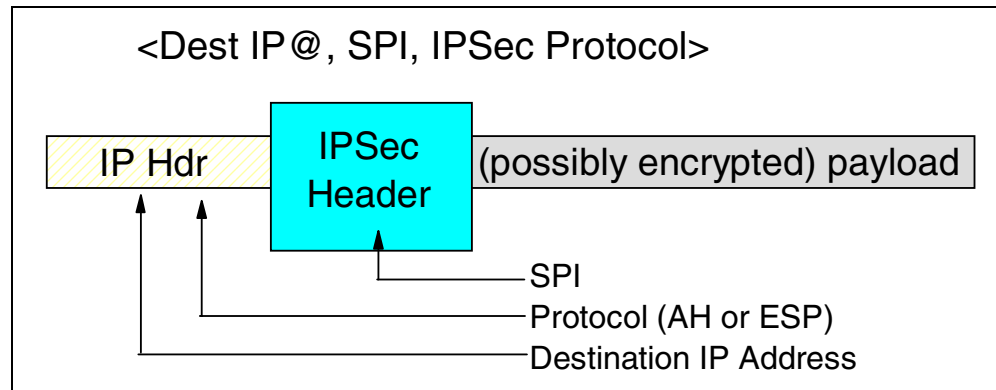


Figure 22. Security Parameters Index (SPI)

If you look at a line trace, the SPIs are visible in the AH or ESP headers. For any connection, different SPIs are used for each direction. This is because, as stated previously, there are different SAs for each direction and different SPIs.

1.9.3 IPsec policy databases

There are two policy components in each IPsec enabled-host:

- **Security Policy Database (SPD)**

The Security Policy Database (SPD) defines how each datagram is to be processed and is similar and related to IP filters. It can specify that:

- Certain datagrams will be discarded and stopped from leaving the host or from being received into an upper layer application.
- Certain datagrams will be permitted to bypass IPsec and go through normal IP send or receive processing.
- Certain datagrams will be sent or received over IPsec protected connections.

- **Security Associations Database (SAD)**

The Security Associations Database (SAD) contains information on all currently active SAs. When the SPD specifies that IPsec is to be used with a datagram, the SAD is consulted to:

- Establish what authentication and encryption algorithms to apply for outgoing datagrams.
- Determine if the received datagram needs to be authenticated or decrypted. The received SPI points to the specific SA in the SAD to be used.

Chapter 2. Introduction to Layer 2 Tunneling Protocol (L2TP)

Many AS/400 networks are a combination of intranets (connecting systems that belong to the same company), extranets (connecting networks that belong to more than one company, usually business partners), and Internet connections. AS/400 customers typically have two or more of the following TCP/IP networking requirements:

- Networking to the Internet
- Networking between geographically dispersed sites in the same company
- Providing remote access to mobile workers
- Networking with other companies (extranets)

Traditionally, companies have satisfied the last three requirements by using private leased or dial-up links. This approach is costly not only in dollars, but also in time and other resources. Issues such as the size of the modem pool and the dispersed geographic locations of the remote sites demand on-going attention.

Layer 2 tunnel protocols are an excellent way of providing cost-effective remote access. When used in conjunction with IPSec, they are an excellent technique for providing secure remote access.

The Internet Engineer Task Force (IETF) works together with vendors of computers and communications equipment standardized L2TP.

Achieving the desired connectivity and security requirements is not a trivial task. In V4R4, the AS/400 system has been enhanced with new remote access features that simplify the implementation of intranets, extranets, and mobile clients, and eliminate the need for third-party boxes.

This chapter provides a general overview of L2TP.

2.1 Remote access overview

Remote connections link single users (mobile or work-at-home users) and branch offices (LANs) to a company campus network. VPNs link the remote sites to the campus using the Internet as the backbone for communications between those locations. Remote sites, by definition, belong to a single company and share a common network administration policy.

Remote sites can be characterized as having a relatively small number of users and, therefore, one default gateway connection to the Internet. The corporate campus may have multiple gateway connections to the Internet.

The primary security emphasis for remote sites is to secure the link between the user or gateway and the corporate office campus. End-to-end (host-to-host) security is optional, and it is dictated by the company's overall security policy.

The network administrator must assign to the remote sites IP addresses that are consistent with the corporate office address space management scheme. IP addresses must be non-overlapping and routable within the corporate network. Deploying a carefully planned IP address scheme minimizes routing table size and changes, scales to multiple remote access servers, and enables support for alternatives to IP routing such as proxy ARP.

To route corporate addresses over the Internet, each remote site gateway and the corporate office gateway must have at least one globally routable IP address for building the IP tunnels.

Client global addresses can be fixed or dynamically assigned by the ISP. Corporate office global addresses are usually fixed. Because a remote client's global IP address may be dynamically assigned, IKE phase 1 host identifier cannot be an IP address, and it should be a permanent identifier such as a host name or e-mail address.

How the remote client's corporate and globally routable IP addresses are assigned and managed varies depending on the tunneling mode used, ISP connection type, and whether the client is a single user or remote LAN. L2TP provides a method to help with the assignment and management of IP addresses.

2.2 The evolution of dial-up networks

This section explores the evolution of dial-up networks from a private infrastructure to an Internet-based infrastructure. This evolution requires the development of new standards and protocols that allow customers to benefit from the advantages provided by modern dial-up networks, without losing the benefits that traditional dial-up networks have to offer.

Nowadays, companies strive to reduce cost and increase flexibility by implementing dial-up networks using the existing Internet infrastructure. To circumvent the high communications and network management costs, companies are looking to outsourcing their remote access services to Internet Service Providers (ISPs). Users connecting to the Internet through ISPs can access corporate services from anywhere in the world.

Virtual Private Networks (VPNs) allow remote clients and servers to participate in a private network even though they are connected through an intermediate network that may be public, such as the Internet. IP Security (IPSec) standards deal with security and integrity but not with addressing and routing issues. This is essentially a tunneling problem to solve.

2.2.1 Traditional dial-up networks

The traditional method for companies to provide connectivity to their networks for mobile and remote users, business partners, and remote branch offices is to install and manage large modem pools and remote-access servers.

In traditional dial-up networks the client, for example, a remote branch office, a business partner, or a mobile worker dials into the corporate network over the public telephone network. The typical dial-in entry point to the corporate network is a modem pool with an associated dial-in access server. The most obvious disadvantages of the traditional dial-up private networks are:

- **High communications cost:** Quite often the connections are long-distance and, therefore, expensive.
- **Limited flexibility and scalability:** Adding remote sites or clients usually requires extra work from the corporate network managers to purchase and configure modems and communications devices compatible with the corporate office equipment.

- **High maintenance and management cost:** As the number of remote users grows, the modem pool, access server ports, and number of telephone lines must be extended.
- **Fast depreciation of the telecommunications devices:** At the current speed of technology, equipment becomes outdated in a short period of time.

Figure 23 shows several examples of traditional dial-up methods.

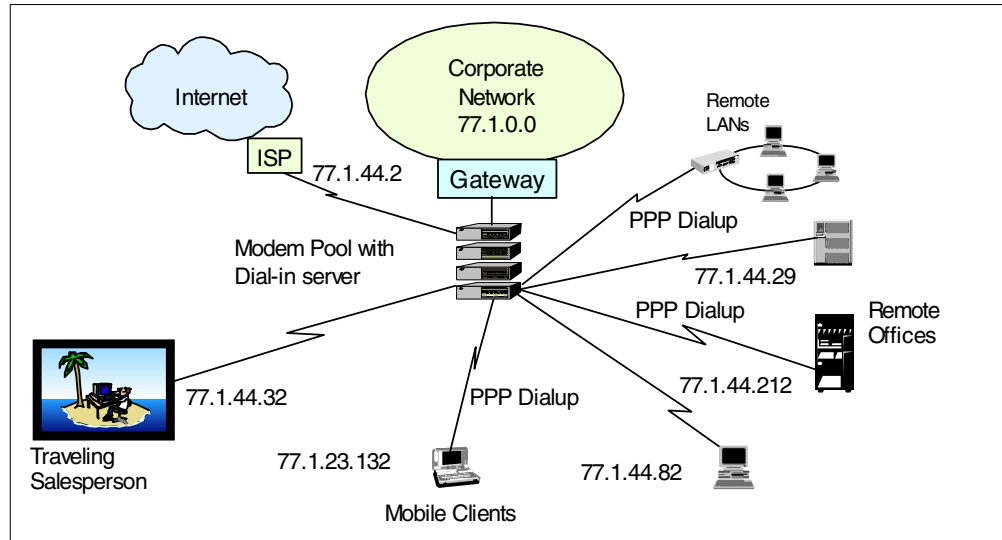


Figure 23. Traditional dial-up private network infrastructure

The traditional dial-up private networks also have some advantages:

- **Remote users are regarded as part of the corporate network:** In traditional dial-up networks, remote users dial directly into the corporate network and, after successful authentication, they are assigned IP addresses in the corporate office address space. This simplifies the access control measurements required if *foreign* and unknown IP addresses were granted connectivity to the corporate campus. Since remote users appear as locally connected to the corporate network, routing is also simplified.
- **Security:** In traditional dial-up networks, the physical links are more secure than on the Internet. Even though the physical links traverse telephone companies and nodes that are not totally under the control of the corporation, the exposure is not as high as on the Internet.
- **Performance:** In traditional dial-up networks, the workload is limited to the company's use and, therefore, easier to predict and control.

Traditional dial-up networks met the requirements in the past and still do today in some particular environments where the number of remote users is limited and the communication costs are not too high. However, in today's business environment, you may also want to connect business partners or suppliers to your corporate network. Some remote clients need access to the entire corporate network. Other clients just need access to a particular subnet or system in the corporate network. At this point, traditional dial-up networks reach their limits.

2.2.2 Modern dial-up networks

Modern dial-up networks exploit the Internet to connect remote clients to the corporate network. On the corporate side, the only requirement is to provide a dedicated link to the Internet. This link can be used for remote access as well as traditional Internet traffic such as e-mail and World Wide Web access.

The modern dial-up network presents several advantages:

- **Low communication costs:** The remote clients dial into the nearest ISP point of presence (PoP). These are usually local calls and therefore save an enormous amount of money compared to long-distance calls.
- **Outsource of network management and maintenance to the ISP:** The modem pool and other sophisticated communications equipment, as well as the technical skills to manage them, are now the ISP's responsibility.
- **Flexibility and scalability:** New remote sites and clients can be easily added as long as there is an ISP PoP in the geographical location.

Figure 24 shows an example of the new dial-up network infrastructure.

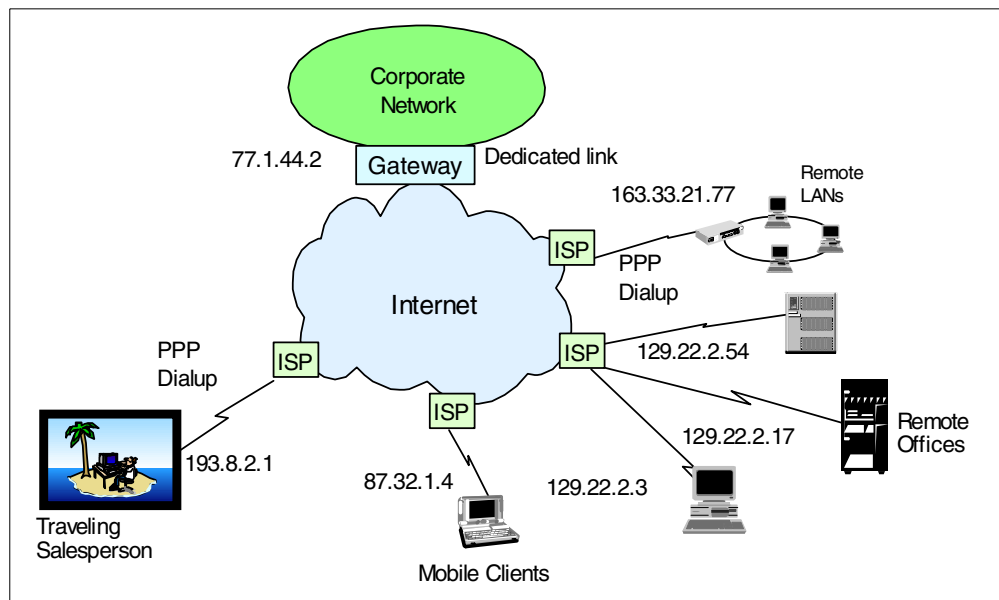


Figure 24. Modern dial-up network infrastructure

The modern dial-up network shown in Figure 24 also opens many new issues:

- **Security over Internet links**
- **IP address assigned to remote clients:** In the traditional dial-up network, the addresses are local to the corporate network address space. In the modern dial-up network, they are usually dynamically assigned by the ISP.
- **Access control for remote clients:** Many companies control access to internal applications and servers by IP address and even by subnet address within the corporate network. The company may also want to control access to the Internet itself. For example, the employees should enter the Internet through the company's Internet gateway and not directly.

All of these issues demand a solution that gives the remote client transparent access to the corporate network and protects the data. L2TP in combination with IPsec is the right answer. It provides transparent access for the remote clients to the corporate network. L2TP extends the local corporate IP address space to a remote client over the intervening Internet. Protecting the L2TP tunnel with IPsec affords the L2TP tunnel IPsec security.

2.3 L2TP overview

The previous sections showed you the requirement for new network services to solve some of the problems introduced by moving traditional dial-up networks to an Internet-based infrastructure. L2TP, in combination with IPsec, addresses the solution to those problems.

This section provides an overview of L2TP concepts. The Layer 2 Tunneling Protocol is an IETF standards track protocol for tunneling PPP. For a complete description of this protocol and the status of the draft, refer to RFC 2661 *Layer Two Tunneling Protocol "L2TP"*. You can obtain the latest version of the RFCs from the Internet Engineer Task Force Web site at: <http://www.ietf.org>

The traditional dial-up network service on the Internet is for registered IP addresses only. In other words, dial-up clients are assigned a globally routable IP address that, naturally, does not belong to the corporate private address space. There is a requirement for a new class of dial-up application services on the Internet. This class of network services supports the assignment of private IP addresses to dial-up remote clients and multiprotocols through PPP across the existing Internet infrastructure.

L2TP is a tunneling protocol that utilizes the functionality of PPP to provide dial-up access through the Internet. Because it uses the existing PPP infrastructure, L2TP inherits some of the advantages of PPP such as dynamic address assignment from a pool of pre-defined IP addresses or from DHCP, user-based authentication, compression, and the capability of transporting multiple protocols such as Netbios and IPX, besides IP. The objective is to extend the corporate network over an intervening network (the Internet, for example) to a remote client. PPP is defined in the RFC 1661 *The Point-to-Point Protocol (PPP)*.

Note: PPP on the AS/400 system only supports the IP protocol. PPP on the AS/400 system does not support address assignment from DHCP.

L2TP manages the tunneling of the link layer (that is, sync HDLC and async HDLC) of PPP. Using L2TP tunnels, it is possible to divorce the location of the initial dial-up server from the location at which the dial-up protocol connection is terminated. Access to the network is provided. L2TP is always point to point.

L2TP extends the PPP model by allowing the Layer 2 (L2) and PPP endpoints to reside on different devices interconnected by a packet-switched network. With L2TP, a user has an L2 connection to an access concentrator, for example, a modem bank, Asymmetric Digital Subscriber Line (ADSL), Digital Subscriber Line Access Multiplexer (DSLAM), and so on. The concentrator then tunnels individual PPP frames to the Network Access Server (NAS). This allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit.

Virtual PPP technology (L2TP) extends the normal PPP session created between the client and the remote-access server to a home gateway on the Internet. The home gateway terminates the PPP session and performs all the functions of a remote-access server, including user authentication and protocol negotiation. In a Virtual PPP link, the L2TP network server can exist behind the corporate firewall, allocating addresses that are internal in the corporate network. In this case, the dial-in user appears to be locally connected to the L2TP network server.

L2TP, as a protocol, combines the benefits of the Point-to-Point Tunneling Protocol (PPTP) developed by Microsoft and the Layer 2 Forwarding protocol (L2F) developed by Cisco Systems. In addition, it has been enhanced with new functions such as authentication and encryption through the IPsec protocol.

2.3.1 L2TP Access Concentrator (LAC)

The LAC is a node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP Network Server (LNS). The LAC can reside either in the dial-in client or in the ISP. When the LAC resides in the ISP, it sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with the L2TP protocol as defined in the RFC 2661 *Layer Two Tunneling Protocol "L2TP"*.

In summary, the LAC is:

- Located at the remote site (ISP or remote dial-in client)
- Peer to the L2TP Network Server (LNS)
- Usually the initiator of incoming calls (also known as L2TP initiator)

2.3.2 L2TP Network Server (LNS)

The LNS is a node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP Access Concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC.

In summary, the LNS is:

- Usually located at the corporate office gateway
- The peer to the LAC
- The logical terminator of the L2TP tunnel or virtual PPP session
- Usually, the responder of incoming calls initiated by the LAC
- The initiator of outgoing calls if it supports dial-on-demand

Figure 25 shows an overview of the LAC and LNS in an L2TP tunnel.

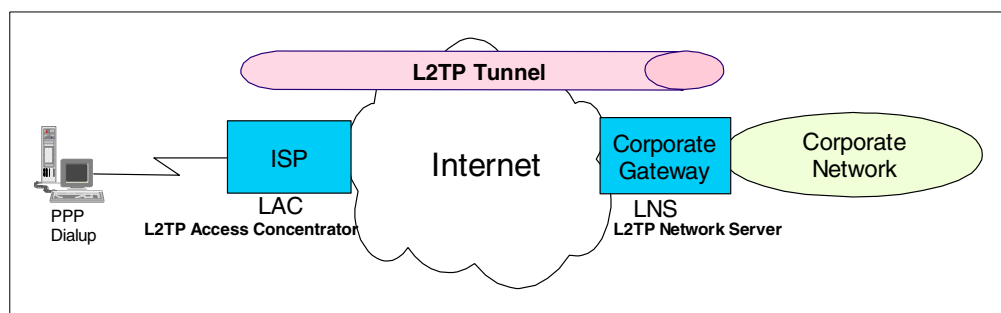


Figure 25. Logical view of LAC and LNS functions in an L2TP tunnel

2.3.3 Call establishment

The common way to initiate a connection is through *incoming calls* when a client initiates a call to an ISP. The ISP, in turn, initiates the tunnel to the corporate office gateway.

Outgoing calls are also supported by the L2TP protocol. This is the case when the corporate office gateway initiates a tunnel to an ISP and instructs the ISP to place a call to the client. Outgoing calls are useful for dial-on-demand scenarios to automate access to remote networks. L2TP dial-on-demand is not supported by the AS/400 system acting as an L2TP Network Server (LNS) in V4R4.

2.3.4 Address allocation

In the modern dial-up network without L2TP, like the one shown in Figure 24 on page 36, the user accepts that the IP addresses may be allocated dynamically from a pool of ISP addresses. This model often means that the remote user has little or no access to their corporate network's resources. This is due to firewalls and other security policies applied by the corporate network when the host has an external IP address.

The L2TP tunnel is viewed as a virtual PPP connection. In the traditional dial-up network, the remote client dials-up into the corporate network through a physical PPP link. The client is assigned a local IP address and is directly connected to the corporate network. L2TP offers this functionality over the Internet. The traditional PPP link is now tunneled into an L2TP tunnel and, therefore, called a *virtual PPP connection*. This virtual PPP connection is tunneled through the Internet to a destination, such as the corporate network gateway. The L2TP network server (LNS) can exist behind the firewall, allocating addresses that are internal to the corporate network address space. The addresses that the corporate office gateway or LNS assigns to the L2TP client can even be part of the block of IP address space that the Internet Assigned Numbers Authority (IANA) has reserved for private Internets as defined in RFC 1918, *Address Allocation for Private Internets*. The blocks of reserved IP address space are:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

For the purpose of PPP protocol handling, the dial-in user appears to be directly connected to the L2TP network server (LNS).

The Network Control Protocol (NCP) is used to negotiate and assign the IP addresses used for the virtual PPP link.

2.3.5 Authentication

The LNS at the corporate office manages authorization the same way it would in a direct dial-up traditional network. The authentication of the user occurs in three phases: the first at the ISP and the second and (optional) third at the corporate office gateway.

In compulsory tunnels where the ISP must support L2TP services, the ISP uses the user name sent by the PPP client to determine that a virtual dial-up service is required. Then, it initiates the tunnel connection to the appropriate corporate gateway. Once the tunnel is established, the ISP allocates a new call ID and

initiates a session by forwarding the authentication information it gathered from the client. The corporate office gateway undertakes the second phase by deciding whether to accept the call. The call start indication includes Challenge Handshake Authentication Protocol (CHAP) authentication information. Based on this information, the corporate gateway may accept or reject the call request. Once the call is accepted, the corporate gateway may pursue a third phase of authentication at the PPP layer.

2.3.6 Security

For the virtual dial-up service, L2TP provides user authentication and authentication of the tunnel endpoints. However, L2TP does not define tunnel protection mechanisms. PPP offers its own compression and encryption, but they are not recommended when security is a requirement for several reasons:

- No key management facilities.
- PPP compression and encryption is stateful what magnifies packet loss.
- No protection of control packets.

The L2TP specification proposes the use of the IPSec protocol suite for protecting L2TP traffic over IP when security is required, for example, over the Internet.

2.3.7 Tunnel modes

L2TP supports two tunnel modes: the *voluntary* and the *compulsory* tunnel. The major difference between these two tunnel modes is the tunnel endpoint.

In a voluntary tunnel, the tunnel ends at the remote client, which must support LAC functions. In a compulsory tunnel, the tunnel ends at the ISP, which must be able to provide LAC services.

2.3.8 L2TP encapsulation

L2TP uses the registered UDP port 1701 (RFC 1700 *Assign Numbers*). The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram. The initiator of an L2TP tunnel picks an available source UDP port (which may be 1701), and sends it to the desired destination address at port 1701. The recipient picks a free port on its own system (which may be 1701), sends its reply to the initiator's UDP port and address and sets its own source port to the free port it found. Once the source and destination ports and addresses are established, they *must* remain static for the life of the tunnel.

Note: In the AS/400 system, L2TP implementation source and destination ports are *always* 1701.

L2TP utilizes two types of messages: *control messages* and *data messages*. Control messages are used in the establishment, maintenance, and clearing of tunnels and calls. Control messages use a reliable Control Channel within L2TP to guarantee delivery.

Data messages are used to encapsulate PPP frames being carried over the tunnel. Data messages are not retransmitted when packet loss occurs. Figure 26 on page 41 provides an overview of L2TP encapsulation modes.

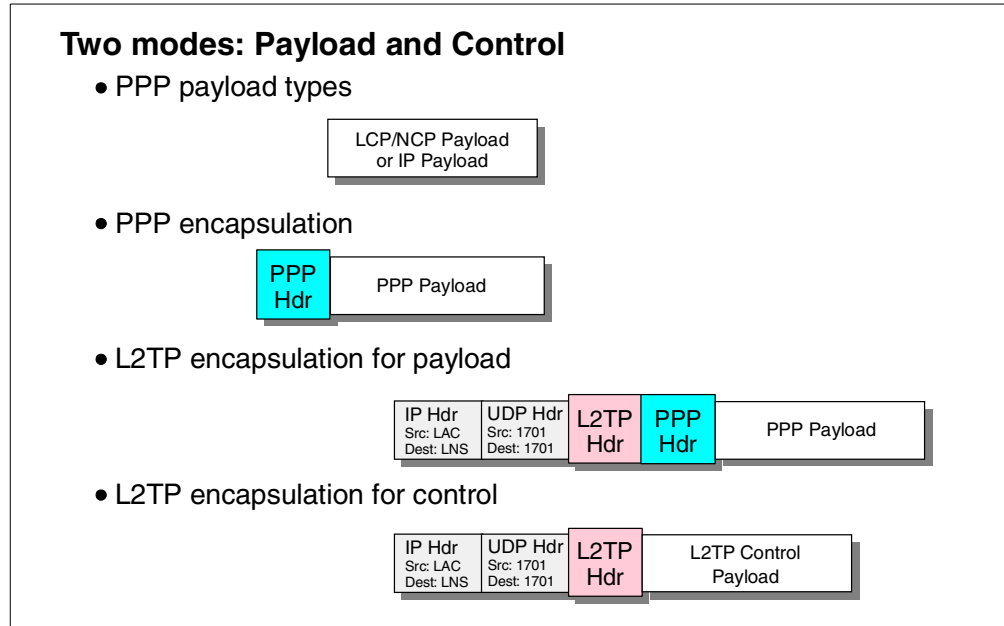


Figure 26. L2TP encapsulation

2.4 L2TP tunnel modes: Compulsory and voluntary

L2TP supports two tunnel modes: the *voluntary* and the *compulsory* tunnel. The major difference between these two tunnel modes is the tunnel endpoint. On the voluntary tunnel, the tunnel ends at the remote client, where the compulsory tunnel ends at the ISP.

2.4.1 L2TP compulsory tunnel

The L2TP compulsory tunnel does not require any configuration on the remote client. The ISP has to provide the L2TP Access Concentrator (LAC) function. The corporate network side has to provide the necessary network and access information to the ISP.

In compulsory tunneling, a tunnel is created without any action from the user and without allowing the user any choice. As a result, the remote dial-in client sends PPP packets to the ISP's Network Access Server (NAS)/LAC, which encapsulates them in L2TP and tunnels them to the LNS. The ISP establishes the L2TP tunnel when the remote client dials in. Refer to Figure 27 on page 42 for an overview of L2TP compulsory tunnel mode.

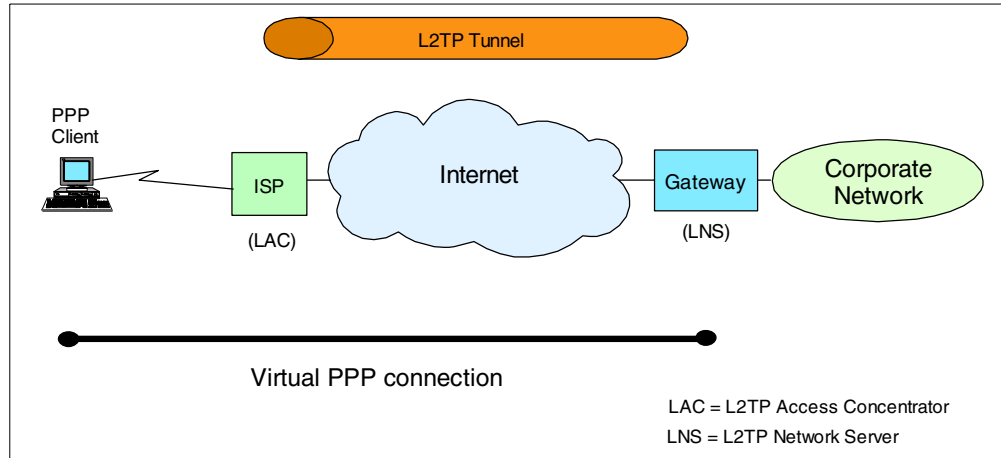


Figure 27. L2TP compulsory tunnel overview

The L2TP compulsory tunnel does not require L2TP support on the remote client. The ISP provides the L2TP Access Concentrator (LAC) function. The corporate office must contract the service with the ISP and provide it with the necessary authentication and configuration information.

A user dials-in to the local ISP and establishes a PPP session with the ISP's network access service (NAS), which answers the incoming call and forms one end of the virtual PPP tunnel.

The ISP notifies the corporate office gateway (the terminator of the virtual PPP tunnel or LNS) when an L2TP session is requested. The LAC in the ISP forwards the client's user name and password. If the user is valid, the LAC and the corporate gateway establish the tunnel and assign a session ID that specifically identifies the user to the tunnel.

Once the user is authenticated and the tunnel is established, the client and the corporate gateway negotiate the PPP session by setting up protocols and allocating network addresses to the client that are usually carved from the corporate network address space. In this model, the tunneling process is transparent to the user.

The dial-in client sends PPP packets to the LAC, which encapsulates them in L2TP and tunnels them to the corporate gateway. When the client establishes the PPP link to the ISP and the ISP connects to the LNS, the LNS assigns an IP address to the client based on the information stored in the virtual PPP profile on the LNS. Typically, this IP address belongs to the corporate network on the other side of the LNS. The ISP does not assign the client a globally routable address that can be used on the Internet. The client has no direct access to the Internet. Instead, the client appears as locally connected to the corporate network and underlies all access and security rules applied to the corporate network. To use the Internet applications, the remote client is forced to use the corporate gateway to the Internet.

The compulsory tunnel also supports a dial-out function. In this case, the LNS gateway sends a request to the ISP's LAC containing dial-out information. The ISP then establishes a dial-up PPP connection to a remote client. The AS/400 system does not support the dial-out function when acting as an LNS.

2.4.1.1 L2TP compulsory tunnel summary

The following points summarize the main characteristics of L2TP compulsory tunneling:

- The client is not assigned a globally routable IP address, therefore:
 - It is protected against intrusion from the Internet.
 - It cannot access the Internet directly, but only through the corporate gateway.
- The client does not need to support L2TP functions.
- The L2TP tunnel is transparent to the client.
- The ISP *must* support LAC functions.
- The ISP initiates the L2TP tunnel.
- L2TP tunnel is between the ISP and corporate network gateway.

Beware that currently (1999), few ISPs support the LAC function. This may change in the near future.

2.4.2 L2TP voluntary tunnel

In voluntary tunneling, a tunnel is created by the user, typically by using an L2TP-enabled client. As a result, the L2TP-enabled client sends L2TP packets to the NAS in the ISP, which forwards them on to the LNS. In voluntary tunneling, the NAS in the ISP does not need to support L2TP, and the LAC resides on the remote client. Additional configuration is required on the remote client side. Refer to Figure 28 for an overview of L2TP voluntary tunneling.

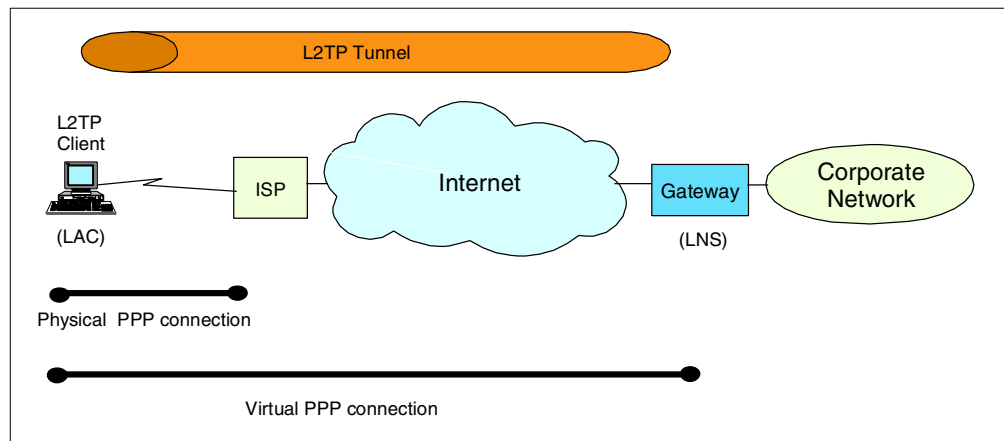


Figure 28. L2TP voluntary tunnel overview

In this tunnel mode, an L2TP-enabled client establishes a PPP session to an ISP. The ISP assigns a globally routable IP address to the client. The client then launches an L2TP session directly to the corporate gateway without any involvement from the ISP. The client must first establish an L2TP tunnel with the corporate gateway using a global IP address. Once the L2TP tunnel has been established, the client and the corporate gateway must negotiate the virtual PPP session by setting up protocols and allocating network addresses for communications with hosts on the corporate network. In this model, the client implementation is more complex. However, it offers more flexibility by enabling multiple access and also eliminates the need to establish secure tunnels with ISPs and corporate gateways. In the voluntary tunnel mode, the combined role of

the client (user and LAC on the same system) is transparent to the corporate gateway.

The client can have multiple tunnels established to different LNS. The client has more than one IP address assigned to it, for example, the globally routable IP address and the virtual PPP endpoint address. Since the client has a globally routable address, it has direct access to the Internet. Due to the corporate network IP address (virtual PPP endpoint), the client also appears as locally connected to the corporate network.

2.4.2.1 L2TP voluntary tunnel summary

The following points summarize the main characteristics of L2TP voluntary tunneling:

- The remote dial-in client must support L2TP Access Concentrator (LAC) functions.
- The configuration of the remote client is more complex.
- The ISP does not need to provide LAC services, and it is not involved in establishing the tunnel.
- The combined role of the client (user and LAC on the same system) is transparent to the corporate gateway.
- The L2TP client is the initiator of the connection and the tunnel to the LNS.
- The client is assigned a globally routable IP address by the ISP.
- Multiple sessions to multiple LNS are possible.
- The client has direct access to the Internet.
- The client is assigned an IP address in the corporate address space by the LNS.

Figure 29 shows an overview of L2TP tunnels, main components, and usage examples.

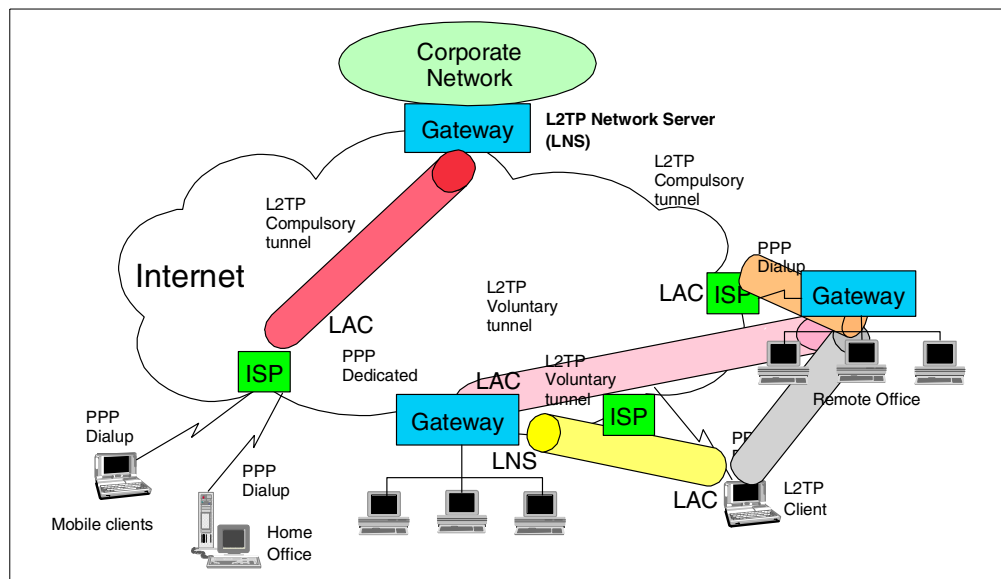


Figure 29. L2TP tunnel modes usage examples

2.4.3 VPN tunnels comparison

There are three main VPN tunnel types that can be built over the Internet. Assuming that the L2TP tunnels are protected by IPSec so that all compared tunnels have the same level of security, the following points summarize the position of the VPN tunnels:

- L2TP compulsory tunnel protected by IPSec:
 - Best suited for home office workers and branch office gateways where the services of the same ISP that provides LAC support can be used.
 - No global IP address assigned to the remote client reducing the need for firewalls or extra filters at the remote client.
 - Does not require L2TP-capable clients.
- L2TP voluntary tunnel protected by IPSec:
 - Best suited for mobile or travelling workers that need to access the Internet through different ISPs, where the LAC support at the ISP cannot be guaranteed.
 - Global and private corporate IP addresses are assigned to the client allowing direct access to the Internet.
- *Native* IPsec tunnels:
 - Best suited for remote sites where the network gateway is connected to the Internet through dedicated links and fixed IP addresses.
 - Create a secure tunnel providing authentication, integrity, encryption, and dynamic key generation even if L2TP support is not available.

2.5 L2TP IP address management

As discussed in 2.3.4, “Address allocation” on page 39, the traditional dial-up network service on the Internet is for registered (also known as globally routable) IP addresses only. L2TP enables the assignment of private IP addresses over the Internet. Figure 30 on page 46 provides an overview of IP address assignment in L2TP tunnels over the Internet.

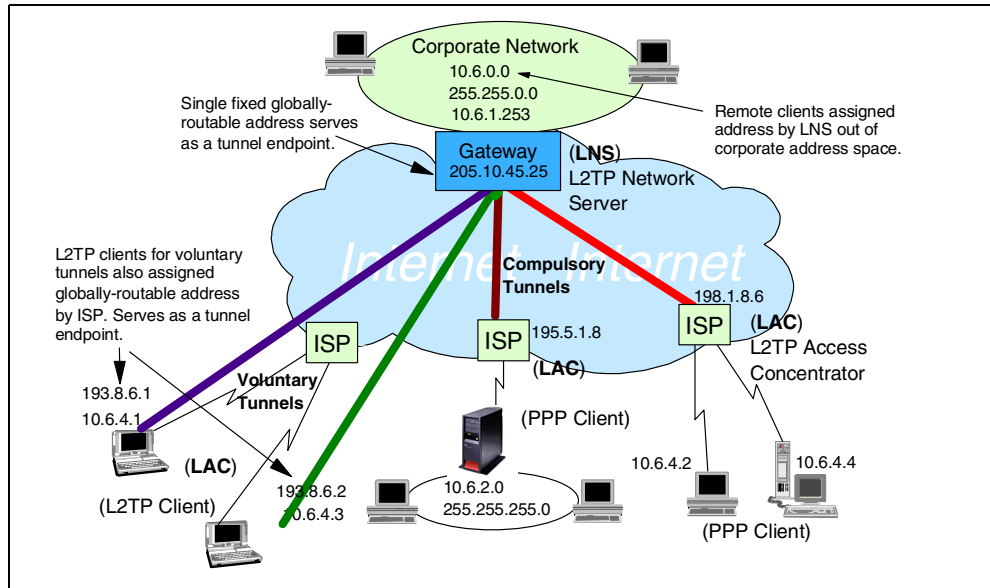


Figure 30. L2TP IP address management

The LNS always needs a globally routable IP address assigned to it on the public interface, whether a voluntary or a compulsory tunnel is used. This address is a fixed address.

In a compulsory tunnel, the remote dial-in client gets only an IP address of the corporate network assigned. This may be a registered IP address of the corporate network or a private IP address (for example, 10.21.1.1). The IP address is assigned by the LNS gateway on the corporate office. The AS/400 system at the branch office is assigned a private IP address (from the corporate network) that cannot be reached from the Internet. In this case, there is little need for a firewall in the branch office. The employees at the branch office can access Internet services like other users in the corporate network through the corporate firewall.

In a voluntary tunnel, the remote client is also the LAC. It gets a globally routable IP address assigned by the ISP and a corporate network IP address assigned by the LNS. The globally routable IP address is the L2TP tunnel endpoint on the client side. The corporate network address is the virtual PPP endpoint address. Both IP addresses may be assigned dynamically, where the globally routable address is assigned by the ISP and the virtual PPP endpoint address is assigned by the LNS gateway on the corporate side.

Using the globally routable IP address, users can access Internet services directly. However, they are exposed to attack since the client is assigned an IP address that can be reached from the Internet. When the remote client (LAC) is an AS/400 system, IP packet filtering rules must be configured to prevent access from outsiders and allow only the L2TP tunnel traffic.

2.6 L2TP security with IPSec

Although L2TP provides cost-effective remote access, it does not provide cryptographically robust security features. For virtual dial-up services, L2TP provides authentication of the tunnel endpoints. However, L2TP does not define tunnel protection mechanisms. Consider these examples:

- Authentication is provided only for the tunnel endpoints but not for each individual packet that flows inside the tunnel. This can expose the tunnel to man-in-the-middle attacks.
- Without per-packet integrity, it is possible to mount denial-of-service attacks by generating bogus control messages that can terminate either the L2TP tunnel or the underlying PPP connection.
- L2TP itself provides no facility to encrypt user data traffic.
- While the payload of the PPP packet can be encrypted, the PPP protocol suite does not provide mechanisms for automatic key generation or automatic key refresh.

The L2TP specification proposes the use of IPSec protocols suite for protecting L2TP traffic over IP. The IPSec protocols Authentication Header (AH) or Encapsulation Security Payload (ESP) can be used to protect the L2TP tunnel. Figure 31 shows a possible scenario using IPSec with an L2TP voluntary tunnel.

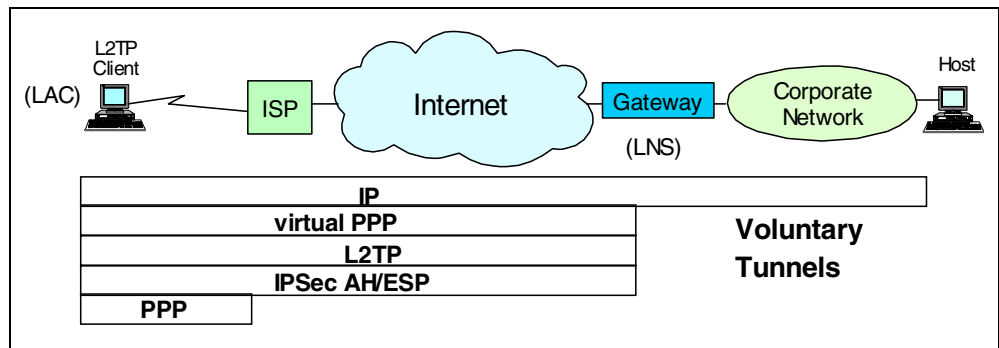


Figure 31. L2TP voluntary tunnel protected by IPSec

Figure 32 shows a possible scenario using IPSec with an L2TP compulsory tunnel.

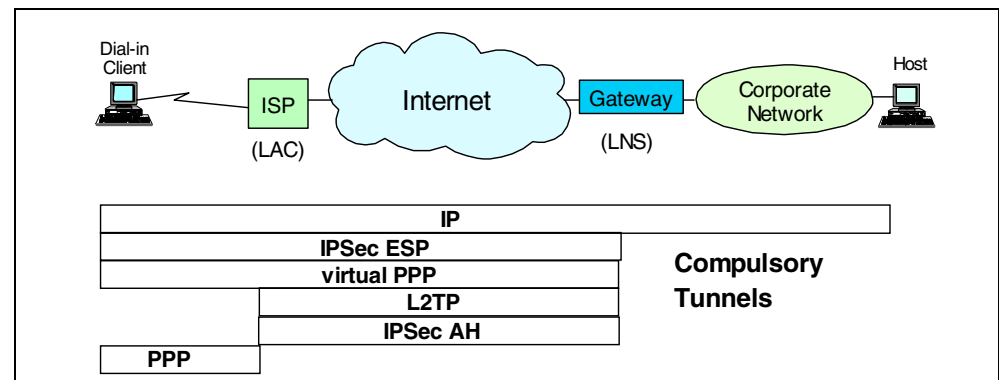


Figure 32. L2TP compulsory tunnel protected by IPSec

If the destination host in the corporate network is also IPSec enabled, the remote client can establish a second VPN connection to the destination host. This provides end-to-end security.

In summary, layer 2 tunnel protocols are an excellent way of providing cost-effective remote access. When used in conjunction with IPSec, they are an excellent technique for providing secure remote access. However, without the complementary use of IPSec, an L2TP tunnel alone does not furnish adequate security for business communications over the Internet.

2.7 L2TP characteristics summary

The following points summarize the main characteristics of L2TP discussed in this chapter:

- The remote client appears as locally connected to the corporate network.
 - The remote client is assigned a local IP address, which makes it appear directly connected to the corporate network, as in traditional dial-up networks.
 - The remote client is subject to the same access control policies to the corporate network resources as locally attached clients.
 - Remote client access can be restricted to the corporate network only.
 - Eliminates the need for opening firewalls for remote clients.
- L2TP tunnels PPP traffic.
 - The basic idea of L2TP is to extend the corporate network over an intervening network (the Internet, for example) to the remote client.
 - The user data traffic is encapsulated in a virtual PPP link and then tunneled into a L2TP tunnel.
 - L2TP supports two tunnel models: voluntary and compulsory.
- L2TP, in combination with IPSec, provides a secure connection over the Internet.
- L2TP should be considered the successor to Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F).
- L2TP is about to become an IETF standard, and it is already supported by all major vendors.

Part 2. VPN implementation on the AS/400 system

OS/400 VPN is a function of Operations Navigator, the graphical user interface (GUI) for the AS/400 system, that allows you to create a secure end-to-end path between any combination of host and gateway.

OS/400 VPN implementation requires you to configure and apply filter rules that allow traffic to flow through the connection. AS/400 customers can take advantage of OS/400 VPN support in a variety of scenarios.

This part describes OS/400 V4R4 VPN implementation, provides an overview of IP filtering configuration on the AS/400 system, and includes sample configuration scenarios involving AS/400 networks.

Chapter 3. AS/400 VPN implementation

This chapter provides an overview of VPN implementation on the AS/400 system. The objective of this chapter is to provide a high level description of OS/400 VPN in V4R4 and to serve as an introduction to various topics. Other chapters in this redbook include specific scenarios and detailed configuration examples. For updates on AS/400 VPN information, log on to the Web site at:

<http://www.as400.ibm.com/vpn>

3.1 AS/400 VPN overview

In V4R3, IBM introduced VPN support on IBM Firewall for AS/400 (5769-FW1). For a description of the VPN implementation on the IBM Firewall for AS/400 product, refer to *IBM Firewall for AS/400: VPN and NAT Support*, SG24-5376.

In V4R4, IBM added VPN natively to OS/400 (5769-SS1). OS/400 VPN support is integrated in the operating system. It is based on the latest Internet Engineering Task Force (IETF) IPsec Drafts. The following list summarizes the main features of OS/400 VPN support in V4R4:

- IPsec protocols
 - Authentication Header (AH)
 - Encapsulated Security Payload (ESP)
 - Internet Key Exchange (IKE)
- Manual connections
 - SPI values and cryptographic keys are predefined and manually refreshed
 - Use manual connections when the VPN partner does not support IKE
 - Configuration not supported by the VPN configuration wizard
- Dynamic key connections
 - IKE, AH, and ESP protocols supported, according to the latest Request For Comments (RFC) specifications
 - Support IKE protocol for dynamic key generation and refresh
 - Pre-shared key authentication
 - Configuration supported by the VPN configuration wizard
- Dynamic IP connections
 - Special case of Dynamic Key connection
 - Remote VPN partner is randomly assigned an IP address by an Internet service provider (ISP)
 - Remote VPN partner initiates the connection
 - Configuration supported by the VPN configuration wizard
- Layer 2 Tunneling Protocol (L2TP) connections
 - Provides a virtual Point-to-Point Protocol (PPP) tunnel across a public network allowing a private corporate address space to be extended out to a remote client
 - Primarily used in remote access scenarios
 - AS/400 supports L2TP Network Server (LNS) and L2TP initiator functions

- Virtual Private Network Address Translation (VPN NAT)

The AS/400 version of NAT that can be used in conjunction with VPN (Conventional NAT and VPN are not compatible)

OS/400 VPN support has been certified by the International Computer Security Association (ICSA). Products that become ICSA certified have met a definable quantitative level of risk reduction against a known set of threats. The ICSA IPsec certification is primarily focused on testing compliance with the specifications, which also implies interoperability with other compliant solutions. For information about ICSA certification, see the Web site at: <http://www.icsa.net>

Refer to *AS/400 Performance Capabilities Reference V4R4* for AS/400 VPN performance test results, which can be electronically accessed on the Web at: <http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R4PDF/AS4PPCP1.PDF>

3.2 VPN software prerequisites

IBM makes the native VPN support available to AS/400 customers in V4R4 at no extra charge. The following software is required to configure OS/400 VPN:

- OS/400 V4R4 (5769-SS1)
- Digital Certificate Manager (DCM) (5769-SS1 option 34)
- Client Access Express for Windows (5769-XE1)
- IBM Cryptographic Access Provider (5769-AC2, or AC3)

Note: The IBM Cryptographic Access Provider products come in three versions:

- 5769-AC1 (40-bit encryption, exportable, *not* supported by VPN)
- 5769-AC2 (56-bit encryption, exportable)
- 5769-AC3 (128-bit encryption, available in U.S. and Canada)

Recent regulations allow U.S. software vendors to export 128-bit encryption products to banks, financial institutions, medical service providers, insurance companies, and subsidiaries of U.S. companies in 45 countries with the approval of the U.S. Department of Commerce. Check with the IBM U.S. Export Regulation Office for the latest information.

Note

OS/400 VPN support can dynamically determine the cryptographic capabilities of the system and only use currently supported algorithms. This means that if 5769-AC2 is installed, the highest security available is Data Encryption Standard (DES). If 5769-AC3 is installed, the highest security available is 3DES. The negotiations for the SAs will not negotiate "down", unless the policy allows it. If Highest Security, Lowest Performance is selected in the VPN configuration wizard for two AS/400 systems, one with 5769-AC2 and the other one with 5769-AC3 system, incompatible policies will result. The key and data policy transforms configured by the wizard must be modified for the negotiation to succeed.

3.3 AS/400 VPN components

AS/400 VPN support consists of the following components:

- VPN configuration GUI (part of Operations Navigator)
- VPN New Connection Wizard
- VPN server jobs
- VPN policy database
- IP packet filtering with ACTION = IPSEC
- Control Language (CL) commands
- Traces and logs for problem determination

The following sections briefly introduce each of these components.

3.3.1 VPN graphical user interface (GUI)

AS/400 Operations Navigator provides a powerful graphical user interface for Windows 95, 98, and NT PC clients to configure, manage, and administer your AS/400 system.

AS/400 VPN requires the Operations Navigator's Network component. This component provides the Virtual Private Networking GUI for you to configure and manage VPN connections. IP Packet Security GUI is also part of Operations Navigator. It is required to configure the IP filters needed for VPN connections.

The Point-to-Point Connection Profiles configuration GUI in Operations Navigator has been enhanced to include L2TP.

3.3.2 New Connection Wizard

The New Connection Wizard guides you through a simple step-by-step configuration process. You input minimum information about your VPN environment, and the Wizard takes over the complex configuration tasks. You can configure the following scenarios using dynamic key connections:

- Host to hosts
- Gateway to host
- Host to gateway
- Gateway to gateway

Dynamic IP Users refers to a VPN connection where the initiator is randomly assigned IP addresses (no fixed IP address). The wizard can configure the following Dynamic IP User connections:

- Gateway to Dynamic IP Users
- Host to Dynamic IP Users

To simplify the task of configuring VPN connections, you should always start by configuring with the wizard, customizing the individual objects later if needed.

The wizard does not support the configuration of Manual Connections and L2TP connections. You must use the VPN configuration GUI to configure those connection types.

3.3.3 CL commands

There are no "green screen" commands available for VPN configuration. The following OS/400 CL commands are related to VPN management and troubleshooting:

- `STRTCPSVR SERVER(*VPN)` to start the VPN server jobs
- `ENDTCPSVR SERVER(*VPN)` to end the VPN server jobs
- `TRCTCPAPP APP(*VPN)` used by service personnel to collect VPN trace information
- `TRCTCPAPP APP(*L2TP)` used by service personnel to collect L2TP trace information

3.3.4 VPN and L2TP server jobs

You must start the VPN server jobs before activating VPN connections. The VPN server jobs run in the QSYSWRK subsystem. These jobs include:

- **QTOKVPNIKE**: This is the Virtual Private Networking key manager job. The VPN key manager listens to UDP port 500 to perform the Internet Key Exchange (IKE) protocols.
- **QTOVMAN**: This is the VPN connection manager job. The related job log contains messages for every connection attempt that fails.

The L2TP jobs are:

- **QTPPPCTL**: PPP control job. Starts when a virtual line (L2TP, initiator, or terminator) is started.
- **QTPPPL2TP**: Layer Two Tunneling Protocol (L2TP) manager job. If you have problems setting up an L2TP tunnel, look for messages in this job log.
- **QTPPPL2SSN**: L2TP session jobs. These are pre-started jobs that, by default, run in QSYSWRK. You can specify another subsystem for these jobs in the virtual line, subsystem configuration.

3.3.5 VPN policy database

The VPN configuration and policy information is stored in the VPN policy database. The VPN policy database consists of the objects shown in Table 1 in QUSRSYS library.

Table 1. VPN policy database objects

Object	Type	Library	Attribute
QATOVDAAH	*FILE	QUSRSYS	PF
QATOVDCDEF	*FILE	QUSRSYS	PF
QATOVDNFLT	*FILE	QUSRSYS	PF
QATOVDNSEL	*FILE	QUSRSYS	PF
QATOVDNESP	*FILE	QUSRSYS	PF
QATOVDNIID	*FILE	QUSRSYS	PF
QATOVDNIPAD	*FILE	QUSRSYS	PF
QATOVDNLID	*FILE	QUSRSYS	PF
QATOVDNMCOL	*FILE	QUSRSYS	PF

Object	Type	Library	Attribute
QATOVDNATP	*FILE	QUSRSYS	PF
QATOVDN1	*FILE	QUSRSYS	PF
QATOVDPKEY	*FILE	QUSRSYS	PF
QATOVDRGRP	*FILE	QUSRSYS	PF
QATOVD1R1	*FILE	QUSRSYS	PF
QATOVD1SRVR	*FILE	QUSRSYS	PF
QATOVD1UCP	*FILE	QUSRSYS	PF
QATOVD1PRP	*FILE	QUSRSYS	PF
QATOVD1SP	*FILE	QUSRSYS	PF
QATOVD1TRN	*FILE	QUSRSYS	PF
QATOVD2LST	*FILE	QUSRSYS	PF
QATOVD2PRP	*FILE	QUSRSYS	PF
QATOVD2SP	*FILE	QUSRSYS	PF
QATOVD2TRN	*FILE	QUSRSYS	PF
QTOVDVPKEY	*VLDL	QUSRSYS	
QTOVDVSKEY	*VLDL	QUSRSYS	
QTOVDBJRN	*JRN	QUSRSYS	

You must include the object listed in Table 1 in your regular backup process.

3.3.6 IP packet security

IP packet security (IP filtering) is an integrated feature of OS/400 that was first introduced in V4R3. IP packet security allows you to implement basic IP packet filtering rules to control traffic flowing into and out of your AS/400 system. Initially, filters supported only DENY and PERMIT as Action type. In V4R4, the Action type IPSEC was added to support VPN-specific traffic.

Filter rules are an important part of the AS/400 VPN implementation. Filter rules are required to funnel traffic through the VPN connection, as well as allow IKE negotiations to occur. When you configure a VPN connection with the New Connection Wizard or the VPN configuration GUI, filters are not created. The configuration of filters is a separate task that you must perform using Operations Navigator's IP Packet Security GUI after configuring the VPN connection.

3.4 Layer Two Tunneling Protocol (L2TP) VPN support

L2TP tunnels can be configured independent of VPN. However, L2TP by itself does not afford the required level of security. We recommend that you always protect the L2TP tunnel with IPSec.

L2TP tunnels are configured through PPP profiles. If an L2TP tunnel is protected by IPSec, a VPN L2TP Connection configuration is also required on the AS/400 initiator.

L2TP support in OS/400 V4R4 includes the following features:

- L2TP Network Server (LNS)
 - In this role, the AS/400 system is the virtual PPP line terminator.
 - Voluntary and compulsory tunnel models are supported.
 - Dial-out or On-Demand functions are *not* supported.
- L2TP initiator
 - In this role, the AS/400 system is the virtual PPP line initiator in an L2TP voluntary tunnel and includes built-in L2TP Access Concentrator (LAC) functions.
 - The AS/400 system does not support the LAC functions required in an ISP environment.

To participate as a client in an L2TP compulsory tunnel, only the regular PPP support is required on the AS/400 system. In a compulsory tunnel, the LAC functions are provided by the ISP.

For more information on L2TP and its configuration on the AS/400 system, refer to:

- Chapter 2, “Introduction to Layer 2 Tunneling Protocol (L2TP)” on page 33
- Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263
- Chapter 8, “L2TP gateway-to-gateway voluntary tunnel” on page 323
- Chapter 9, “L2TP compulsory tunnel” on page 351
- Chapter 10, “Secure remote access for PC clients over the Internet” on page 419

3.5 Virtual Private Network Network Address Translation (VPN NAT)

Conventional Network Address Translation (NAT) allows you to hide internal network IP addresses from an untrusted network. You can use NAT to dynamically translate your internal network IP addresses to public IP addresses for communicating with the untrusted network. This is sometimes referred to as masquerading.

Another objective of NAT is to resolve address conflicts. It allows two networks with overlapping address spaces to be connected without necessarily having to change one set of addresses.

Unfortunately, conventional NAT cannot be used with IPSec protocols, because:

- In tunnel mode, ESP encrypts the inner IP addresses. Therefore, they cannot be translated by NAT.
- AH authenticates inner and outer IP addresses. Therefore, they cannot be translated.
- Even in transport mode, where ESP does not encrypt, nor authenticate the IP addresses, the Security Associations (SAs) are defined in terms of the destination IP address. Therefore, it cannot be changed.

The AS/400 system provides a unique solution, Virtual Private Network Network Address Translation (VPN NAT). VPN NAT works differently from conventional OS/400 NAT because it translates addresses before applying IKE and IPSec protocols. It compares to static NAT in OS/400 V4R3 in that the address translation is one-to-one, bi-directional, and fixed (in this case) for the length of the VPN connection.

VPN NAT should be used in the following situations:

- You do not trust the remote VPN partner, and you want to hide your internal network IP address.
- The IP addresses of the two VPN partner networks conflict.

For more information on VPN NAT, refer to Chapter 13, “VPN Network Address Translation (VPN NAT)” on page 551.

3.6 Planning considerations

Before you start implementing a Virtual Private Network using AS/400 VPN support, you need to do some planning and information gathering.

You should have a sound system and network security policy in place prior to implementing VPN. Also, your VPN policy should be part of your network security policy. If you are using VPN to protect the data flowing through the intervening network, you should determine the security level that you require at both ends, before the data enters the tunnel and after it is returned.

This section explores planning considerations. However, it is *not* a complete VPN planning guide.

3.6.1 Verify TCP/IP communications and routing

Before you start implementing VPNs, it is important to make sure that regular TCP/IP communications and routing is in place. VPN adds encryption and complexity, which make debugging of problems more difficult. Therefore, it is critical to verify end-to-end communications *before* configuring the VPN connections.

3.6.2 VPN through firewalls and routers

In many environments, IP packet filtering is implemented on firewalls and routers to protect private networks from intrusions from the Internet. In situations where AS/400 VPN connections traverse firewalls or routers that perform IP packet filtering as shown in Figure 33 on page 58, the firewall or router configuration must be changed to allow VPN traffic to flow through.

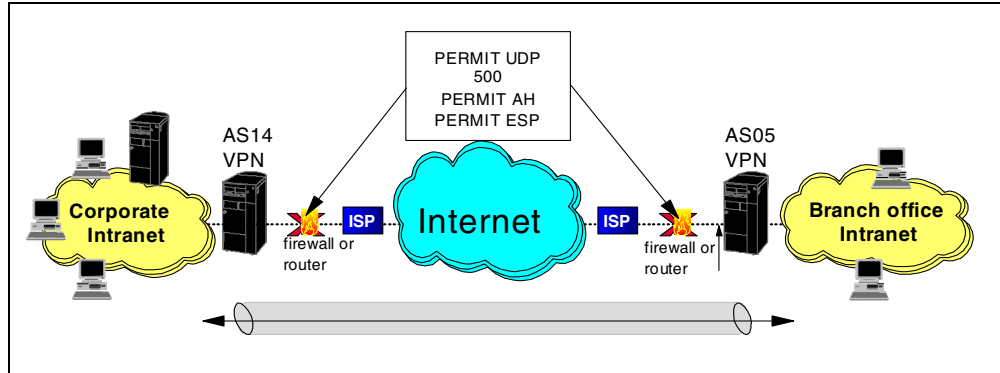


Figure 33. Allowing VPN traffic through firewalls

Specifically, the following configuration changes are required for the firewalls or routers:

- Enable IP forwarding
- Permit IKE (protocol UDP, port 500)
- Permit AH (protocol number 51) and ESP (protocol number 50), which are different protocols from TCP, UDP, or ICMP

Note

The firewall or router filter rules *must* support filtering of the relatively new AH and ESP protocols.

IBM Firewall for AS/400 (5769-FW1) from V4R3 onward is an example of a firewall whose filter rules allow you to permit AH and ESP protocols. Refer to Chapter 12, “Don’t forget a firewall: Protecting your VPN server” on page 515, for a description of the filter rules that are required on a firewall to allow a VPN tunnel to traverse it.

3.6.3 Interoperability

Most networks are built with equipment from multiple vendors and platforms. To implement secure multi-vendor networks based on IPsec standards, it is important to understand the characteristics of the VPN implementations to guarantee interoperability. The industry-standard IPsec protocols on which the OS/400 VPN implementation is based have been rapidly developing and evolving in the last couple of years. You cannot assume interoperability until these technologies become more mature.

The ICSA Web page shows all of the vendors that have been certified. The AS/400 VPN support should be able to interoperate with them. For ICSA vendor certification, go to the Web site at: <http://www.icsa.net>

3.6.3.1 IBM Firewall for AS/400 (5769-FW1)

In V4R3, IBM introduced VPN support on IBM Firewall for AS/400 (5769-FW1). Refer to *IBM Firewall for AS/400: VPN and NAT Support*, SG24-5376, for a description of the VPN implementation on the IBM Firewall for AS/400 product. IBM Firewall for AS/400 was one of the first IBM VPN implementations. Since

then, the IPSec standards have evolved, making it incompatible with newer implementations such as OS/400 VPN.

3.6.3.2 IKE authentication mechanism

The OS/400 V4R4 VPN implementation supports pre-shared keys as the key protection (IKE phase 1) authentication mechanism for IKE connections. In a future OS/400 release, authentication through digital certificates will be supported, but it is not supported in V4R4.

3.6.3.3 Keys and Security Parameters Index format

For dynamic connections, you must specify the pre-shared key in ASCII format, while other VPN implementations, such as AIX V4.3.2, require a hexadecimal format. For an example, refer to Chapter 17, “Host-to-host VPN: AS/400 to AIX server” on page 769.

For manual connections, the AS/400 inbound and outbound keys must be entered in hexadecimal format. The Security Parameter Index (SPI) values are also in hexadecimal format on the AS/400 system. Refer to Chapter 19, “Manual connection VPN: AS/400 to eNetwork Firewall” on page 845, for a configuration example.

3.6.3.4 Supported IPSec protocols and transforms

For interoperability, it is important that the VPN partners support compatible protocols and transforms.

Note

Triple DES (3DES-CBC or 3DES) is only available when 5769-AC3 IBM Cryptographic Access Provider for AS/400 is installed.

Table 2 summarizes the main characteristics of VPN implementations on IBM platforms.

Table 2. Protocols and transforms supported by IBM VPN implementations

Products/ platforms	AH Transforms	ESP Transforms (Encryption)	ESP Transforms (Authentication)	IKE Transforms (Encryption)	IKE Transforms (Authentication)	Diffie- Helman Groups
OS/400 V4R4	HMAC (MD5, SHA)	DES, 3DES, NULL	HMAC (MD5, SHA), None	DES, 3DES	MD5, SHA	1, 2
Firewall for AS/400	Keyed MD5	CDMF, DES	N/A	N/A	N/A	N/A
Firewall 3.3 NT	HMAC (MD5, SHA)	CDMF, DES, 3DES, NULL	HMAC (MD5, SHA), None	N/A	N/A	N/A
Firewall 3.3 AIX	Keyed MD5	CDMF, DES	N/A	N/A	N/A	N/A
Firewall 4.0 AIX	HMAC (MD5, SHA)	CDMF, DES, 3DES, NULL	HMAC (MD5, SHA), None	DES, 3DES	MD5, SHA	1, 2
CS/390 V2R7	Keyed MD5, HMAC (MD5, SHA)	CDMF, DES, 3DES, NULL	HMAC (MD5, SHA), None	N/A	N/A	N/A

Products/ platforms	AH Transforms	ESP Transforms (Encryption)	ESP Transforms (Authentication)	IKE Transforms (Encryption)	IKE Transforms (Authentication)	Diffie- Helman Groups
CS/390 V2R8	HMAC (MD5, SHA)	CDMF, DES, 3DES, NULL	HMAC (MD5, SHA), None	DES, 3DES	MD5, SHA	1, 2
AIX V4.3.2 and 4.3.3	Keyed MD5, HMAC (MD5, SHA)	CDMF, DES, 3DES, NULL	HMAC (MD5, SHA), None	DES, 3DES	MD5, SHA	1, 2
2210, 2212, 2216 routers	HMAC (MD5, SHA)	CDMF, DES, 3DES, NULL	HMAC (MD5, SHA), None	DES, 3DES	MD5, SHA	1, 2

RC4 support

The AS/400 VPN support has been enhanced after V4R4 general availability to include the ESP RC4 encryption protocol as an option for data policy (IKE phase 2). This enhancement is available through the following AS/400 PTFs (or superseding):

- MF23279 (5769999)
- SF58010 (5769SS1)
- Operations Navigator Service Pack SF59557

The fixes listed here allow you to configure RC4 128-bit fixed key. RC4 is only available for the Cryptographic Access Provider 5769-AC3 product (128-bit encryption). Using RC4 will result in better performance, but we recommend that you use it between AS/400 VPN servers due to potential interoperability problems.

3.6.3.5 U.S. versus export cryptographic support

IBM Cryptographic Access Provider 5769-AC3 (USA/Canada) supports 3DES encryption algorithm, while the strongest encryption algorithm supported by 5769-AC2 is DES. The encryption transforms configured by the VPN Configuration Wizard when you select Highest security, lowest performance are different depending on which product is installed. Use the information provided on Table 5 on page 64 to configure the connections to match the remote AS/400 VPN partner. Take into account the version of the IBM Cryptographic Access Provider product installed.

3.6.3.6 Replay protection

Replay protection for inbound datagrams is required by the IPSec standards. The AS/400 VPN implementation requires replay protection, and there is no parameter to disable it. At present, some VPN implementations from other vendors do not honor replay protection. If you want to disable replay protection on the AS/400 system, the last eight bytes of the connection name or connection group name must be NOREPLAY (all upper case), for example, myvpnNOREPLAY.

3.6.3.7 Terminology

VPN terminology may differ from platform to platform. Table 3 shows a list of AS/400 VPN terms and equivalent terms found in other platforms during our tests.

Table 3. AS/400 VPN terminology

AS/400 term	Equivalent terms found in other platforms
Key Policy (IKE phase 1)	
Select identity protection	Select main mode negotiation
Do not select identity protection	Select aggressive mode negotiation
Key Policy Diffie-Hellman Group	
Default 768-bit MODP	Group 1
Default 1024-bit MODP	Group 2
Data Policy (IKE phase 2) Diffie-Hellman Perfect Forward Secrecy Group	
Default 768-bit MODP	Group 1
Default 1024-bit MODP	Group 2

3.6.4 Basic planning

Use the prerequisite checklist (Table 4) to ensure that the software components required for VPN support are installed, the QRETSVRSEC system value is set to "1," and TCP/IP routing is configured and tested before attempting to implement a VPN connection.

Note

- The system value QRETSVRSEC determines whether security data needed by a server to authenticate a user or remote system can be retained on this AS/400 system. For VPN to work, QRETSVRSEC *must* be set to 1 (data is retained). To change this system value, enter the command:

```
CHGSYSVAL SYSVAL(QRETSVRSEC) VALUE('1')
```

- If normal TCP/IP communications cannot be established between the required endpoints, VPN will not function. Because data encryption is likely to be used under VPN (which, by design, means line traces cannot be fully interpreted), problem determination can be particularly difficult if routes have not been established correctly beforehand.

All the answers in the prerequisite checklist (Table 4) must be yes before proceeding with the VPN connection implementation.

Table 4. Prerequisite checklist planning worksheet

Prerequisite checklist	Answers (Yes/No)
Is OS/400 V4R4 (5769-SS1) or later installed?	
Is the Digital Certificate Manager option (5769-SS1 Opt. 34) installed?	

Prerequisite checklist	Answers (Yes/No)
Is Cryptographic Access Provider (5769-AC2 or 5769-AC3) installed?	
Is AS/400 Client Access Express (5769-XE1) installed?	
Is AS/400 Operations Navigator installed?	
Is the Network component of Operations Navigator installed?	
Is TCP/IP Connectivity Utilities for AS/400 (5769-TC1) installed?	
Is the retain server security data (QRETSVRSEC) system value set to 1?	
Is TCP/IP configured in the AS/400 system (including IP interfaces, routes, local host name, and local domain name)?	
Is normal TCP/IP communication successfully established between the required endpoints?	
If the VPN tunnel traverses firewalls or routers that implement IP packet filtering, do the firewall or router filter rules support AH and ESP protocols?	
Are the firewalls or routers configured to permit IKE (UDP port 500), AH, and ESP protocols?	
Are the firewalls configured to enable IP forwarding?	

3.6.5 Selecting the VPN connection type

There are many factors that affect the choice of VPN connection type. The flow chart in Figure 34 on page 63 helps you to decide what is the appropriate type of VPN connection for each scenario.

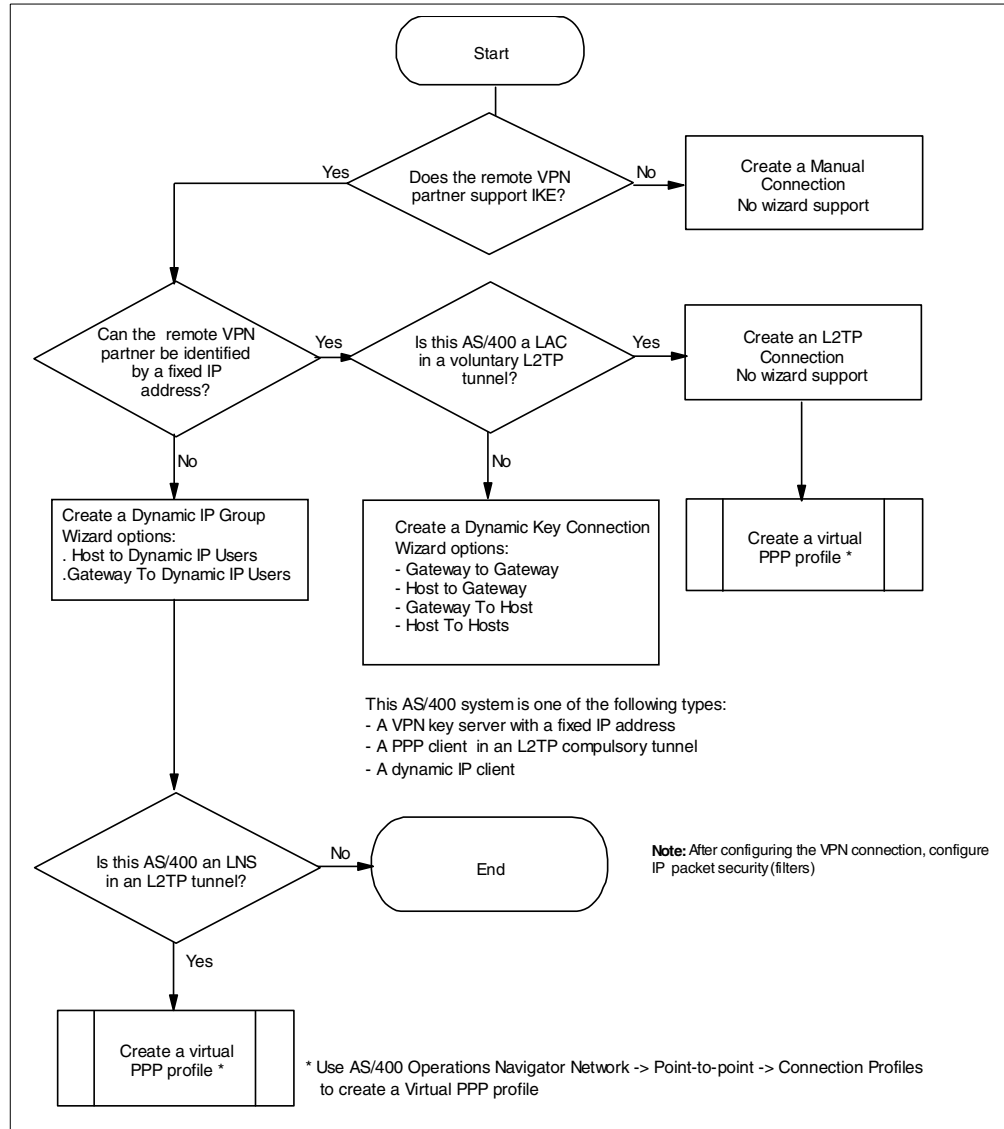


Figure 34. Selecting the VPN connection type

3.6.6 New Connection Wizard planning

The New Connection Wizard simplifies the VPN configuration process. It can be used to configure Dynamic Key Connections or Dynamic IP Connections. Use the wizard key policy window to specify the type of key policy (IKE phase 1) that you want it to configure. Use the wizard Data Policy window to specify the type of data policy (IKE phase 2) that you want it to configure. The wizard presents you with the following options:

- Highest security, lowest performance
- Balance security and performance
- Minimum security, highest performance

Table 5 and Table 6 on page 64 show the protocols and transforms configured by the wizard for each option.

Table 5. VPN Configuration Wizard - Key protection (IKE phase 1) transforms

Field	Value
Key Protection Transform for Minimum Security, Highest Performance (HP)	
Hash Algorithm	MD5
Encryption Algorithm	DES-CBC
Diffie-Hellman Group	Group 1 = Default 768-bit MODP
Key Protection Transform for Balanced Security and Performance (BS)	
Hash Algorithm	MD5
Encryption Algorithm	DES-CBC
Diffie-Hellman Group	Group 1 = Default 768-bit MODP
Key Protection Transform for Highest Security, Lowest Performance (HS)	
Hash Algorithm	SHA
Encryption Algorithm	5769-AC3: 3DES-CBC (See Note) 5769-AC2: DES-CBC
Diffie-Hellman Group	Group 1 = Default 768-bit MODP

Table 6. VPN Configuration Wizard - Data protection (IKE phase 2) transforms

Field	Value
Data Protection Transform for Minimum Security, Highest Performance (HP)	
Protocol	AH
Authentication Algorithm	HMAC-MD5
Encryption Algorithm	Not applicable
Data Protection Transform for Balanced Security and Performance (BS)	
Protocol	ESP
Authentication Algorithm	HMAC-MD5
Encryption Algorithm	DES-CBC
Data Protection Transform for Highest Security, Lowest Performance (HS)	
Protocol	ESP
Authentication Algorithm	HMAC-SHA
Encryption Algorithm	5769-AC3: 3DES-CBC (See Note) 5769-AC2: DES-CBC

Note: Selecting the wizard Highest Security, Lowest Performance options on an AS/400 system with 5769-AC2 installed generates key and data policies that are incompatible with the same selection on an AS/400 system with 5769-AC3 installed. The transforms can be changed manually.

The New Connection Wizard uses default values for other VPN configuration parameters. The Virtual Private Networking default values can be changed as

explained in 3.7.6, “Changing the Virtual Private Networking GUI default values” on page 76. Table 7 shows the Virtual Private Networking default values shipped by IBM and used by the wizard if you don’t change them.

Table 7. Virtual Private Networking default values used by the New Connection Wizard

Parameter	Default value
Identity protection (ISAKMP main mode) - Initiator - Responder	Not selected Do not allow identity protection
Diffie-Hellman Perfect Forward Secrecy (PFS) when protecting data	Not selected
Key Management (Key Policy, IKE phase 1)	
- Maximum key lifetime	60 minutes (See Note)
- Maximum size limit	No size limit
Key Expiration (Data Policy, IKE phase 2)	
- Expire after	1440 minutes (See Note)
- Expire at size limit	No size limit
Connection lifetime	Never expires

Note

At the time this redbook was written, the default values of Key lifetime for the IKE phase 1 and Expire after for IKE phase 2 were as shown in Table 7. However, the correct settings should be inverted. Key lifetime for IKE phase 1 should be longer than the Expire after value for IKE phase 2. We recommend that you change the default values to 1440 minutes for *Maximum key lifetime* and 60 minutes for *Expire after*. The default values will be corrected by a later Service Pack of Operations Navigator.

Finally, develop a plan for implementing the VPN connection that includes information such as the type of identifier that the local and remote VPN servers will use, identifier values (IP address, user@domain, host name, subnet, etc.), and pre-shared keys. The implementation chapters of this redbook include VPN configuration planning worksheets that you can use to gather configuration information.

3.6.7 Key policy (IKE phase 1) and data policy (IKE phase 2) lifetime and size limits

The discussion in this section applies to both key policy (IKE phase 1) and data policy (IKE phase 2) key life values.

As a responder, the AS/400 IKE server implementation negotiates key life successfully, as long as the same attributes are proposed and in policy. For example, if time is proposed but not size, then to match, an AS/400 policy must be configured that defines a time, but no size (*No size limit*). If time and size are proposed, then to match, an AS/400 policy must be configured that defines both time and size.

The following examples show how the AS/400 IKE implementation handles various proposed key lifetime and size limits:

- If 30 minutes and 100,000 kilobytes (KB) are proposed:
 - If the AS/400 policy defines 30 minutes with no size (*No size limit*), there will not be a match.
 - If the AS/400 policy defines 15 minutes and 50,000 KB, there will be a match, and the SA (Security Association) will be deleted (the keys will be re-negotiated) after 15 minutes or 50,000 KB. In other words, the keys will be refreshed after 15 minutes or 50,000 bytes.
 - If the AS/400 policy defines 45 minutes and 1,500,000 KB, there will be a match. However, the AS/400 system stops using the SA after 30 minutes or 100,000 KB, and the keys are re-negotiated. In summary, the keys will be refreshed every 30 minutes or 100,000 KB.
 - If the AS/400 policy defines 15 minutes and 150,000 KB, there will be a match. However, the AS/400 system deletes the SA after 15 minutes or stops using the SA after 100,000 bytes and the keys are re-negotiated. In summary, the keys will be refreshed every 15 minutes or 150,000 KB (whichever comes first).
- If 30 minutes and no size are proposed:
 - If the AS/400 policy defines 15 minutes and *no size limit*, there will be a match, and the keys will be re-negotiated after 15 minutes.
 - If the AS/400 policy defines 45 minutes and *no size limit*, there will be a match, and the keys will be re-negotiated after 30 minutes.
 - If the AS/400 policy defines 30 minutes and 50,000 KB, there will be no match.
- If 100,000 KB and no lifetime are proposed:

There will never be a match since the AS/400 implementation requires a lifetime value to be defined. This is to prevent the situation where keys may never be refreshed because the maximum size is never reached.

These examples show that the AS/400 IKE server always matches a key life proposal as long as the same attributes (time and size) are proposed and configured locally. When different times or sizes are proposed and locally configured, the smallest value wins.

The minimum key lifetime value in the AS/400 implementation for phase 1 is 15 minutes, and it is 5 minute for phase 2. As a responder, the AS/400 system always uses the lower (lesser) times. However, it must be greater than the minimum of 15 minutes or 5 minutes. For example, if a remote system proposes a key lifetime for phase 2 of 4 minutes, it will not be accepted.

3.6.8 IP packet security planning

To complete the VPN configuration, you need to configure IP packet security (filtering). Consider the existing network connections to understand what impact introducing the new filter rules required for VPN connections will have. If a filter file is being used on the same physical interface as the one to which VPN filter rules apply, you must add the new filter rules to the existing file.

For dynamic connections, three IP filter rules must be defined (Figure 35):

- Two IP packet filter rules to allow IKE traffic to flow between the key servers
- One IPSEC filter rule to define local and remote addresses and services that are allowed to use the VPN tunnel

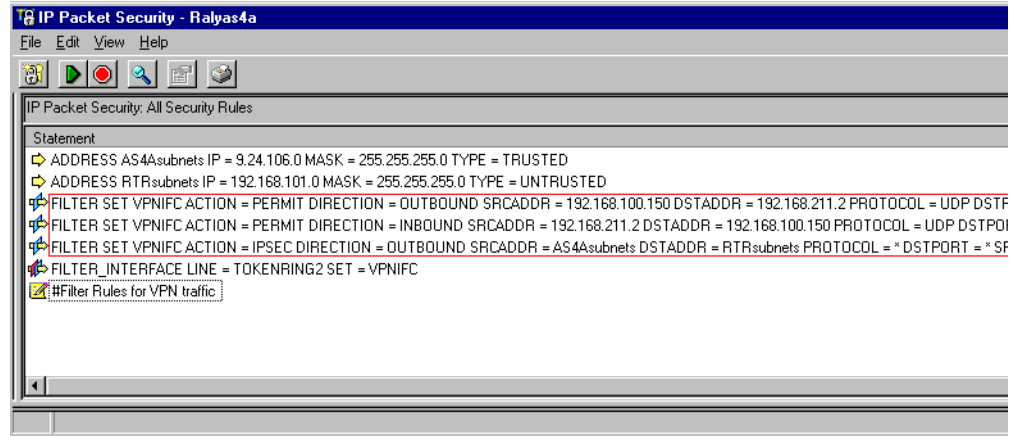


Figure 35. Example of dynamic key connection IP filter rules

Only the IPSEC filter rule is required for manual connections.

Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for details on IP packet security for VPN connections.

3.6.9 Miscellaneous planning considerations

There are other issues that may affect your VPN implementation. This section provides some examples.

3.6.9.1 Restricting services in the VPN connection

You may want to limit services on VPN connections. For example, you may want to allow only Telnet traffic through the VPN connection and block all other services such as FTP, SMTP, POP, and LPD. You can limit services using the policy filter rule (action IPSEC), or the definition of the connection. Refer to 4.3, “Refining the traffic for active connections: Connection granularity” on page 129, for details on how to limit the traffic allowed in a VPN connection.

3.6.9.2 Restricting dynamic key connection initiation

You can specify that only one of the VPN partners is allowed to start the connection in the Initiation section of the dynamic key connection group. By default, either system can initiate the connection.

3.6.9.3 Automatically starting a VPN connection

For the dynamic key connections and manual connections where the AS/400 system is the initiator, the VPN connection can start automatically. You can specify automatic starting of the VPN connection by selecting the **Start when TCP/IP is started** parameter of the dynamic key group and manual connection. Selecting this option simplifies the operation of VPN connections.

A VPN connection starts automatically when an interface becomes active (Start TCP/IP Interface (STRTCPIFC) command). Filter rules must be active on the line

and the VPN server must be started. Likewise, a VPN connection starts automatically, when the VPN server jobs start (STRTCPSVR SERVER(*VPN)). Filter rules must be active on the line and the interface must be started.

3.6.9.4 Automatically ending a VPN connection

You can automatically end a VPN connection by defining a value for the connection lifetime. By default, VPN connections never expire.

3.6.9.5 VPN PC clients

The PC Windows client in a remote access VPN must support IPSec, and, optionally, L2TP. Currently, there are VPN Windows clients on the market that support IPSec protocols, such as SafeNet/Soft-PK by IRE. Other Windows clients support L2TP in combination with IPSec, such as WinVPN by Wind River Systems. You need to plan the client product that you will use if secure tunnels between your AS/400 system and remote PC clients are required in your network. Refer to Chapter 10, "Secure remote access for PC clients over the Internet" on page 419, and Chapter 11, "Secure LAN access for PC clients in the intranet" on page 467, for more information about VPN PC clients.

3.6.9.6 Virtual Private Network Address Translation

If you do not trust your remote VPN partner, or there are conflicts between the two VPN partner networks, you need to implement VPN NAT. Refer to Chapter 13, "VPN Network Address Translation (VPN NAT)" on page 551, for a detailed description of VPN NAT implementation on the AS/400 system.

3.7 VPN configuration overview

VPN is configured using the Virtual Private Networking configuration GUI provided in V4R4 by Operations Navigator, part of Client Access/400 Express for Windows. For dynamic connections, a New Connection Wizard is provided. Use the wizard whenever possible to simplify the configuration process. If needed, use the VPN configuration GUI to customize the objects created by the wizard.

The wizard does not support manual and L2TP connections. You must configure these connection types using the VPN configuration GUI. In addition, for L2TP connections, you must configure a Virtual PPP profile.

All VPN connections require you to configure IP filter rules after creating the connection.

3.7.1 VPN configuration GUI: AS/400 Operations Navigator

AS/400 Operation Navigator's Network component provides the IP packet security and Virtual Private Networking GUIs, which are needed for VPN configuration. In turn, the Virtual Private Networking GUI provides the New Connection Wizard, which simplifies the process of creating VPN connections for dynamic key connections and dynamic IP groups.

The AS/400 Operations Navigator Network component is also used to create virtual PPP connections, which are required for L2TP connections.

3.7.1.1 Starting the AS/400 Operations Navigator Network component

To use the AS/400 Operations Navigator Network component, perform the following steps:

1. Start the AS/400 Operations Navigator for your AS/400 system.
2. Sign on when prompted.
3. Expand **Network**.

The window shown in Figure 36 is displayed.

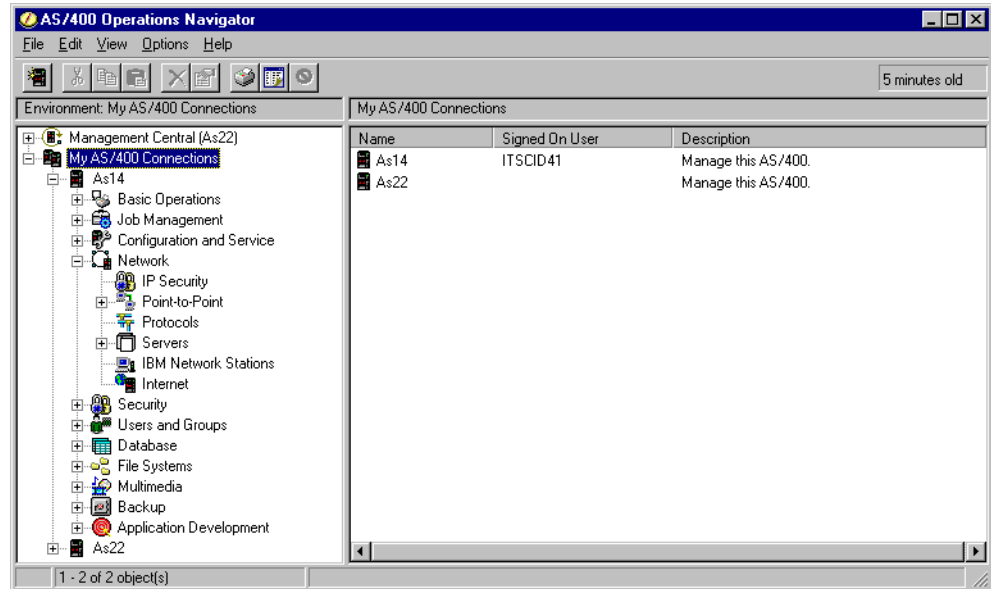


Figure 36. AS/400 Operations Navigator Network component

3.7.1.2 Starting the IP Packet Security GUI

To use the IP Packet Security GUI, perform the following steps:

1. At the AS/400 Operations Navigator Network component window (Figure 36), click **IP Security**.
2. Double-click **IP Packet Security** on the right panel of the window (Figure 37 on page 70).

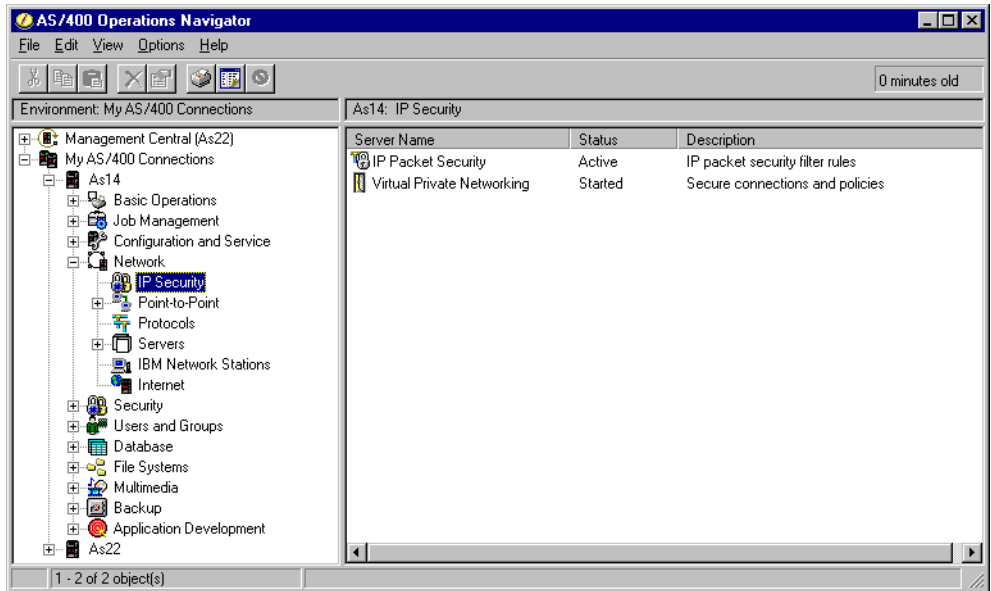


Figure 37. AS/400 Operations Navigator - IP Security

Figure 38 shows the IP Packet Security GUI.

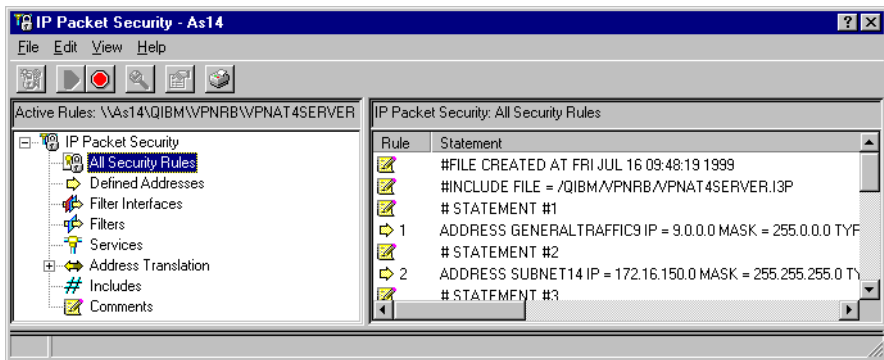


Figure 38. IP Packet Security GUI

3.7.1.3 Starting Virtual Private Networking GUI

To use the Virtual Private Networking GUI, perform the following steps:

1. At the AS/400 Operations Navigator Network component window (Figure 37), click **IP Security**.
2. Double-click **Virtual Private Networking** on the right panel of the window (Figure 37).

Figure 39 on page 71 shows the Virtual Private Networking GUI.

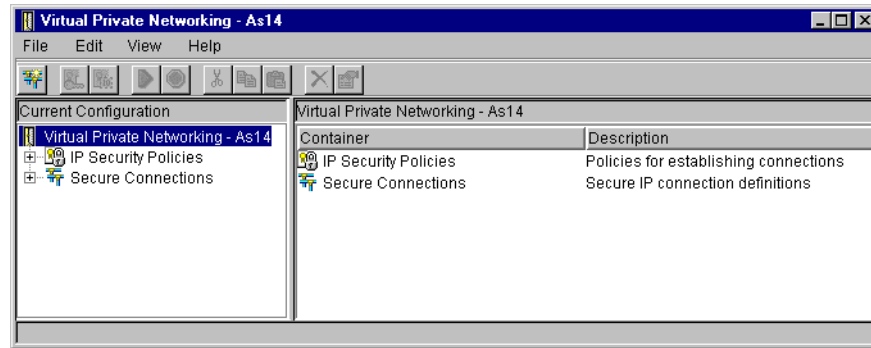


Figure 39. Virtual Private Networking GUI

3.7.2 Starting the New Connection Wizard

Use the New Connection Wizard to simplify the configuration of the VPN objects for dynamic key connections and dynamic IP connections.

Before you use the wizard, review and change the default values to fit your configuration requirements. Refer to 3.7.6, “Changing the Virtual Private Networking GUI default values” on page 76, for information on how to change the default security values.

To start the New Connection Wizard, perform the following steps:

1. At the Virtual Private Networking GUI window (Figure 39), click **File** from the menu bar.
2. Select **New Connection**.
3. Select, for example, **Gateway to Gateway**, from the pull-down menu. This starts the New Connection Wizard for a gateway-to-gateway connection (Figure 40 on page 72).

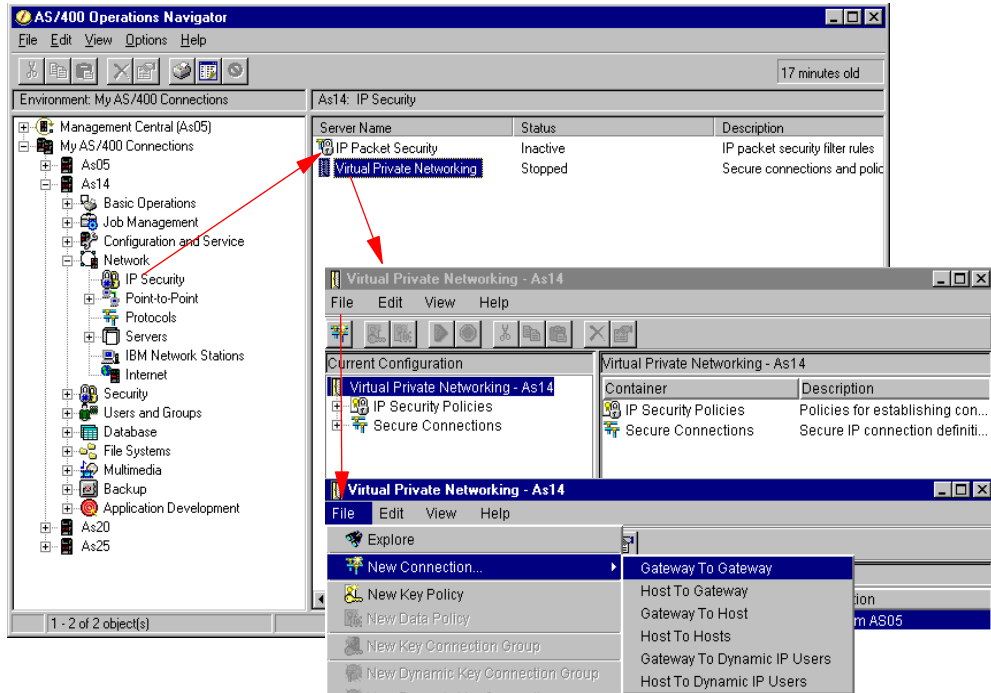


Figure 40. Starting the New Connection Wizard

Figure 41 shows the New Connection Wizard welcome window.

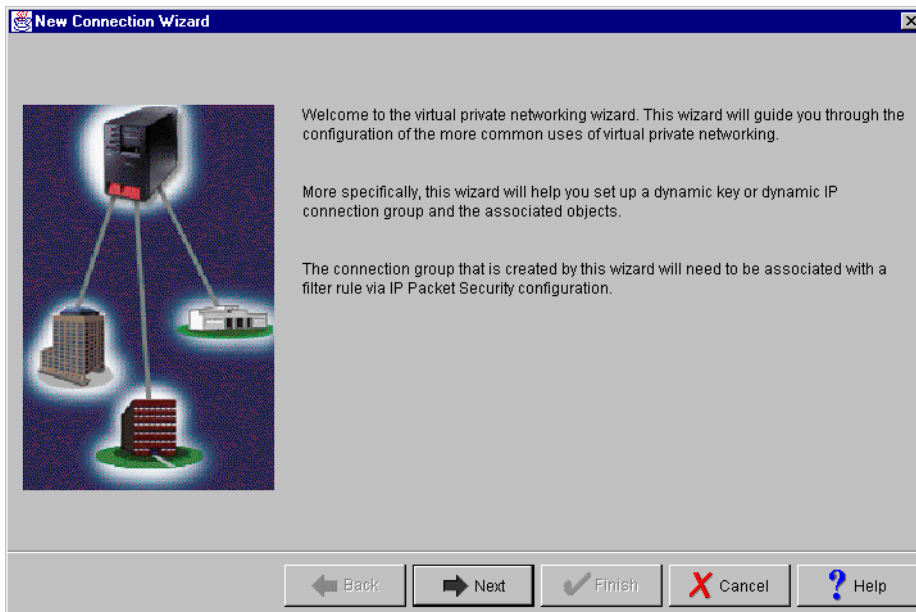


Figure 41. New Connection Wizard welcome window

Follow the wizard windows providing your input. The implementation chapters of this redbook include several examples that show you step-by-step how to configure a VPN connection using the wizard.

The last window presented by the New Connection Wizard (Figure 42 and Figure 43 on page 73) shows you the summary of the parameters as entered by you and

a list of VPN objects that will be created for final confirmation. If any of the parameters is incorrect, you can click **Back** to re-enter the correct information.

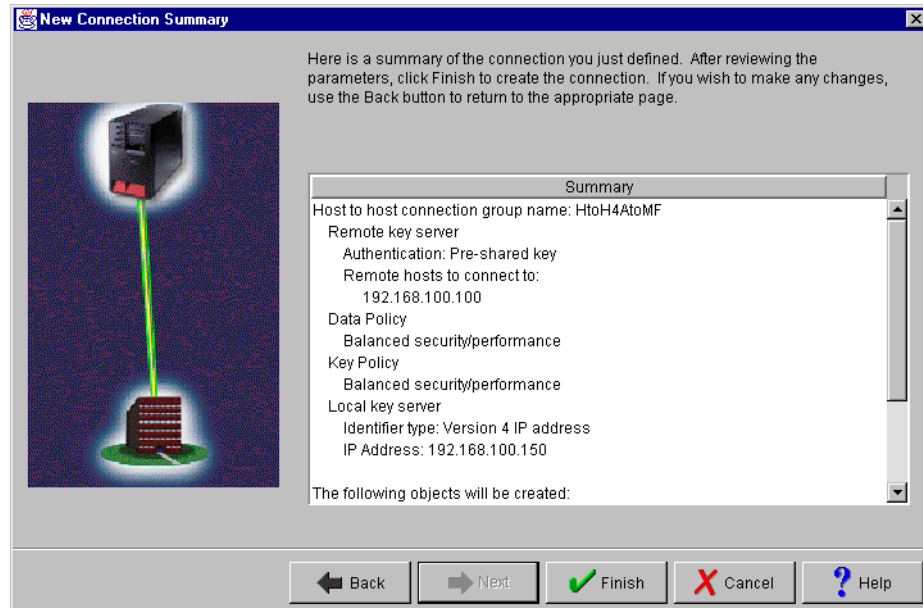


Figure 42. New Connection Wizard parameters summary

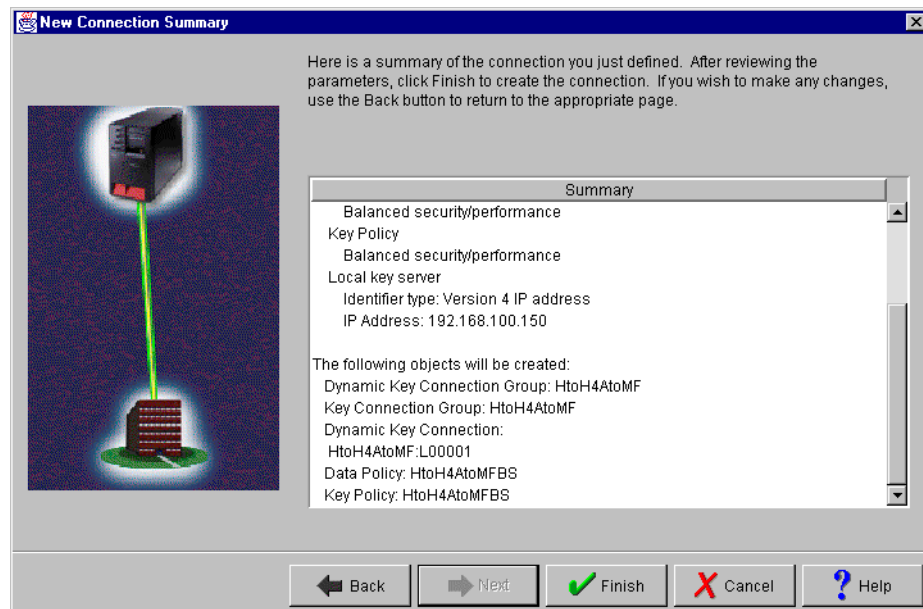


Figure 43. New Connection Wizard - Objects created by the wizard

After creating the VPN objects using the New Connection Wizard, you can customize them if needed in those cases where some of the values selected by the wizard are not appropriate. For information on the parameter values configured by the wizard, refer to 3.6.6, "New Connection Wizard planning" on page 63.

At this point, you must configure the corresponding IP filters using the IP Packet Security GUI.

3.7.3 VPN configuration objects created by the wizard

Figure 44 shows a summary of objects created by the New Connection Wizard for dynamic key connections.

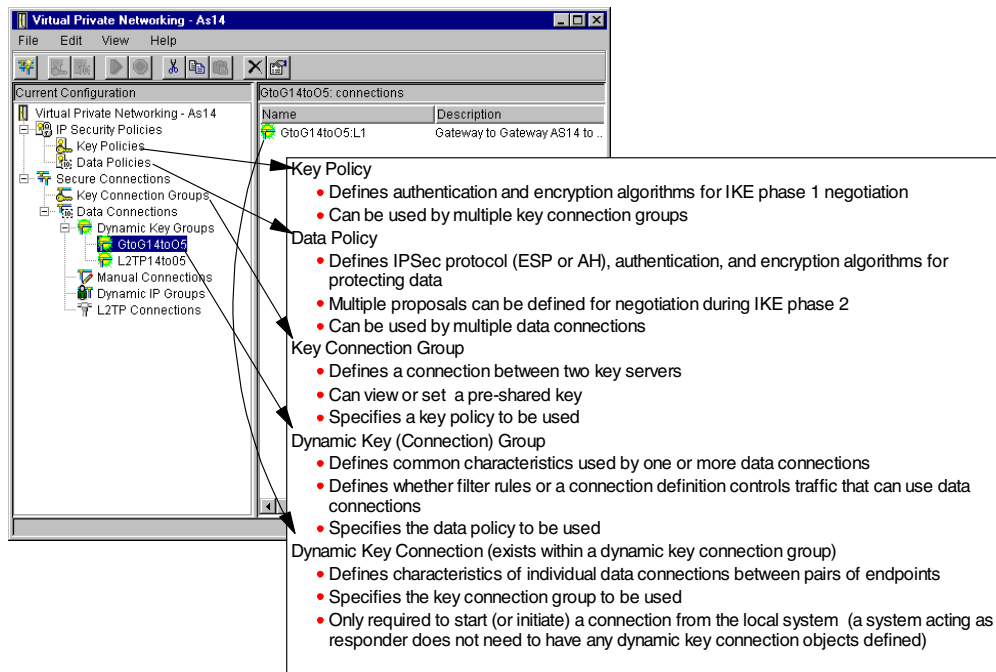


Figure 44. Summary of objects created by wizard - Dynamic key connections

The wizard names the key policy and the data policy objects with the name you provided for the connection group with one of the following suffixes appended to the name:

- **HS:** Highest security, lowest performance
- **BS:** Balance security and performance
- **HP:** Minimum security, highest performance

For example, if the connection group name you enter is GtoG14to05 and you select Balance security and performance, the key and data policy names are GtoG14to05BS.

The dynamic key connection, GtoG14to05:L1 shown in Figure 44, is only used on the AS/400 system that is the initiator of the connection. The wizard always creates a dynamic key connection with the connection group name that you provided followed by :L1, L2, etc. A system acting as a responder does not need to have any dynamic key connection objects defined.

3.7.4 VPN configuration object relationships

Figure 45 on page 75 summarizes the type of information held in each configuration object and their relationship with the dynamic key connections. The objects above the dotted line can be customized through the AS/400 Operations Navigator Virtual Private Networking GUI. The objects below the dotted line can be customized through the AS/400 Operations Navigator IP Packet Security GUI.

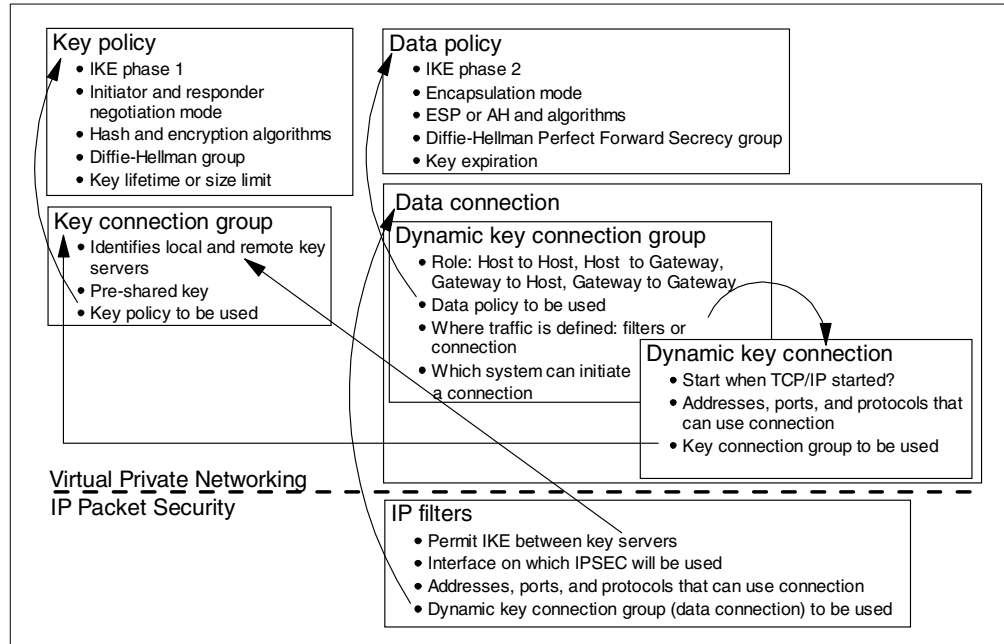


Figure 45. Object relationships for dynamic key connections

Note: The wizard does not configure IP packet security. You must configure IP filters after creating the VPN connection group by using IP Packet Security GUI in Operations Navigator.

3.7.5 Customizing the VPN configuration objects created by the wizard

Once the wizard creates the VPN configuration objects shown in Figure 45, you can customize the parameters configured by the wizard using the Virtual Private Networking GUI.

Figure 46 shows the Virtual Private Networking GUI fully expanded. You can edit the properties of the objects and change the parameters.

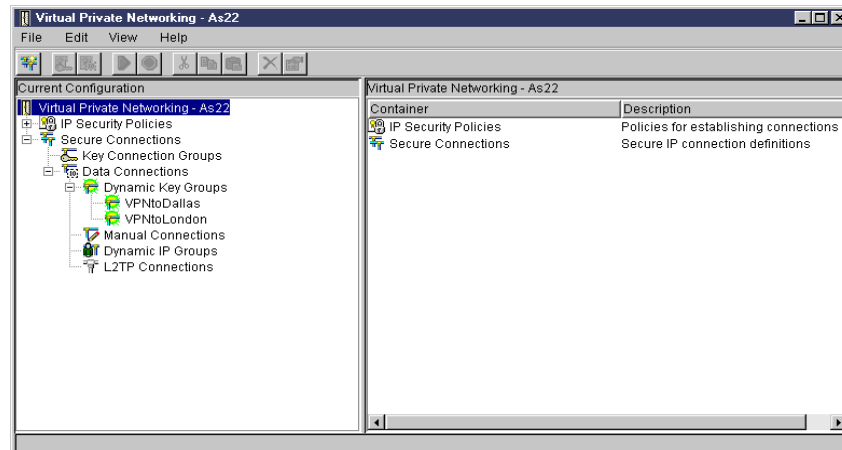


Figure 46. Virtual Private Networking GUI

You can also change the default security values used by the wizard. The following section explains how.

3.7.6 Changing the Virtual Private Networking GUI default values

You can change the default security values shipped with the OS/400 VPN support. The system uses these values to seed the panels that you use to create new policies and connections. The wizard also uses the default security values, except for the IP security level, which is specified by the user in the Key Policy and Data Policy windows.

Table 8 lists the Virtual Private Networking GUI default values that can be customized. For the default values shipped by IBM, see Table 7 on page 65.

Table 8. Virtual Private Networking GUI default values

Virtual Private Networking GUI default fields	Supported values
IP security level	<ul style="list-style-type: none"> – Highest security, lowest performance – Balance security and performance – Minimum security, highest performance
Use identity protection (ISAKMP main mode) when negotiating key policies	Select, or un-select
Use Diffie-Hellman perfect forward secrecy when protecting data	Select, or un-select
Key Management (Key Policy, IKE phase 1)	
Maximum key lifetime	A value between 15 and 525,600 in minutes
Maximum size limit	<ul style="list-style-type: none"> – No size limit – A value between 5 and 9,999,999 in KB
Key Expiration (Data Policy, IKE phase 2)	
Expire after	A value between 5 and 525,600 in minutes
Expire at size limit	<ul style="list-style-type: none"> – No size limit – A value between 10,240 and 9,999,999 in KB
Connection lifetime	<ul style="list-style-type: none"> – Never expires – A value between 1 and 525,600 in minutes

To change the default security values, perform the following steps:

1. At the Virtual Private Networking GUI menu bar, click **Edit->Defaults** (Figure 47 on page 77).

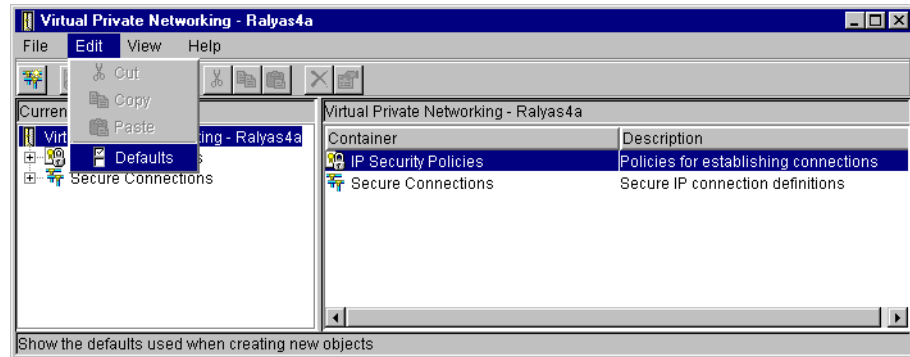


Figure 47. Starting Virtual Private Networking Defaults window

- At the Virtual Private Networking Defaults window, select the appropriate page to change the default security values (Figure 48).

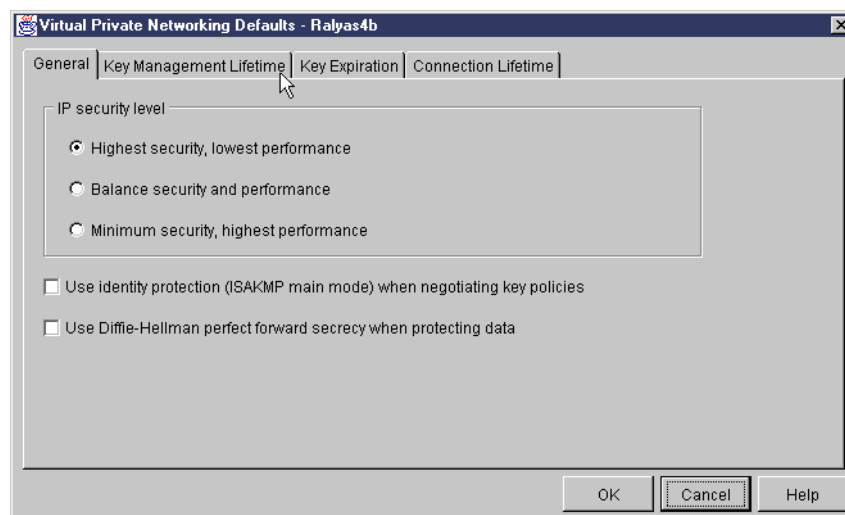


Figure 48. Virtual Private Networking Defaults window

- Click **OK**.

Note

At the time this rebook was written, the default values of the Key lifetime for the IKE phase 1 and Expire after parameters for IKE phase 2 were as shown in Table 7 on page 65. However, the correct settings should be inverted. Key lifetime for IKE phase 1 should be longer than the Expire after value for IKE phase 2. We recommend that you change the default values to 1440 minutes for *Maximum* key lifetime and 60 minutes for *Expire after*. The default values will be corrected by a later Service Pack of Operations Navigator.

3.7.7 Configuring manual connections

We encourage you to use the New Connection Wizard whenever possible to reduce the complexity of creating VPN connections. However, manual connections and L2TP connections cannot be configured with the New

Connection Wizard. You must use the Virtual Private Networking GUI to configure manual connections. Figure 49 shows how to create a new manual connection configuration with the Virtual Private Networking GUI.

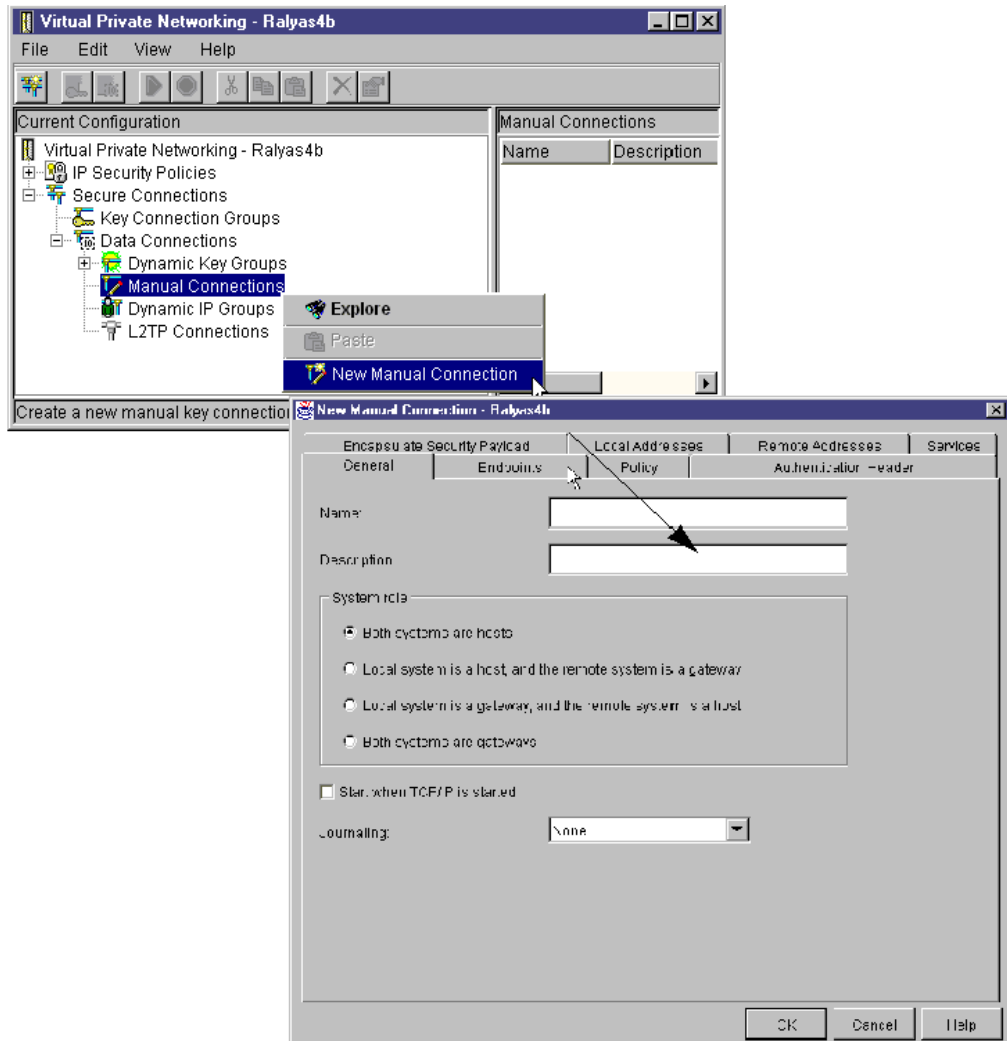


Figure 49. Configuring manual connections

Navigate sequentially through all the tabs to configure the manual connection. Chapter 19, “Manual connection VPN: AS/400 to eNetwork Firewall” on page 845, provides an example of a manual connection configuration.

3.7.8 Configuring L2TP connections

The L2TP tunnel is configured through a PPP profile. If the L2TP tunnel is protected by IPSec, a VPN configuration is also required. AS/400 Operations Navigator’s Network component provides the configuration GUIs for PPP profiles and VPN.

The following configuration is required if the L2TP tunnel is IPsec protected:

1. Configure a virtual PPP profile.
2. If the AS/400 system is the L2TP initiator, you must configure an L2TP connection using the Virtual Private Networking GUI. The wizard does not support this connection type.
3. If the AS/400 system is the terminator of the L2TP tunnel, configure a dynamic IP connection using either the New Connection Wizard or the Virtual Private Networking GUI.
4. Configure IP packet filtering.

Creating a virtual line (L2TP)

To configure the L2TP tunnel, you must configure a PPP connection profile with a Line connection type Virtual line. You can specify the role of the local AS/400 system in the Mode type parameter. A virtual point-to-point profile must be created regardless of whether the AS/400 system acts as an LNS or L2TP initiator.

To use the AS/400 Operations Navigator Network component to create a virtual point-to-point connection, follow these steps:

1. Start AS/400 Operations Navigator for your AS/400 system.
2. Sign on when prompted.
3. Expand **Network**.
4. Expand **Point-to-Point**.
5. Right-click **Connection Profiles**.
6. Select **New Profile** as shown in Figure 50.

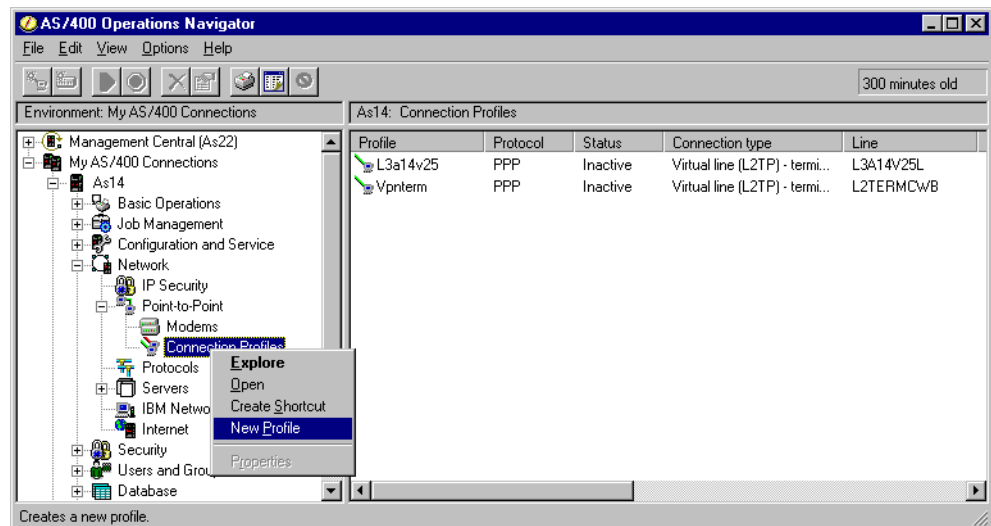


Figure 50. Creating a Point-to-point connection profile

Figure 51 on page 80 shows the New Point-to-Point Profile Properties window.

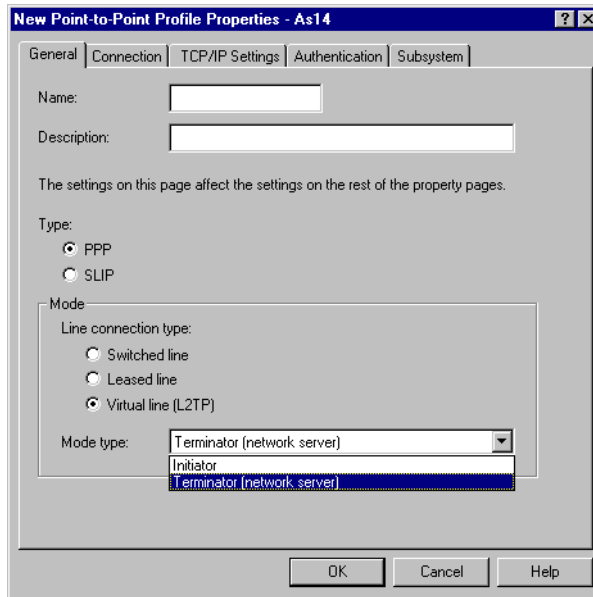


Figure 51. New Point-to-Point Profile Properties window

To configure L2TP, select:

- **PPP** for Type
- **Virtual line (L2TP)** for Line connection type
- **Initiator** or **Terminator** (depending on the AS/400 system role) for Mode type

For more information about configuring L2TP tunnels, refer to:

- Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263
- Chapter 8, “L2TP gateway-to-gateway voluntary tunnel” on page 323
- Chapter 9, “L2TP compulsory tunnel” on page 351

Creating an L2TP connection with the Virtual Private Networking GUI

To protect the L2TP tunnel with IPSec, you must configure the following VPN connection types:

- Host to Dynamic IP Users connection on the LNS AS/400 system. Use the wizard to configure this connection.
- L2TP connection on the L2TP initiator AS/400 system. The wizard does not support this connection type.

To create an L2TP connection with the Virtual Private Networking GUI, perform the following steps:

1. At the Virtual Private Networking GUI, expand **Secure Connections**.
2. Expand **Data Connections**.
3. Right-click **L2TP Connections**.
4. Select **New L2TP Connection** as shown in Figure 52 on page 81.

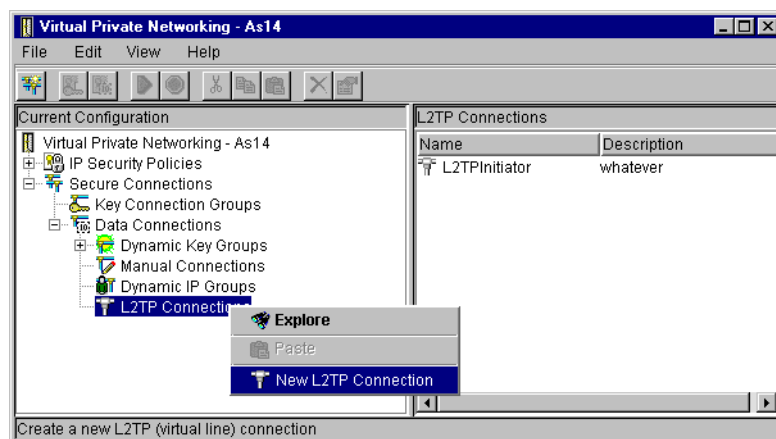


Figure 52. Creating a new L2TP connection

The New L2TP Connection window is displayed as shown in Figure 53.

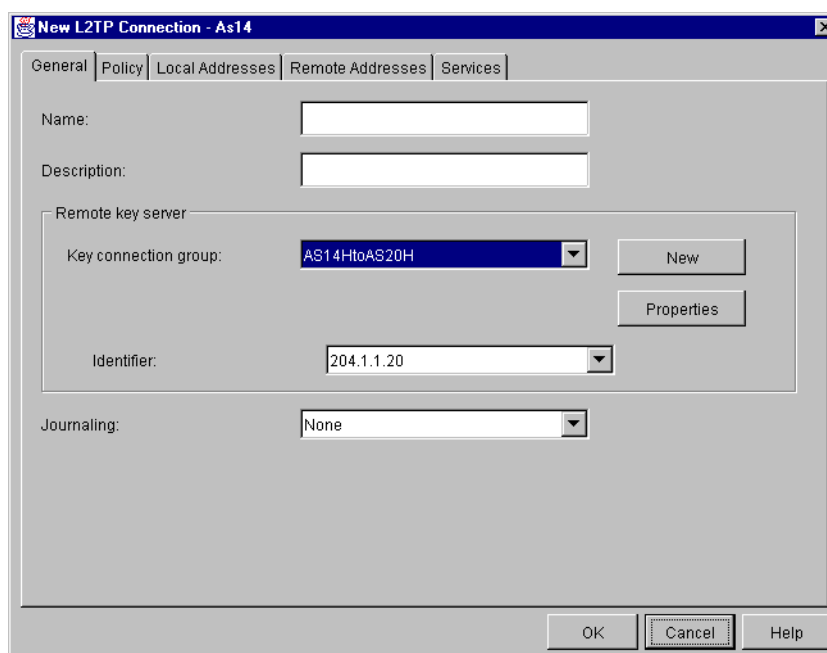


Figure 53. New L2TP Connection window

Navigate sequentially through all the tabs to configure the L2TP connection. For complete examples of how to configure L2TP connections, refer to:

- Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263
- Chapter 8, “L2TP gateway-to-gateway voluntary tunnel” on page 323
- Chapter 9, “L2TP compulsory tunnel” on page 351

IP filter rules for L2TP connections

Three IP filter rules are required for L2TP Connections protected by IPSec:

- Two IP filter rules to allow IKE negotiations (protocol UDP, port 500) between the key servers.
- One IPSEC filter rule with services to allow protocol UDP port 1701.

3.7.9 Deleting a VPN connection

To completely delete a VPN connection, you must delete all the objects associated with it. The number and class of objects vary depending on the VPN connection type. Figure 54 provides an overview of objects you need to delete for the various VPN connection types.

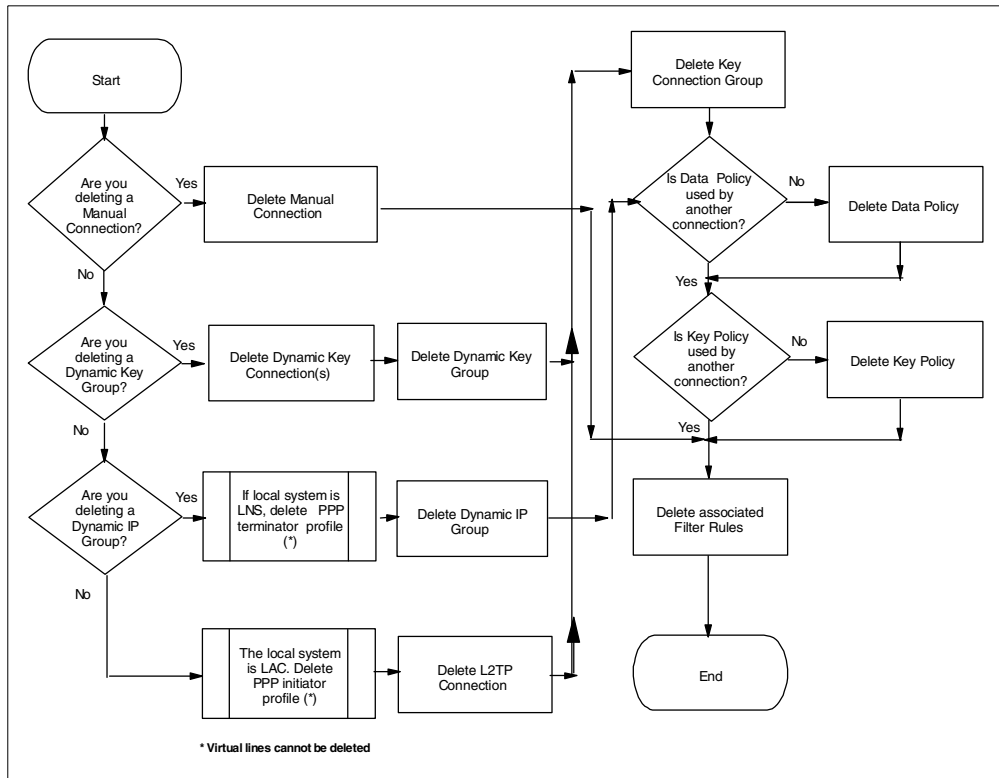


Figure 54. Deleting a VPN connection and related objects

To delete a VPN configuration object, right-click on it, and select **Delete** from the pull-down menu as shown in Figure 55.

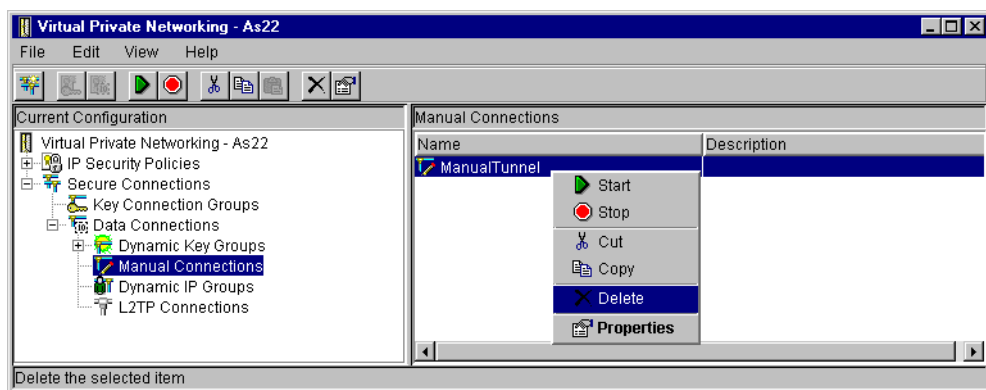


Figure 55. Deleting a manual connection

Figure 56 on page 83 shows how to delete a connection profile that configures an L2TP tunnel.

Tip

Deleting a PPP connection profile does not delete the virtual line associated with it. You cannot delete a virtual line.

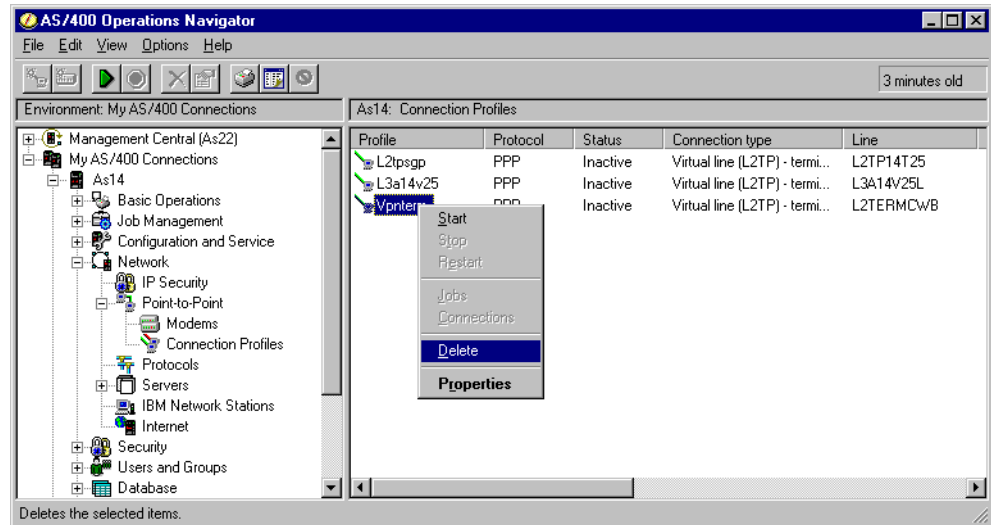


Figure 56. Deleting a PPP connection profile

3.7.9.1 Deleting the IP filter rules

If the filter entries you need to delete are in a filter file that is currently active, you must deactivate IP packet security first. Refer to 3.8.1.3, “Deactivating IP packet security” on page 86, for more information on how to deactivate IP packet security.

To delete IP filter rules, perform these steps:

1. Deactivate the filters.
2. At the IP Packet Security window menu bar, click **File->Open**.
3. Select the rules file you want to change, and click **Open**.
4. Click **Filters**.
5. Right-click the filter rule you want to delete, and select **Delete** from the pull-down menu as shown in Figure 57 on page 84.

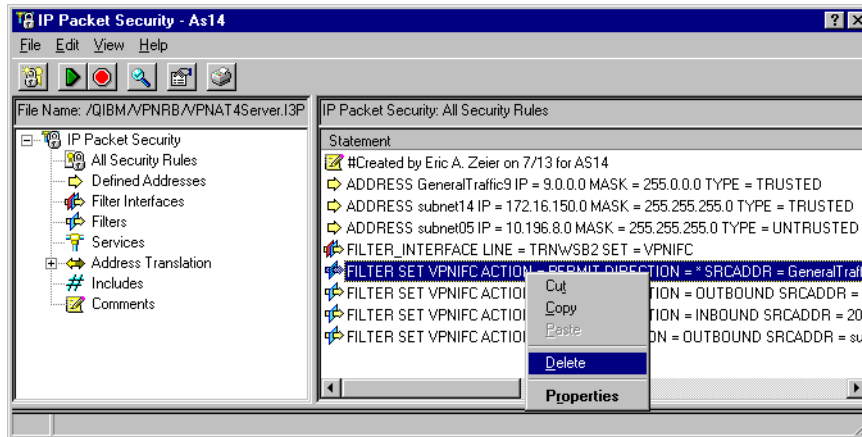


Figure 57. Deleting an IP filter rule

3.7.10 Configuring IP filters

Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for general information of IP filters and VPN connections.

3.8 VPN operations and management

Use Operations Navigator GUI to operate and manage your VPN environment. This section describes the main tasks involved with the operation and management of AS/400 VPNs.

3.8.1 IP packet security operations

The following sections describe tasks related to managing IP packet security. You must activate IP packet security before starting VPN connections.

3.8.1.1 Checking IP packet security status

Perform the following tasks to check the status of IP packet security:

1. Start Operations Navigator.
2. Sign on when prompted.
3. Expand **Network**.
4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking. The status of the IP Packet Security server should be *Active* before attempting to start the VPN connections.

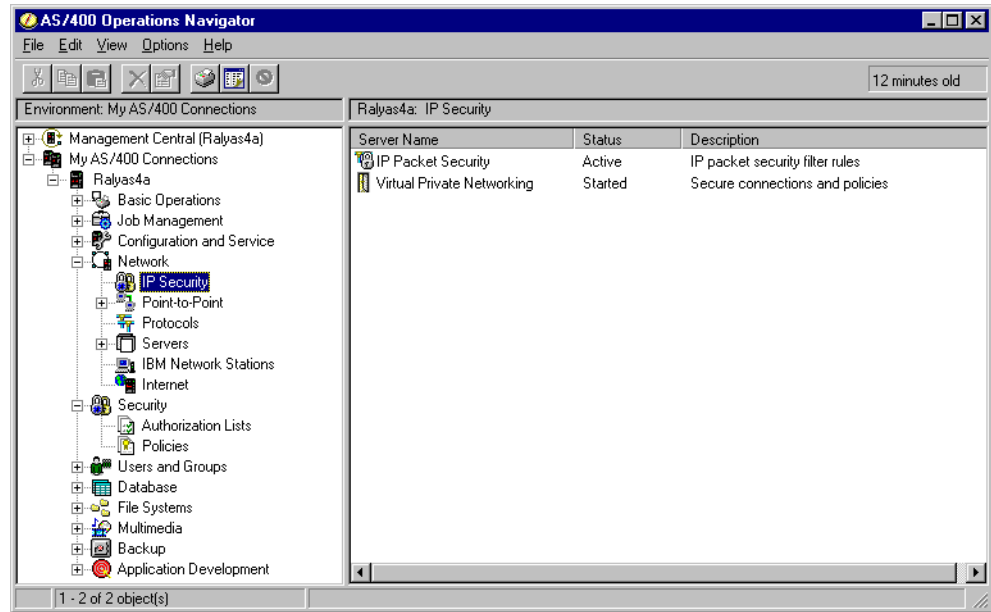


Figure 58. IP Security servers status

3.8.1.2 Activating IP packet security

Perform the following steps to activate IP packet security:

1. At the IP Packet Security GUI menu bar, click **File->Open**.
2. At the Open Rules File window, select the rules file to activate.
3. Back at the IP Packet Security GUI, click the green triangle icon on the menu bar to activate IP packet security (Figure 59). Alternatively, click **File->Activate**.

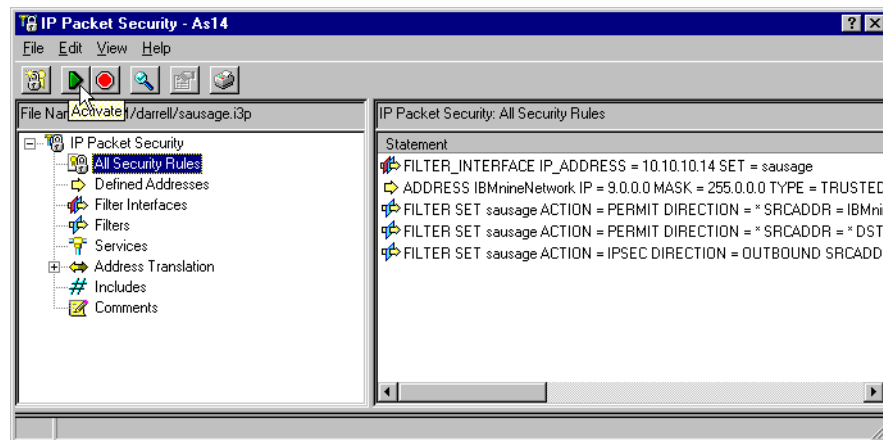


Figure 59. Activating IP packet security

4. A window is displayed with a message advising you that the rules file will be verified and, if successful, it will be activated. Click **Yes** to continue activating the filters.

A message appears at the bottom of the window to inform you that IP packet security was activated successfully (Figure 60 on page 86).

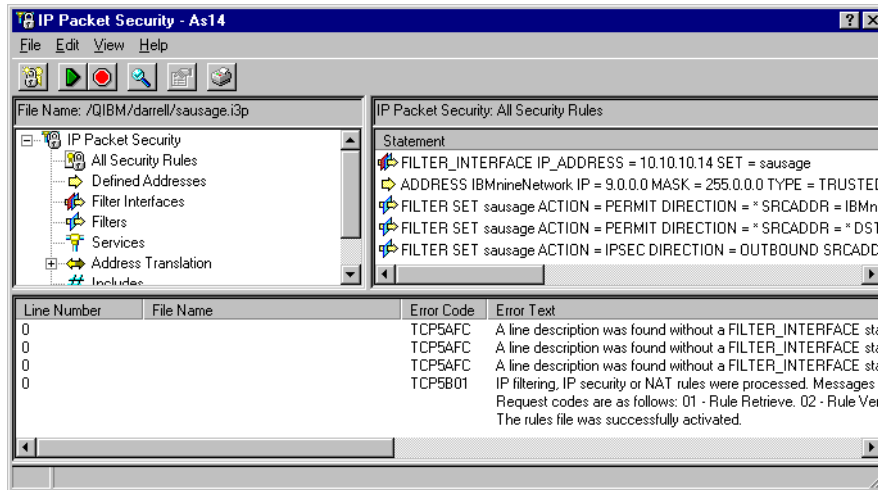


Figure 60. Activating IP packet security

Tip

IPLing the system automatically activates the filter rules file that was active before the IPL.

3.8.1.3 Deactivating IP packet security

IP packet security cannot be deactivated if one or more VPN connections are started. Verify that the VPN connections are stopped before attempting to deactivate IP filters. However, IP packet security can be ended if there are no active VPN connections, even if VPN server jobs are still active.

Tip

If you have more than one filter rules file on your system, take note of the currently active file *before* deactivating IP packet security. Once the filters are deactivated, it is not possible to determine the name of the last filter rules file that was active on the system.

Perform the following steps to deactivate IP packet security:

1. At the IP Packet Security GUI, click the red dot icon to deactivate IP packet security (Figure 61 on page 87).

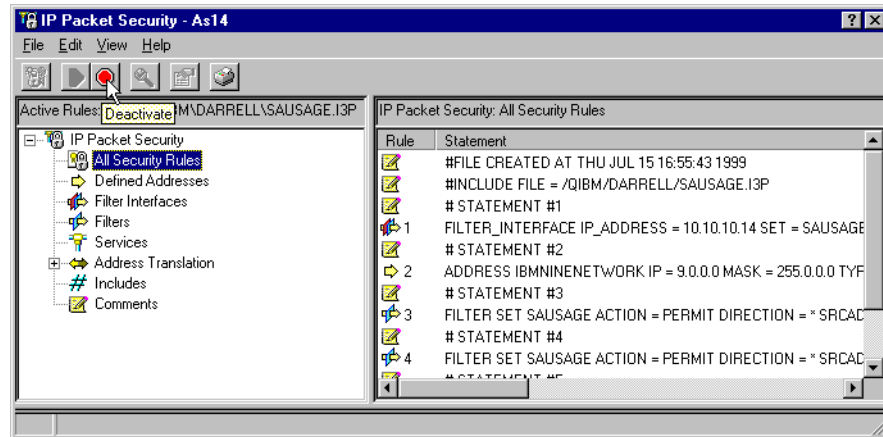


Figure 61. Deactivating IP packet security

2. A confirmation window prompts you to confirm that you want to continue. Click **Yes**.

A message appears at the bottom panel of the window to inform you that the previously active rules were deactivated successfully (Figure 62).

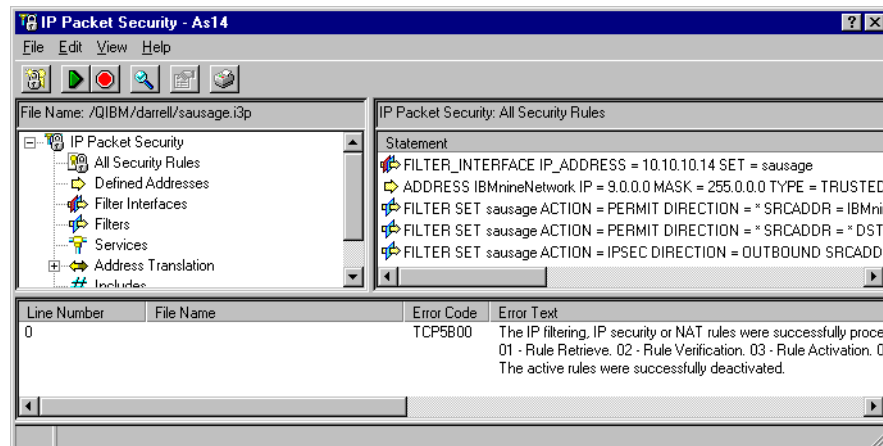


Figure 62. IP packet security deactivated

Tip

Use the Remove TCP/IP Table (RMVTCPTBL) command to remove any IP filter table from use:

```
RMVTCPTBL TBL (*ALL)
```

3.8.2 VPN server operations

The VPN server consists of the jobs QTOKVPNIKE and QTOVMAN in subsystem QSYSWRK described in 3.3.4, “VPN and L2TP server jobs” on page 54. This section describes the tasks you need to perform to operate the VPN server jobs. The VPN server jobs must be started before VPN connections can be established.

3.8.2.1 Checking the VPN server jobs status

Use the Work Subsystem Jobs (`WRKSBSJOB SBS(QSYSWRK)`) command to verify that the jobs QTOKVPNIKE and QTOVMAN are active. Alternatively, use Operations Navigator to perform the following steps:

1. Start Operations Navigator for your AS/400 system.
2. Sign on when prompted.
3. Expand **Network**.
4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking.

If the status of the Virtual Private Networking server is *Started*, as shown in Figure 58 on page 85, then the VPN server jobs are started.

3.8.2.2 Manually starting the VPN server jobs

Use the Start TCP Server (`STRTCPSVR SVR(*VPN)`) CL command to start the VPN server jobs. Alternatively, use Operations Navigator to perform the following steps:

1. Start Operations Navigator from the desktop.
2. Expand the AS/400 system, for example, **RALYAS4A**. Sign on when prompted.
3. Expand **Network** (Figure 63).

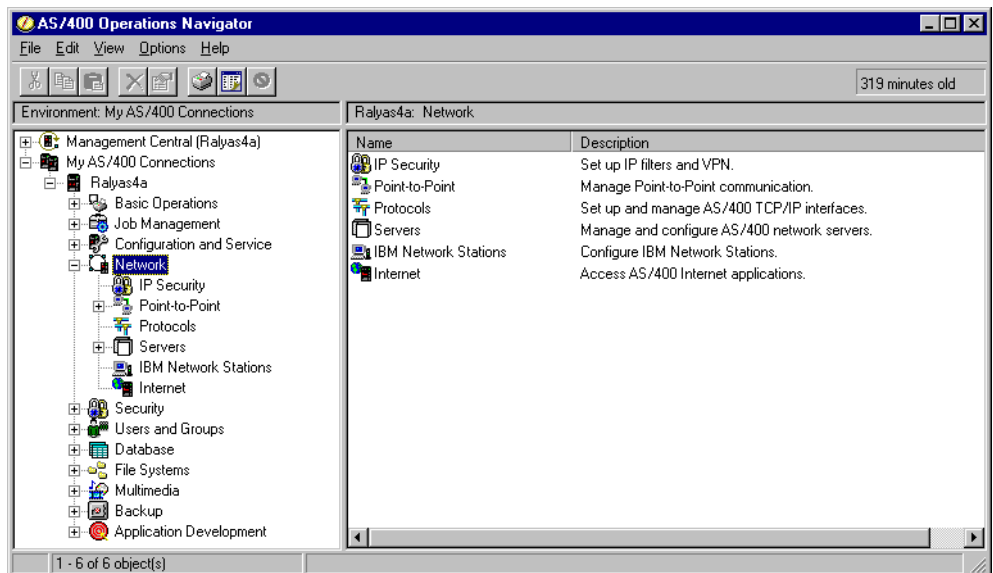


Figure 63. Operations Navigator - Expanding Network

4. Click **IP Security** to reveal two server names in the right panel: *IP Packet Security* and *Virtual Private Networking*.
5. Right-click **Virtual Private Networking**.
6. Select **Start** from the pull-down menu (Figure 64 on page 89).

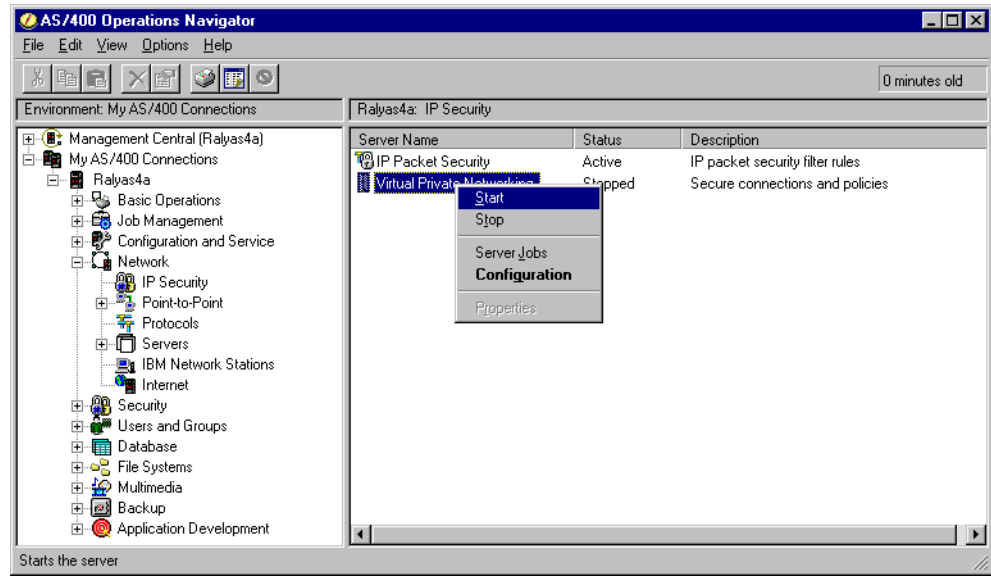


Figure 64. Starting the VPN jobs manually

3.8.2.3 Automatically starting VPN server jobs when TCP/IP starts

You can configure the TCP/IP server jobs that you want to start when TCP/IP starts. In V4R4, VPN server jobs are configured to start when TCP/IP starts by default. You can specify whether you want to start Virtual Private Networking at TCP/IP start time by performing the following steps:

1. Start Operations Navigator from the desktop.
2. Click **Network->Protocols->TCP/IP**.
3. Select **Servers to Start**.
4. Check (or uncheck not to start) **Virtual private networking**. See Figure 65 on page 90.

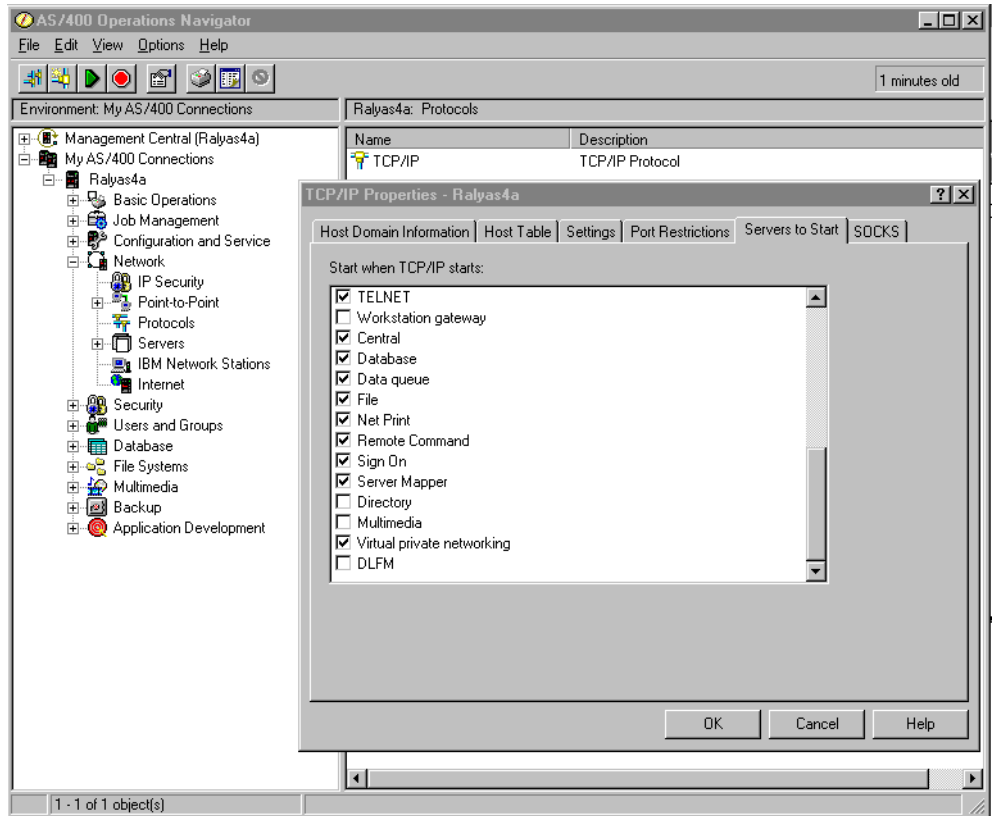


Figure 65. Automatically starting VPN server jobs at TCP/IP start

5. Click **OK**.

3.8.2.4 Manually ending VPN server jobs

Use the End TCP Servers (`ENDTCPSVR SVR(*VPN)`) CL command to end the VPN server jobs. Alternatively, use Operations Navigator to perform the steps described in 3.8.2.2, “Manually starting the VPN server jobs” on page 88, but select **Stop** from the pull-down menu.

Note: Ending the VPN server jobs ends all the active connections immediately.

3.8.3 VPN connections operations

This section describes the tasks associated with the operations of VPN connections on the AS/400 system.

3.8.3.1 Starting VPN connections

You must start the VPN connection on the AS/400 system that acts as the *initiator* of the connection. The AS/400 system that acts as the *responder* must be ready to receive a connection initiation request from the remote partner. However, no manual operations are required on the responder system.

Prior to starting a VPN connections, the following services must be started on both AS/400 VPN partners (connection initiator and responder):

- TCP/IP
 - If TCP/IP is not started, use the Start TCP/IP (`STARTTCP`) command to start it.
- IP packet security
 - Check the status of IP packet security (refer to 3.8.1.1, “Checking IP packet security status” on page 84).
 - If IP packet security is not active, perform the steps described in 3.8.1.2, “Activating IP packet security” on page 85, to activate it.
- Virtual Private Networking server jobs
 - Check the Virtual Private Networking server jobs status as described in 3.8.2.1, “Checking the VPN server jobs status” on page 88.
 - If the Virtual Private Networking server jobs are not started, start them as described in 3.8.2.2, “Manually starting the VPN server jobs” on page 88.

3.8.3.2 Manually starting Dynamic Key Connections

To start Dynamic Key Connections manually, perform the following steps:

1. At the Virtual Private Networking GUI, expand **Secure Connections**.
2. Expand **Data Connections**.
3. Expand **Dynamic Key Groups**.
4. Click the dynamic key group for the VPN connection that you want to start.
5. Right-click on the VPN connection on the right panel, and select **Start** (Figure 66).

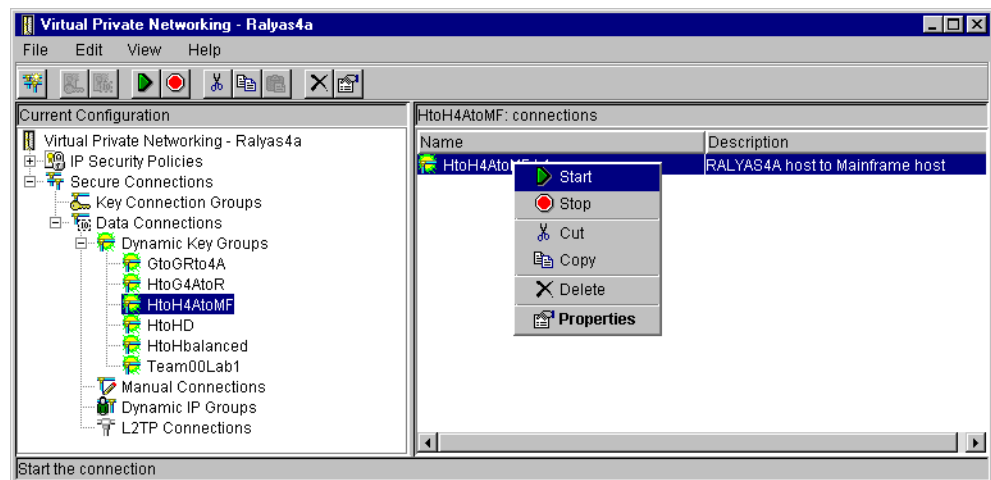


Figure 66. Starting a dynamic key VPN connection

3.8.3.3 Automatically starting Dynamic Key Connections

Dynamic Key Connections can be automatically started when an interface that has associated filter rules with action=IPSEC is started. That is, starting the interface triggers the connection to start. The same is true for manual connections. To configure Dynamic Key Connections to automatically start, perform the following steps:

1. Right-click on the connection, and select **Properties** from the pull-down menu (Figure 66).

2. Check **Start when TCP/IP is started** (Figure 67).

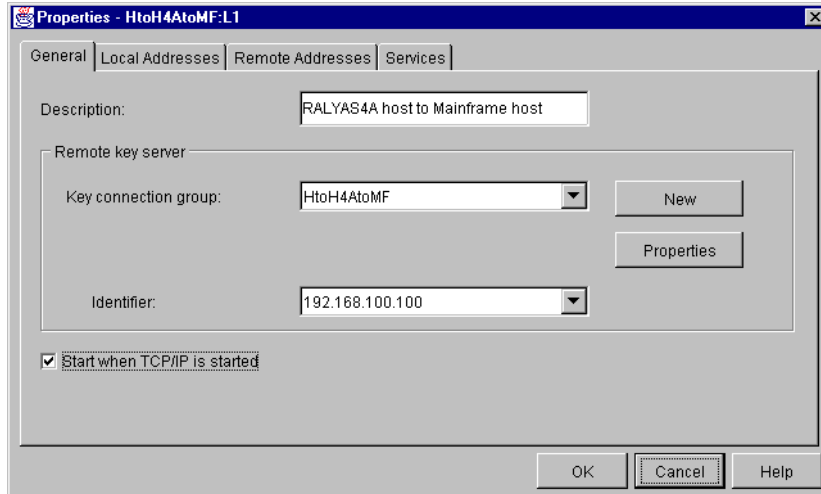


Figure 67. Automatically starting a dynamic key connection

3. Click **OK**.

3.8.3.4 Manually starting Manual Connections

To manually start Manual Connections, perform the following steps:

1. At the Virtual Private Networking GUI, expand **Secure Connections**.
2. Expand **Data Connections**.
3. Click **Manual Connections**.
4. Right-click the VPN connection that you want, and select **Start** from the pull-down menu (Figure 68).

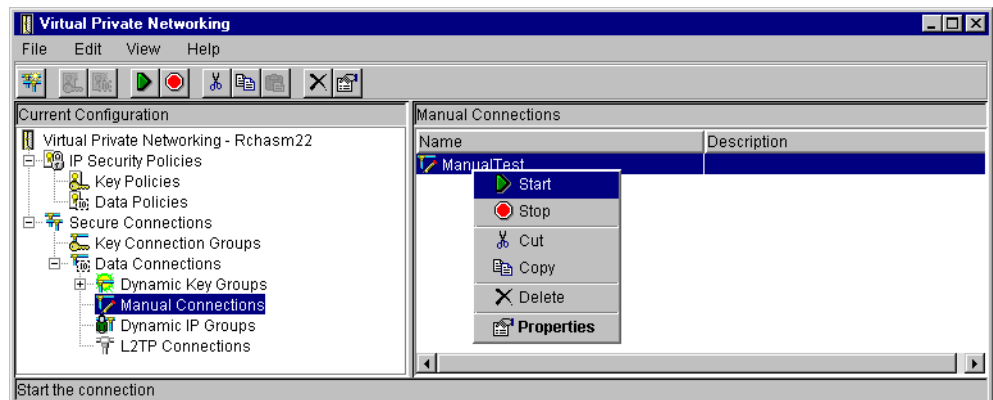


Figure 68. Starting a manual connection

5. You must repeat these steps on the remote system at the other end of the connection since both sides must start a manual connection.

3.8.3.5 Automatically starting Manual Connections

Manual Connections can be automatically started. To configure Manual Connections to automatically start, perform the following steps:

1. Right-click on the connection, and select **Properties** from the pull-down menu (Figure 68 on page 92).
2. Check **Start when TCP/IP is started** (Figure 69).

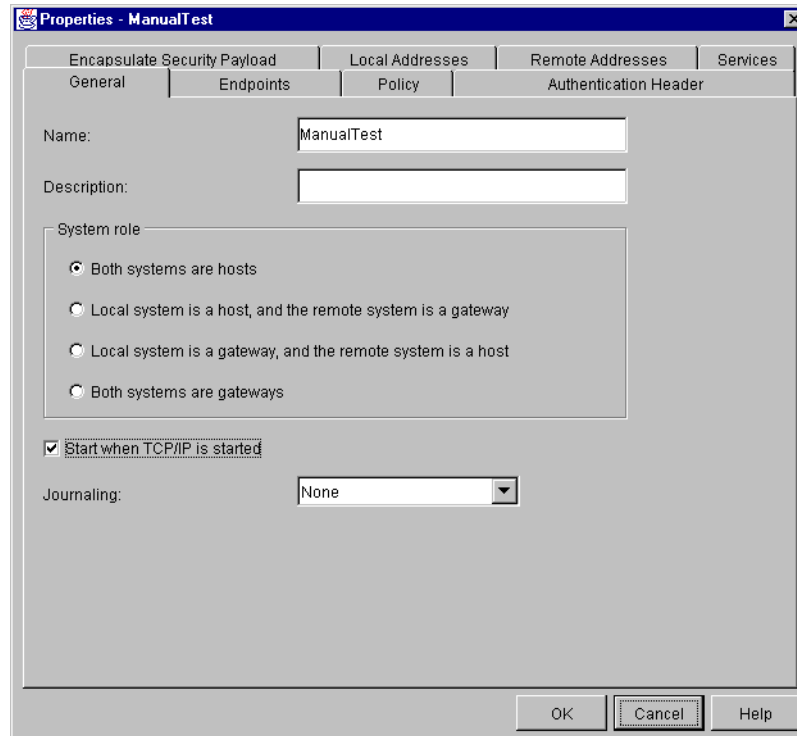


Figure 69. Automatically starting a manual connection

3. Click **OK**.

3.8.4 Starting L2TP and VPN connections on the AS/400 LNS

The AS/400 system, acting as the L2TP Network Server (LNS), is the terminator of the L2TP tunnel and the responder of the VPN connection (assuming that the L2TP connection is protected by IPSec). The remote client is responsible for initiating both the L2TP tunnel and the VPN connection.

Note: The process described in this section assumes that the L2TP tunnel is protected by IPSec. Therefore, both the L2TP tunnel and the VPN connection are started.

3.8.4.1 Starting the L2TP connection on the AS/400 LNS

Perform the following steps on the LNS AS/400 system to prepare its end of the L2TP tunnel:

1. Activate IP packet security as described in 3.7.1.2, "Starting the IP Packet Security GUI" on page 69.

Note: IP filters must be active before the virtual PPP connection profile is started.
2. Start Operations Navigator, and expand the LNS AS/400 system.
3. Expand **Network->Point-to-Point->Connection Profiles**.

- On the right panel, right-click the LNS connection profile identified by Connection type Virtual line (L2TP) - terminator. For example, right-click **L2tptoas20**, and select **Start** as shown in Figure 70.

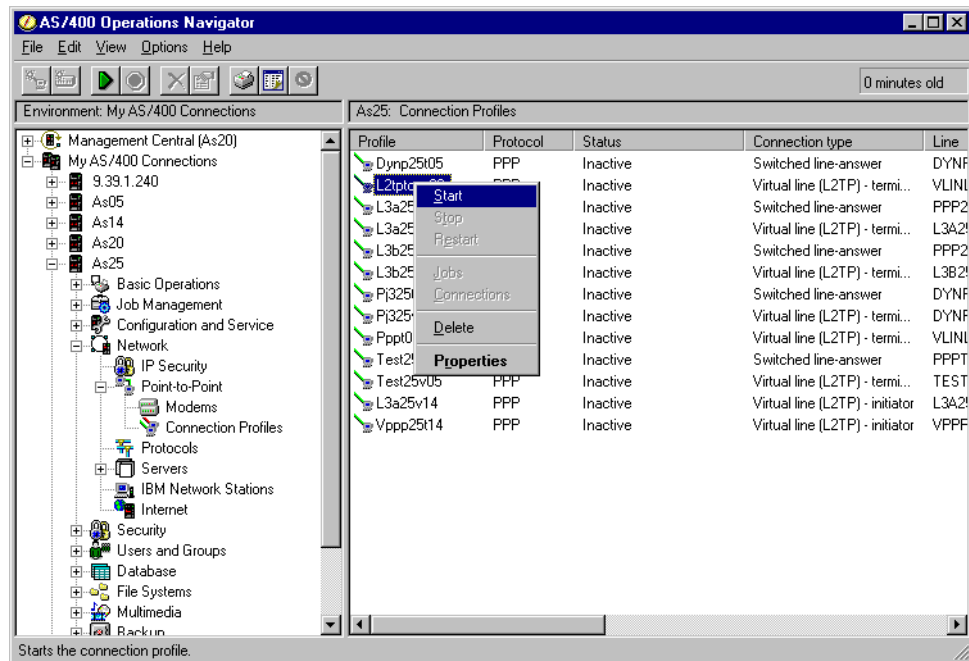


Figure 70. AS/400 LNS L2TP terminator - Starting a virtual PPP connection profile

- After the connection profile starts, refresh the window (press **F5** to refresh) to check the connection status. The status should be **Waiting for connection requests** as shown in Figure 71.

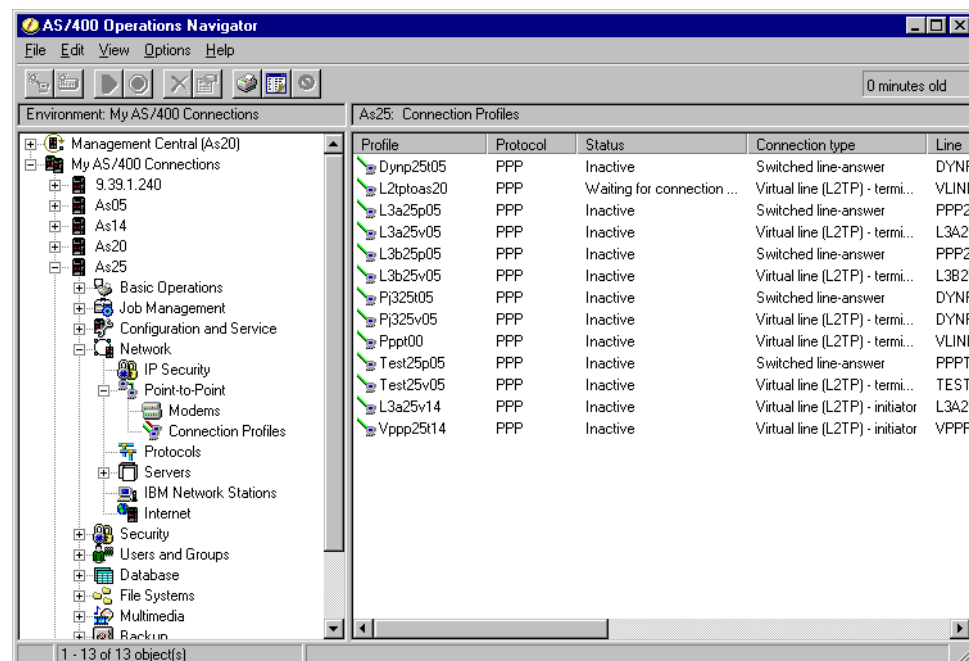


Figure 71. AS/400 LNS L2TP connection terminator - Waiting for connection requests

3.8.4.2 Starting the VPN connection on the AS/400 LNS

To prepare the AS/400 LNS to respond to a VPN connection initiation request from the remote client, start the VPN server jobs as described in 3.8.2.2, “Manually starting the VPN server jobs” on page 88, and 3.8.2.3, “Automatically starting VPN server jobs when TCP/IP starts” on page 89.

3.8.5 Starting L2TP and VPN connections on the AS/400 L2TP initiator

The AS/400 system, acting as the L2TP client, is the initiator of the L2TP tunnel and the initiator of the VPN connection (assuming the L2TP connection is protected by IPSec). Therefore, it is responsible for initiating both the L2TP tunnel and the VPN connection.

3.8.5.1 Starting the L2TP connection on the AS/400 L2TP initiator

To start the L2TP connection on an AS/400 L2TP initiator in a voluntary tunnel, perform the following steps:

1. Activate IP packet security as described in 3.7.1.2, “Starting the IP Packet Security GUI” on page 69.
2. Start Operations Navigator, and expand the L2TP initiator AS/400 system.
3. Expand **Network->Point-to-Point->Connection Profiles**.
4. On the right panel, right-click the PPP switch line dial profile to establish the connection to the ISP (PPPDIALUP in our example). Select **Start** from the pull-down menu.
5. Press **F5** to refresh the window. The status should be *Active* as shown in Figure 72. Allow for some delay before the status changes to *Active*.

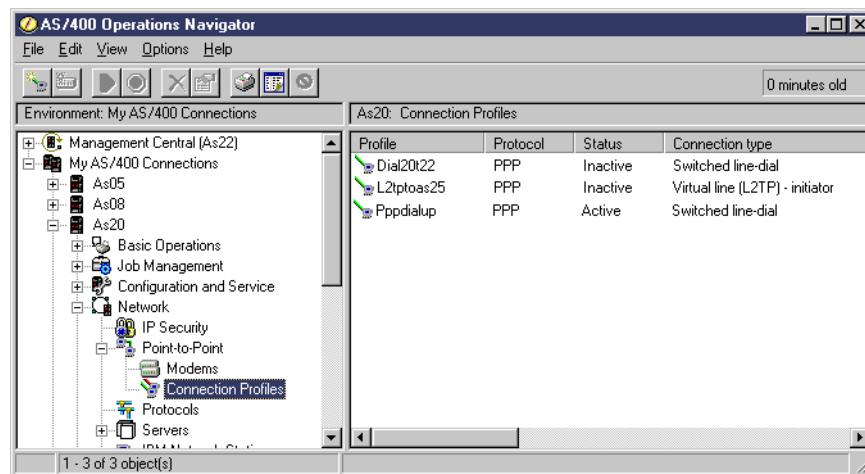


Figure 72. AS400 L2TP initiator - PPP dial-up connection Active status

6. On the right panel, right-click the Virtual PPP connection profile identified by Connection type Virtual line (L2TP) - initiator. For example, right-click **L2tptoas25**, and select **Start** as shown in Figure 73 on page 96.

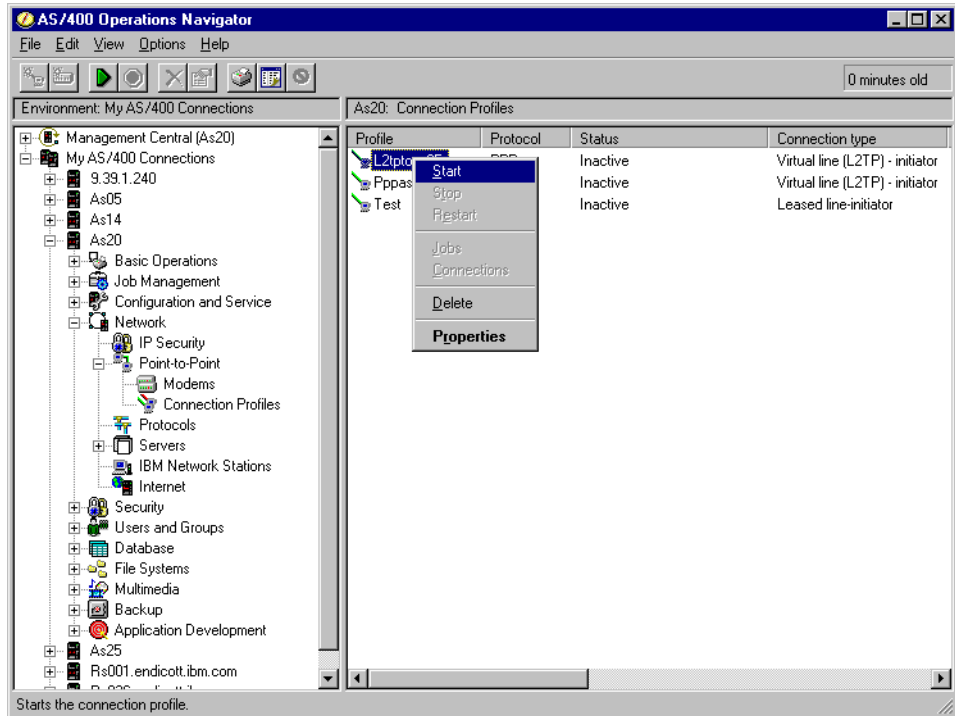


Figure 73. AS/400 L2TP initiator (L2TP connection initiator) - Starting a virtual PPP connection

7. Press **F5** to refresh the window. When the L2TP tunnel starts successfully, the connection status is Active connections as shown in Figure 74.

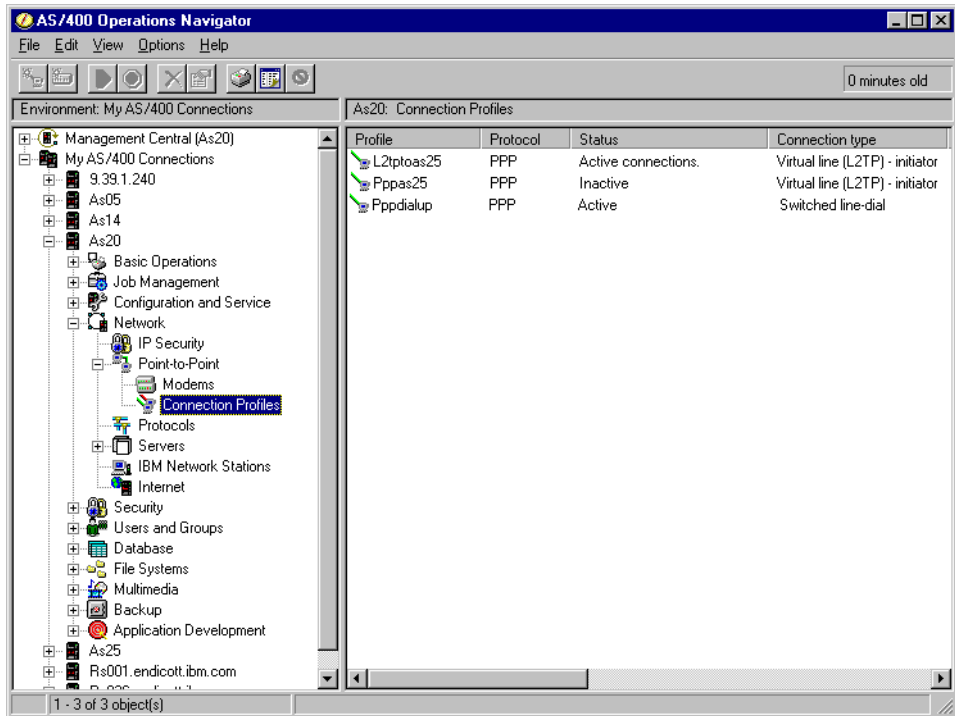


Figure 74. AS/400 L2TP connection initiator - Active connections

3.8.5.2 Starting the VPN connection on the AS/400 L2TP initiator

The VPN connection is initiated automatically when the L2TP PPP connection profile starts as described in 3.8.5.1, “Starting the L2TP connection on the AS/400 L2TP initiator” on page 95. No additional task is needed to activate the VPN connection that protects the L2TP tunnel.

3.8.6 Checking the VPN connections status

The Virtual Private Networking GUI includes the Active Connections window, which allows you to monitor the status of the VPN connections.

To start the Active Connections window, perform the following steps:

1. At the Virtual Private Networking GUI window, select **View->Active Connections** as shown in Figure 75.

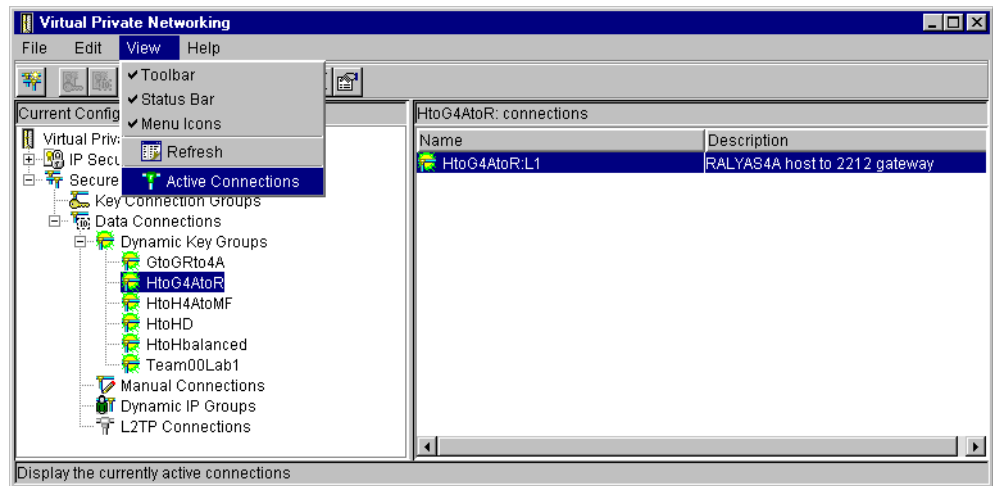


Figure 75. Starting the Active Connections window

The Active Connections GUI is displayed as shown in Figure 76.

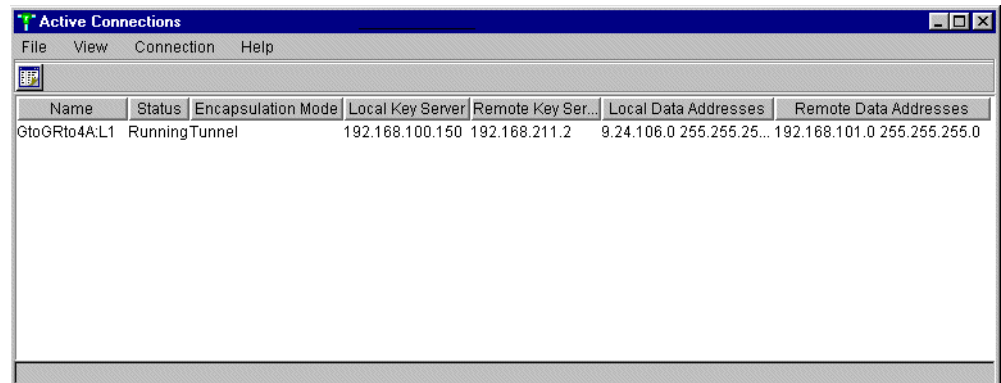


Figure 76. Active Connections window

3.8.6.1 Customizing the Active Connection window

To customize the fields displayed by the Active Connections window, perform the following steps:

1. At the Active Connections window, click **View->Preferences** (Figure 77).

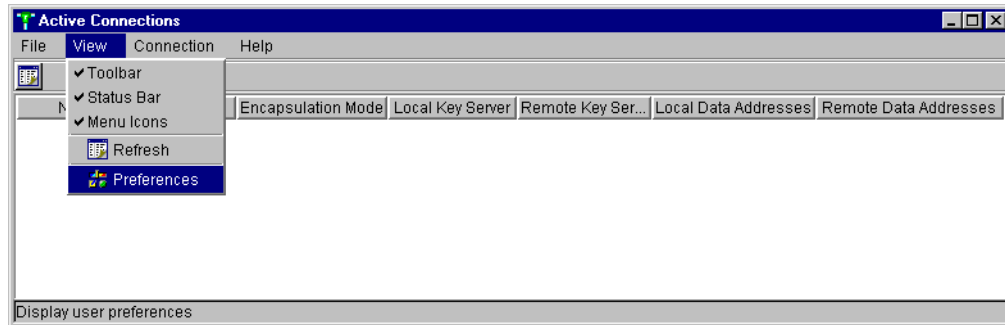


Figure 77. Customizing the Active Connections window

2. Select **Automatic timed refresh** if you want to refresh the Active Connections window automatically. Specify the refresh interval as shown in Figure 78.

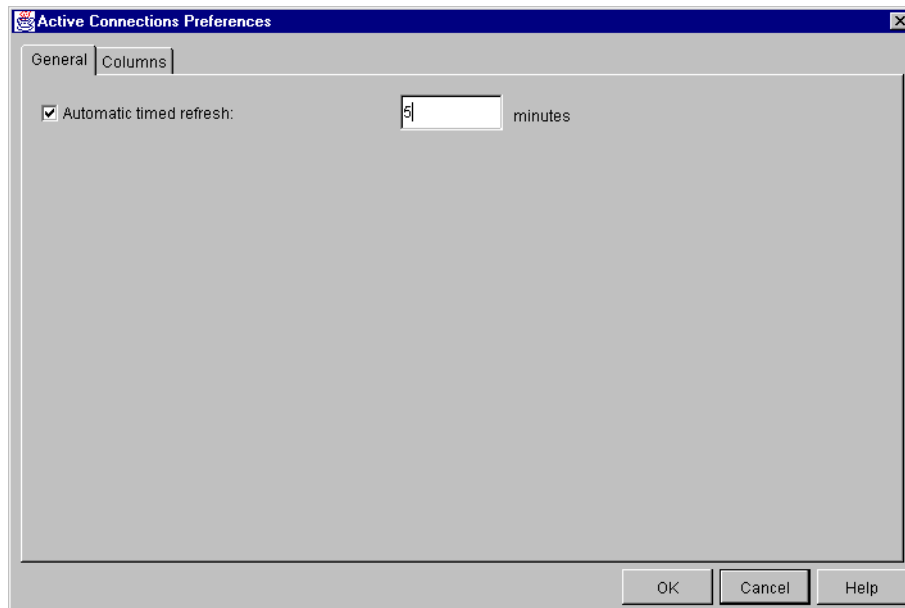


Figure 78. Active Connection window - Automatic timed refresh

3. Click the **Columns** tab (Figure 78).

As shown in Figure 79 on page 99, the right panel in the Active Connections Preferences - Columns window shows the list of columns that are currently displayed on the Active Connections window. The left panel shows the columns that are not displayed on the Active Connections window. Add or remove columns as desired.

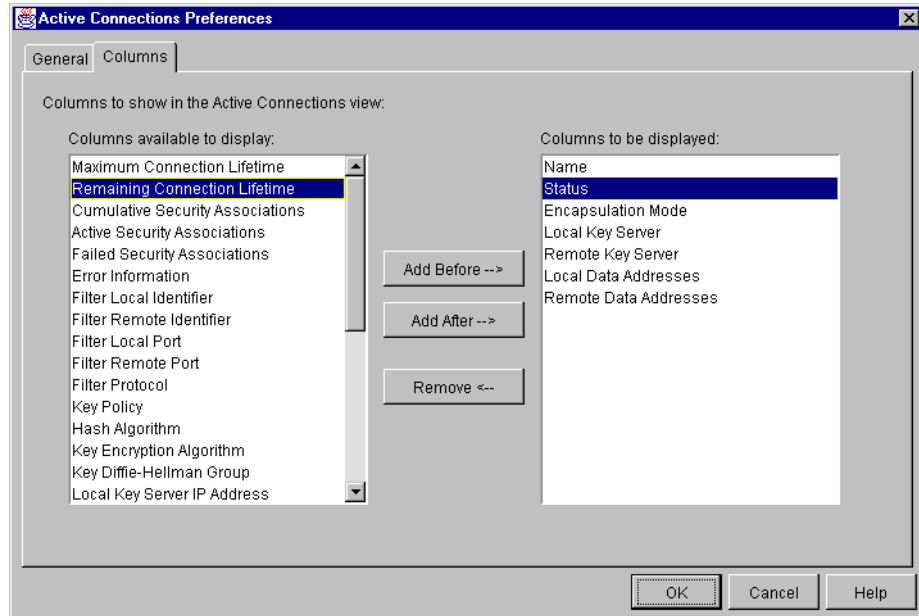


Figure 79. Selecting columns to display in the Active Connections window

You can rearrange the column sequence in the Active Connections window by dragging and dropping columns. You can also resize column widths from the Active Connections window by dragging and dropping column boundaries

For example, if you want the Local Key Server column to appear to the right of the Status column, perform the following steps:

1. At the Active Connections window, click and drag the **Local Key Server** column (Figure 80).

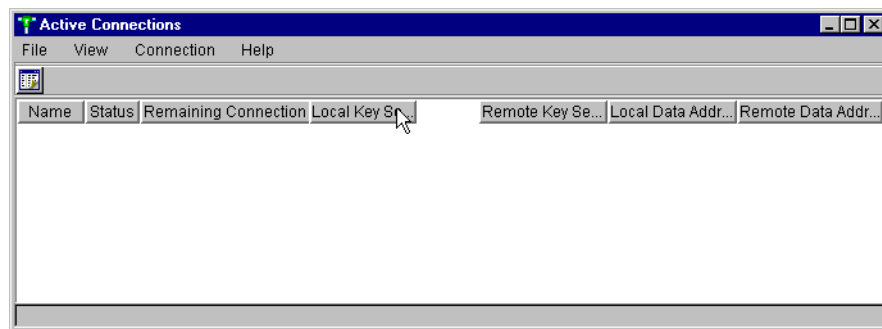


Figure 80. Dragging the Local Key Server column

2. Drop the **Local Key Server** column to the right of the Status column.

This changes the sequence of columns in the Active Connections windows as shown in Figure 81 on page 100.

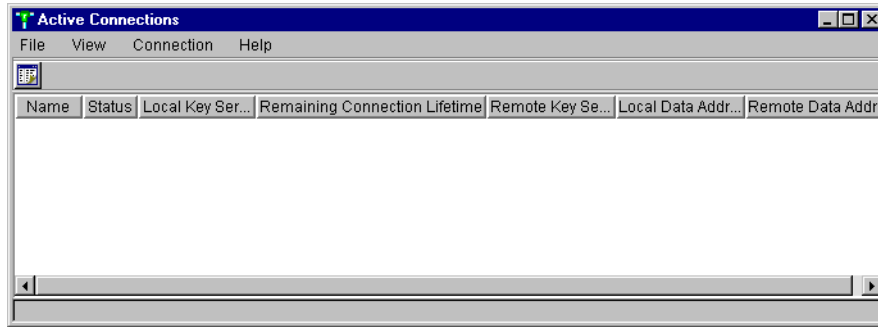


Figure 81. Local Key Server column moved

3.8.7 Stopping VPN connections

The simplest way to end a VPN connection is through the Active Connections window. Perform the following steps:

1. At the Active Connections window, right-click the VPN connection that you want to end.
2. Select **Stop** as shown in Figure 82.

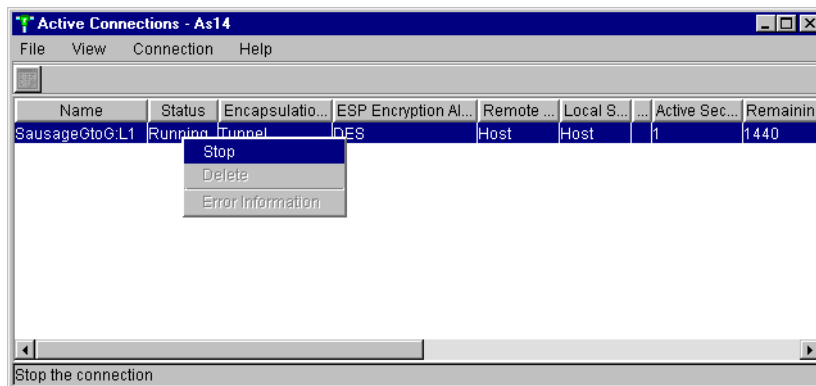


Figure 82. Stopping VPN connection from the Active Connections window

You can also stop VPN connections following the steps described in 3.8.3.2, “Manually starting Dynamic Key Connections” on page 91, and 3.8.3.4, “Manually starting Manual Connections” on page 92, but select **Stop** instead of *Start*.

For manual connections, you may also want to stop it on the remote system. Since both sides need to be active for a manual connection to protect traffic, stopping one side will effectively stop the connection.

3.8.7.1 Automatically ending VPN connections

VPN connections can be automatically ended by specifying a connection lifetime value. The VPN connection ends automatically when the connection lifetime expires. You can configure a connection lifetime in the Properties->Policy window of the following objects:

- Dynamic key group
- Manual connection
- Dynamic IP group
- L2TP connection

When the connection lifetime expires, the VPN connection ends even if there is active traffic flowing through it.

3.9 Backup and recovery considerations

Plan to back up the VPN Policy Database and IP packet filter rules file on a regular basis or every time you change the VPN configuration or IP packet filter configuration.

Back up the VPN Policy Database in one of the following ways:

- Use the OS/400 Save Object (`SAVOBJ`) command to back up the VPN Policy Database objects in the QUSRSYS library. Refer to Table 1 on page 54 for a list of the VPN configuration object.
- Save the library QUSRSYS using one of the following commands:
 - `SAVLIB LIB(QUSRSYS)`
 - `SAVLIB LIB(*NONSYS)`
 - `SAVLIB LIB(*ALLUSR)`
- Since the VPN configuration objects reside in the QUSRSYS library, they are saved when a full system save is performed.

Use the `SAV` command to back up the IP packet filter rules file from the IFS.

Important

Ensure that the system value QRETSVRSEC is set to 1 prior to restoring any VPN configuration data.

Chapter 4. AS/400 IP filtering overview

Internet Protocol (IP) packet filtering is the core component of any security server such as firewalls, routers, and hosts. IP packet security was introduced as part of V4R3 OS/400. The IP packet filtering component protects your system by filtering packets according to rules that you specify. You define the policies that determine the types of packets that are permitted or denied access to your system or network.

In V4R4, the IP packet filtering component was enhanced to support VPN. You must use IP packet security to create and apply VPN policy filter rules.

The VPN configuration wizard does not configure IP filtering. Therefore, you must complete the VPN configuration by configuring the required filters. IP filter rules direct outbound traffic through the IP Security Architecture (IPSec) protocol, and allow Internet Key Exchange (IKE) negotiations.

Keep in mind that the filter rules you create affect all IP traffic on the system. One mistake can stop all users from using your AS/400 system.

Before you configure IP filtering, you must be familiar with TCP/IP protocol and addressing. This chapter provides an overview of IP filtering implementation on the AS/400 system, particularly as it pertains to VPN.

4.1 How IP filtering works

IP filtering examines every IP packet coming into and out of an interface and compares them against a set of filter rules that are written for that interface. If the IP packet matches the rule, the IP filtering software performs the *action* that the rule defines. If there is no match, the system drops the IP packet. The last filter rule in a filter rules file has an implicit action, *deny*. Therefore, if an IP packet being examined by the IP filtering component does not match any rule in the file, it always matches the implicit last rule that causes it to be dropped.

IP packet filtering provides the ability to selectively block IP traffic based on information in the IP and protocol specific (for example, TCP and UDP) packet headers. A set of rules specifies which IP packets are to be permitted and which are to be denied. The decision to permit or deny specific packets is based on:

- Destination IP address
- Source IP address
- Protocol (for example, TCP, TCP/Starting, UDP, ICMP, AH, ESP)
- Destination port (for example, 80=HTTP and 23=Telnet)
- Source port
- Direction (inbound, outbound, or both)
- Packet fragments

The packet filter component uses the source and destination address, together with the protocol ID, to determine the packets that may access services specified by the destination port. On the AS/400 system, filter applies to a physical interface.

IP protocols

Figure 83 shows the most common higher level protocols that can be specified in a filter rule.

Protocol	Protocol number
Internet Control Message Protocol (ICMP)	01
Transmission Control Protocol (TCP)	06
User Datagram Protocol (UDP)	17
Authentication Header (AH)	51
Encapsulating Security Payload (ESP)	50

Figure 83. Common IP protocols and their protocol numbers

Well-known ports

The TCP/IP services have associated *well-known* port numbers. This allows client applications to send a session start packet to the well-known port number, rather than having to first consult a *port mapper*. Figure 84 contains a list of well-known ports for common Internet applications.

Service	Port/Protocol
FTP-Data	20/TCP
FTP-Command	21/TCP
TELNET	23/TCP
SMTP	25/TCP
DNS	53/UDP 53/TCP
HTTP	80/TCP
POP	110/TCP
SNMP	161/UDP
IKE	500/UDP
L2TP	1701/UDP

Figure 84. Well-known ports for common Internet applications

For a complete list of well-known ports, refer to RFC 1700 *Assign Numbers*.

The range for assigned ports is 0 through 1023. When a client wishes to start a conversation, they are required to use a source port value greater than 1023. Ports over 1023 are called *ephemeral ports*.

Fragmentation

IP can handle fragmentation and re-assembly of IP datagrams. The maximum length of an IP datagram is 65,535 bytes (or octets). There is a requirement for all TCP/IP hosts to support IP datagrams of up to 576 bytes without fragmentation.

Fragments of a datagram all have a header, which is copied from the original datagram. They are treated as normal IP datagrams while being transported to their destination. Note, however, that if one of the fragments gets lost, the complete datagram is considered lost since IP does not provide any acknowledgment mechanism. The remaining fragments will simply be discarded by the destination host.

There is a limit on the size of the frame for the data link layers such as Ethernet and Token Ring. This characteristic of the link layer is called *maximum transmission unit (MTU)*. Most types of networks have an upper limit. If the IP datagram is larger than the MTU, IP performs what is known as *fragmentation*, which breaks down the original datagram into smaller pieces to fit the MTU. The fragments are reassembled at the destination.

In a series of fragmented packets, only the first fragment contains the identifying header for higher level protocols such as TCP and UDP. Later fragments can override header fields such as the source and destination address. This allows attackers to misuse the fragment assembly algorithm to create forged packets and force them through the gateway.

The default for native OS/400 filter rules is to not permit fragments, but you can change this value. Refer to RFC 1858, *Security Considerations for IP Fragment Filtering*, for more information.

Logging

An IP filtering solution is inadequate unless it provides you with some means of logging the packet activity. This feature is especially useful for problem determination, monitoring for disallowed events, gathering statistics, and so on.

In most IP filtering implementations, you specify the logging level on each filter rule. Turning logging on for all rules can be useful while identifying configuration problems. However, it may be excessive for day-to-day operations and will most likely cause a degree of performance overhead.

Security administrators are typically interested in packets that were denied entry rather than packets which were successfully permitted. As such, logging is usually turned on for any deny rules that are defined.

OS/400 uses *journaling* to log packet activity. Specifying `FULL` for the journaling field within the filter rule means a journal entry is created every time the action specified for the filter occurs. The journals that keep records of filter activity are located in QUSRSYS/QIPFILTER. Model output files that you must use to copy the journal entries are in QSYS/QATOFIPF.

Tip

The last rule in a filter rules file is an implicit DENY *ALL rule. Since it is an *unwritten* rule, no logging (journaling = OFF) takes place when packets match the implicit DENY *ALL. To log packets that match the DENY *ALL rule, you must explicitly add a written rule at the end of the file. Specify `Journaling=FULL` in the explicit DENY *ALL rule.

Action

Each IP packet that attempts to access (inbound) or leave (outbound) your system is compared sequentially, from top to bottom, against each filter rule in the filter rules file. If there is a match, the action specified in the ACTION field is performed. The possible actions are:

- **PERMIT:** Allow the datagram to flow.
- **DENY:** Drop the packet.
- **IPSEC:** Apply IPsec protocols to the packet as defined by the associated connection group.

Tip

The system discards any packets that do not match a specific rule. As a backup security measure, the default *deny* rule automatically activates any time an undefined packet crosses your system. It is *important* to note that the default deny rule *only* applies to the physical interface on which the filter rules file is active. If the AS/400 system has other physical interfaces with no active filter rule files, those interfaces are *not* protected.

Filter rules file

On the AS/400 system, the IP filter rules are stored in a file that resides in the integrated file system. The filter rules file is created and edited through the IP Packet Security GUI in Operations Navigator.

Filter rule

The filter rule entry includes the fields that establish the criteria used to decide whether the packet should be allowed or dropped.

Defined addresses

On the AS/400 IP filtering implementation, you cannot specify a subnet or set of IP addresses as a source or destination IP address in a filter rule. The defined address allows you to configure a subnet or set of IP addresses and to give it a name. Use the name specified in the defined address to refer to the subnet or set of IP addresses in a filter rule.

Filter interfaces

A set of filter rules are applied to an IP network interface, which is a direct connection to a network (line description), or point-to-point profile. This set of filters is associated with the physical interface to which this logical interface is connected.

Tip

You can specify an IP address in the Line parameter of a new filter interface. It does not mean that the set of filter rules applies only to that specific IP address, but to the network interface associated with that IP address.

Set name

Each filter rule has a label called "Set." All rules with the same set name are grouped together.

In general, place all FILTER statements in a single set unless there are good reasons to do otherwise. For example, a group of FILTER statements that permits a particular protocol, such as FTP, is often a natural grouping. Name the set after the protocol. Then, you may decide to put that set on an interface. Likewise, you can create a PERMIT *ALL rule to be placed at the end of the file for testing purposes only. Place this rule in its own set and name it, for example, TEST. Add the set to the interface only when needed.

The order in which the sets are processed in the filter rules file depends on the order in which the sets are added to the interface. For example, if you configure a filter interface `FILTER_INTERFACE LINE=TRN1 SET=C, A, B`, all rules in set C are processed first, followed by rules in set A and B.

Services

Services is the combination of protocol, source port, and destination port. You can define a *Services Alias* to give a name to the services. You can later refer to the services by name in the filter rules, instead of specifying the protocol, source, and destination port each time.

4.1.1 IP filter rules examples

In this section, we present two examples to help you understand the filtering process. The first example shows the AS/400 system as a security gateway that connects two networks. The filters on the gateway control the traffic from the untrusted network that attempts to access the trusted network.

The second example shows the AS/400 system as a host. The filters on the host control the traffic that attempts to access this AS/400 system.

4.1.1.1 AS/400 system as a security gateway

Figure 85 on page 108 shows an AS/400 security gateway placed between the *untrusted network* (also called *non-secure*, and sometimes *public*) and the *trusted network* (also called *secure network* or *private network*). The characteristics of this example are:

- The AS/400 system acting as security gateway has two physical interfaces, which are shown as interface **1** and **2** in Figure 85 on page 108.
- Interface **1** is connected to the non-secure or untrusted network.
- Line description *public* is defined over the physical interface connected to the untrusted network.
- Interface **2** is connected to the secure or trusted network.

- Line description *internal* is defined over the physical interface connected to the trusted network.
- *IP forwarding* is enabled on the AS/400 security gateway.

IP forwarding

Enabling IP datagram forwarding on the AS/400 system causes the IP layer to forward Internet Protocol (IP) datagrams between different networks. Use the Change TCP/IP Attributes (`CHGTCPA IPDTGFWD(*YES)`) command to specify that the IP layer must act as a gateway.

To understand the flow of the datagrams and how the filter component on the AS/400 system controls the traffic, position yourself on the interface where the filters are active.

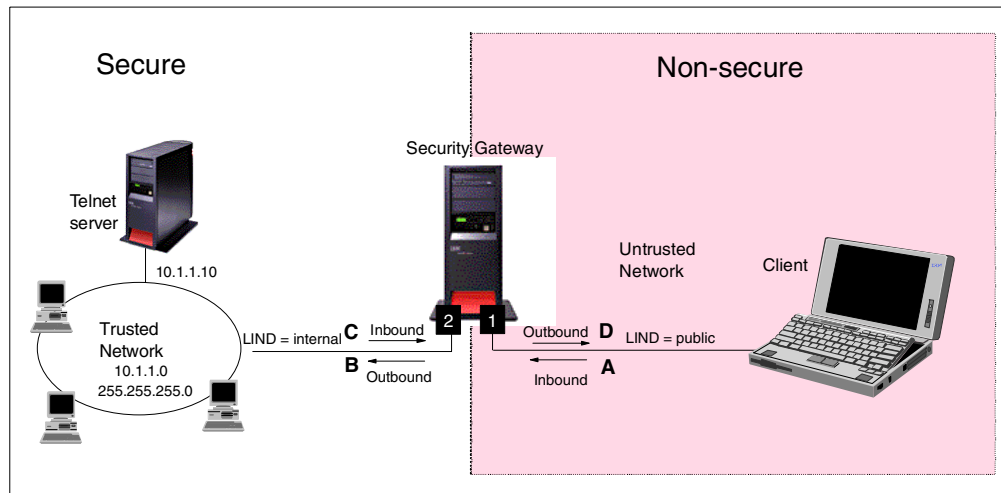


Figure 85. Datagrams flowing through an AS/400 security gateway

The objective of this example is to show you the filter rules that you need to configure in the security gateway to allow *only* Telnet requests from the client to the Telnet-SSL port of the server in the internal network.

The following filter rules are defined on the non-secure interface:

- Permit *inbound* packets from the non-secure network (IP address *any* (*)) to the SSL-Telnet server (IP address 10.1.1.10 mask 255.255.255.255 and port 992). This rule is shown as **A** in Figure 85.

```
FILTER SET = NONSECURE ACTION = PERMIT DIRECTION = INBOUND
SRCADR = * DSTADR = 10.1.1.10 PROTOCOL =TCP
DSTPORT = 992 SRCPORT > 1023 FRAGMENTS = NONE JRN = OFF
```

- Permit outbound packets from the SSL-Telnet server to the non-secure network. This rule is shown as **D** on Figure 85.

```
FILTER SET = NONSECURE ACTION = PERMIT DIRECTION = OUTBOUND
SRCADR = 10.1.1.10 DSTADR = * PROTOCOL =TCP
DSTPORT > 1023 SRCPORT = 992 FRAGMENTS = NONE JRN = OFF
```

- Define a filter interface associated with the AS/400 interface connected to the non-secure network. Add the `NONSECURE` set name to it.

```
FILTER_INTERFACE INTERFACE=PUBLIC SET = NONSECURE
```

On the secure interface, you may decide not to control the traffic at all and, therefore, not to configure filters on this interface. If you prefer to filter the traffic on the secure interface to add an additional level of control, configure the following filter rules:

- Define the address to configure the internal network subnet:

```
ADDRESS Internal IP=10.1.1.0 MASK 255.255.255.0 TYPE = TRUSTED
```

Note: The `Type` parameter is ignored. It is only used for Network Address Translation (NAT) configuration.

- Permit all inbound and outbound traffic to and from the internal network.

```
FILTER SET = SECURE ACTION = PERMIT DIRECTION = *
SRCADR = Internal DSTADR = Internal PROTOCOL = *
DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
```

Tip

The only time a *direction* of both (*) is applicable in a filter rule is when the source and destination IP addresses are the same and the source and destination ports are the same.

- Permit outbound traffic from the non-secure network to the SSL-Telnet server. This rule is shown as **B** on Figure 85 on page 108.

```
FILTER SET = SECURE ACTION = PERMIT DIRECTION = OUBOUND
SRCADR = * DSTADR = 10.1.1.10 PROTOCOL = TCP
DSTPORT = 992 SRCPORT > 1023 FRAGMENTS = NONE JRN = OFF
```

- Permit inbound traffic from the SSL-Telnet server to the non-secure network. This rule is shown as **C** on Figure 85 on page 108.

```
FILTER SET = SECURE ACTION = PERMIT DIRECTION = INBOUND
SRCADR = 10.1.1.10 DSTADR = * PROTOCOL = TCP
DSTPORT > 1023 SRCPORT = 992 FRAGMENTS = NONE JRN = OFF
```

- Define a filter interface associated with the AS/400 interface connected to the secure network. Add the `SECURE` set name to it.

```
FILTER_INTERFACE INTERFACE=INTERNAL SET = SECURE
```

4.1.1.2 AS/400 system as a host

Figure 86 on page 110 shows an AS/400 system as a host. In this case, the IP filters control the traffic attempting to flow inbound to and outbound from the host AS/400 system. In this case, the AS/400 system is connected *only* to the internal or secure network. The characteristics of this example are:

- The AS/400 system acting as host has a single physical interface shown as interface **1** in Figure 86 on page 110.
- Interface **1** is connected to the secure or trusted network.
- Line description `TRNLIN` is defined over the physical interface connected to the trusted network.
- *IP forwarding* is *not* enabled on the AS/400 host.

The objective of this example is to show you the filter rules that you need to configure in the host to allow *only* Telnet requests from the client to the Telnet-SSL port of the server.

The following filter rules are defined on the interface:

- Define an address to configure the internal network subnet:

```
ADDRESS Internal IP=10.1.1.0 MASK 255.255.255.0 TYPE = TRUSTED
```

Note: The Type parameter is ignored. It is only used for NAT configuration.

- Permit all inbound and outbound traffic to and from the internal network.

```
FILTER SET = HOST ACTION = PERMIT DIRECTION = *
SRCADR = Internal DSTADR = Internal PROTOCOL = *
DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
```

- Permit *inbound* packets from the non-secure network (IP address *any* (*)) to the SSL-Telnet server (IP address 10.1.1.10, mask 255.255.255.255 and port 992).

```
FILTER SET = HOST ACTION = PERMIT DIRECTION = INBOUND
SRCADR = * DSTADR = 10.1.1.10 PROTOCOL = TCP
DSTPORT = 992 SRCPORT > 1023 FRAGMENTS = NONE JRN = OFF
```

- Permit outbound packets from the SSL-Telnet server to the non-secure network.

```
FILTER SET = HOST ACTION = PERMIT DIRECTION = OUTBOUND
SRCADR = 10.1.1.10 DSTADR = * PROTOCOL =TCP
DSTPORT > 1023 SRCPORT = 992 FRAGMENTS = NONE JRN = OFF
```

- Define a filter interface associated with the AS/400 interface connected to the secure network. Add the `HOST` set name to it.

```
FILTER_INTERFACE INTERFACE=TRNLN SET = HOST
```

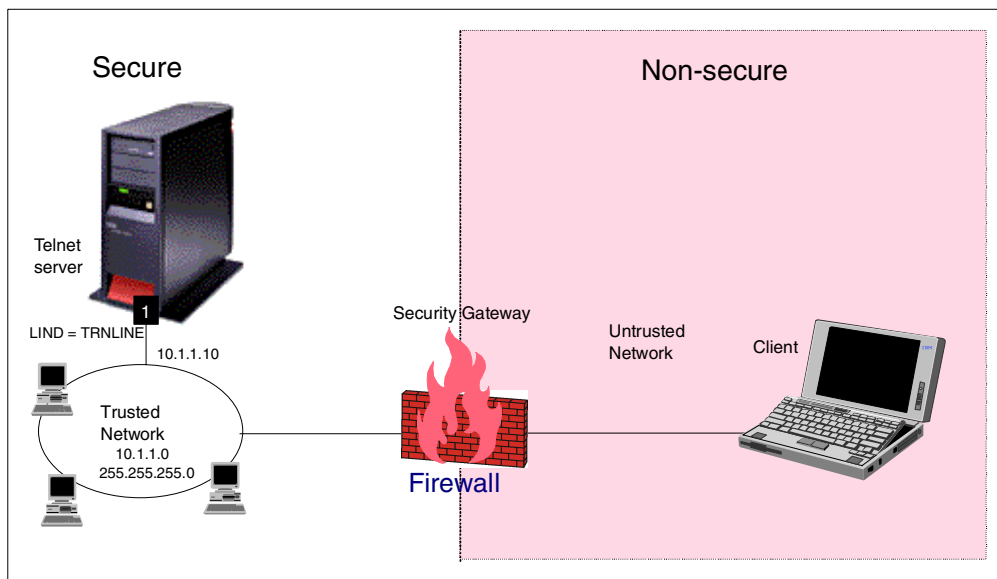


Figure 86. IP filtering on the host AS/400 system

4.1.2 IPsec-related IP filter rules

To implement the IPSEC function, you must first configure a set of IP filter rules on the AS/400 VPN server. The IPsec-related filter rules are:

- **IKE negotiation rules:** You must configure inbound and outbound PERMIT rules to allow protocol UDP, source and destination port 500 for IKE negotiations to take place between the AS/400 VPN server and the VPN partner.

Note

You do *not* need to configure IKE filter rules for a *manual* VPN connection. By definition, no IKE negotiations take place on a manual VPN.

- **IPSEC filter rule:** The IPSEC filter rule, also known as *policy filter*, dictates the set or subset of traffic that must be submitted to IPsec protocols. You define the data endpoints of the connection in the IPSEC filter rule. The connection group name associated with the IPSEC filter rule dictates the data treatment applied to the traffic. AS/400 IP filtering support was enhanced in V4R4 to support Action IPSEC (besides PERMIT and DENY available in V4R3).

Tip

All the IKE PERMIT rules must appear *before* the first IPSEC filter rule in the filter rules file.

Figure 87 on page 112 shows an example of the IKE outbound filter rule for a host-to-host VPN, where the local host is assigned IP address 204.1.14 and the remote host is assigned IP address 204.1.1.20.

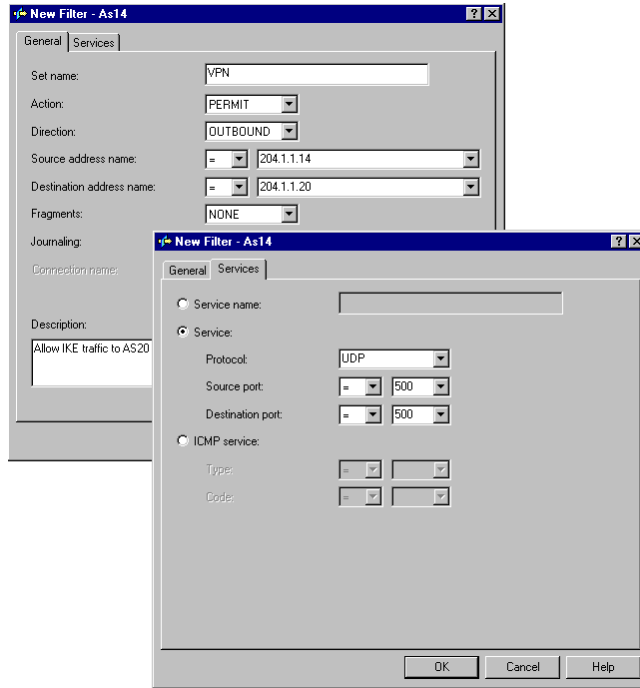


Figure 87. IKE outbound filter rule

Figure 88 shows the corresponding IKE inbound filter rule.

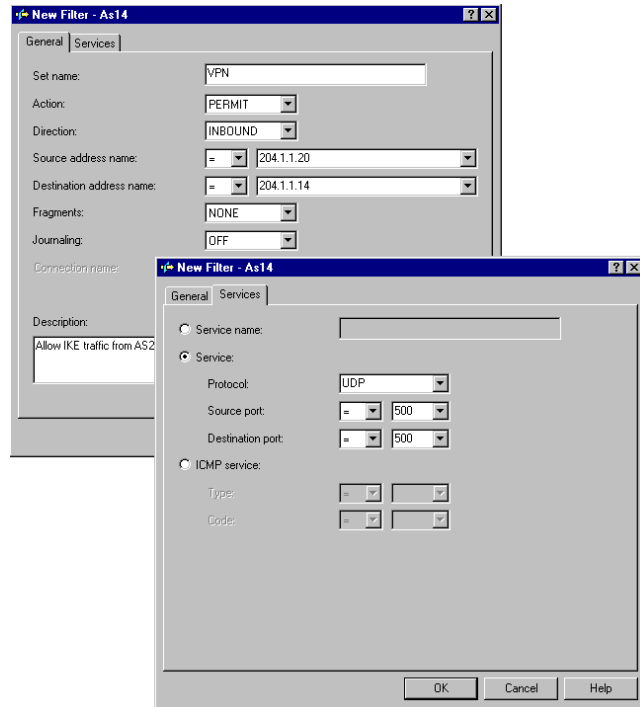


Figure 88. IKE inbound filter rule

To start connections for a connection group, a policy filter (filter rule with action IPSEC) for that connection group must be active on the appropriate interfaces.

Figure 89 shows the corresponding IPSEC filter rule. In a host-to-host connection, the data endpoint IP addresses are the same as the VPN server IP addresses. The IPsec protocols, transforms, and other IPsec-related specifications are defined in the connection group associated with the IPSEC filter rule. The connection group must be created *before* configuring the IPSEC filter rule.

Tip

When you select Action IPSEC, OUTBOUND is automatically selected for you and greyed out for Direction. The corresponding INBOUND IPSEC filter rule is implicitly configured.

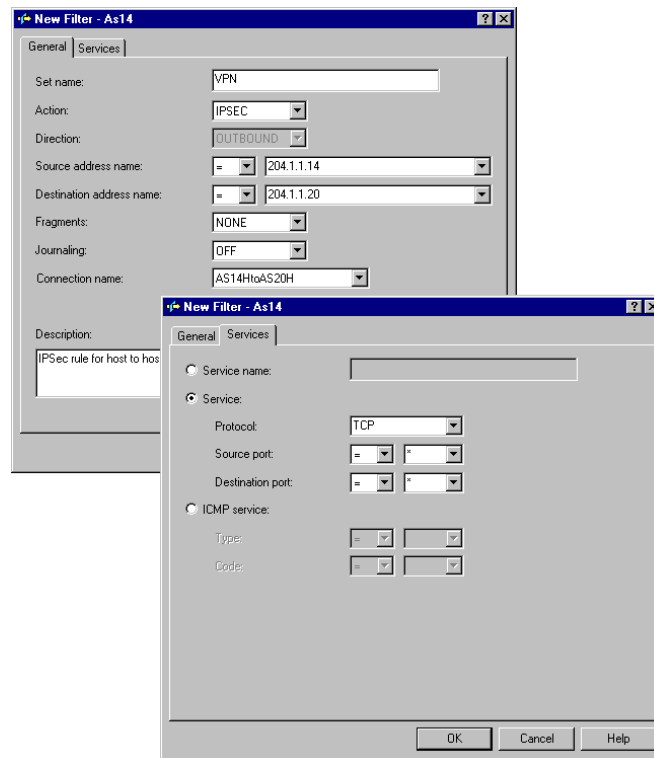


Figure 89. IPSEC filter rule

Note: There is a one-to-one relationship between the connection group and the IPSEC filter rule. In other words, it is not possible to have two IPSEC filter rules associated with the same connection group.

4.1.3 AS/400 IPsec processing logic

IP filtering and IPsec are implemented at the IP layer in the TCP/IP protocol stack.

Figure 90 on page 114 shows a simplified flow chart that outlines the key steps followed by an inbound datagram.

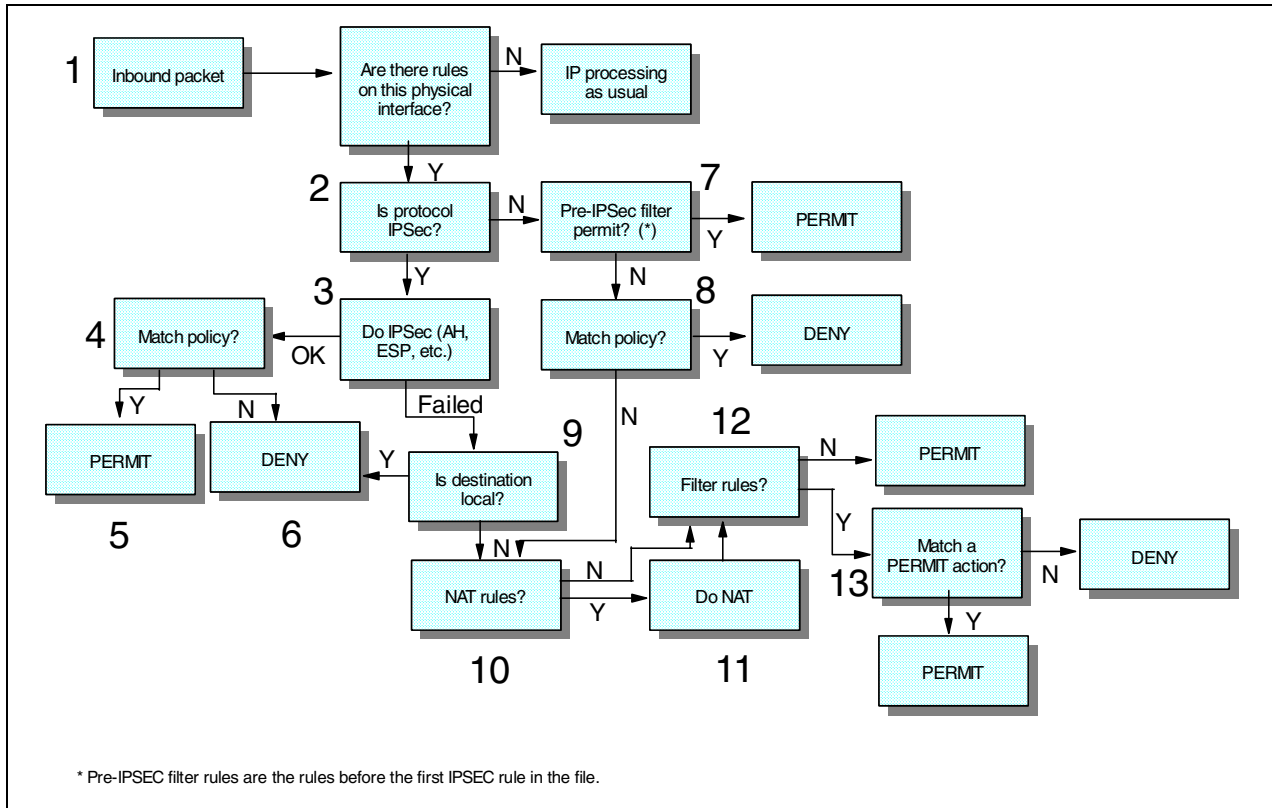


Figure 90. IP filtering and IPSec processing - Inbound datagram

A brief explanation of each step shown in Figure 90 follows:

1. The VPN server receives an IP datagram over a physical interface. Are IP filter rules active on the interface?
 - (Y) - Go to step 2.
 - (N) - Proceed with IP processing.
2. Does the IP payload contain an IPSec protocol (AH or ESP)?
 - (Y) - Go to step 3.
 - (N) - Go to step 7.
3. Perform IPSec processing as defined by the security association (SA). What is the packet's status after performing the IPSec security checks?
 - (OK) - Go to step 4.
 - (Failed) - Go to step 9.

Note: *Fail* means that the packet did not pass the actions specified by the SA. For example, AH or ESP failed to authenticate the packet, and ESP produced an invalid packet after decrypting the data (anti-replay test failure). Fail may also indicate the inability to find a valid security association (SA) for this datagram (either there is no active VPN connection for this traffic or the SA is expired).

4. Is there a VPN policy (IPSEC filter rules) loaded that matches this packet's details?

Note: A VPN policy is loaded on a per-interface basis, if an interface has any policy filters (IPSEC filter rule). The simplest way for you to check if there is a VPN policy loaded on the interface is to use Operations Navigator and look at the currently loaded rules shown by default. If there are any FILTER statements with the action = IPSEC, then each interface to which they are applied has VPN policy loaded.

- (Y) - Go to step 5.
- (N) - Go to step 6.

5. Permit the packet for IP processing.

6. Deny the packet.

7. Does the packet match a filter rule with the action PERMIT?

- (Y) - Permit the packet for IP processing. This stage is required here to allow non-IPSec IKE packets to succeed. Otherwise, step 8 may deny it.
- (N) - Go to step 8.

8. Is there a VPN policy loaded that matches this packet's details?

Note: This policy check is looking for inbound datagrams in the clear (without security protocols applied to them) that should have been processed by IPSec. Non-IPsec traffic on inbound is compared against the system-generated inbound IPSEC filter rule. If a match occurs, it means that a datagram should have been processed by IPSec protocols (tunneled), but wasn't.

- (Y) - This packet should have been protected by an IPSec protocol and is not. Deny the packet.
- (N) - Go to step 10.

9. Is the packet's destination IP address locally defined on this system?

- (Y) - The local system is the intended host. The packet should have passed IPSec processing. Go to step 6.
- (N) - The local system may be acting as a security gateway. Go to step 10.

10. Does the packet match a NAT rule defined in the filter rules file?

- (Y) - Go to step 11.
- (N) - Go to step 12.

11. Perform network address translation. Go to step 12.

12. Is there any filter rule that matches the packet now?

- (Y) - Go to step 13.
- (N) - Permit the packet for IP processing.

13. Is there a filter rule with action PERMIT that matches this packet's details?

- (Y) - Permit the packet for IP processing.
- (N) - Deny the packet.

Note

Pre-IPSEC filter rules are the IKE rules before the first IPSEC rule in the file. All pre-IPSEC filter rules must have direction (*) or be written as a contiguous inbound/outbound pairing.

Figure 91 shows a simplified flow chart that outlines the key steps followed by an outbound datagram.

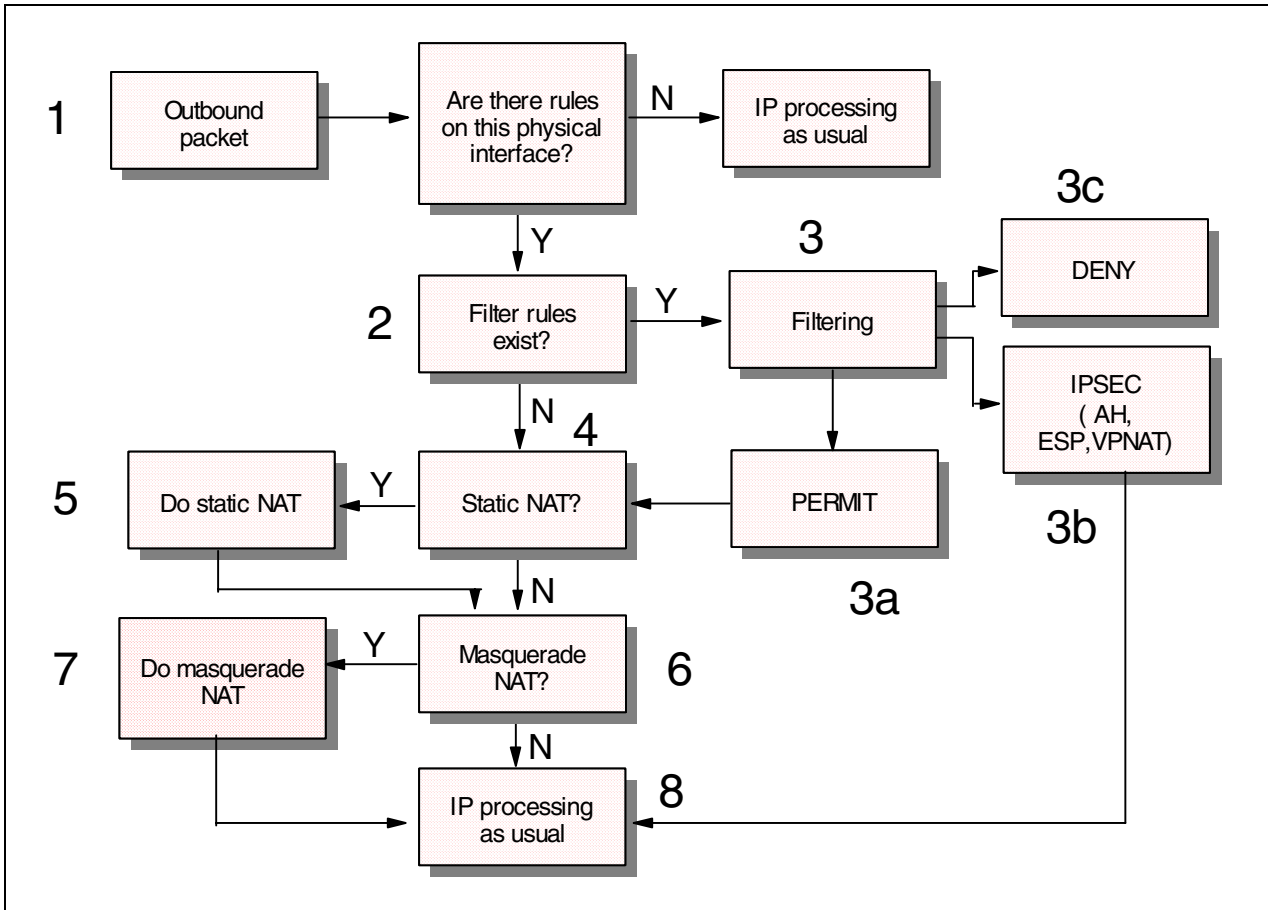


Figure 91. IP filtering and IPsec processing - Outbound datagram

A brief explanation of each step shown in Figure 91 follows:

1. An outbound packet attempts to leave the system through a physical interface. Are there IP filter rules active on this physical interface?
 - (Y) - Go to step 2.
 - (N) - Continue with regular IP processing.
2. Are there filter rules defined?
 - (Y) - Go to step 3.
 - (N) - If there are no IP filter rules, there is no implicit "deny all" rule either. However, there may be NAT rules. Go to step 4.

3. What is the ACTION in the filter rule?
 - a. PERMIT - Go to step 4.
 - b. IPSEC - Perform IPsec processing as defined by the security association, and then go to step 8.
 - c. DENY - If the packet matches a deny rule or does not match one of the rules above, then it is dropped.
4. Does the packet match a static NAT directive within the file?
 - (Y) - Go to step 5.
 - (N) - Go to step 6.
5. Perform the static network address translation. Go to step 6.
6. Does the packet match a masquerade NAT directive within the file?
 - (Y) Go to step 7.
 - (N) The activated file has no directives. Go to step 8.
7. Perform the masquerade network address translation. Go to step 8.
8. Proceed out of the interface.

4.1.4 Network Address Translation (NAT) considerations

Network Address Translation (NAT) was introduced on the AS/400 system in V4R3. NAT allows you to map an IP address specified in IP packets. Because of this, NAT and IPsec do not work together. There are a number of problems that make these two protocols incompatible. NAT changes IP addresses which causes authentication to fail when the datagram is processed by IPsec.

There are other techniques that you can use in situations where NAT applies. Tunneling protocols and Virtual Private Network Network Address Translation (VPN NAT) are examples of the mechanisms that you can use to replace NAT when configuring VPNs.

4.2 Configuring IP packet security

Use the IP Packet Security GUI from Operations Navigator to configure IP filter rules. This section explores the mechanics of creating a filter rules file on the AS/400 system through a simple example. Operations Navigator V4R4 and OS/400 V4R4 VPN support were used to configure the examples in this section.

Figure 92 on page 118 shows the sample network used to illustrate the process of creating filters. The example in this section shows how to configure filters on AS20.

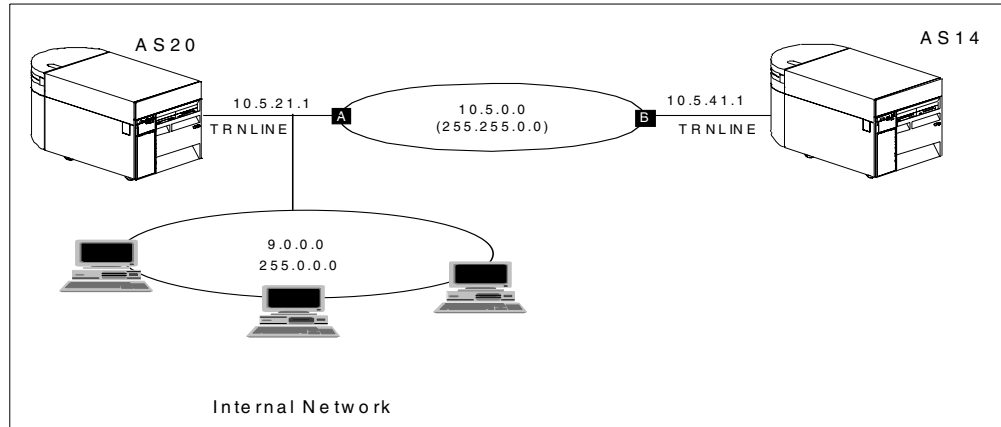


Figure 92. IP filtering configuration - Sample network

The next section shows how to configure on AS20 the filters to meet the following objectives:

- Allow IKE negotiations between AS20 and AS14.
- Add an IPSEC filter rule to process VPN traffic between AS20 and AS14.
- Allow all inbound and outbound traffic with the internal network.

4.2.1 Creating a new filter rules file

On the AS/400 system, the filter rules reside in a filter rules file. You create the file, add and edit the rules, and activate the filter rules using the IP Packet Security GUI in Operations Navigator.

Perform the following steps to create the sample filter rules file:

1. Start Operations Navigator on your desktop.
2. Expand your **AS/400 system** (AS20 in our example)->**Network->IP Security**. IP Packet Security and Virtual Private Networking are displayed on the right panel as shown in Figure 93 on page 119. Note the *Inactive* and *Stopped* status.

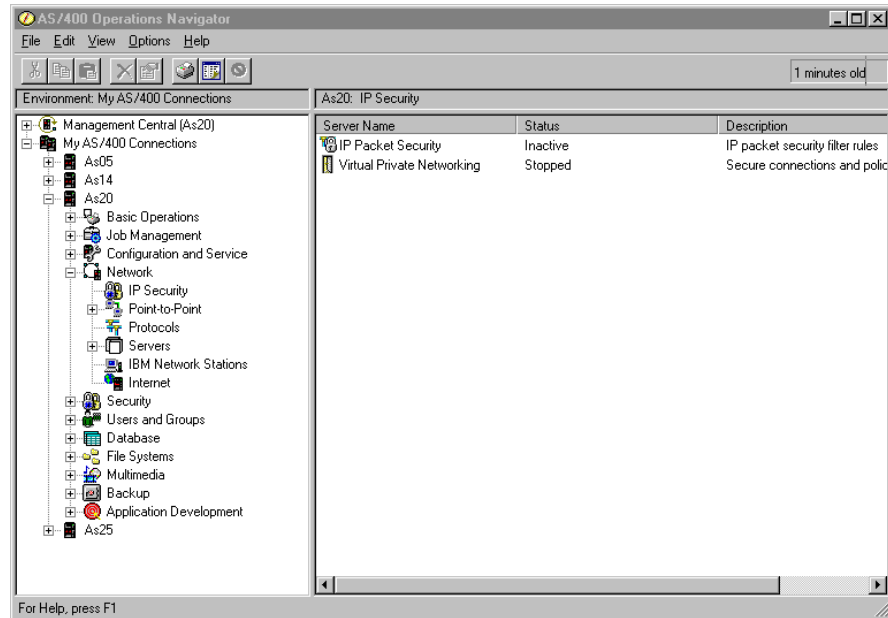


Figure 93. Operations Navigator - IP Packet Security

3. Double-click **IP Packet Security**. The graphical editor that allows you to create filter rules in a new rules file starts, as shown in Figure 94.

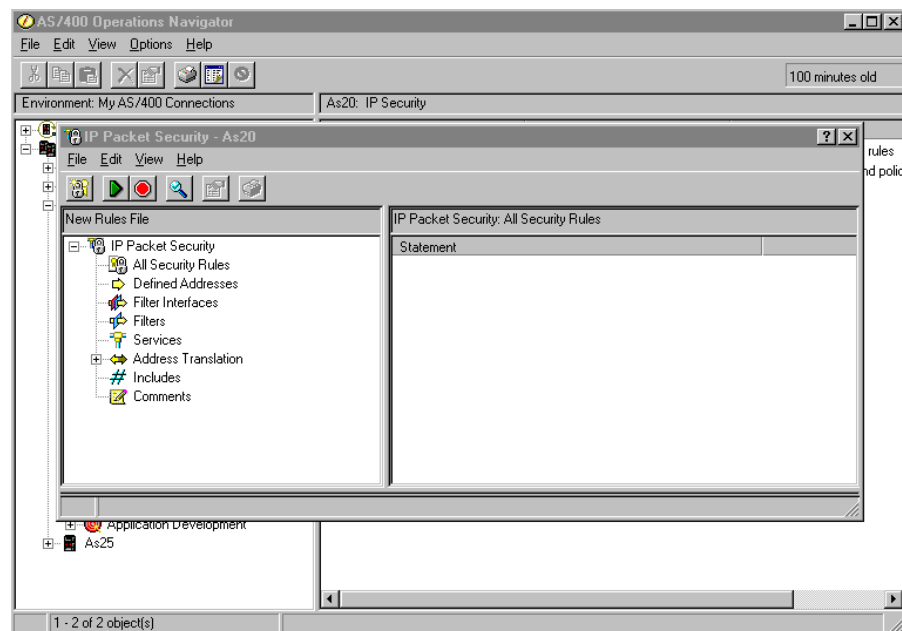


Figure 94. IP Packet Security - New Rules File

4. To add the IKE outbound filter rule, right-click **Filters**, and select **New Filter**. The New Filter - General window shown in Figure 95 on page 120 is displayed.

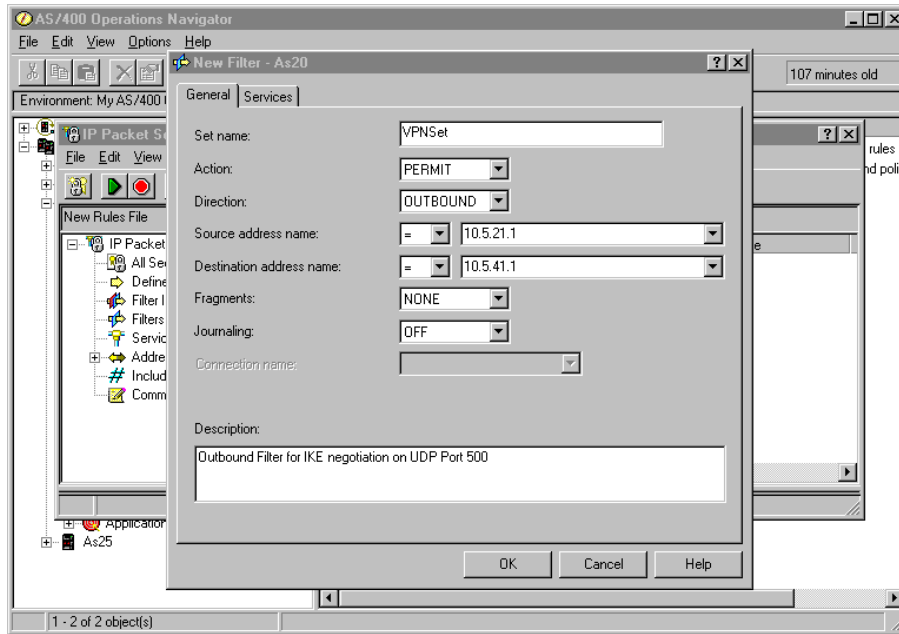


Figure 95. IKE outbound filter rule - General window

5. Complete the New Filter general window by specifying the key servers source and destination IP addresses.
6. Click the **Services** tab. The Services window is displayed as shown in Figure 96.

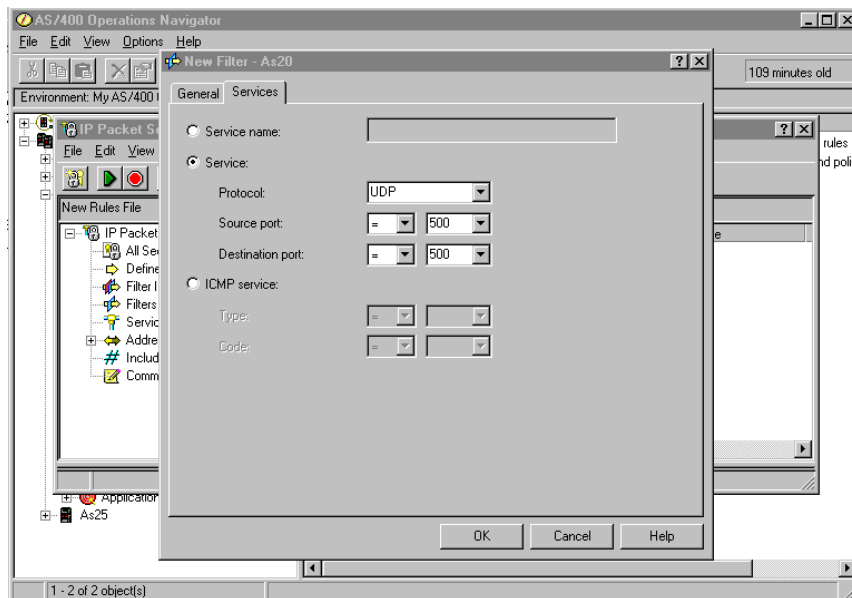


Figure 96. IKE outbound filter rule - Services window

7. In the Services window, specify protocol UDP, source and destination ports 500 to permit outbound IKE.
8. Click **OK**.

9. Create the second filter rule to permit inbound IKE negotiations. Right-click **Filters**, and select **New Filter**.
10. Complete the New Filter - General window as shown in Figure 97.

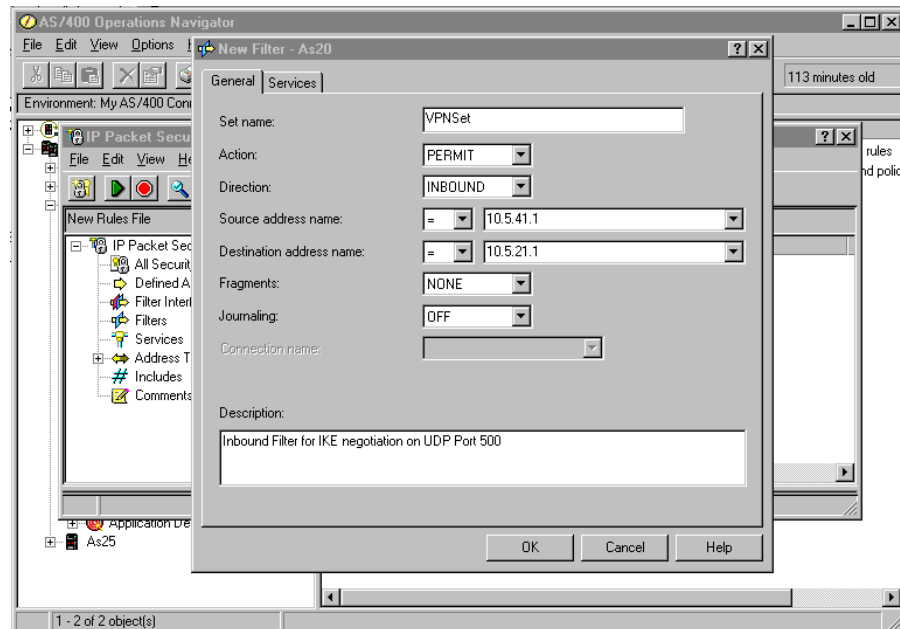


Figure 97. IKE inbound filter rule - General window

11. Click the **Services** tab.
12. Complete the Services page for the IKE inbound filter rule with the same values shown in Figure 96 on page 120.
13. Click **OK**.

Tip

The inbound and outbound filter rules defined for UDP port 500 are used by the IP Security Architecture (IPSec) protocol during the IKE negotiation process. We recommend that you define an explicit address pair for both ends of the VPN connection, as we did in this example. By configuring explicit source and destination addresses, you limit the partners allowed to participate in the IKE negotiation, with the local host decreasing the risk of denial of service attacks. The alternative is to use an asterisk (*) character as a wild card in the Direction, Source and Destination address fields. This approach reduces the number of filter rules needed for IKE negotiation, but does not limit the partners.

14. Create the IPSEC filter rule that will tunnel the datagrams through the VPN connection specified in this rule. All IP packets with the source and destination IP addresses specified in this filter rule will be processed by the VPN server.

The source and destination IP addresses in the IPSEC filter rule are the data endpoints of the connection. The IPSEC filter rule dictates the set or subset of traffic in the connection, and the connection name dictates the data treatment applied to the traffic. In a host-to-host connection, the key server IP addresses and the data endpoints IP addresses are the same.

Right-click **Filters**, and select **New Filter** to define the third and last filter used for the VPN connection as shown in Figure 98.

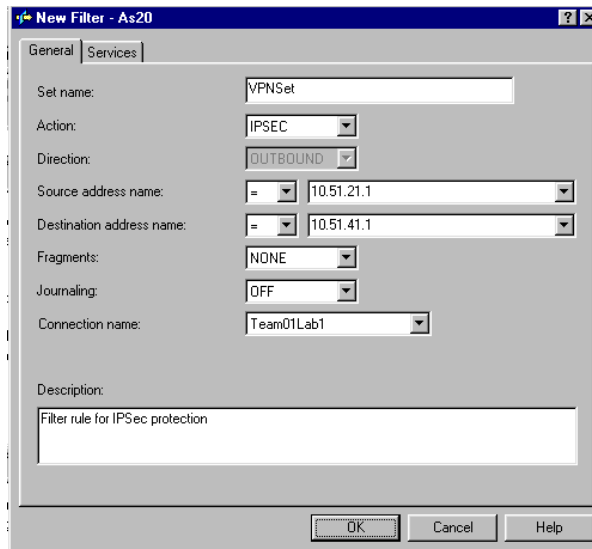


Figure 98. IPSEC filter rule - General window

15. Select Action **IPSEC**. Notice that Direction **OUTBOUND** is automatically selected and greyed out. The corresponding **INBOUND** IPSEC filter rule is implicitly created in the filter rules file.
16. Enter the source and destination data endpoint IP address and select the connection to be associated with this IPSEC filter rule. The connection must be created *before* configuring the filter rule.
17. Click the **Services** tab.
18. Specify the protocol, source, and destination ports for the traffic in this connection. In our example, all protocols and ports are allowed (Figure 99).

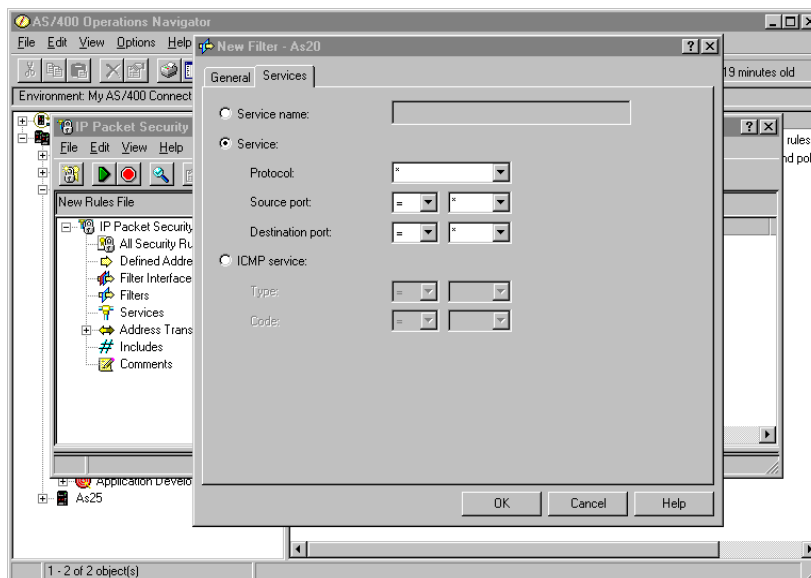


Figure 99. IPSEC filter rule - Services window

19. Click **OK**.

Tip

Place *all* the IPSEC filter rules under all other rules in the file.

An exception to this rule is when you want to tunnel the traffic between some specific data endpoints, while leaving the rest of the traffic unaffected. In this case, configure IPSEC filters to protect the traffic that should be tunneled using one or more VPN connections. Place the IPSEC filter rules under other rules in the file, but add a last rule that permits all general traffic. That is, all traffic not for the VPN connections should work as if no filtering were being done at all. The way to do this is to configure a "permit all" filter and put it last, after the IPSEC filters.

In the following steps, you define a subnet and add a filter rule to permit all traffic from your trusted network. In our example, we enable unrestricted inbound and outbound traffic to and from the internal network (9.0.0.0). For more information, refer to "Defined addresses" on page 106.

20. Define the subnet. Left-click **Defined Addresses**, and select **New Defined Address** (Figure 100).

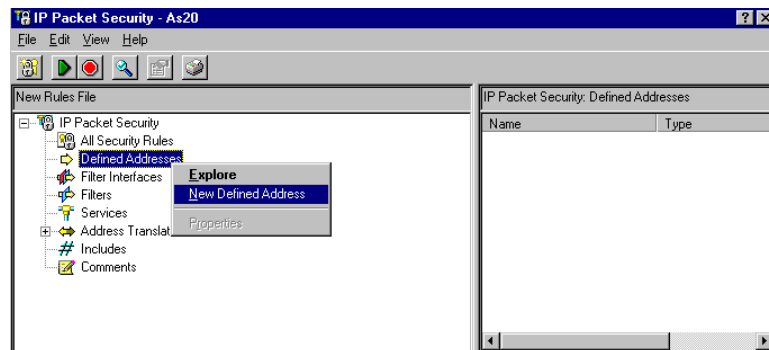


Figure 100. Defined Address - Defining a subnet

21. Enter the required information in the New Defined Address window. The Address name field identifies the subnet you are defining. The IP specification (subnet mask and IP address) defines the set of IP addresses (Figure 101 on page 124).

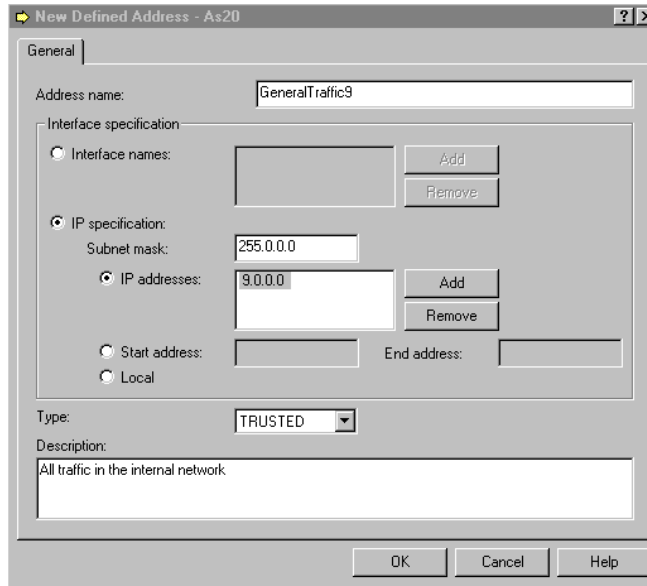


Figure 101. Defined Address - Subnet name and IP definition

22. Click **OK**.

23. Left-click **Filters**, and select **New Filter**.

24. Enter the parameters in the New Filter - General window as shown in Figure 102. Notice the fields Action (**PERMIT**) and Direction (*****), which indicates both **INBOUND** and **OUTBOUND** directions. The source and destination address name are the name of the addresses that you previously defined (**GeneralTraffic9**).

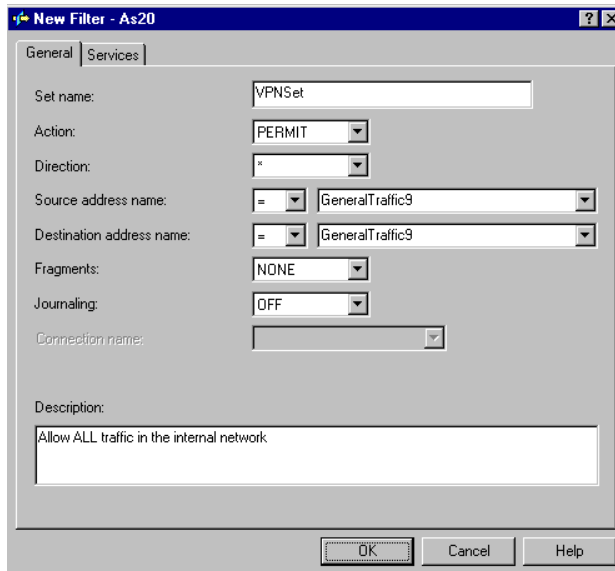


Figure 102. Filter rule to permit all TCP/IP traffic in the internal network (Part 1 of 2)

Tip

The only time a *direction* of both (*) is applicable in a filter rule is when the source and destination IP addresses are the same and the source and destination ports are the same.

25. Click the **Services** tab.

26. To allow all TCP/IP traffic in this subnet, select **Services** and allow all (*) for the Protocol, Source port, and Destination port fields (Figure 103).

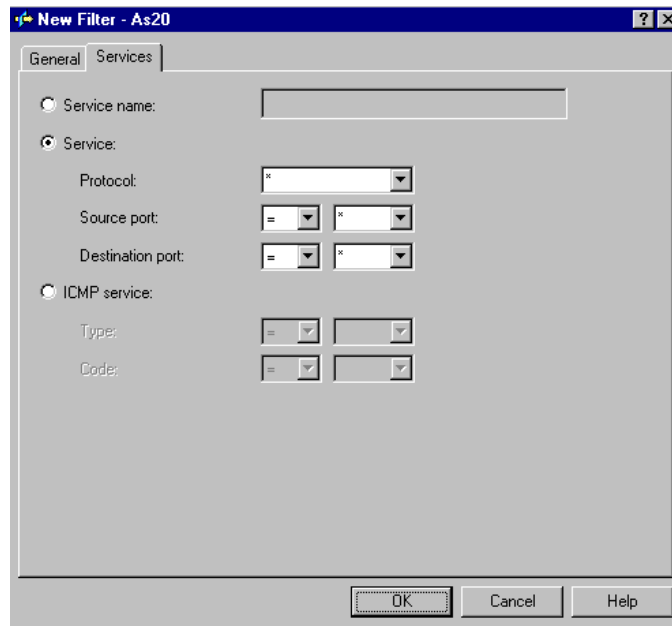


Figure 103. Filter rule to permit all TCP/IP traffic in the internal network (Part 2 of 2)

27. Click **OK**.

28. Move the GeneralTraffic9 filter rule to the top to improve performance when processing filters for traffic in the internal network. You can move rules around by dragging and dropping the rule at the desired position in the file.

Tip

Place the filter rules that most datagrams will match more often at the top of the filter rules file to improve performance.

You must associate the filter rules previously created to a physical interface on the AS/400 system. Refer to "Filter interfaces" on page 106, and to "Set name" on page 107, for more information.

29. Right-click **Filter Interfaces**, and select **New Filter Interface**. The New Filter Interface window is displayed as shown in Figure 104 on page 126.

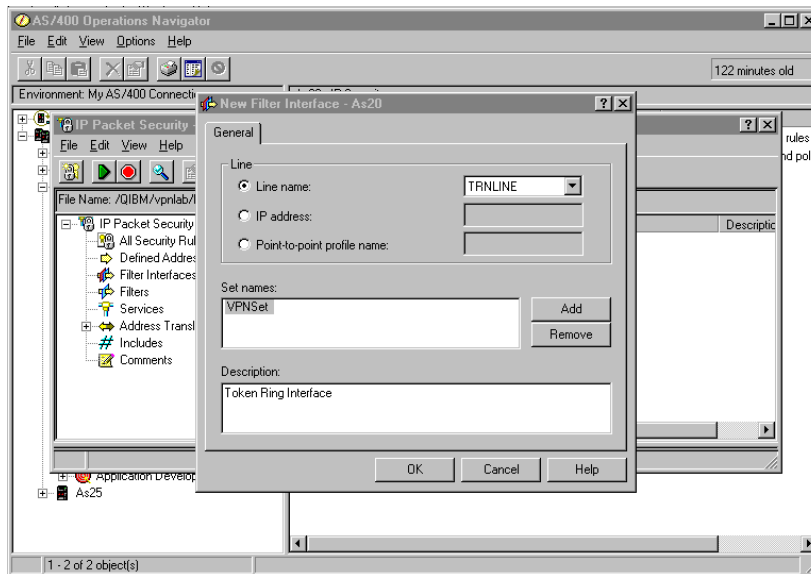


Figure 104. Filter interface

30. Click **Line name**, and select **TRNLINE** from the pull-down menu. This is the name of the line description that is associated with the physical interface to which the filter rules will be associated.
31. Click **Add**, and specify **VPNSet** for the Set name. This is the set name used for each rule in the file.
32. Add a meaningful description.
33. Click **OK**.
34. Click **All Security Rules** to list all the filter rules in the file as shown in Figure 105.

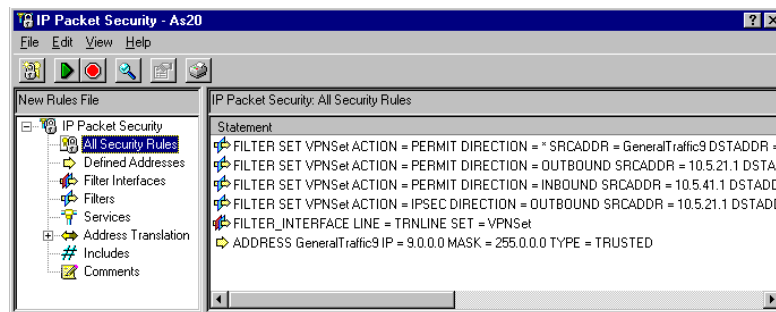


Figure 105. List of all security rules

35. Click **File**, and select **Save As** to save the filter rules in a file in the IFS.

Tip

By default, the Save Rules File As window displays the QIBM directory. *Do not* save your file into the following directory:

/QIBM/UserData/OS400/TCPIP/CONFIGURATION

If you save your file into this directory, and later you need to use the Remove TCP Table (RMVTCPTBL TBL(*ALL)) command to deactivate IP Packet Filtering, all files within the /QIBM/UserData/OS400/TCPIP/CONFIGURATION directory will be deleted.

36. At the Save Rules File As window, select the directory where you want to store the filter rules file, and specify a file name as shown in Figure 106.

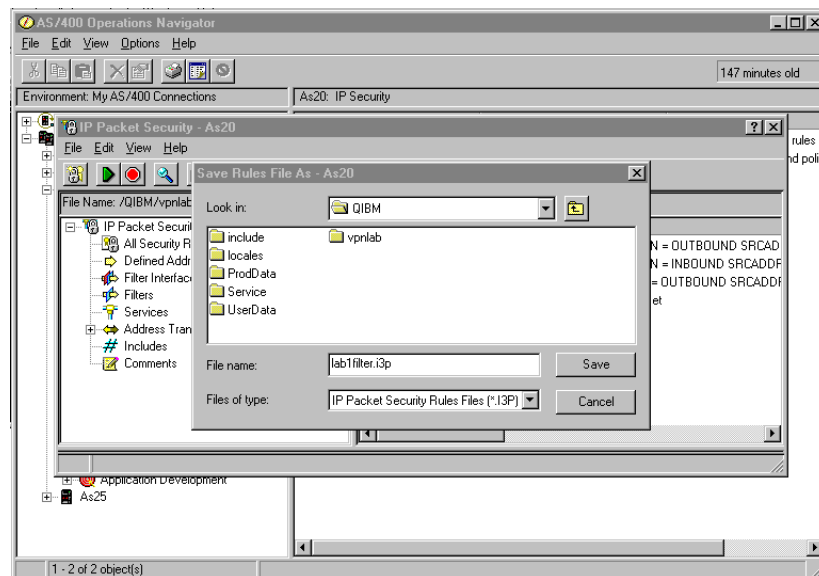


Figure 106. Save Rules File As Window

37. Click **Save**.

38. Click **File**, and select **Activate**. A window appears that asks if you want to verify and activate the filter rules file as shown in Figure 107.

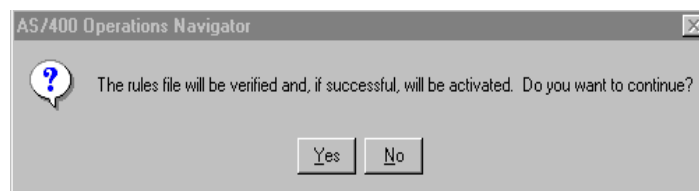


Figure 107. Filter activation

Note: Filters can also be verified without being loaded. This can help isolate problems before actually loading the filter rules file.

39. Click **Yes**.

Once the verification process finishes, the IP Packet Security window displays a message area where you can find information about the verification and activation status (Figure 108).

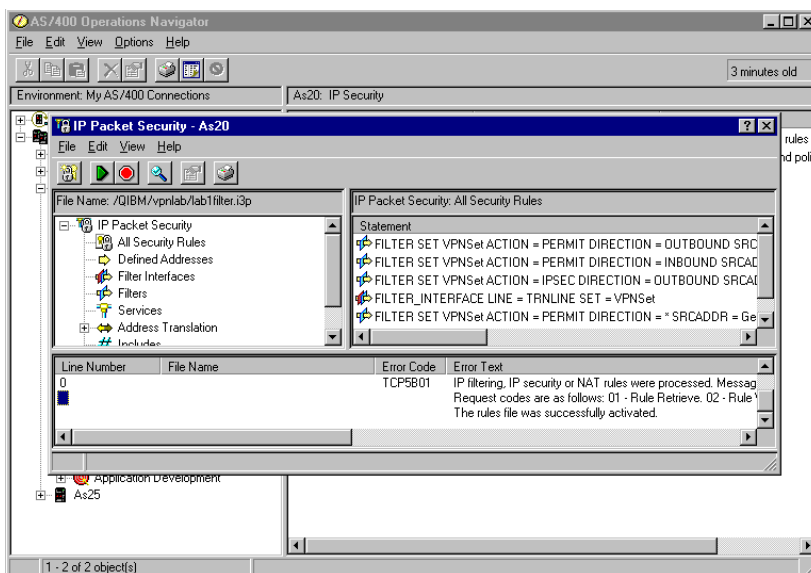


Figure 108. Filter activation status

40. Select **File** from the main menu, and then select **Close** to exit from the IP packet security configuration.

4.2.2 Updating an existing filter rules file

After creating a filter rules file, you may need to add, change, or remove filter rules. To update an existing filter rules file, perform the following steps:

1. From Operations Navigator, expand your AS/400 system, and double-click **Network->IP Security->IP Packet Security**.
2. If the filter rule file that you want to update is active, deactivate the filters by clicking the *stop* icon on the tools bar. Alternatively, click **File->Deactivate**.
3. To open the existing filter rules file that you want to update, click **File->Open**.
4. In the Open Rules File window, select the directory and file as shown in Figure 109.

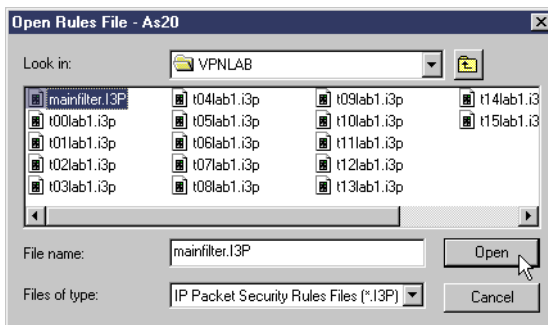


Figure 109. Opening an existing filter rules file

5. Click **Open**.

- The existing rules are displayed. You can edit, move, or delete existing rules or create new ones.

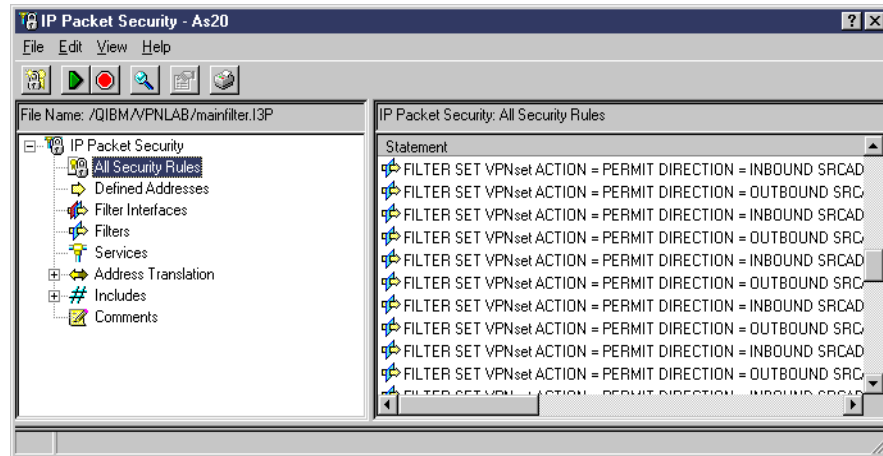


Figure 110. Editing an existing filter rules file

- Once you finish with the changes, click the green *start* icon on the tool bar to verify, save, and activate the filter rules. Alternatively, click **File**, and select **Verify**, **Activate**, **Save**, **Save as...**, or **Close** as appropriate.

4.2.3 Deactivating all active filters: Remove TCP/IP Table

The Remove TCP/IP Table (RMVTCPTBL) command is used to remove (unload) any IP Filter Table, IP Network Address Translation Table, or both, from use.

The purpose of this command is to provide a way to stop IP filters, NAT, or both if you mistakenly activated a filter rules file and can no longer access the AS/400 system with Operations Navigator.

You can submit this command from any command entry screen at a 5250 workstation, including the system console and an SNA Display Station Passthru session. To stop active filter rules, enter the following command:

```
RMVTCPTBL TBL(*All)
```

All filter rules files in the directory `/QIBM/UserData/OS400/TCPIP/CONFIGURATION` are deleted by the `RMVTCPTBL` command.

4.3 Refining the traffic for active connections: Connection granularity

The VPN connection, *dynamic key connection*, or, simply called, *connection*, is a relationship between two IPSec endpoints that protect a specific set of IP traffic between them in a predefined manner, according to each endpoint's security policy. A VPN dynamic key connection is a VPN connection that uses the Internet Key Exchange protocol (IKE) to periodically refresh keying material.

Dynamic key connections are created from *dynamic key (connection) groups*, which are user-specified objects that are associated one-to-one with a user-specified filter rule when that filter rule's action is IPSEC. This filter rule is called an *anchor filter rule* or a *policy filter*. All connections created from a specific dynamic key group have the same security policy.

One or more connections can be created from a single dynamic key group, depending on that group's *connection granularity*. Connection granularity defines the subset of the IP traffic that is associated with this dynamic key group and will be associated with each connection created from this dynamic key group.

Perhaps an analogy can help to explain this concept. A dynamic key connection group is like a pie. The pieces of that pie are individual VPN connections. Note that all connections fit within the pie after which they are named. The next question is how to cut the pieces: How many pieces shall we allow? What shapes? etc. The answers to these questions concern *granularity*. The VPN policy filter (action IPSEC) defines the pie.

The Policy window in a dynamic key (connection) group that allows you to specify a set of parameters that define the traffic for active connections. In our analogy, it allows you to cut the pie into pieces.

Using these parameters, you can define the following characteristics for the traffic in the connection:

- Local addresses
- Local ports
- Remote addresses
- Remote ports
- Protocol

Connection granularity is the definition of the traffic in the connection through the configuration of the parameters listed above.

The policy filter rule, that is, the IP filter rule with action = IPSEC, always controls the "maximum" traffic within the VPN connection. Connection granularity then defines, for each connection associated with a connection group, how much of that "maximum" traffic is allowed.

The possible values for each parameter are:

- Filter rule
- Connection
- Single value from connection

For example, say you only wanted to allow one large piece of pie that exactly fills the plate. With no subdividing at all, the pie = the piece, no cutting of this pie. This is achieved by setting values in the Policy parameters to Filter rule. That is, the connections that can be started must have exactly the same values as in the policy filter (IPSEC filter). In this case, only one connection can start (the pie = the piece).

In another example, you want to allow each IP address in a range to have its own VPN connection. In the analogy, this corresponds to allowing a fixed known number of pie pieces, each one very small. This is done by setting, for example, the granularity value to *Single value from connection*.

The third granularity value, Connection, corresponds to allowing pieces of varying sizes. The number that actually fits depends on how large the previous cut pieces were. Clearly, if the first piece is half of the pie, the second piece cannot be two-thirds of it.

The following sections explain how to configure the parameters that define the connection's traffic. We also explore how to limit the services in an active connection based on the definition of its traffic.

4.3.1 Connection initiator and responder

Before we describe the parameters in the Policy window, we need to define the role of the *connection initiator* and *connection responder*:

Connection initiator

The connection initiator is the system that starts the connection. The initiator proposes that the IPsec transforms be used. It also proposes the data endpoints (local and remote IP addresses) and services (protocols and local and remote ports) that can use the connection.

Connection responder

The connection responder accepts or rejects the initiator's proposal.

You can specify which system is allowed to initiate the connection by configuring the General window - Initiation section in the dynamic key connection group. To display or change the Initiation values, follow these steps:

1. Right-click the dynamic key connection group, and select **Properties** as shown in Figure 111.

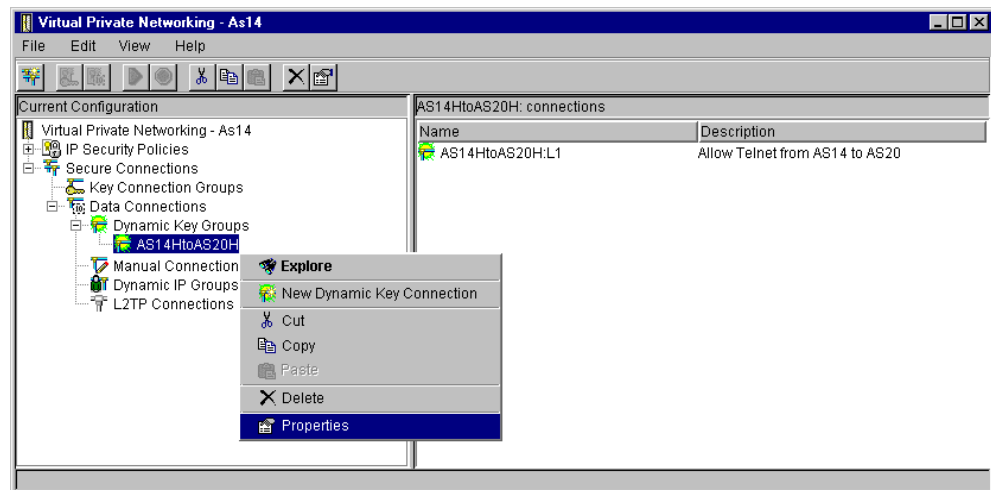


Figure 111. Dynamic key connection group - Properties

2. Specify which system can initiate the connection in the Initiation section as shown in Figure 112 on page 132.

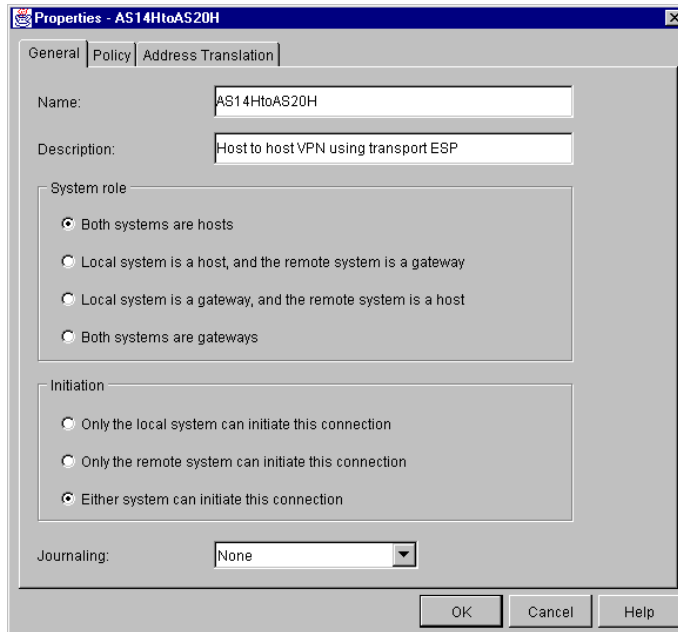


Figure 112. Dynamic key connection group - Initiation values

Tip

In Dynamic IP Groups VPNs, the AS/400 system is always the responder. In L2TP Connections VPNs, the AS/400 system is always the initiator.

When an AS/400 system performs the responder role, you must have a Dynamic Key Group, but you do not need to configure a dynamic key connection as shown in Figure 113.

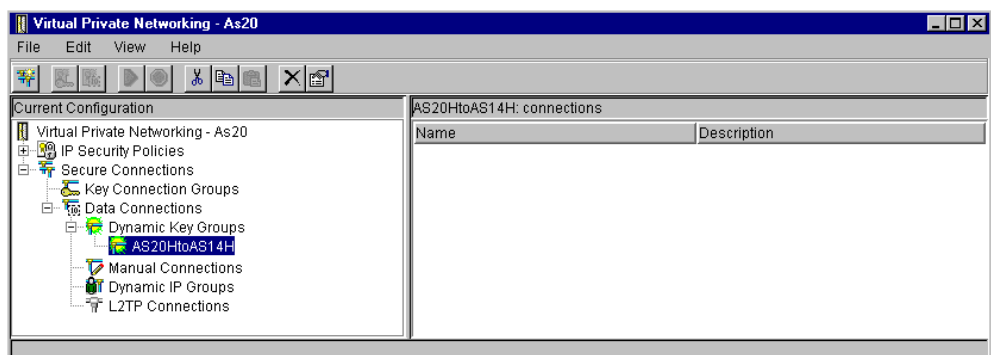


Figure 113. No dynamic key connection configuration on the responder

The Active Connections window on the AS/400 system that acts as a responder shows the name of the dynamic key connection group followed by :R1, :R2, etc. as shown in Figure 114 on page 133.

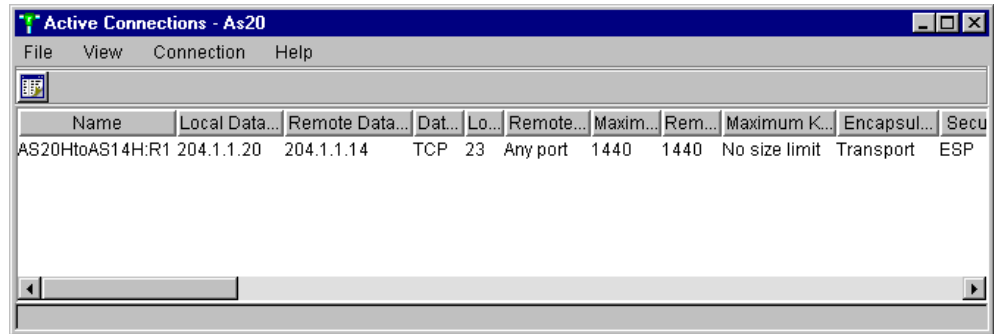


Figure 114. Active Connections window on the responder AS/400 system

Note that if you configure the VPN on the *responder* AS/400 system using the New Connection wizard, the wizard configures a dynamic key connection by default. In this case, unless you explicitly delete the dynamic key connection created by the wizard, the responder uses the existing connection name in the Active Connection window when a matching connection is initiated remotely. In this case, the naming convention is the connection name followed by :L1, :L2, etc.

On the initiator, the Active Connection window shows the dynamic key connection name followed by :L1, :L2, etc.

Tip

If you configured a dynamic key connection on your system and a connection is either initiated from or responded to that matches the dynamic key connection's local and remote address and services, the connection name will be whatever that dynamic key connection name is. It will also have a dynamic-key-connection-group:L1, :L2, etc. identifier. Otherwise, the connection name will be dynamic-key-connection-group:R1, :R2 etc. A manual connection will always have a manual-connection-name:L999999.

4.3.2 Configuring the traffic for active connections parameters

The parameters in the Policy window of a dynamic key connection group, dynamic IP groups, and L2TP connections allow you to define the traffic in the active connections. Figure 115 on page 134 shows the parameters in the Policy window.

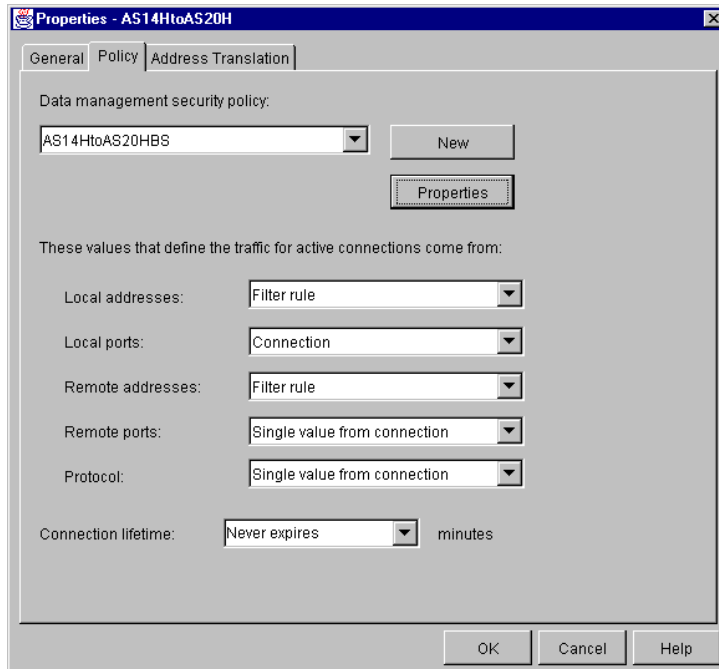


Figure 115. Policy page

For each parameter, you can specify one of the following three options:

- **Filter rule:** The value for the parameter is defined in the IPSEC filter rule which is associated with this connection group.
- **Connection:** The value for this parameter is defined in the dynamic key connection if this system is the connection initiator. If this system is the responder, the value proposed by the initiator will be accepted within the limits of the responder's IPSEC filter rule associated with this connection group. When you specify *Connection* for a parameter in the Policy window, the corresponding values in the connection configuration must be:
 - *Local Addresses:* Single IP address, subnet or range
 - *Remote Addresses:* Single IP address, subnet or range
 - *Local port:* Any port, or single port value
 - *Remote port:* Any port, or single port value
 - *Protocol:* Any protocol, or single protocol value
- **Single value from connection:** The value for this parameter is defined in the dynamic key connection if this system is the connection initiator. If this system is the responder, the value proposed by the initiator will be accepted within the limits of the responder's IPSEC filter rule associated with this connection group. The only difference between *Connection* and *Single value from connection* is that *Single value from connection* additionally restricts the value to be a single address, port, or protocol. When you specify *Single value from connection* for a parameter in the Policy window, the corresponding values in the connection configuration must be:
 - *Local Addresses:* Single Version 4 IP address
 - *Remote Addresses:* Single Version 4 IP address
 - *Local port:* Single port value
 - *Remote port:* Single port value
 - *Protocol:* UDP or TCP

Note

The IPSEC filter rule associated with the connection group on the initiator and the responder defines the outer boundaries of the policy. In other words, specifying Connection or Single value from connection for a parameter in the Policy page must always translate to the same value or a subset of the values allowed by the IPSEC filter rule.

4.4 Restricting services in VPN connections

You can use the parameters in the Policy window to limit the services allowed in the VPN connection. This section includes scenarios to illustrate the following configurations:

- Allow only Telnet in one direction between two hosts. Restrict traffic by the IPSEC filter configuration.
- Allow only Telnet in one direction between two hosts. Restrict traffic by the dynamic key connection configuration.
- Allow only Telnet in both directions between two hosts. Restrict traffic by the dynamic key connection configuration.
- Allow normal FTP in one direction between two hosts in addition to Telnet.

4.4.1 Scenarios network configuration

Figure 116 shows the simple network used for the scenarios in this section. A host-to-host VPN is configured between AS14 and AS20. The scenarios show how to limit services in the VPN between the two systems.

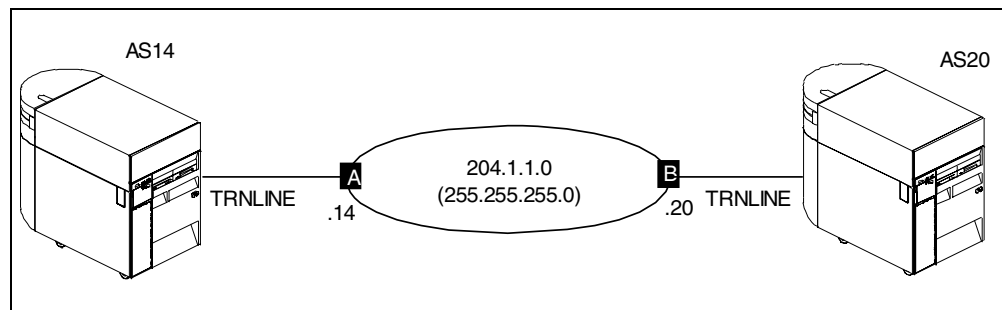


Figure 116. Host-to-host network configuration

4.4.2 Scenario 1: Restricting services to Telnet-only by IPSEC filter

The objectives of this scenario are:

- The VPN connection between the systems may only be started by AS14.
- Telnet from AS14 (Telnet client) to AS20 (Telnet server) is the only service allowed in the VPN.
- Restrict services by IPSEC filter configuration.

4.4.2.1 Scenario configuration

To configure the VPN to meet the scenario objectives, perform the following steps:

1. Configure the VPN on AS14 using the New Connection wizard. Figure 117 shows the wizard configuration summary on AS14.

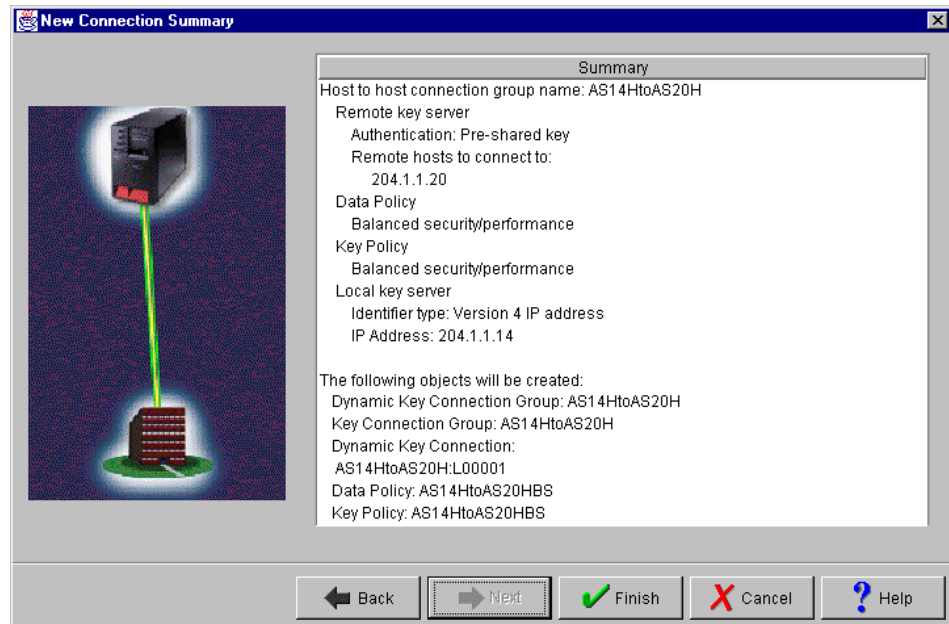


Figure 117. Host-to-host configuration summary on AS14

2. Configure the VPN on AS20 using the New Connection wizard. Figure 118 shows the wizard configuration summary on AS20.

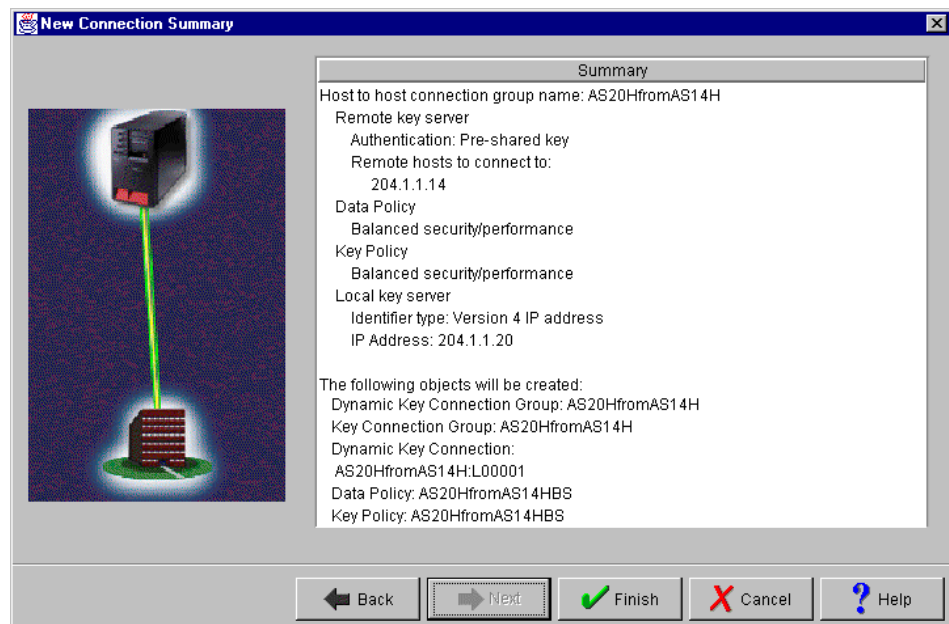


Figure 118. Host-to-host configuration summary on AS20

3. Change the Initiation parameter configured by the wizard on AS14 to restrict the connection initiation to AS14 only. Right-click the key connection group **AS14HtoAS20H** created by the wizard, and select **Properties**.
4. In the general window, select **Only the local system can initiate this connection** as shown in Figure 119.

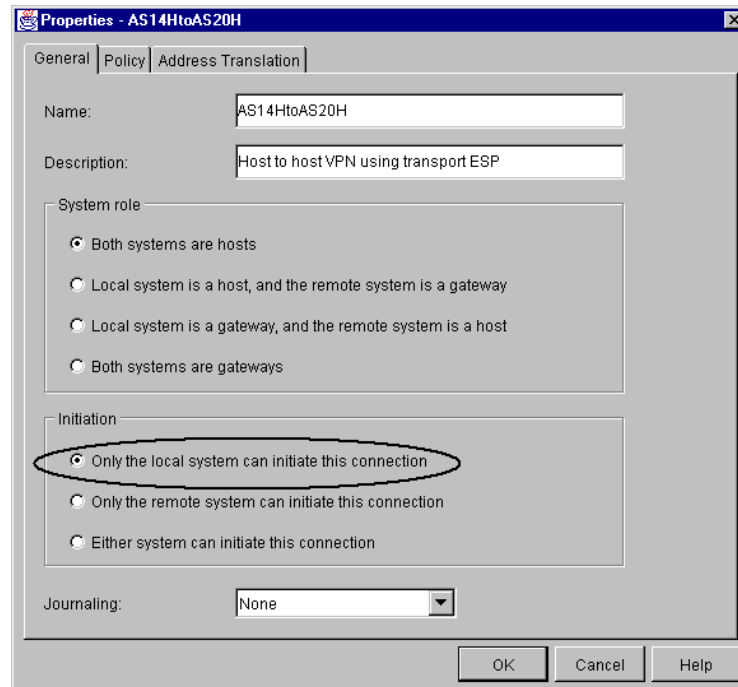


Figure 119. Configuring AS14 as an initiator only

5. Click **OK** to save the value.
6. Change the Initiation parameter configured by the wizard on AS20 to restrict the connection initiation to AS14 only. In other words, configure AS20 as a responder only. Right-click the key connection group **AS20HfromAS14H** created by the wizard, and select **Properties**.
7. In the general window, select **Only the remote system can initiate this connection** as shown in Figure 120 on page 138.

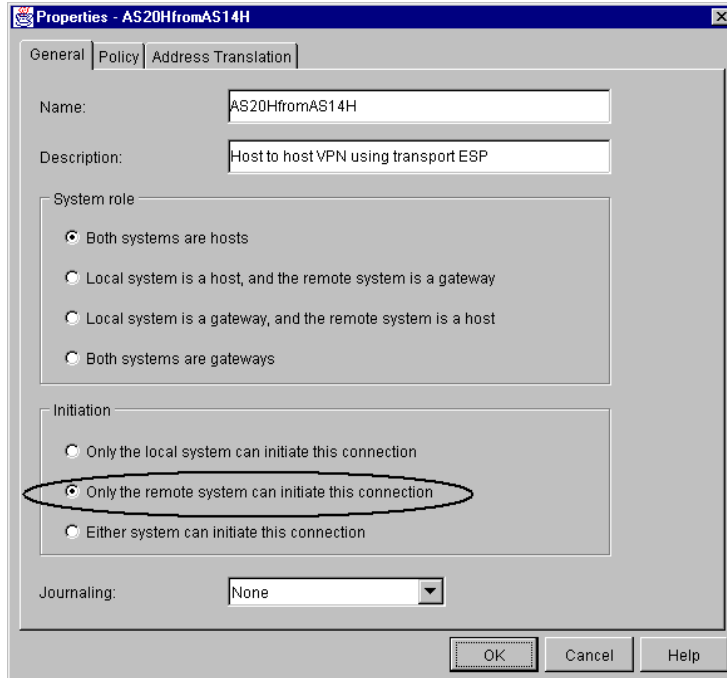


Figure 120. Configuring AS20 as a responder only

8. The wizard configured the Policy page values on AS14 that define the traffic for active connections as shown in Figure 121.

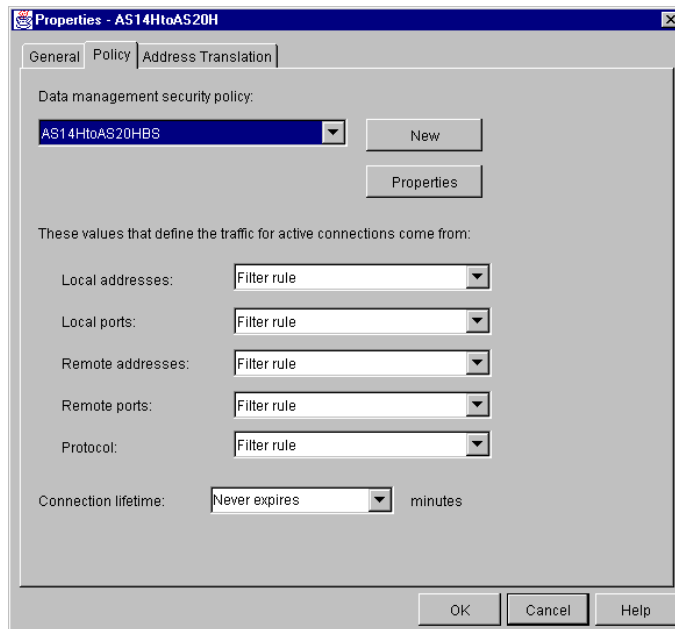


Figure 121. Policy page on AS14 - Connection traffic defined by IPSEC filter rule

9. The IPSEC filter rule on AS14 is defined as shown in Figure 122 on page 139.

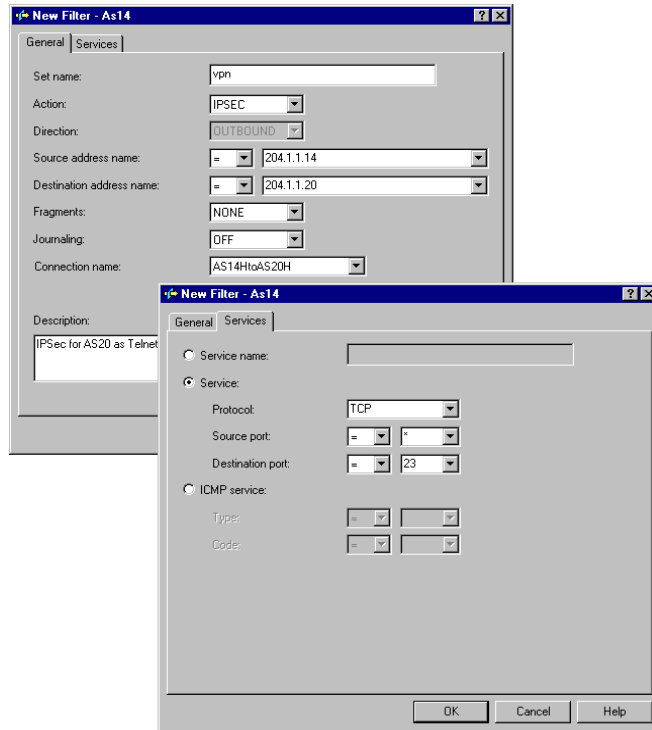


Figure 122. AS14 IPSEC filter rule restricts traffic to Telnet only from AS14 to AS20

Notice that the IPSEC filter rule on AS14 limits the protocol to TCP, local port to any port (the client Telnet on AS14 will use a port greater than 1023), and remote port to 23 (Telnet server on AS20).

10. The wizard configured the Policy page values on AS20 that define the traffic for active connections as shown in Figure 123.

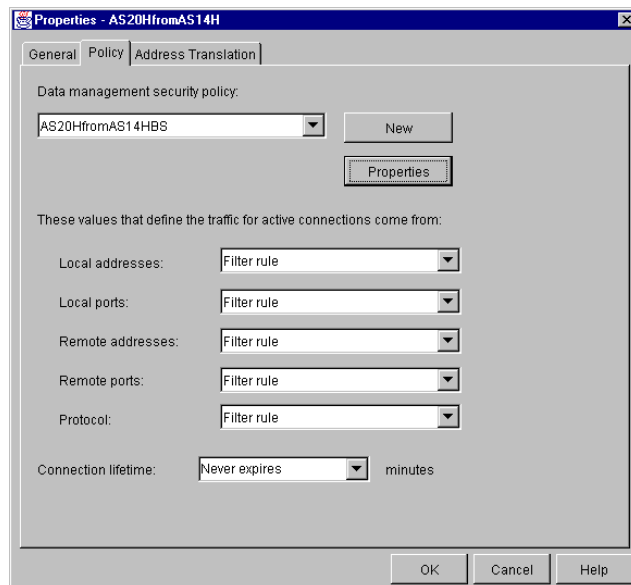


Figure 123. Policy page on AS20 - Connection traffic defined by IPSEC filter rule

11. The IPSEC filter rule on AS20 is defined as shown in Figure 124 on page 140.

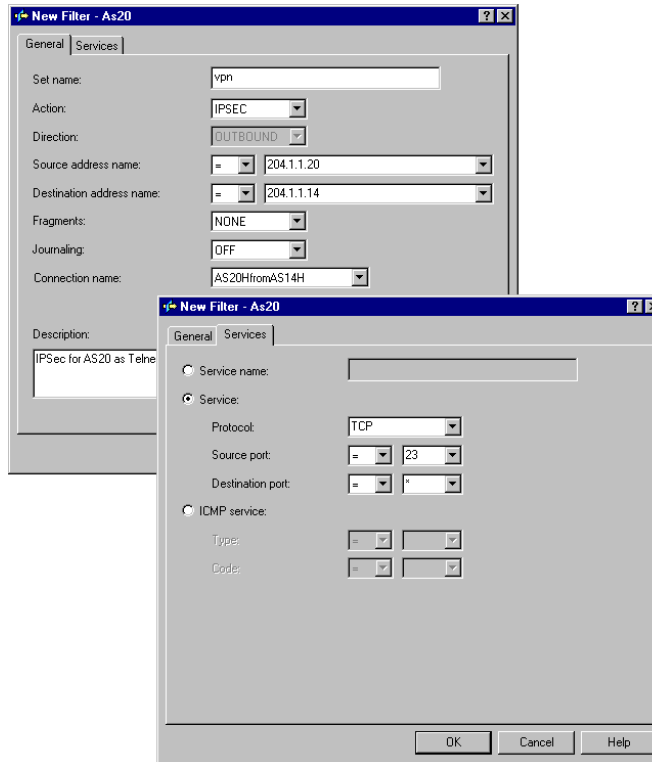


Figure 124. AS20 IPSEC filter rule restricts traffic to Telnet only from AS14 to AS20

4.4.2.2 Verification tests

Table 9 shows a summary of the verification tests run in the host-to-host VPN connection in this scenario.

Table 9. Limiting traffic to Telnet only from AS14 to AS20 by IPSEC filter configuration

Direction	Start connection	Telnet	FTP	PING
From AS14 to AS20	YES	YES	NO	NO
From AS20 to AS14	NO	NO	NO	NO

Figure 125 shows the Active Connections window on AS20.

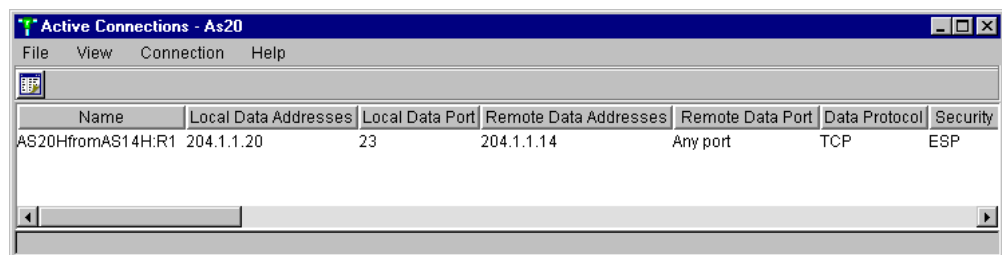


Figure 125. Active connections window on AS20 after successful start of VPN

4.4.3 Scenario 2: Restricting services to Telnet-only by connection

This section presents the same scenario described in 4.4.2, “Scenario 1: Restricting services to Telnet-only by IPSEC filter” on page 135. Here, we

describe the implementation that limits the services by configuring the appropriate values on the VPN connection. The objectives of this scenario are:

- The VPN connection between the systems may only be started by AS14.
- Telnet from AS14 (Telnet client) to AS20 (Telnet server) is the only service allowed in the VPN.
- Restrict services by the connection configuration.

4.4.3.1 Scenario configuration

To configure the VPN to meet the scenario objectives, perform the following steps:

1. Repeat step 1 on page 136 through step 7 on page 137 to configure the VPN connection on AS14 and AS20 using the New Connection Wizard. You will also change the Initiation parameters to restrict the initiation of the VPN to AS14.
2. On AS14 (connection initiator), change the values that define the traffic for active connections in the Policy page of the dynamic key connection group (AS14HtoAS20H) as shown in Figure 126.

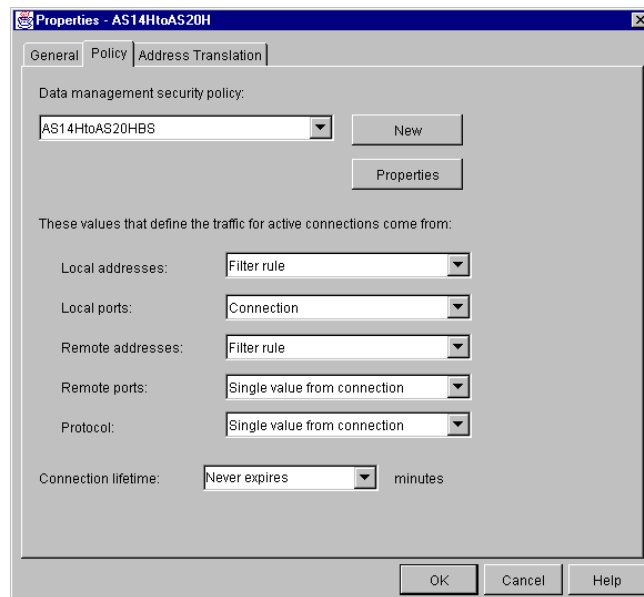


Figure 126. AS14 Policy window - Restricting services by connection configuration

The following list explains the value of the parameters shown in Figure 126:

- **Local Addresses - Filter rule:** The IP addresses for the local data endpoint is defined in the IPSEC filter rule associated with this dynamic key connection group.
- **Local ports - Connection:** The local ports are defined in the connection configuration. The VPN server accepts anything the connection offers within the limits of the associated IPSEC filter rule.
- **Remote Addresses - Filter rule:** The IP addresses for the remote data endpoint is defined in the IPSEC filter rule associated with this dynamic key connection group.

- **Remote ports - Single value from connection:** The remote ports are defined in the connection configuration. It must be a single port number.
 - **Protocol - Single value from connection:** The protocol is defined in the connection configuration. It must be a single protocol, for example TCP.
3. Right-click the dynamic key connection under the dynamic key connection group (AS14HtoAS20H:L1 in this scenario), and select **Properties**.
 4. Click the **Services** tab.
 5. Fill in the parameters in the Services window as shown in Figure 127.

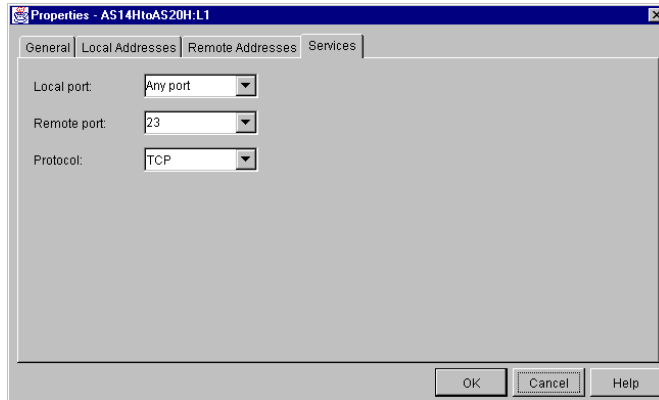


Figure 127. Dynamic key connection service window for AS14HtoAS20H:L1

The values for the parameters in the dynamic key connection group Policy window (Figure 126 on page 141) that specify Connection or Single value from connection are defined here. Notice that when Connection is specified, the value is Any. When Single value from connection is specified in the Policy window, the value is an explicit single port or protocol number.

6. On AS14, configure the IPSEC filter rule associated with this connection as shown in Figure 128 on page 143.

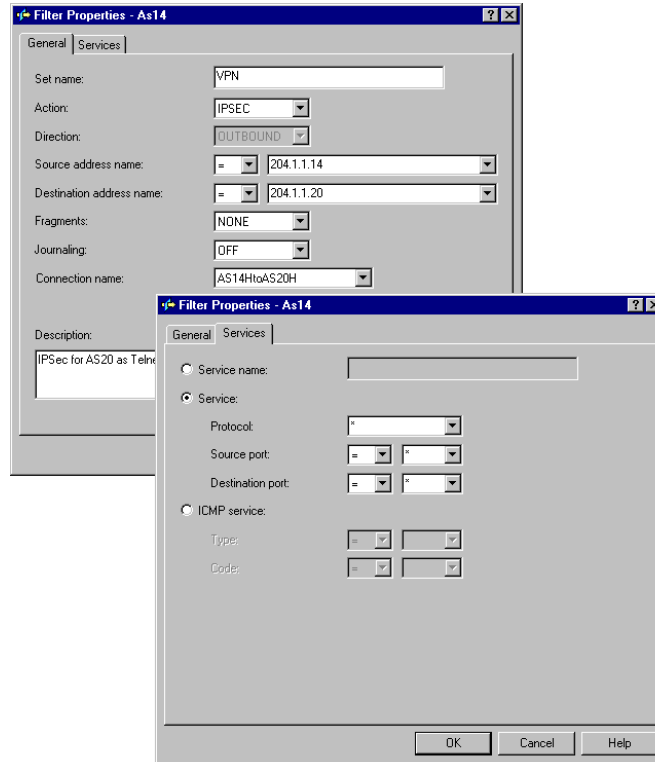


Figure 128. AS14 IPSEC filter rule defines data endpoints - Services restricted by connection

The IPSEC filter rule on AS14 defines the IP addresses for the data endpoints in the general window. The Services window has been changed to allow all protocols and ports since the services restrictions are configured in the connection.

7. On AS20, use the same configuration as in 4.4.2, “Scenario 1: Restricting services to Telnet-only by IPSEC filter” on page 135. See Figure 123 and Figure 124 on page 140.

Since AS20 is the responder, changing the values in the Policy window to Connection or Single value from connection and opening the services in the IPSEC filter rule to ALL (wildcard (*)) means that the responder will accept what the initiator proposes. For the responder to enforce the services that the local system can provide over the VPN, it must configure the protocol and ports in the IPSEC filter rule associated with the connection.

If you allowed all services in the IPSEC filter rule on the responder, AS20, the most you could do to restrict traffic is to define Single value from connection in the policy page of the dynamic key connection group. This restricts the initiator in that it can only request a single service, but it can choose whichever single service it wants. Also, the initiator can define an additional VPN connection to request another single service and the responder would accept it.

4.4.3.2 Verification tests

Table 10 shows a summary of the verification tests run in the host-to-host VPN connection in this scenario.

Table 10. Limiting traffic to Telnet only from AS14 to AS20 by the connection configuration

Direction	Start connection	Telnet	FTP	PING
From AS14 to AS20	YES	YES	NO	NO
From AS20 to AS14	NO	NO	NO	NO

4.4.4 Scenario 3: Allowing Telnet only in both directions

The objective of this scenario is to configure the VPN to allow Telnet in both directions. No other service is allowed in the VPN. In this scenario, each system runs Telnet clients and a Telnet server.

4.4.4.1 Scenario configuration

At first glance, it seems possible to implement this scenario by configuring a second dynamic key connection under the same dynamic key connection group to mirror the connection configuration in 4.4.2, “Scenario 1: Restricting services to Telnet-only by IPSEC filter” on page 135, or 4.4.3, “Scenario 2: Restricting services to Telnet-only by connection” on page 140.

However, two connections with the same characteristics (but swapping local and remote addresses and ports) creates a condition known as *overlap*. If both VPN connections were active and an IP datagram specified both local and remote port 23, it would not be possible to determine through which connection that datagram should be routed. Notice that port 23 is included in port Any. Therefore, even when unlikely, this is a possible situation. The AS/400 system VPN connection manager job audits this condition and fails to start the second connection.

Figure 129 shows the error message in the QTOVMAN job log when you attempt to start a connection that produces an overlap condition.

```
Message ID. . . . : TCP8604
Message . . . . . : VPN connection AS14HtoAS20H:L2 failed an audit.
Cause . . . . . : The audit that failed was 100. CONNECTION OVERLAPS WITH
EXISTING CONNECTION. There are several audits that may fail. Some likely
```

Figure 129. Overlap error message

AS14 configuration

In the previous scenarios, AS14 was the Telnet client and the VPN connection was configured accordingly. In this scenario, we add a connection to accept Telnet requests on AS14’s Telnet server.

To configure AS14 to allow Telnet requests on port 23 over a VPN connection, create the following objects:

- Dynamic key connection group
- Dynamic key connection
- IPSEC filter rule

The key policy, data policy, and key connection group configured in the previous scenarios can be used here. Therefore, there is no need to configure those objects again.

To configure AS14 for this scenario, perform the following steps:

1. On the Virtual Private Networking window, right-click **Dynamic Key Groups**, and select **New Dynamic Key Connection Group**.

Figure 130 shows the configuration details for the new dynamic key connection group on AS14.

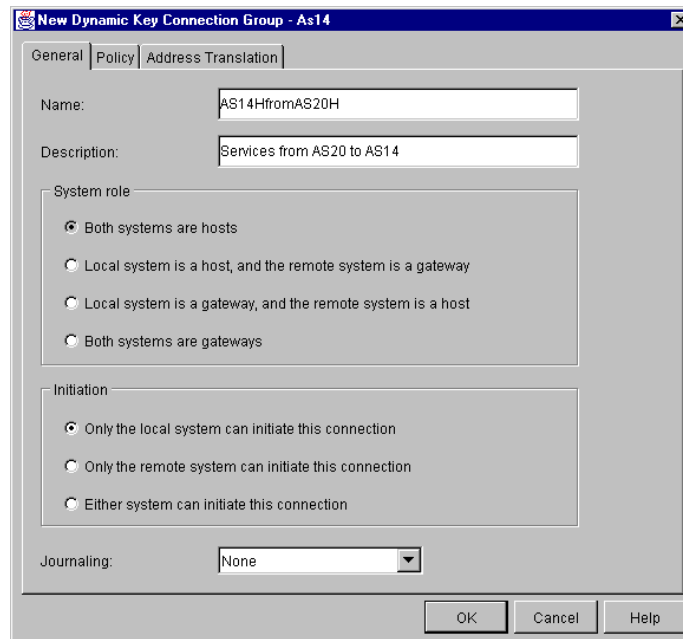


Figure 130. New Dynamic Key Connection group to allow Telnet requests from AS20

2. Click the **Policy** tab.
3. Configure the parameters that define the traffic in the connection as shown in Figure 131.

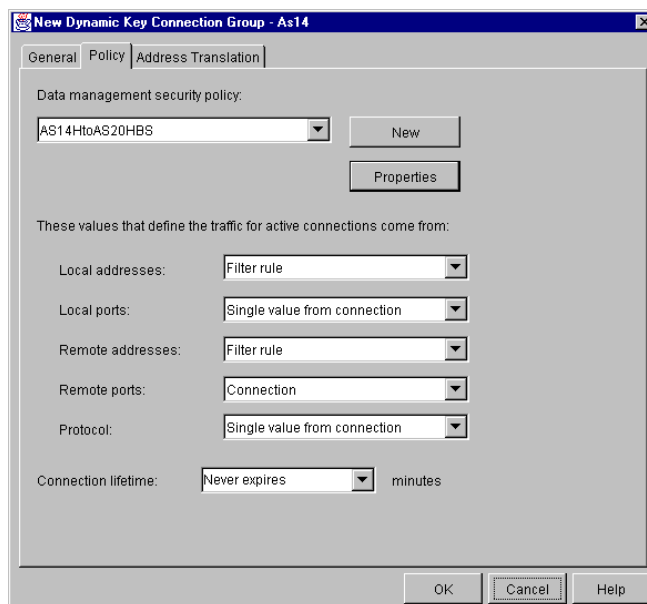


Figure 131. AS14 Policy window configured to allow Telnet client requests from AS20

4. Configure the dynamic key connection associated with the dynamic key connection group configured above. Right-click the dynamic key connection group (AS14HfromAS20H), and select **New dynamic key connection**. The New Dynamic Key Connection window shown in Figure 132 is displayed.

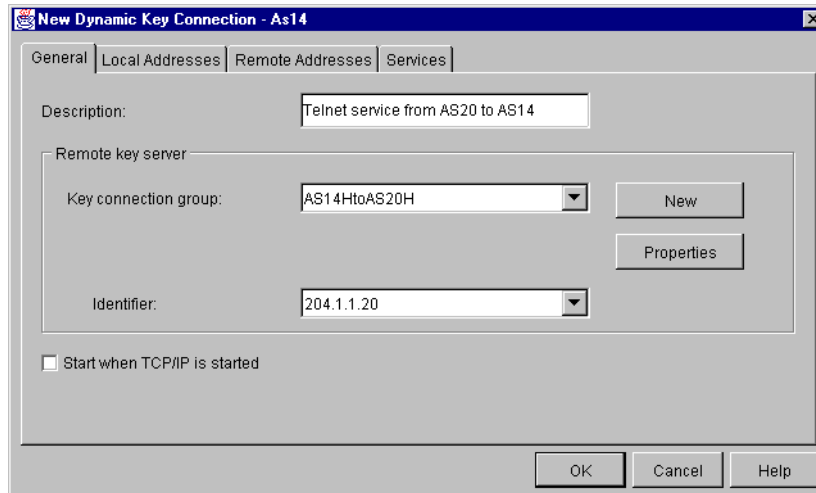


Figure 132. AS14 New Dynamic Key Connection configuration

5. Select the Key connection group **AS14HtoAS20H**, which was configured by the wizard in 4.4.2, “Scenario 1: Restricting services to Telnet-only by IPSEC filter” on page 135.
6. Click the **Local Addresses** tab, and enter the local data endpoint IP address as shown in Figure 133 on page 147.
7. Click the **Remote Addresses** tab, and enter the remote data endpoint IP address as shown in Figure 133 on page 147.

Note: The local and remote addresses that will be able to use this connection are defined in the IPSEC filter rule as it was specified in the Policy window (see Figure 131 on page 145). However, the VPN configuration GUI requires you to fill in these fields when you configure a new connection.

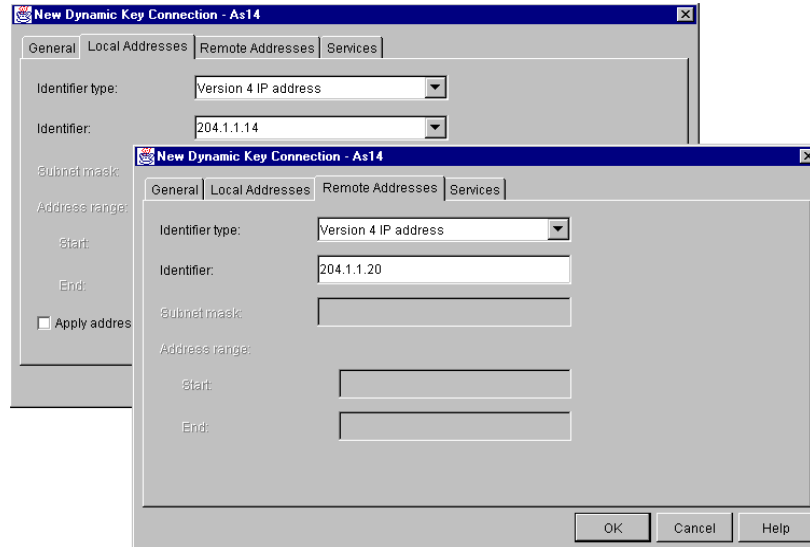


Figure 133. AS14 New Dynamic Key Connection - Local and remote address

8. Click the **Services** tab.
9. Configure the services that allow you to receive Telnet requests over this VPN connection:
 - Local port: 23
 - Remote port: Any (Telnet client port greater than 1023)
 - Protocol: TCP

Figure 134 shows the services window with the values required for this scenario. Compare these values to the dynamic key connection group policy configuration on Figure 131 on page 145.

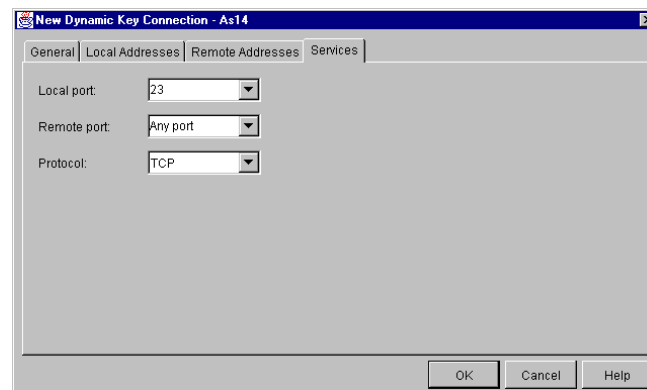


Figure 134. AS14 New Dynamic Key Connection Services window

10. Configure the IPSEC filter rule associated with the new dynamic key connection group. Notice that there is a one-to-one relationship between the IPSEC rule and the dynamic key connection group. Therefore, you must create a new IPSEC filter rule that processes the traffic for this connection as shown in Figure 135 on page 148.

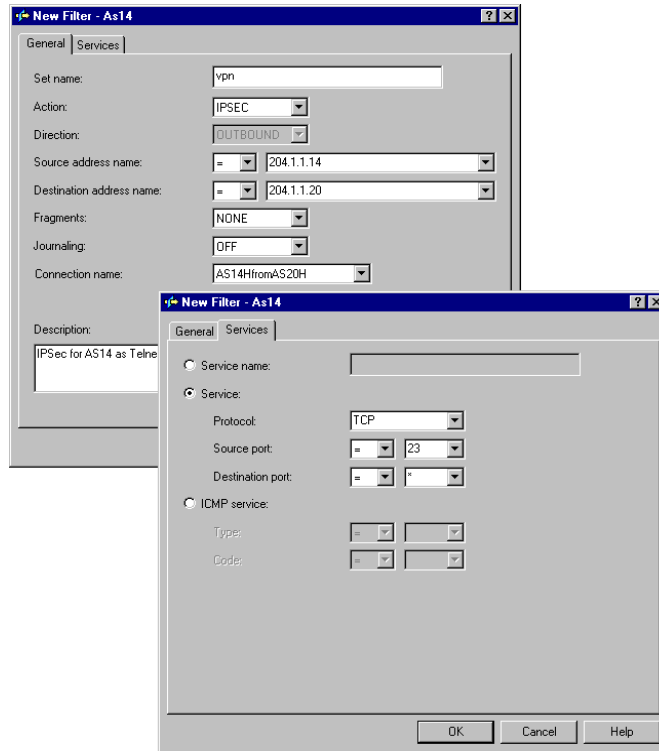


Figure 135. AS14 IPSEC filter rule associated with AS14HfromAS20H

Notice that, on the Policy window (Figure 131 on page 145), even when we defined the protocol, source, and destination ports as Connection or Single value from connection, we need to configure them in the IPSEC filter rule to distinguish them from the traffic that will match the IPSEC filter rule configured in Figure 128 on page 143.

Once created, this rule is positioned at the bottom of the filter file. The original IPSEC filter rule, which was configured in Figure 128 on page 143, overrides the new rule since it allows all source ports, all destination ports, and all protocols.

Therefore, we have to rearrange the IPSEC filter rules so that the new rule defined in Figure 135 is the rule configured in Figure 128 on page 143. Figure 136 shows how to drag and drop rules in the filter file to change the order.

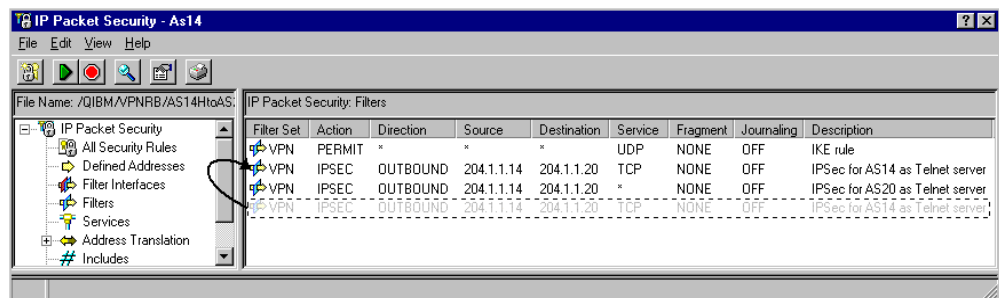


Figure 136. Repositioning IPSEC filter rules on AS14

Note

This scenario could have been implemented by specifying Filter rule for all values of the Policy window in the dynamic key connection group configured in Figure 131 on page 145 and using the same IPSEC filter rules.

AS20 configuration

You must configure the responder end of the VPN connection on AS20. This connection must allow AS20 Telnet clients to access the Telnet server on AS14.

The key policy, data policy, and key connection group configured in the previous scenarios can be used here. Therefore, there is no need to configure those objects again.

On the responder system AS20, configure the following objects:

- Dynamic key connection group
- IPSec filter rule

Complete the following steps:

1. On the Virtual Private Networking window, right-click **Dynamic Key Groups**, and select **New Dynamic Key Connection Group**.

Figure 137 shows the General window for the new dynamic key connection group on AS20.

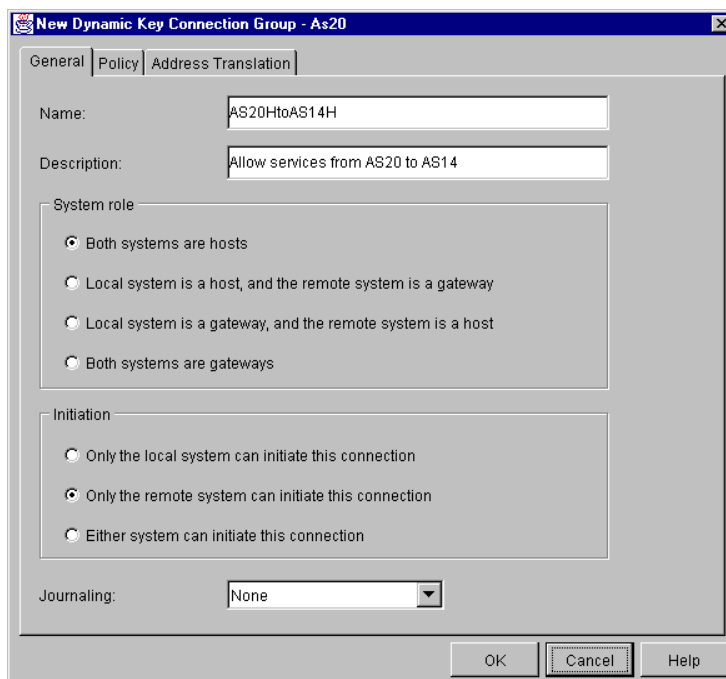


Figure 137. AS20 New Dynamic Key Connection Group

2. Click the **Policy** tab.
3. Configure the parameters that define the traffic for active connections in the Policy window as follows:

- **Local Addresses: Filter rule:** The value for the local data endpoint is defined in the IPSEC filter rule associated with this connection.
- **Local ports: Connection:** The port values proposed by the initiator AS14 are accepted as long as they are within the boundaries of the IPSEC filter rule on the responder AS20. AS14 must propose multiple values for this field (*Any port*). This field represents a valid set of ports that the Telnet clients on AS20 may use.
- **Remote Addresses: Filter rule:** The value for the remote data endpoint is defined in the IPSEC filter rule associated with this connection.
- **Remote ports: Single value from connection:** The ports values proposed by the initiator AS14 are accepted as long as they are within the boundaries of the IPSEC filter rule on the responder AS20. AS14 must propose a single value for this field (23). This field represents the port that the Telnet server on AS14 may use.
- **Protocol: Single value from connection:** The protocol proposed by the initiator AS14 is accepted as long as it is within the boundaries of the IPSEC filter rule on the responder AS20. AS14 must propose a single value for this field (TCP). This field represents the protocol that the Telnet application may use.

Figure 138 shows the Policy configuration on AS20.

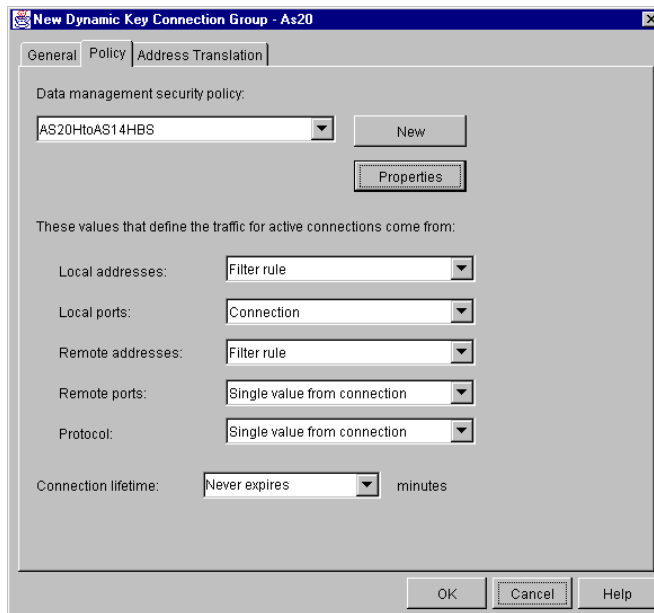


Figure 138. AS20 Policy window configured to allow Telnet client traffic from AS20 to AS14

4. Configure the IPSEC filter rule associated with the new dynamic key connection group. Notice that there is a one-to-one relationship between the IPSEC rule and the dynamic key connection group. Therefore, you must create a new IPSEC filter rule that processes the traffic for this connection as shown in Figure 139 on page 151.

The IPSEC filter rule on AS20 must enforce that only the Telnet service, when proposed by the initiator, is accepted.

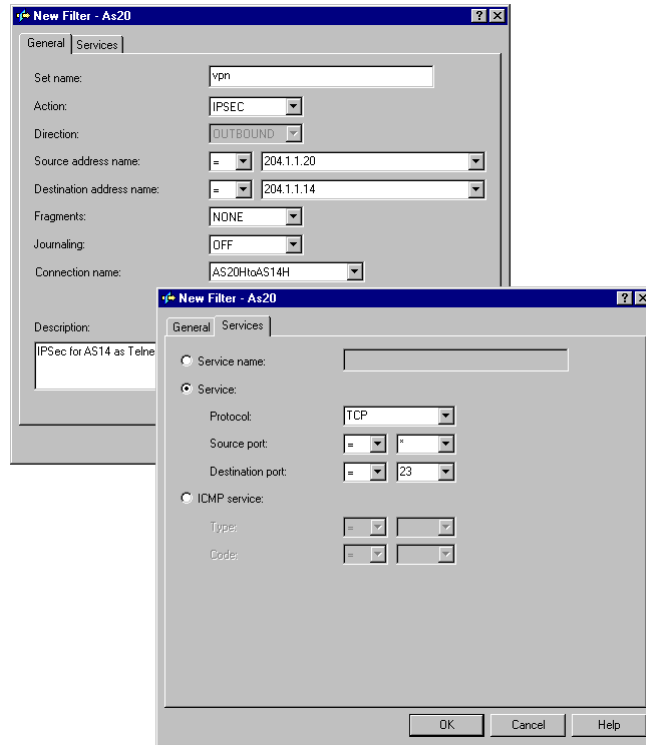


Figure 139. AS20 IPSEC filter rule associated with AS20HtoAS14H

4.4.4.2 Verification tests

After configuring both connections, reactivate filters and start each VPN connection separately. To verify the traffic direction, we started the connection that allows AS14 Telnet clients to access the Telnet server on AS20. After verifying the traffic, we stopped this connection and started the one that allows Telnet clients on AS20 to access the Telnet server on AS14. Finally, we tested both connections that are active at the same time to verify the bi-directional Telnet traffic.

The two VPN connections for this scenario are:

AS14HtoAS20H:L1 Allows traffic to the Telnet server on AS20

AS14HfromAS20H:L1 Allows traffic to the Telnet server on AS14

Table 11 shows a summary of the verification tests run when AS14HtoAS20H:L1 was started.

Table 11. AS14HtoAS20H:L1 test results

Direction	Start connection	Telnet	FTP	PING
From AS14 to AS20	YES	YES	NO	NO
From AS20 to AS14	NO	NO	NO	NO

Table 12 on page 152 shows a summary of the verification tests run when AS14HfromAS20H:L1 was started.

The AS14HtoAS20H:L1 connection was stopped and the AS14HfromAS20H:L1 was started. Table 12 shows the actions performed to test the link.

Table 12. AS14HfromAS20H:L1 test results

Direction	Start connection	Telnet	FTP	PING
From AS14 to AS20	YES	NO	NO	NO
From AS20 to AS14	NO	YES	NO	NO

When both connections started, we could Telnet in both directions simultaneously over the VPN link.

Figure 140 shows the Active Connections window on AS20 when both connections were started.

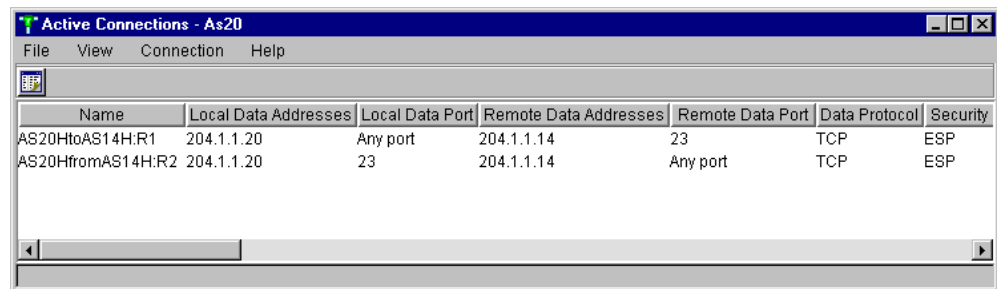


Figure 140. Active connections window on AS20 with both VPN connections running

4.4.5 Scenario 4: Allowing normal mode FTP in one direction

File Transfer Protocol (FTP) is a common TCP application used for transferring files between hosts. It is different from other TCP/IP applications in that FTP requires two separate TCP connections: the data connection and the command connection. The data connection carries the data, and the command connection is used for commands and results.

This section discusses how to configure a VPN connection to enable FTP between two hosts. Before discussing the specifics of the VPN configuration, we need to review the concepts of FTP *passive mode* and *normal mode*.

4.4.5.1 FTP normal mode

Figure 141 on page 153 shows a normal mode FTP connection with the following characteristics:

- The server listens on well-known port 21 for the command connection and uses port 20 to open the data connection.
- The client allocates two ports above 1023. One port is used for the data connection, and the other one is used for the command connection.
- The client opens the command channel to the server and sends an FTP PORT command to tell the server the second port number allocated by the client.
- The server opens a data channel on the client from server port 20 to the port specified by the client in the PORT command.

This data channel connection is in the opposite direction (server to client) from most protocols. Most firewalls are configured to block connection initiation (TCP

start) from the non-secure side to the secure side. Therefore, if the FTP client is behind a firewall attempting to access an FTP server on the Internet, it is likely that the firewall will block FTP normal mode.

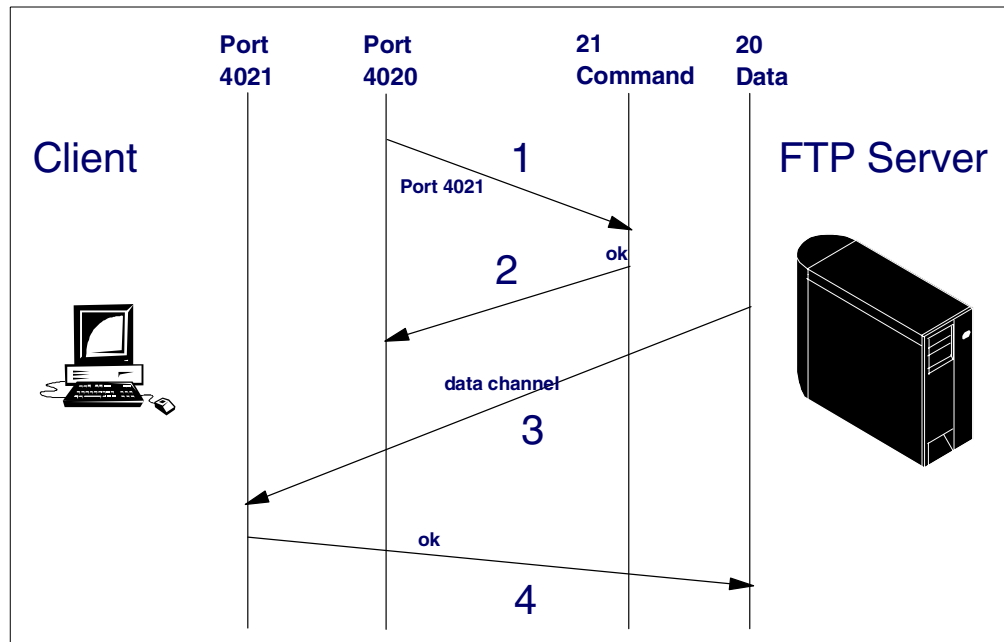


Figure 141. Normal mode FTP connection

To avoid the problem described above, a *firewall friendly* FTP, FTP passive mode (PASV), was developed.

4.4.5.2 FTP passive mode

Figure 142 on page 154 shows a passive mode FTP connection with the following characteristics:

- The server listens on well-known port 21 for the command connection. It uses port 20 and the source port when opening the data channel.
- The client allocates two ports above 1023. One port is used for the data connection, and the other one is used for the command connection.
- The client opens the command channel to the server and sends an FTP PASV.
- Upon receiving the PASV command, the server allocates a second port for the data channel above 1023 and tells the client the number of this port.
- The client opens a data connection from its port to the random port the server communicated to it.

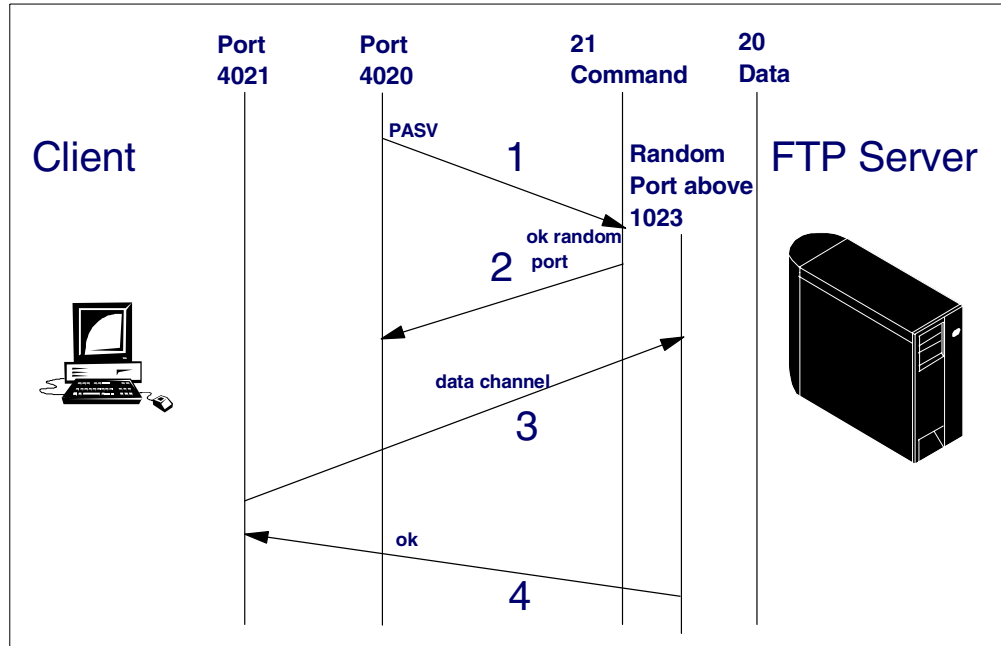


Figure 142. Passive mode FTP connection

4.4.5.3 Normal mode FTP versus passive mode in a VPN connection

In passive mode FTP, both connections are initiated by the client, which solves the firewall problem described in 4.4.5.1, “FTP normal mode” on page 152. However, allowing passive mode FTP traffic on a VPN connection requires you to configure the IPSEC filter rule on the server side to allow all ports since it is not possible to specify a port range. To enforce *only* FTP server traffic through the VPN, normal mode FTP must be used. Using normal mode FTP in a VPN connection does not cause the firewall problem described in 4.4.5.1, “FTP normal mode” on page 152. Even if the VPN traverses a firewall, the firewall filters must only be opened to allow the IPSec protocols.

In this scenario, normal mode FTP is used.

4.4.5.4 Scenario objectives

The objectives of this scenario are:

- Allow normal mode FTP from AS14 (FTP client) to AS20 (FTP server).
- Combine the FTP service with the existing Telnet service from AS14 (Telnet client) to AS20 (Telnet server).
- Restrict services on the client (AS14) via the connection configuration and on the server (AS20) via the IPSEC Filter configuration.

4.4.5.5 Scenario configuration

This section describes the configuration required on AS14 and AS20 to add FTP to the existing Telnet service through the VPN.

AS14 configuration

The following objects are configured as part of the VPN that allows Telnet from the AS14 client to the AS20 server and were created in 4.4.3, “Scenario 2: Restricting services to Telnet-only by connection” on page 140.

1. The IPSEC filter rule on the initiator, AS14, which is used to process Telnet conversations from AS14 to AS20 is currently configured to allow all services from any port to any port. Refer to Figure 143.

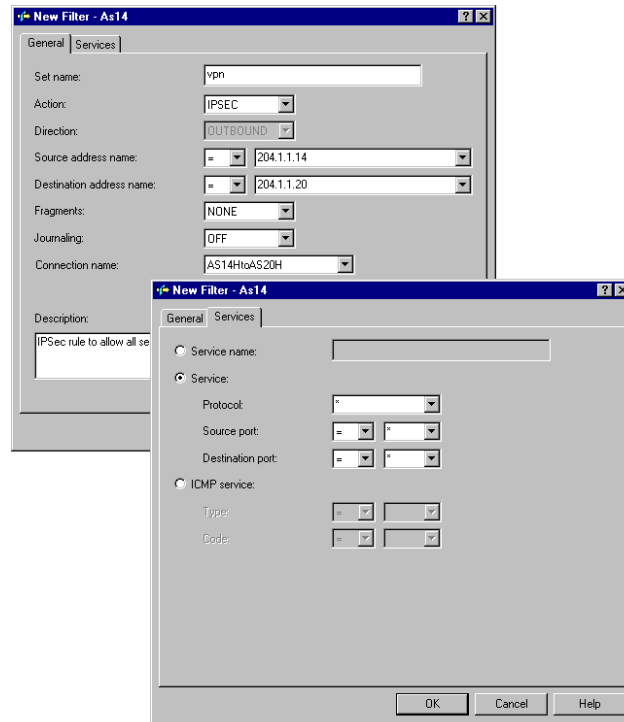


Figure 143. IPSEC filter rule on AS14 configured to allow all traffic through AS14HtoAS20H

When AS14 FTP client opens a control session on AS20 FTP server, the source IP address is 204.1.1.14, source port is any port greater than 1023 (*any* in the filter rule configuration), destination address is 204.1.1.20, and destination port 21. Therefore, the IPSEC filter rule shown in Figure 143, which was originally configured to allow Telnet traffic, can also be used for FTP.

2. AS14HtoAS20H is the VPN dynamic key connection group associated with the IPSEC filter rule shown in Figure 143. Figure 144 on page 156 shows the current policy configuration for the dynamic key connection group, AS14HtoAS20H, on AS14.

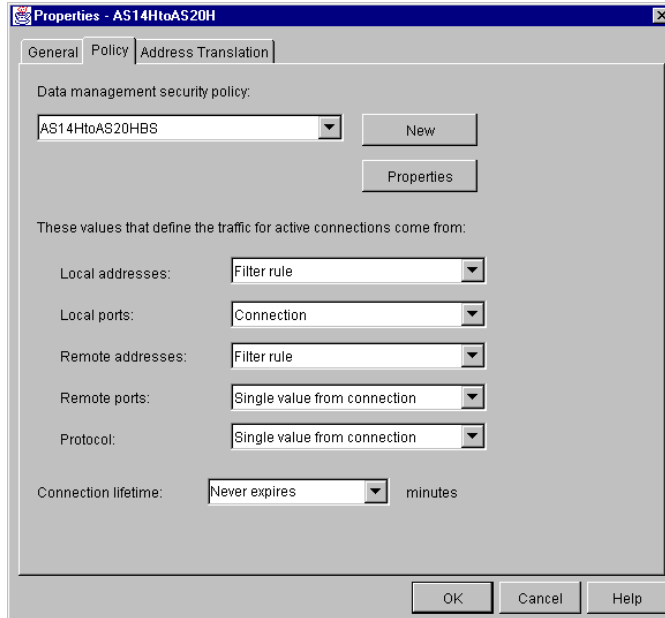


Figure 144. AS14HtoAS20H policy configuration on the connection initiator (AS14)

The policy page is configured to allow client/server conversations from AS14 to AS20. This configuration suits the one required for FTP also. Therefore, the only additional objects that you need to define on AS14 are two dynamic key connections under the existing dynamic key connection group (AS14HtoAS20H) to process traffic destined for ports 20 and 21.

3. To create the connection that allows AS14 to open a control channel on AS20, right-click on the AS14HtoAS20H dynamic key connection group, and select **New Dynamic Key Connection**. The window shown in Figure 145 is displayed.

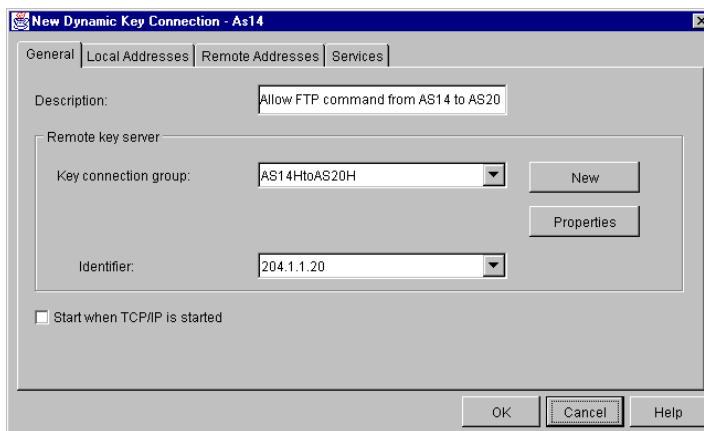


Figure 145. Configuring the new dynamic key connection for FTP command client traffic from AS14

4. In the Remote key server parameter, select the existing key connection group **AS14HtoAS20H**.
5. Click the **Local Addresses** tab.
6. Enter 204.1.1.14 as the local address.

7. Click the **Remote Addresses** tab.
8. Enter 204.1.1.20 as the remote address. Remember that the local and remote addresses used as data endpoints are defined in the IPSEC filter rule, but the VPN configuration GUI requires you to fill in these parameters here.
9. Click the **Services** tab.
10. Fill in the parameters in the Services window as shown in Figure 146.

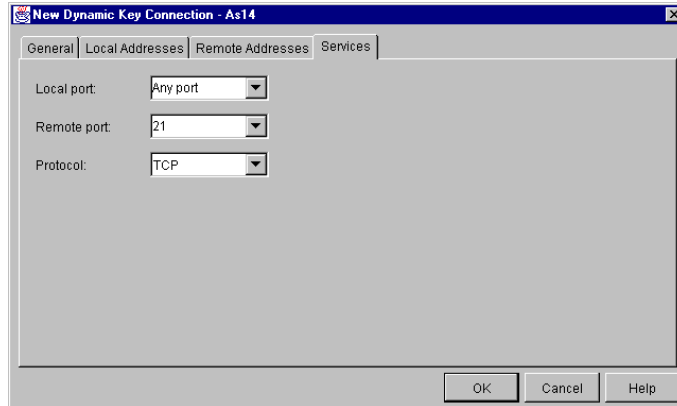


Figure 146. AS14 Services window configuration to request FTP command services on AS20

11. Click **OK**.
 12. To configure the connection that allows AS14 to open a data channel on AS20, repeat step 3 on page 156 through step 11 on page 157.
- The General and Services pages of this connection are shown in Figure 147.

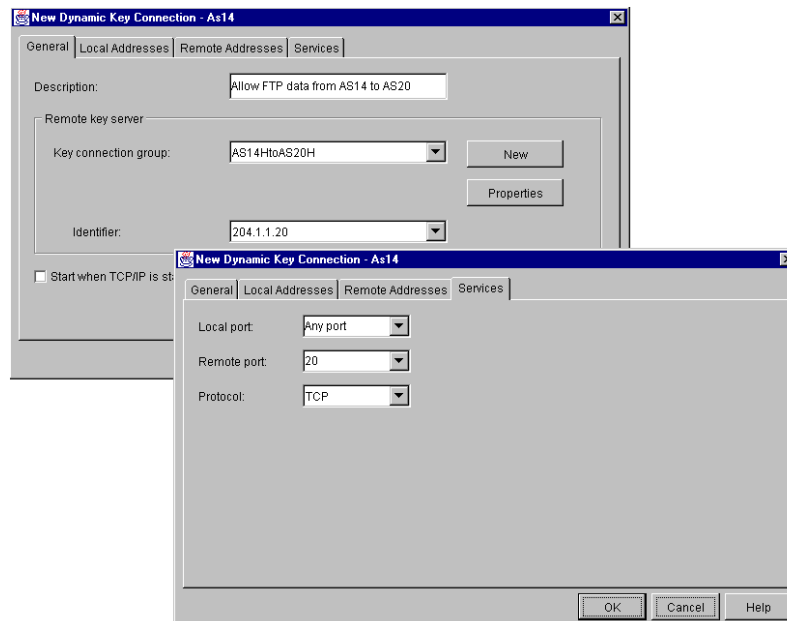


Figure 147. AS14 General and Services windows to request FTP data services on AS20

Figure 148 on page 158 shows all the dynamic key connections defined under AS14HtoAS20H.

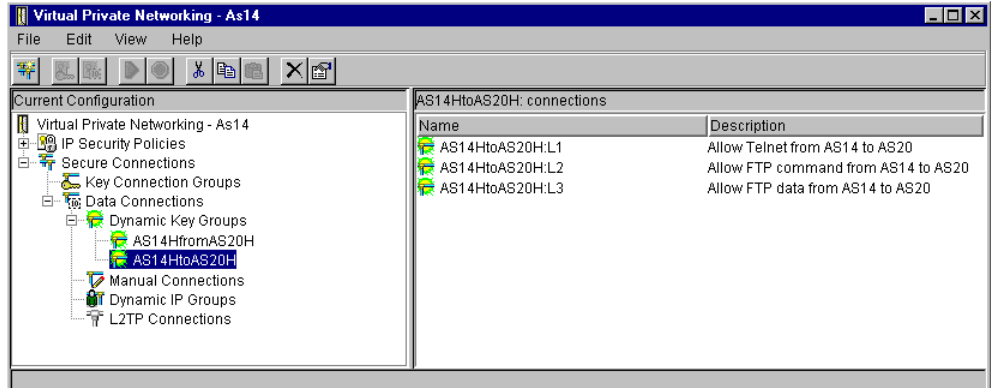


Figure 148. The dynamic key connections under the AS14HtoAS20H dynamic key connection group

This completes the VPN configuration required on AS14 to allow FTP and Telnet client traffic to AS20 servers.

AS20 configuration

The IPSEC filter rule on the responder (AS20) must be configured to restrict the the traffic in the active connection to *only* the services that you want to allow. Figure 124 on page 140 shows the IPSEC filter rule configured on AS20 to allow incoming Telnet requests to the Telnet server running on AS20. The source port (23) restricts the traffic in the dynamic key connection group associated with this IPSEC filter rule to the Telnet server only.

To enable FTP server through a VPN connection, you need to configure two new dynamic key connection groups and IPSEC filter rules to allow FTP clients to open control command (port 21) and data connections (port 20) on AS20. Perform the following steps:

1. Create a new dynamic key connection group to allow the FTP control channel on the AS20 FTP server. Select the existing key policy and data policy created for the Telnet connection. Figure 149 on page 159 shows the configuration of the new dynamic key connection group AS20ftpcAS14H.

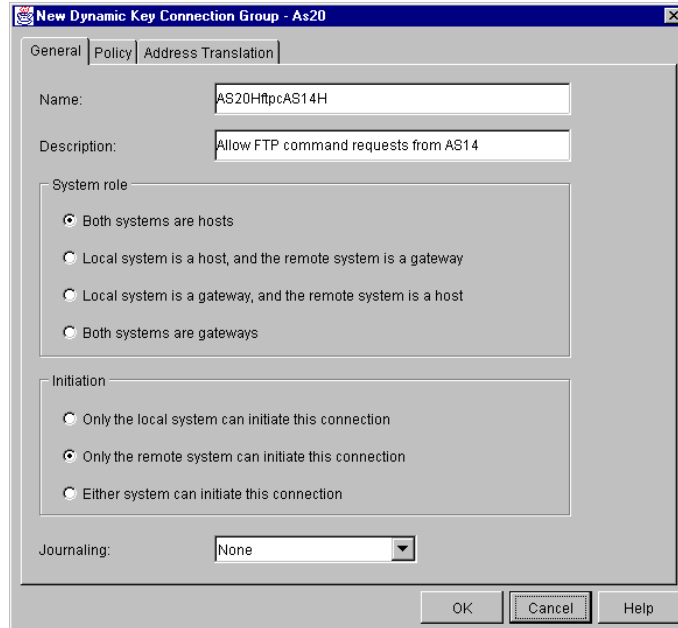


Figure 149. Dynamic key connection group to allow FTP command channel on AS20 FTP server

2. Click the **Policy** tab. Configure the parameters that control the traffic for active connections with the same characteristics as the Telnet connection. Figure 150 shows the settings.

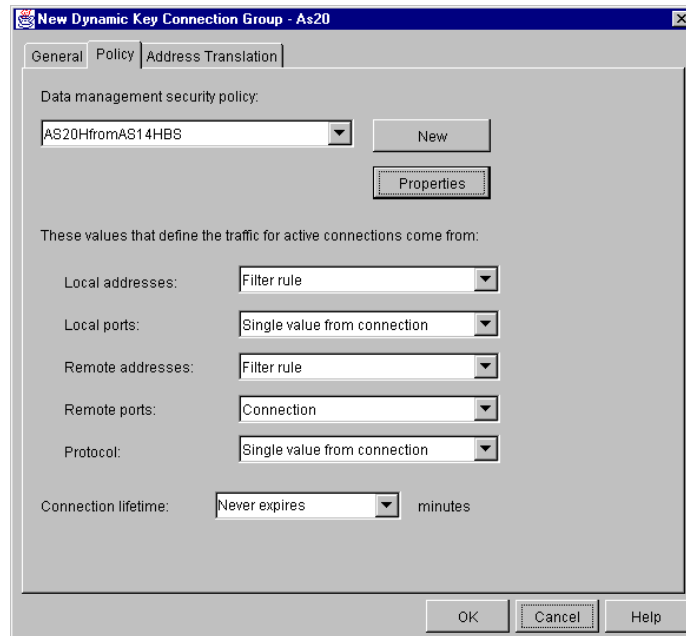


Figure 150. AS20HftpAS14H Policy window

3. Configure the IPSEC filter rule associated with this dynamic key connection group (AS20HftpAS14H) as shown in Figure 151 on page 160.

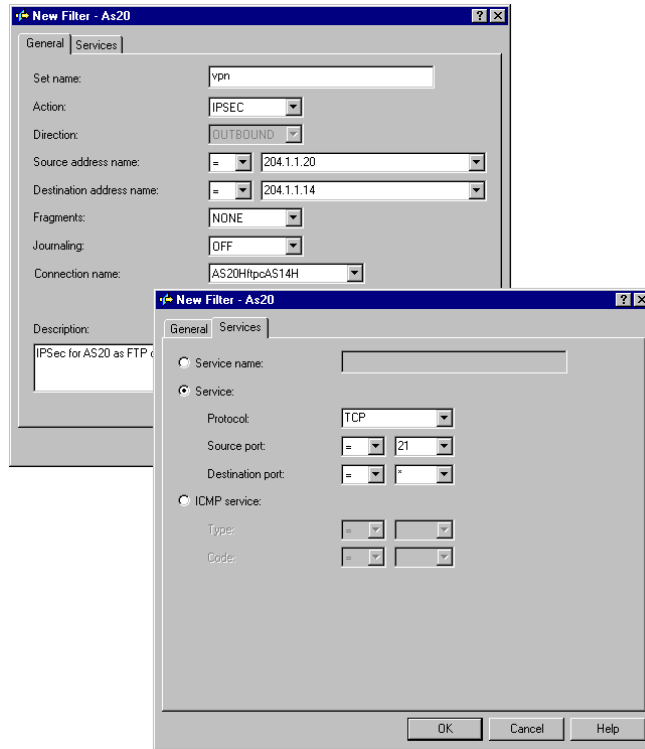


Figure 151. IPSEC filter rule for FTP control service on AS20

4. Create a new dynamic key connection group to allow the FTP data channel on the AS20 FTP server. Select the existing key policy and data policy created for the Telnet connection. Figure 152 shows the configuration of the new dynamic key connection group AS20ftpdAS14H.

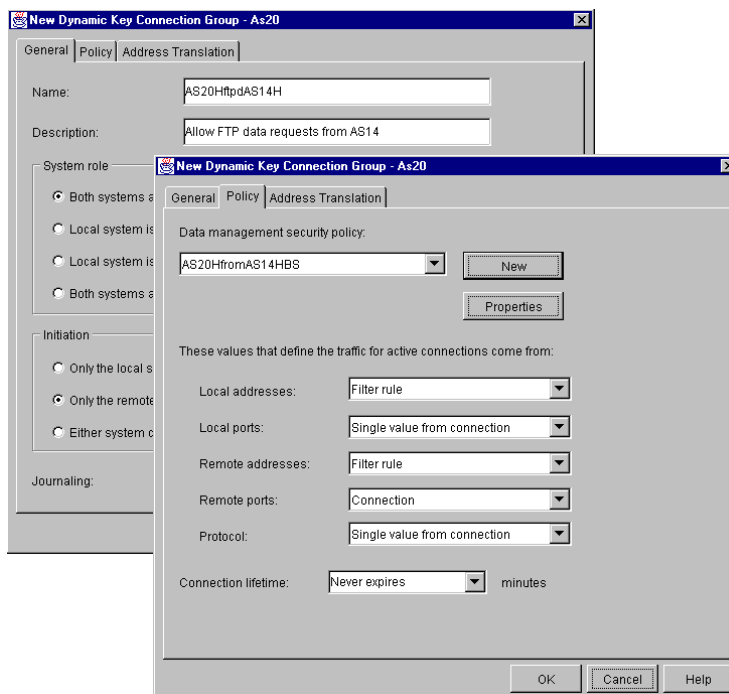


Figure 152. Defining the dynamic key connection group for the FTP data service on AS20

Note

The services are really restricted by IPSEC filter rule on AS20 since we configured multiple IPSEC filter rules (and dynamic key connection groups), one for each local TCP port used. Setting up the granularities for the three dynamic key connections groups on the server as all Filter rule has the same effect and is probably more clear.

- 5. Configure the IPSEC filter rule associated with this dynamic key connection group (AS20HftpdAS14H) as shown in Figure 151 on page 160.

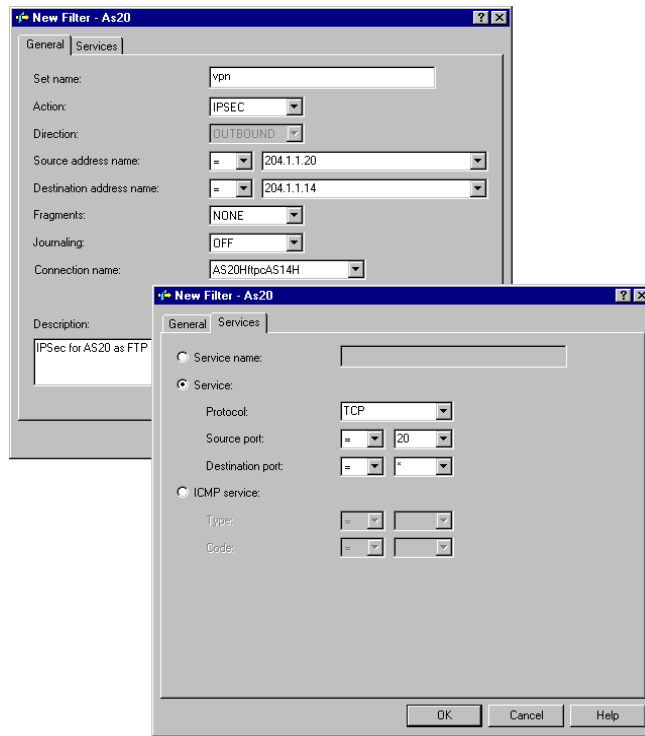


Figure 153. IPSEC filter rule for FTP data service on the AS20

4.4.5.6 Verification tests

On the AS/400 system, FTP passive mode is the default. To switch to the FTP normal mode used in this scenario, open a control connection on the server (simply start FTP), and send the command `SENDFASV 0`.

Table 13 shows a summary of the verification tests run for this scenario.

Table 13. Limiting traffic to Telnet and FTP from AS14 to AS20 tests results

Direction	Start connection	Telnet	FTP control	FTP data
From AS14 to AS20	YES	YES	YES	YES
From AS20 to AS14	NO	NO	NO	NO

Figure 154 on page 162 shows the active connections window on AS20.

Name	Local Data Addresses	Local Data Port	Remote Data Addresses	Remote Data Port	Data Protocol	Security
AS20HfromAS14H:R1	204.1.1.20	23	204.1.1.14	Any port	TCP	ESP
AS20HftpAS14H:R2	204.1.1.20	21	204.1.1.14	Any port	TCP	ESP
AS20HftpdAS14H:R3	204.1.1.20	20	204.1.1.14	Any port	TCP	ESP

Figure 154. Active Connections window on AS20 showing both Telnet and FTP service available

Chapter 5. Getting started: AS/400 host-to-host VPN

A machine acting as a host in a VPN connection is, at the same time, the VPN server and the data endpoint of the connection. The VPN host must support IPSec protocols. The hosts in a host-to-host VPN are also VPN servers. They perform the IKE negotiations and apply the IPSec protocols to the IP datagrams that flow through the secure tunnel. They are also the origin and destination of the data that flows in the VPN tunnel. Contrast this with the description of a VPN gateway, which is in Chapter 6, “Gateway-to-gateway VPN” on page 199. A host-to-host VPN guarantees end-to-end security. See 1.3, “VPN requirements” on page 9, for a description of the security features in a VPN.

Transport mode is most often used in a host-to-host VPN. Refer to 1.5.2, “AH transport and tunnel modes” on page 16, and 1.6.2, “ESP transport and tunnel modes” on page 20, for information on how the IP datagrams are processed in transport mode.

This chapter introduces the concept of host-to-host VPN with AS/400 systems acting as hosts. The objective of this chapter is to introduce, by example, a simple VPN configuration on the AS/400 system. To keep the example simple, we removed the complexity introduced in a real life scenario by firewalls, IP addressing requirements, routing, etc. Other chapters in this redbook cover more advanced topics. You can reproduce this example on a local LAN using two AS/400 systems to get started with AS/400 VPN configuration.

5.1 Business partner VPN connection (AS/400 host-to-AS/400 host)

This scenario presents two business partners that want to communicate with each other using their AS/400 systems over the Internet. Information that is transmitted between the two AS/400 systems is highly confidential and must be protected while traversing the Internet. Besides, since both hosts belong to different companies, the VPN partners don't fully trust each other. The data should not flow in the clear within the remote partner's network. Authentication, integrity, and encryption must be guaranteed end-to-end. Figure 155 on page 164 represents this scenario.

5.1.1 Scenario characteristics

This scenario has the following characteristics:

- The two intranets belong to different companies and are not fully trusted. The VPN tunnel must start and end at the data endpoints.
- AS/400 AS14 and AS/400 AS20 are running OS/400 V4R4 with VPN support.
- Both networks are connected to the Internet through routers and firewalls. The IP filter rules in the firewalls must be opened to allow IKE negotiations and IPSec protocols between the VPN partners. Refer to Chapter 12, “Don't forget a firewall: Protecting your VPN server” on page 515, for information on how to configure the firewall filters to allow a VPN tunnel to flow through them.

Note

Unlike the branch office scenarios, where we can assume that a consistent addressing plan is implemented across the company's intranets, in a business-to-business scenario, you need to consider addressing issues. Business partners implement an addressing scheme independently of one another. In this case, it is possible that both companies use private (globally ambiguous) IP addresses in their networks, and that some of those addresses overlap. In this case, conventional routing protocols will not be able to resolve these ambiguities.

In the host-to-host scenarios that apply to intercompany VPNs, we make the assumption that one or more of the following techniques is used to resolve addressing problems:

- The systems are assigned unique globally routable IP addresses. Even if the systems are assigned globally routable addresses, they still most likely will not have connectivity since their networks may be protected by firewalls. In this case, a tunnel solution similar to the one described below solves the problem.
- If the systems are assigned private IP addresses, they don't overlap.
- If the systems are assigned private IP addresses, a tunneling protocol is used between the gateways that connect both companies' networks to the intervening network (for example, the Internet). In this context, the gateways are firewalls, routers, or any other appliance. Some possible mechanisms include Frame Relay, MPLS, IPSec, L2TP, L2F, PPTP. It is important to note that the gateway-to-gateway tunnel between the firewalls or routers is totally transparent to the host-to-host configuration, such as the one shown in this chapter.

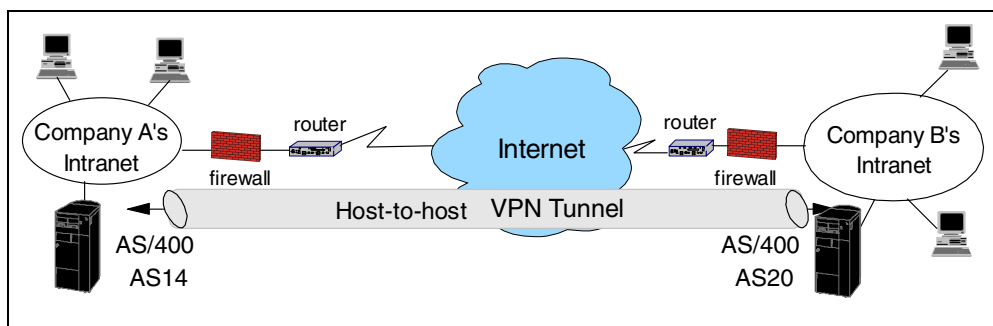


Figure 155. Overview of a customer host-to-host scenario

5.1.2 Scenario objectives

The objectives of this scenario are:

- Protect the traffic that flows between AS14 and AS20 over the Internet and within the internal networks with highest security protocols.
- AS14 in company A can only access AS20 in company B and vice versa.
- IKE phase 1 keys should be refreshed every 3 hours (180 minutes).

- IKE phase 2 keys should be refreshed every 5 minutes since the data is highly confidential and only a small volume of data is transmitted throughout the day.

Tip

It is difficult to prescribe phase 1 and phase 2 lifetimes and lifetimes since they are application specific. In general, phase 2 keys are refreshed more often than phase 1 keys. Key refreshes cost some system resources. That cost increases with the number of connections and lower lifetimes or lifetimes. We used a phase 1 key lifetime of 3 hours, and a phase 2 key lifetime of 5 minutes in this scenario. A phase 1 lifetime of 3 to 8 hours and phase 2 lifetime of 15 to 30 minutes are reasonable ranges even in this highly confidential application.

- Only AS14 can initiate the VPN connection.
- AS14 must automatically start the VPN connection when the 10.196.11.1 interface is started.
- The VPN connection must be stopped automatically at the end of the business day.

5.1.3 Scenario network configuration

Figure 156 shows our simple network configuration for the AS/400 host-to-AS/400 host scenario. Notice that in our test network, we created two IP interfaces on the AS/400 systems: 10.196.11.* to represent the IP addresses used for the VPN connection, and 192.168.1.* to represent the IP address used to communicate with internal hosts.

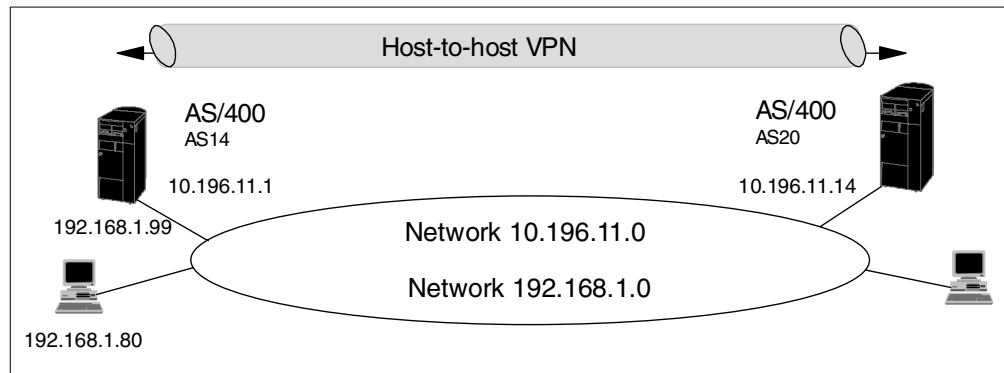


Figure 156. AS/400 host-to-host AS/400 scenario network configuration

5.1.4 Software prerequisites

Refer to 3.2, “VPN software prerequisites” on page 52, for a list of the software required on the AS/400 system.

5.1.5 Task summary

The following list summarizes the tasks performed to implement this VPN host-to-host environment:

1. Verify IP connectivity.
2. Complete the planning worksheets for AS14.
3. Change the VPN security default values to meet the requirements before configuring the VPN with the New Connection Wizard.
4. Create a host-to-host VPN connection on the AS14 using the New Connection Wizard.
5. Customize the host-to-host VPN connection created by the wizard on AS14 using the Virtual Private Networking GUI.
6. Configure IP packet filters on the AS14 to complete the VPN configuration.
7. Complete the planning worksheet for AS20.
8. Create a host-to-host VPN connection on AS20 using the New Connection Wizard.
9. Customize the host-to-host VPN connection on the AS20 using the Virtual Private Networking GUI.
10. Configure IP packet filters on the AS20 for the VPN connection.
11. Start the VPN connection.
12. Perform verification tests.

5.2 Verifying IP connectivity

Before starting the VPN configuration, verify connectivity and routing between the two AS/400 systems. A simple PING command run on AS20 checks that the IP connectivity to AS14 is working:

```
PING RMTSYS('10.196.11.1') LCLINETA('10.196.11.14')
```

Repeat the PING test in the reverse direction to confirm that IP connectivity also works from AS14 to AS20. Run the following command on AS14:

```
PING RMTSYS('10.196.11.14') LCLINETA('10.196.11.1')
```

Note

In a real life environment, verifying the end-to-end route is not as simple as in our test network. Some of the reasons are:

- The PING command is blocked by routers and firewalls in the path. You may need to either temporarily allow PING by changing filters or use another service to verify connectivity.
- If a tunneling protocol is used between the gateways that connect both companies' networks to the intervening network, host-to-host connectivity may only be possible through the VPN.

If it is not possible to test end-to-end connectivity *before* configuring the VPN, split the path into smaller segments and verify each segment.

5.3 Configuring a host-to-host VPN on the AS/400 system (AS14)

The following sections take you step-by-step through the configuration of the VPN and filters on the AS/400 VPN host AS14.

5.3.1 Completing the planning worksheets for AS14

Complete the planning worksheets to gather the information you need to create a host-to-host VPN connection with the VPN configuration wizard. Table 14 shows the planning worksheet for this scenario from the perspective of the VPN host AS14 in company A.

Table 14. AS14 New Connection Wizard planning worksheet

This information needed to create VPN with the New Connection Wizard	Scenario answers
What is the type of connection to be created? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Host
What is the name of the connection group?	HtoH14to20
What type of security and system performance is required to protect the keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest security, lowest performance
How is the local VPN server identified?	IP address
What is the IP address of the local VPN server?	10.196.11.1
How is the remote VPN server identified?	IP address
What is the IP address of the remote server?	10.196.11.14
What is the pre-shared key?	AndrewBryan
What type of security and system performance is required to protect the data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest security, lowest performance

The wizard provides the highest level of protection for protecting both key and data information based on the values in Table 14. Refer to 3.6.6, “New Connection Wizard planning” on page 63, for a description of the protocols and transforms configured by the wizard.

Table 15 on page 168 shows the information you need to configure IP filters to complete the VPN configuration.

Table 15. AS14 Planning worksheet - IP filter rules

This is the information needed to create the IP filters to support the VPN connection	Scenario answers
Is the local VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, the VPN server acts as a host. If no, the VPN server acts as a gateway.	Host
Is the <i>remote</i> VPN server acting as a host or gateway ?	Host
What is the name used to group together the set of filters that will be created?	VPNSET
If the local VPN server is acting as a gateway... – What is the IP address of the local ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	Not applicable
If the <i>remote</i> VPN server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	Not applicable
What is the IP address of the local VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	10.196.11.1
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	10.196.11.14
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRNLINE
What other IP addresses, protocols, and ports are permitted on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	192.168.1.0

Because we are configuring a host-to-host connection, the VPN servers and the data endpoints have the same IP addresses. The subnet 192.168.1.0 represents the internal network. The filters should permit internal network traffic without restrictions.

A filter set name, VPNSET, is used to group all the filter rules together and apply them to an interface. The interface is TRNLINE.

5.3.2 Changing the default security values

Before you use the New Connection Wizard to configure a VPN connection, you should review the default security values that the wizard will use, and change them if needed. Refer to 3.6.6, “New Connection Wizard planning” on page 63, for information in the default security values. Refer to 3.7.6, “Changing the Virtual Private Networking GUI default values” on page 76, for information on updating the default values.

Tip

The default security values are used any time the New Connection Wizard is run, or when new objects are created.

To satisfy the objectives of a key lifetime for IKE phase 1 and phase 2, and to stop the connection automatically at the end of the business day, change the default security values as follows:

1. At the Virtual Private Networking window, click **Edit->Defaults**.
2. Click the **Key Management Lifetime** tab.
3. Enter 180 minutes for Maximum key lifetime as shown in Figure 157. This value applies to phase 1 key lifetime.

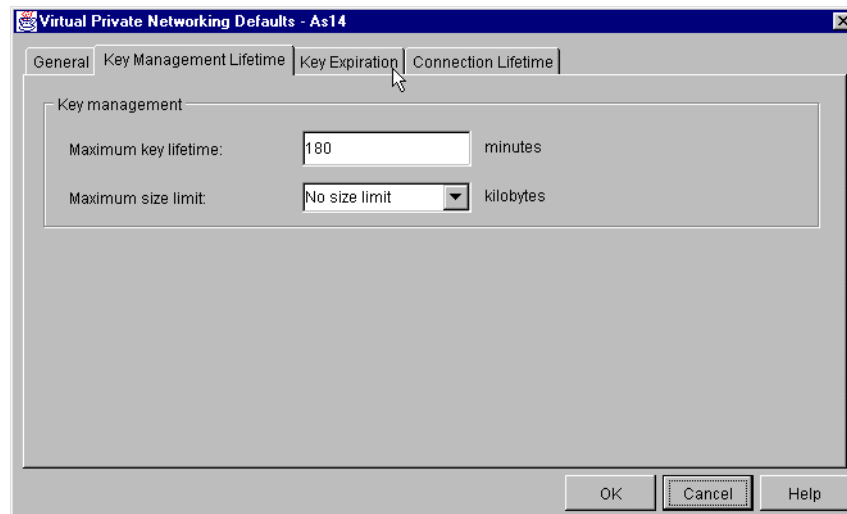


Figure 157. Changing default phase 1 maximum key lifetime

4. Click the **Key Expiration** tab.
5. Enter 5 minutes for Expire after as shown in Figure 158 on page 170. This value applies to phase 2 key lifetime.

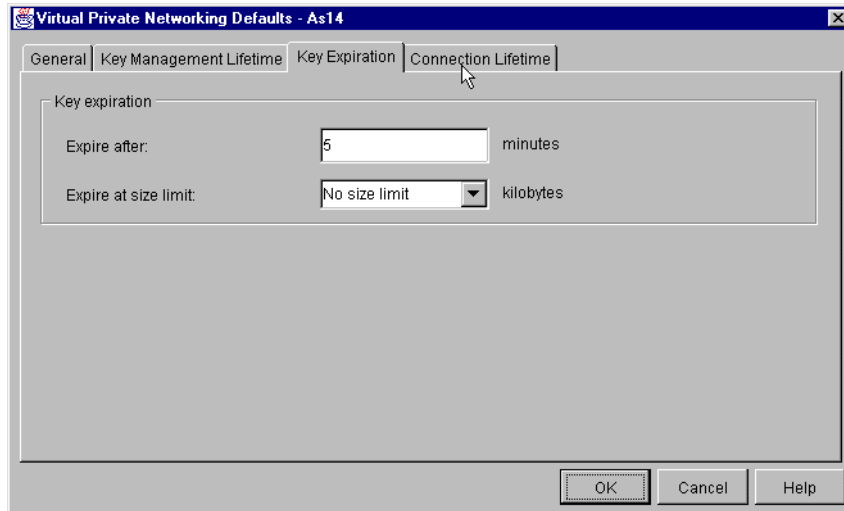


Figure 158. Changing default phase 2 maximum key lifetime

Note

At the time this redbook was written, the default values of key lifetime for the IKE phase 1 and Expire after for IKE phase 2 were incorrect. The correct settings should be inverted. Key lifetime for IKE phase 1 should be longer than the Expire after value for IKE phase 2. We recommend that you change the default values to 1440 minutes for *Maximum key lifetime* and 60 minutes for *Expire after* or customize them according to your security policy. In any case, phase 1 key lifetime should be several times longer than phase 2 key lifetime. The default values will be corrected by a later Service Pack of Operations Navigator.

6. Click the **Connection Lifetime** tab.
7. Enter 480 minutes for Time as shown in Figure 159 on page 171. The connection is stopped automatically 8 hours after it is started.

Note

When the connection lifetime is reached, the connection stops operating until you start it again. Even if there are active TCP/IP connections in the tunnel, the VPN connection stops when this time is reached. Once the connection stops, you can manually start it again, or it will start when the 10.196.11.1 interface is started.

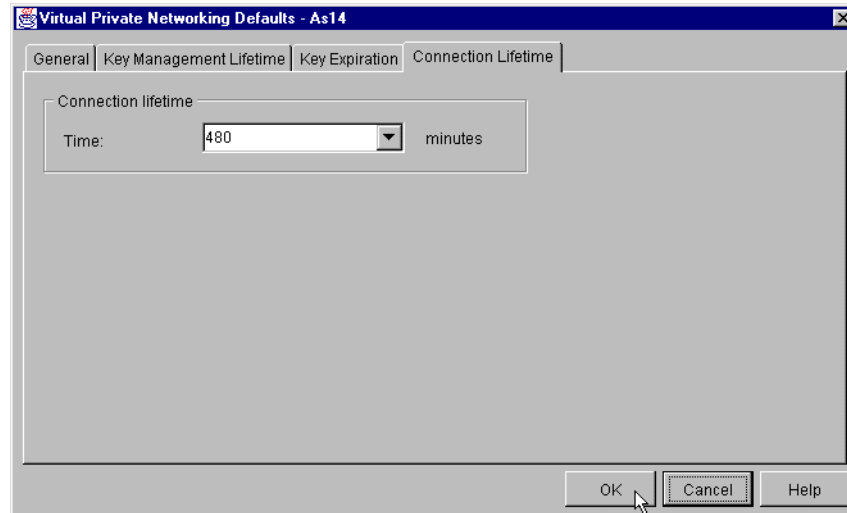


Figure 159. Changing default connection lifetime

8. Click **OK**.

For more information on IKE key lifetimes, refer to 3.6.7, “Key policy (IKE phase 1) and data policy (IKE phase 2) lifetime and size limits” on page 65.

5.3.3 Configuring a host-to-host VPN on AS14

Perform the following steps to configure the host-to-host VPN on AS14:

1. Start Operations Navigator from your desktop.
2. Expand your AS/400 system, which in this case is **AS14**. Sign on when prompted.
3. Expand **Network**.
4. Double-click **IP Security** to reveal two server names in the right window: IP Packet Security and Virtual Private Networking. You must configure both of these, but start with *Virtual Private Networking*.

Note

At this stage, Virtual Private Networking may already have a status of *started* since the default is for the server to automatically start when TCP/IP starts. The server can be either *started* or *stopped* during the following steps.

5. At the Virtual Private Networking GUI menu bar (Figure 160 on page 172), click **File->New Connection**.
6. Select **Host to Hosts**. This starts the New Connection Wizard for a host-to-host connection.

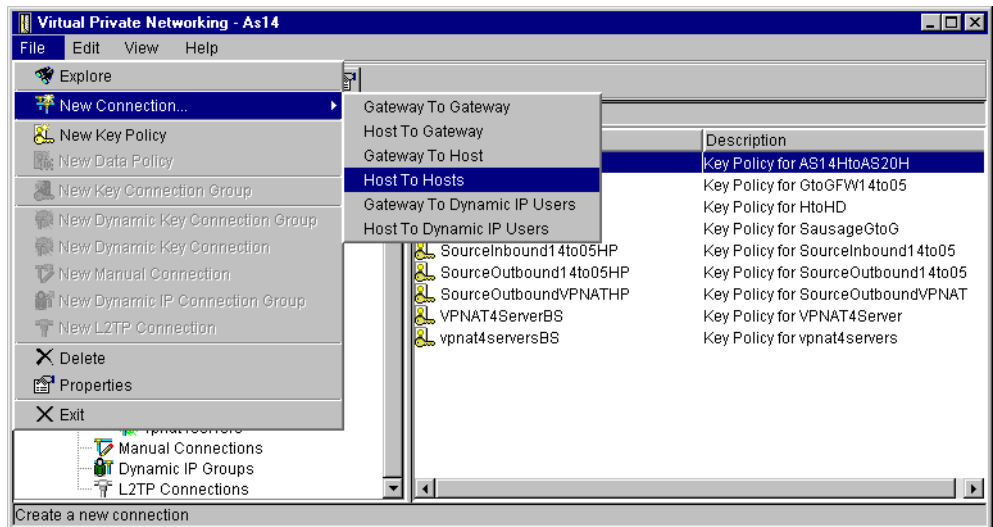


Figure 160. New Connection -> Host to Hosts

7. Click **Next** after reading the welcome window.
8. At the Connection Name window (Figure 161), enter `HtoH14to20` for the Name of the connection group. `HtoH14to20` is the name from the worksheet in Table 14 on page 167. This name is used for all the objects that the wizard creates for this connection. It is case sensitive. Also enter a description for the configuration.

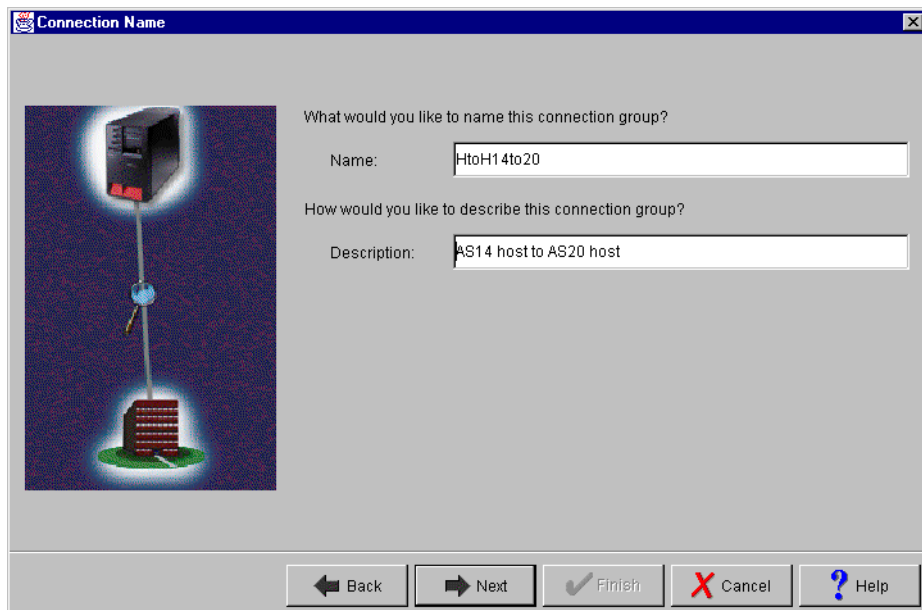


Figure 161. Connection Name window

9. Click **Next**.
10. At the Key Policy window (Figure 162 on page 173), specify the level of authentication or encryption protection that IKE uses during phase 1 negotiations. Phase 1 establishes the keys that protect the messages that flow during subsequent phase 2 negotiations. Phase 2 protects the data itself. Select **Highest Security, lowest performance** as specified on the worksheet.

The wizard chooses the appropriate encryption and authentication algorithms based on the selection you make here.

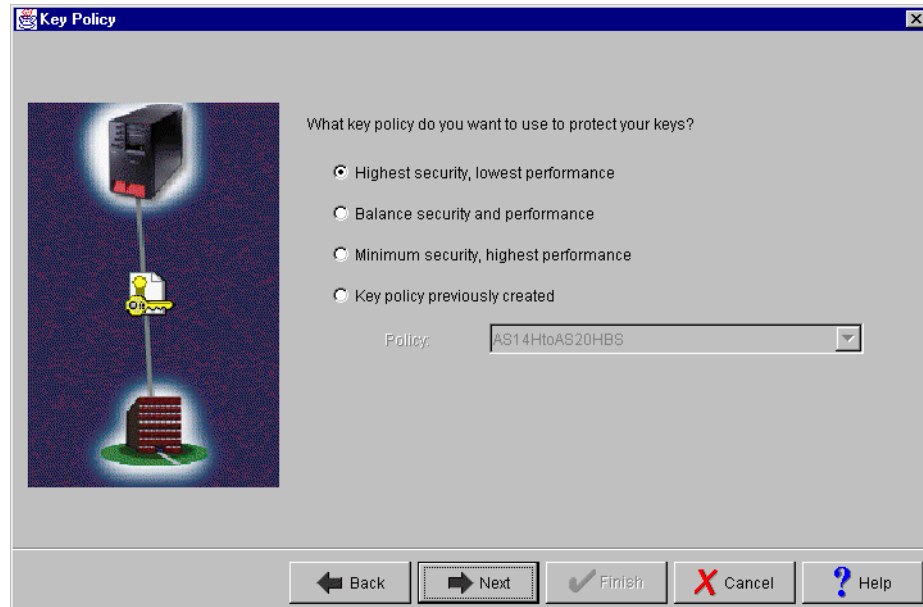


Figure 162. Key Policy window

11. Click **Next**.

12. At the Local Identifier window (Figure 163 on page 174), specify the identity of the local key server. In other words, specify the local AS/400 that acts as the VPN host, which in this case, is AS14. Leave Identifier type as the default value, which is **Version 4 IP address**. For the IP Address parameter, use the pull-down list to select the IP address of the interface that is connecting to the remote VPN host AS20. Refer back to the planning worksheets and to the network configuration in Figure 156 on page 165. Select **10.196.11.1** for AS14.

Note: Figure 163 on page 174 shows various IP addresses, including 10.10.10.14, 10.186.11.1, and so on, that we do not reference anywhere in this scenario. These interfaces are configured on AS14, but are used for other scenarios and projects and should be ignored here.

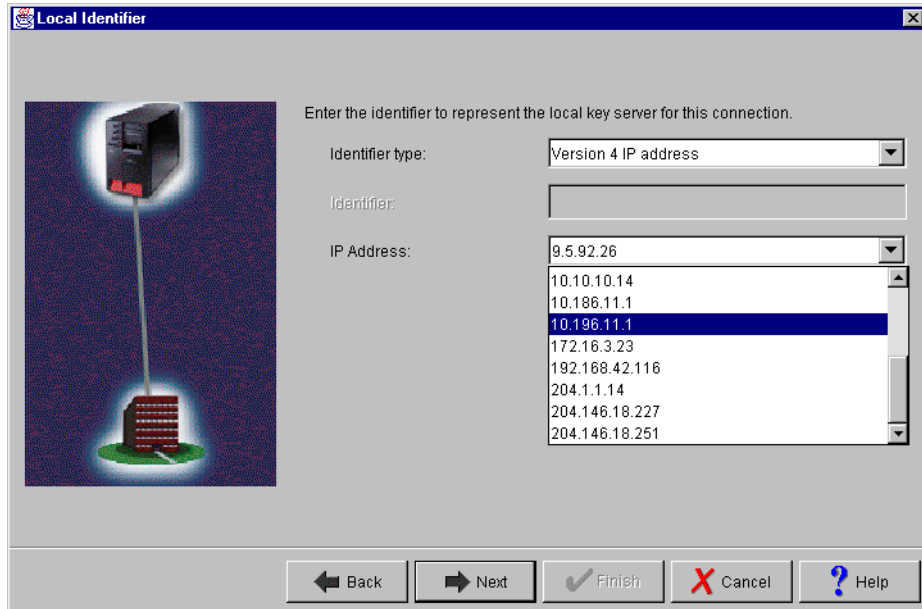


Figure 163. Local Identifier window pull-down list

13. Click **Next**.

14. At the Remote Hosts window (Figure 164), click **Add** to add a new remote identifier for AS20.

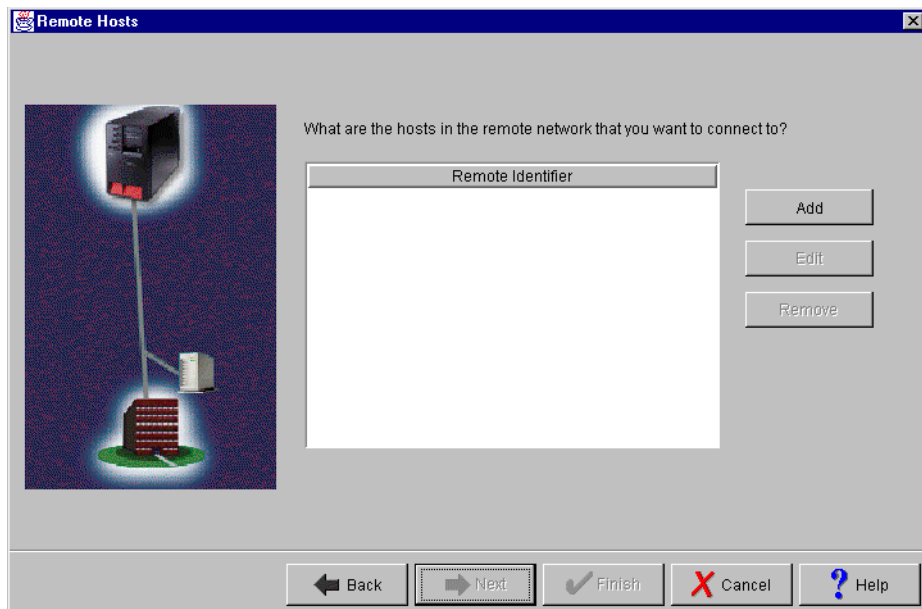


Figure 164. Remote Hosts window

15. At the Remote Identifier window (Figure 165 on page 175), enter details about the remote key server, as well as the pre-shared key. The pre-shared key is the shared secret that IKE uses to generate the actual keys for Phase 1. Enter the AS20 IP address 10.196.11.14. Specify AndrewBryan in the Pre-shared key parameter. Remember, the same pre-shared key must be entered when configuring VPN on the remote AS/400 system, AS20.

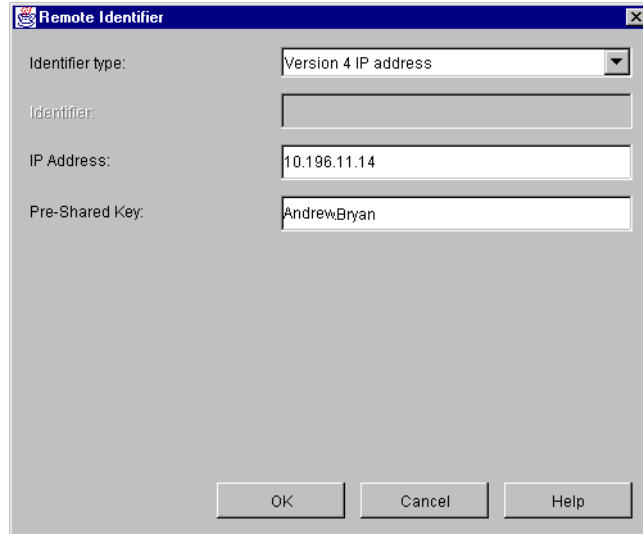


Figure 165. Remote Identifier window

16. Click **OK**.

17. Back at the Remote Hosts window (Figure 164 on page 174), click **Next**.

18. On the Data Policy window (Figure 166), specify the level of authentication or encryption that IKE uses to protect data flowing through the host-to-host VPN tunnel during phase 2 negotiations. For this example, select **Highest security, lowest performance**, **lowest performance** as specified on the worksheet in Table 14 on page 167.

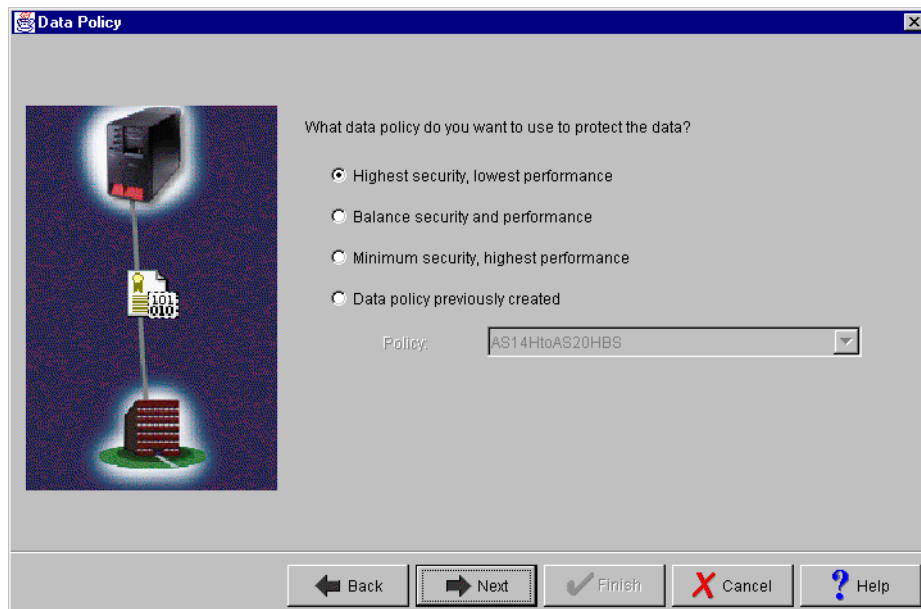


Figure 166. Data Policy window

19. Click **Next**.

20. The final window (Figure 167 on page 176) summarizes the configuration values entered. Scroll down to see a list of the configuration objects that the wizard will create when you click Finish. Check the configuration values against the worksheet. If changes need to be made, click **Back**.

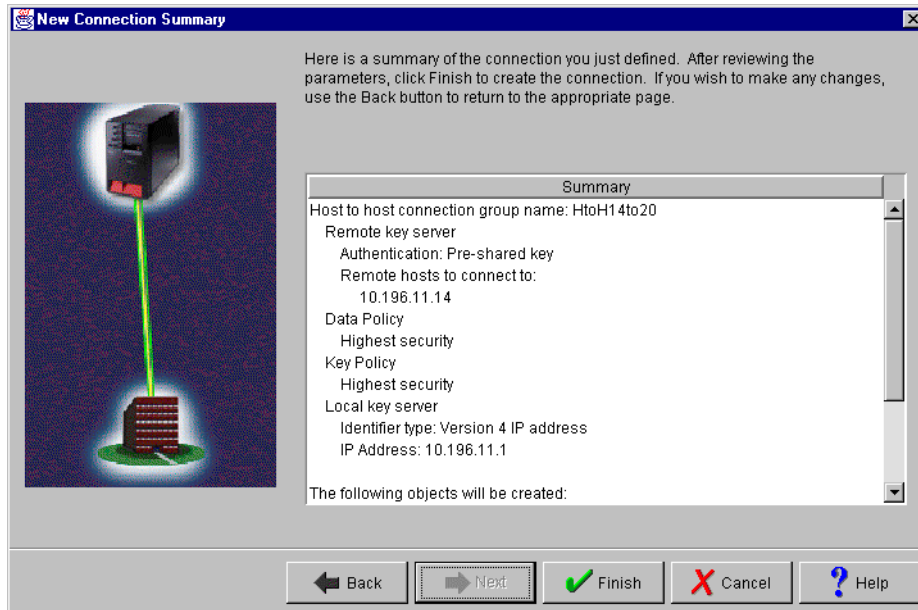


Figure 167. New Connection summary window

21. Click **Finish**.

The wizard creates the various objects that were configured for this VPN connection. After a short delay (and assuming there are no errors), the initial Virtual Private Networking GUI window is displayed.

5.3.4 Customizing the VPN configuration created by the wizard on AS14

Sometimes, you may need to use the VPN configuration GUI to change some of the values configured by the wizard. For example, one of the objectives of this scenario is that VPN connections can only be initiated by AS14. Another objective is to start the connection automatically. The steps that you must follow to customize the wizard configuration depend on the VPN object and parameter you need to change. Several examples in this redbook show how to customize different parameters depending on the scenario requirements.

To configure AS14 to be the initiator of the VPN connections in this scenario, perform the following steps:

1. At the Virtual Private Networking GUI, expand **Secure Connection->Data Connection->Dynamic Key Groups**.
2. Right-click the **HtoH14to20** Dynamic Key Group, and select **Properties** as shown in Figure 168 on page 177.

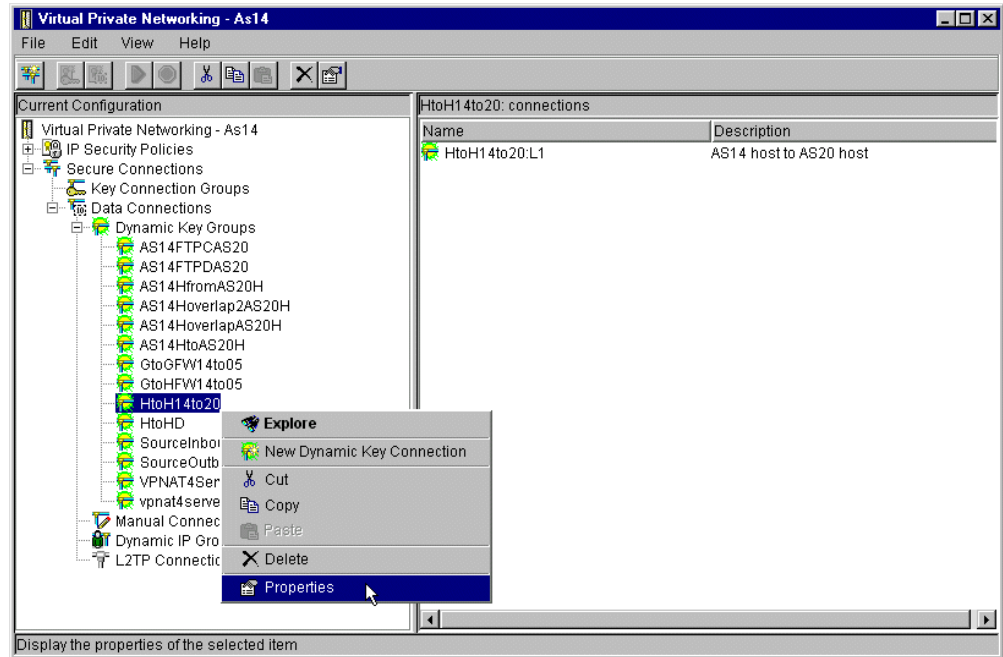


Figure 168. Customizing the Dynamic Key (connection) Group

3. At the Dynamic Key Group Properties - General page (Figure 169), select **Only the local system can initiate this connection** for the Initiation parameter.

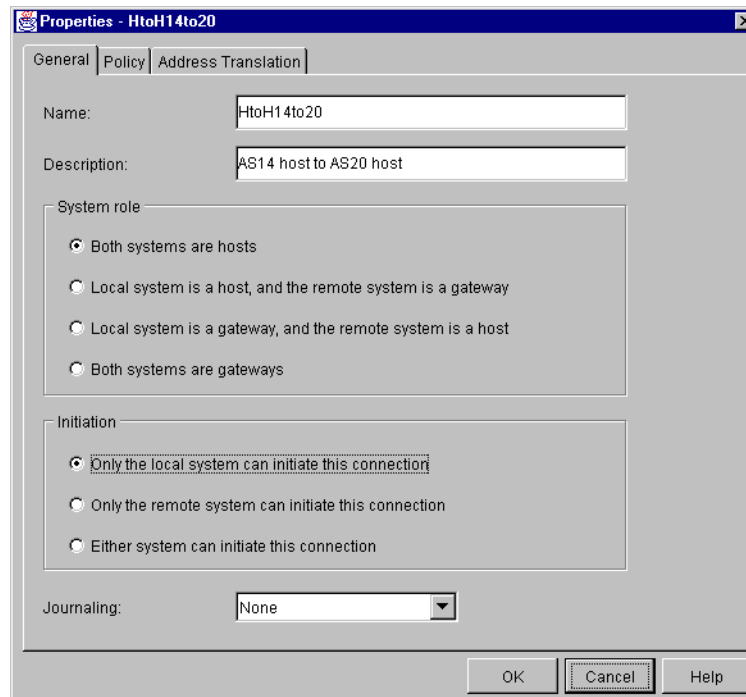


Figure 169. Dynamic Key Group Properties General page - AS14 as the connection initiator

4. Click **OK**.

You can specify automatic starting of the VPN connection by selecting the Start when TCP/IP is started parameter of the Dynamic Key Connection. This VPN connection will start when the 10.196.11.1 interface is started and filter rules are activated that have IPSEC filter rules associated with this connection. Perform the following steps:

1. On the right panel of the Virtual Private Networking GUI window, right-click the **HtoH14to20:L1** Dynamic Key Connection, and select **Properties** as shown in Figure 170.

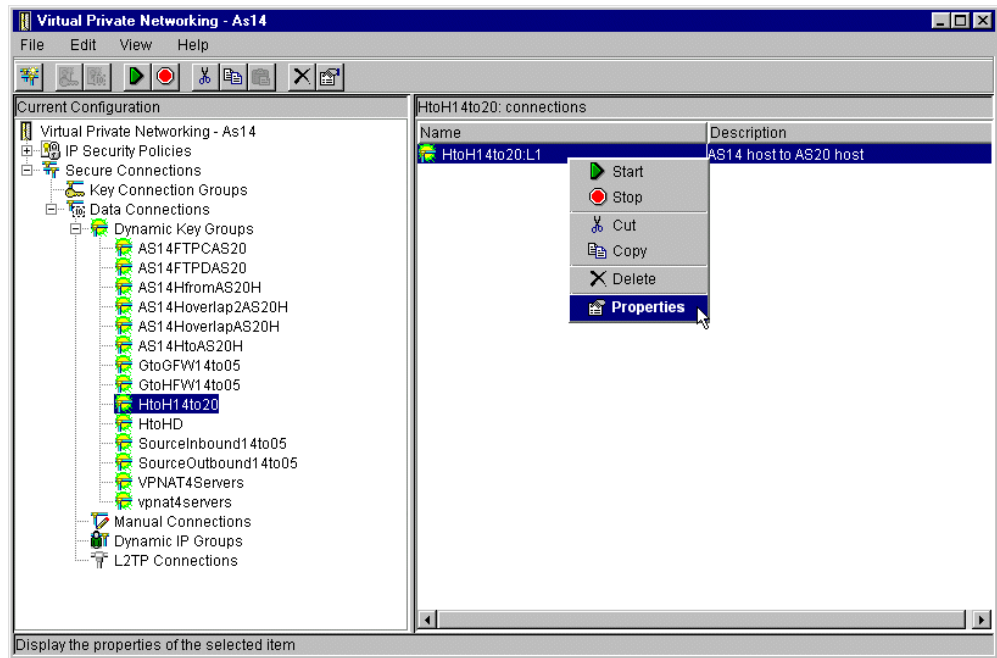


Figure 170. Customizing the Dynamic Key Connection

2. At the Dynamic Key Connection Properties General page (Figure 171), select **Start when TCP/IP is Started**.

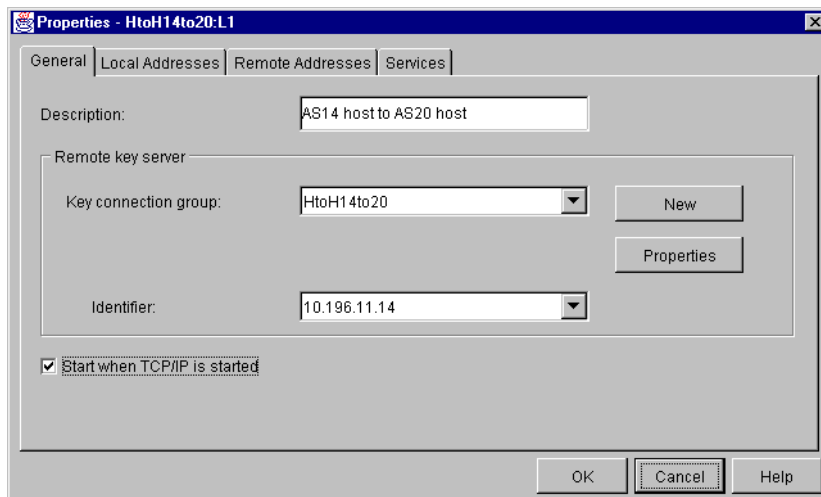


Figure 171. Dynamic Key Connection Properties

3. Click **OK**.

This completes the VPN configuration customization for AS14.

5.3.5 Configuring IP packet security on AS14

The Virtual Private Networking New Connection Wizard does *not* configure IP filtering. Complete this task manually by using the IP Packet Security GUI. Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for information on how to configure filters on the AS/400 system. Perform the following steps:

1. From Operations Navigator, expand your **AS/400 system->Network**, and then select **IP Security**.
2. Double-click **IP Packet Security** on the right panel (Figure 172).

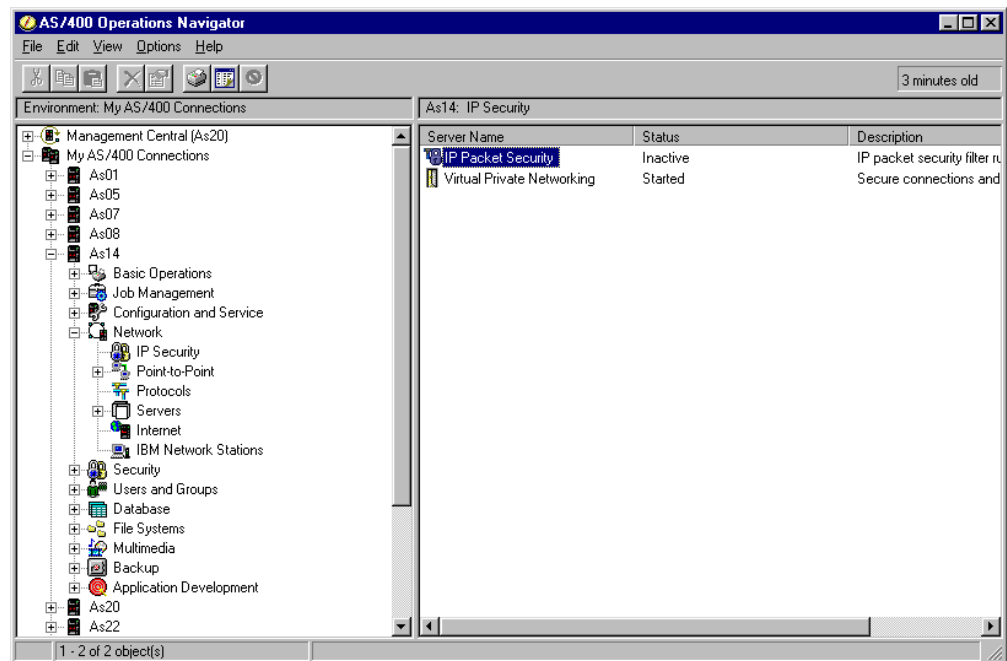


Figure 172. Starting IP Packet Security configuration

3. Right-click **Defined Addresses**, and select **New Defined Address** as shown in Figure 173 on page 180. You are configuring the subnet 192.168.1.* that represents the internal network.

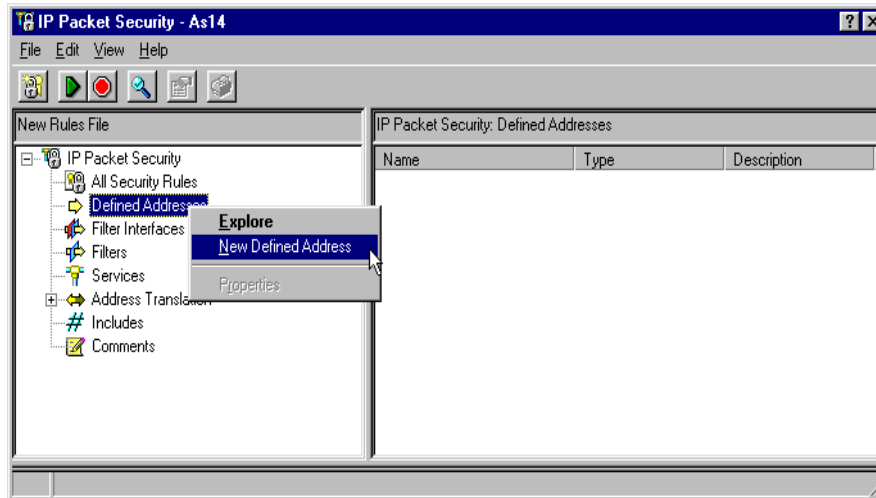


Figure 173. Configuring a new Defined Address to represent the internal network

4. Enter `InternalNetwork` for Address name.
5. Enter `255.255.255.0` for Subnet mask.
6. Click **Add**.
7. Enter `192.168.1.0` for the subnet IP address.
8. Enter `All hosts in the internal network company A` for Description.
9. Click **OK**. See Figure 174.

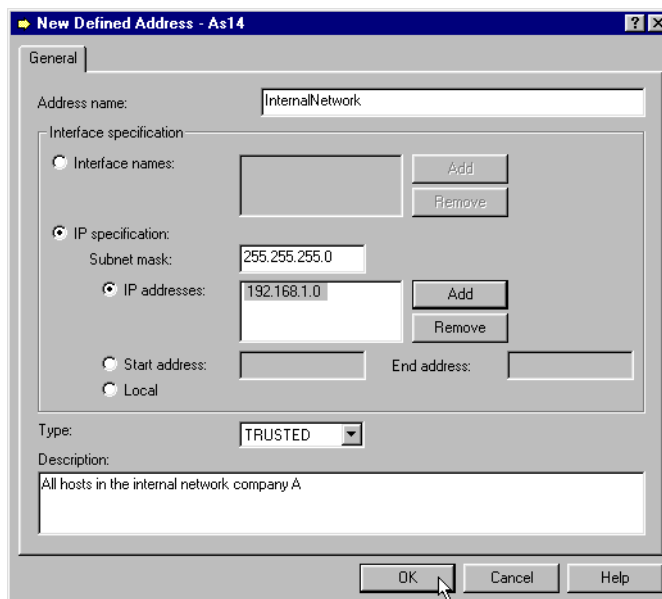


Figure 174. InternalNetwork defined address

10. Right-click **Filters**->**New Filter** (Figure 175 on page 181) to create a filter rule to permit general traffic inbound to and outbound from this host in the internal network.

Tip

This filter rule to permit the internal network traffic is *very* important, especially on a machine that has one physical interface with multiple logical IP interfaces. If you are running Operations Navigator on the PC with address 192.168.1.80 (see Figure 156 on page 165) and you don't have this rule to permit unrestricted internal network traffic, then, when you activate filters, by default all internal traffic will be denied. This may be what you wanted. If it isn't, you need to access the system console and issue the Remove TCP/IP Table (RMVTCPTBL TBL(*ALL)) command to remove the IP filters.



Figure 175. IP Packet Security GUI - Creating a filter rule

11. To permit IP traffic from and to the internal network, fill in the New Filter window as shown in Figure 176 on page 182. All associated filter rules (for example, all rules for one interface) should have the same Set name. In this example, use `VPNSET` for the Set Name.

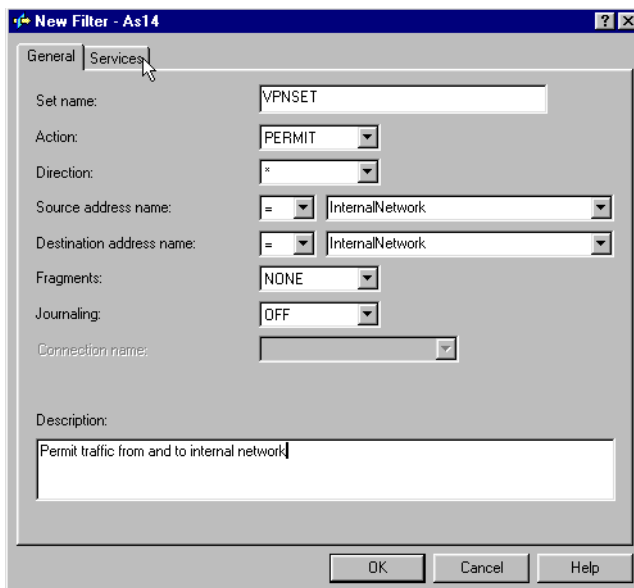


Figure 176. Permit inbound traffic from and outbound traffic to the internal network

12. Click the **Services** tab.

13. To permit all IP traffic from and to hosts in the internal network, complete the New Filter - Services window as shown in Figure 177.

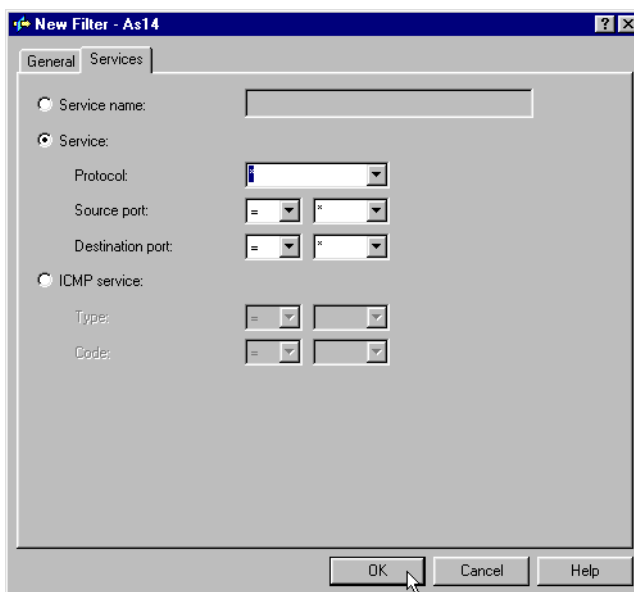


Figure 177. Allowing all protocols and ports

14. Click **OK**.

Create two filter rules to allow IKE traffic to flow into and out of the AS/400 system.

15. For the first filter rule (Figure 178 on page 183), specify `VPNSET` for the Set name parameter. Select **PERMIT** for the Action parameter and **OUTBOUND** for the Direction parameter. Specify the local AS14 AS/400 system's address,

10.196.11.1, in the Source address name field, and the remote AS20 AS/400 system's address, 102.196.11.14, in the Destination address name field.

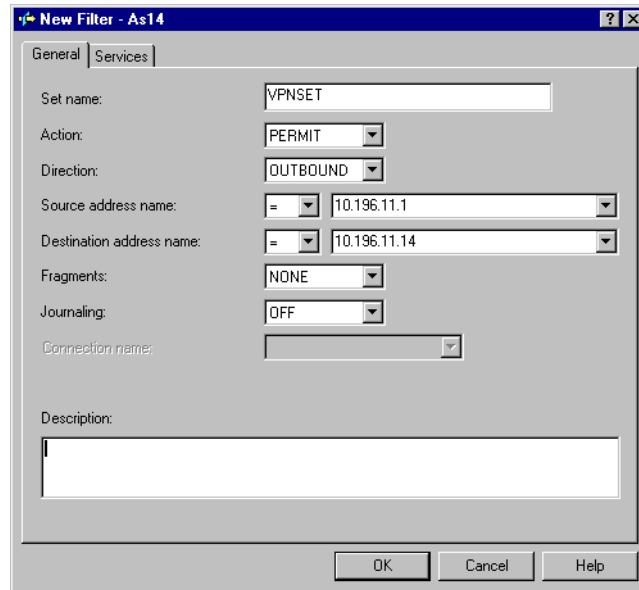


Figure 178. Outbound IKE filter rule

16. Click the **Services** tab.

17. On the Services page (Figure 179), select **Service**, and choose UDP for Protocol. Specify 500 for the Source port and Destination port parameters.

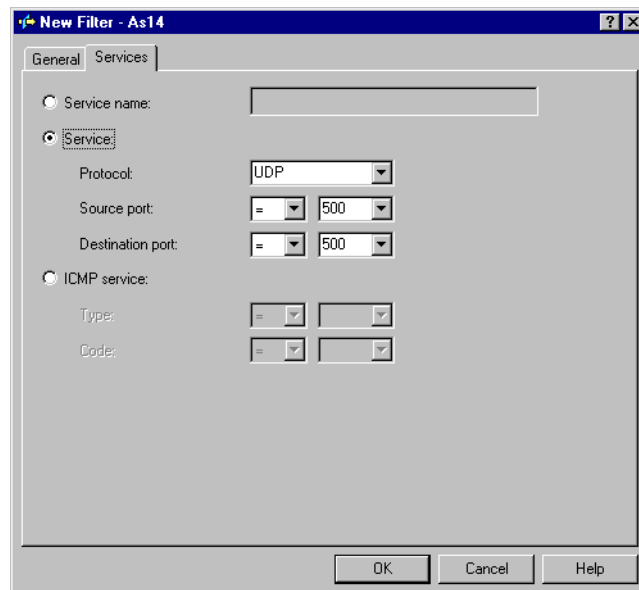


Figure 179. IKE filter rule services

18. Click **OK**.

19. For the second filter rule (Figure 180 on page 184), specify `VPNSET` for the Set name parameter. Select **PERMIT** for the Action parameter and **INBOUND** for the Direction parameter. Specify the remote AS20 AS/400 system address,

10.196.11.14, in the Source address name field and the local AS14 AS/400 system address, 10.196.11.1, in the Destination address name field.

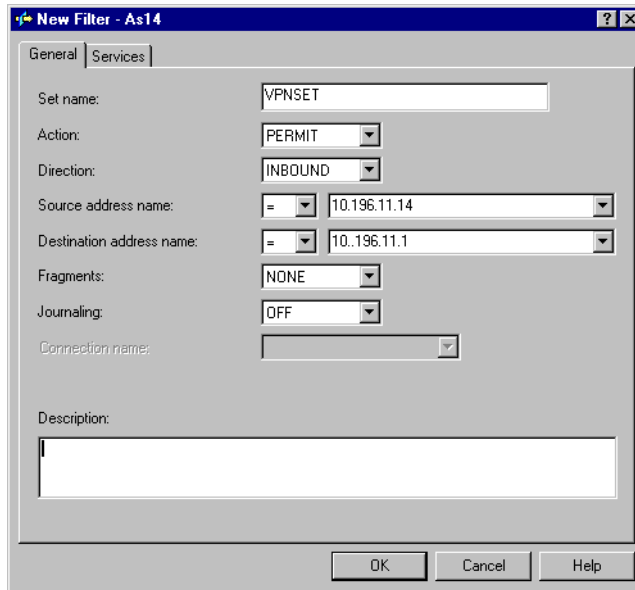


Figure 180. Inbound IKE filter rule

20. Click the **Services** tab.

21. On the Services page (Figure 181), select **Service**, and set Protocol to **UDP**. Specify 500 for the Source port and Destination port parameters.

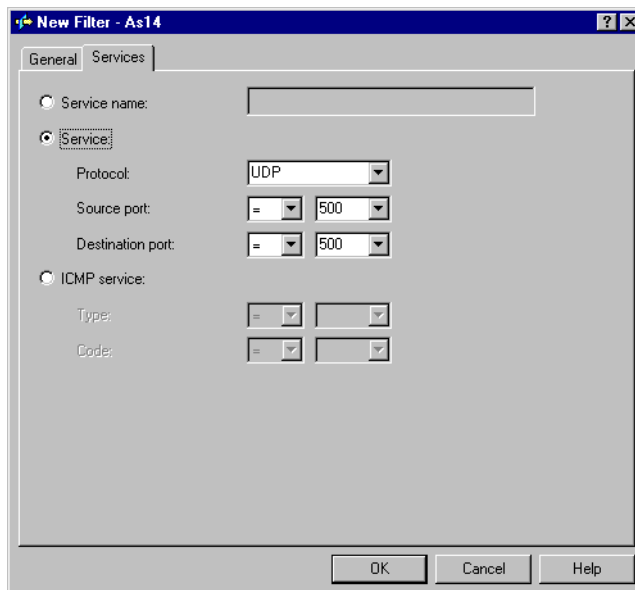


Figure 181. IKE filter rule services

22. Click **OK**.

23. Create another filter rule (Figure 182 on page 185) to allow data traffic to use the VPN tunnel. Use the same filter Set name, `VPNSET`, and specify **IPSEC** in the Action field. With an IPSEC filter rule, Direction is always set to **OUTBOUND** and grayed out. In the Source and Destination address

parameters, specify 10.196.11.1 and 10.196.11.14 respectively. The Connection name is, in fact, the data connection that in this case is a dynamic key connection *group*. Use the pull-down menu to list all the data connection names that are configured on this system, and select **HtoH14to20**.

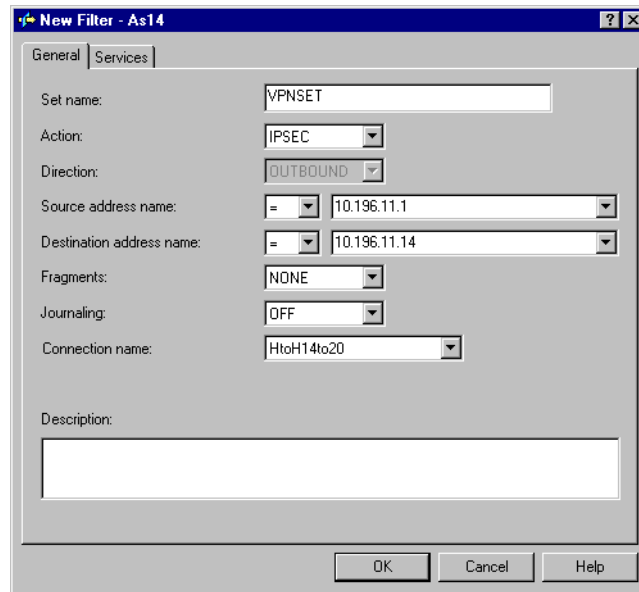


Figure 182. IPSEC filter rule

24. Click the **Services** tab.

25. On the Services page (Figure 183), select **Service**, and enter wildcard (*) in the Protocol, Source port, and Destination port fields. This allows any protocol using any port to use this filter rule and, therefore, the Virtual Private Network tunnel.

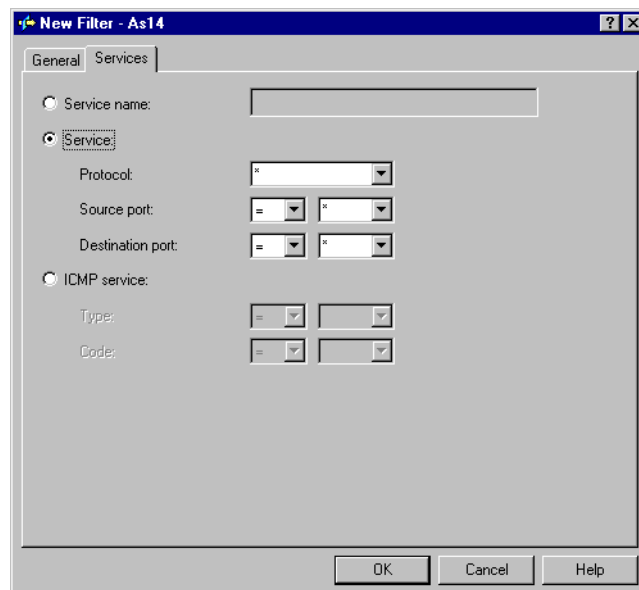


Figure 183. IPSEC filter rule service

26. Click **OK**.

Finally, create a filter interface rule to tie the filter rules to the required interface.

27. Right-click **Filter interfaces** at the IP Packet Security GUI and select **New filter interface**.

28. The same line description connects AS14 to the remote AS20 across the Internet and to the internal network. In this example, it is **TRNLINE**. Use the pull-down list for the line parameter (Figure 184) to select **TRNLINE**.

29. Click **Add** for the Set name parameter, and enter `VPNSET` for the filter set name.

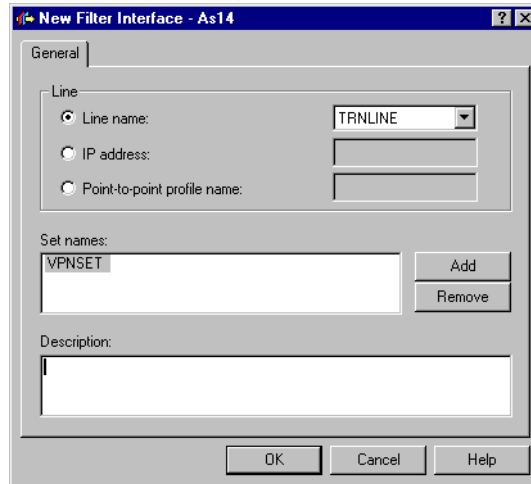


Figure 184. Filter interface rule

30. Click **OK**.

31. Back at the IP Packet Security GUI, click **File->Save** from the menu bar to save the filter rules file into the IFS with an extension of `i3p`. In this example, a subdirectory, `VPNRB`, was created under the directory `QIBM`. Save the filter rules file as `HtoH14to20.i3p` into `/QIBM/VPNRB`.

Figure 185 on page 187 shows the summary of the IP filter rules for this scenario.

```

IP Packet Security: All Security Rules
#Defined Address for the internal network
ADDRESS InternalNetwork IP = 192.168.1.0 MASK = 255.0.0.0 TYPE = TRUSTED
#Permit all traffic in internal network
FILTER SET VPNSET ACTION = PERMIT DIRECTION = * SRCADDR = InternalNetwork
    DSTADDR = InternalNetwork PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE
    JRN = OFF
#IKE filter rules
FILTER SET VPNSET ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 10.196.11.14
    DSTADDR = 10.196.11.1 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
    FRAGMENTS = NONE JRN = OFF
FILTER SET VPNSET ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 10.196.11.1
    DSTADDR = 10.196.11.14 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
    FRAGMENTS = NONE JRN = OFF
#IPSEC filter rule
FILTER SET VPNSET ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 10.196.11.1
    DSTADDR = 10.196.11.14 PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE
    JRN = OFF CONNECTION_DEFINITION = HtoH14to20
#Filter interface
FILTER_INTERFACE LINE = TRNLINE SET = VPNSET

```

Figure 185. AS14 IP filters summary

5.4 Configuring a host-to-host connection on AS20

The following sections summarize the configuration of the VPN and filters on the AS/400 VPN host AS20.

5.4.1 Completing the planning worksheets for AS20

Complete the planning worksheets to gather the information you need to create a host-to-host VPN connection with the VPN configuration wizard. Table 16 shows the planning worksheet for this scenario from the perspective the AS/400 VPN server AS20 AS/400 system. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 16. AS20 New Connection Wizard planning worksheet

This information needed to create VPN with the New Connection Wizard	Scenario answers
What is the type of connection to be created? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Host
What is the name of the connection group?	HtoH20to14
What type of security and system performance is required to protect the keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest security, lowest performance
How is the local VPN server identified?	IP address
What is the IP address of the local VPN server?	10.196.11.14

This information needed to create VPN with the New Connection Wizard	Scenario answers
How is the remote VPN server identified?	IP address
What is the IP address of the remote server?	10.196.11.1
What is the pre-shared key?	AndrewBryan
What type of security and system performance is required to protect the data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest security, lowest performance

The wizard provides the highest level of protection for protecting both key and data based on the values in Table 16.

Table 17 summarizes the information you need to create the IP filter rules.

Table 17. AS20 Planning worksheet - IP filter rules

This is the information needed to create the IP filters to support the VPN connection	Scenario answers
Is the local VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, the VPN server acts as a host. If no, the VPN server acts as a gateway.	Host
Is the <i>remote</i> VPN server acting as a host or gateway ?	Host
What is the name used to group together the set of filters that will be created?	VPNIFC
If the <i>local</i> VPN server is acting as a gateway ... – What is the IP address of the local ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	Not applicable
If the <i>remote</i> VPN server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	Not applicable
What is the IP address of the local VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	10.196.11.14
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	10.196.11.1

This is the information needed to create the IP filters to support the VPN connection	Scenario answers
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRNLINE
What other IP addresses, protocols, and ports are permitted on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	192.168.1.0

In summary, both the VPN and filter configurations are similar to the ones configured for AS14 in 5.3, “Configuring a host-to-host VPN on the AS/400 system (AS14)” on page 167, but swap IP addresses, change connection names, and configure AS20 as the terminator of the VPN connection.

5.5 Configuring a host-to-host VPN on AS20

Before using the New Connection Wizard to configure the VPN, change the default security values on AS20 as described in 5.3.2, “Changing the default security values” on page 169.

Use the New Connection Wizard to create the VPN configuration on AS20 by performing the following steps:

1. At the Virtual Private Networking GUI menu bar (Figure 186), click **File->New Connection**.

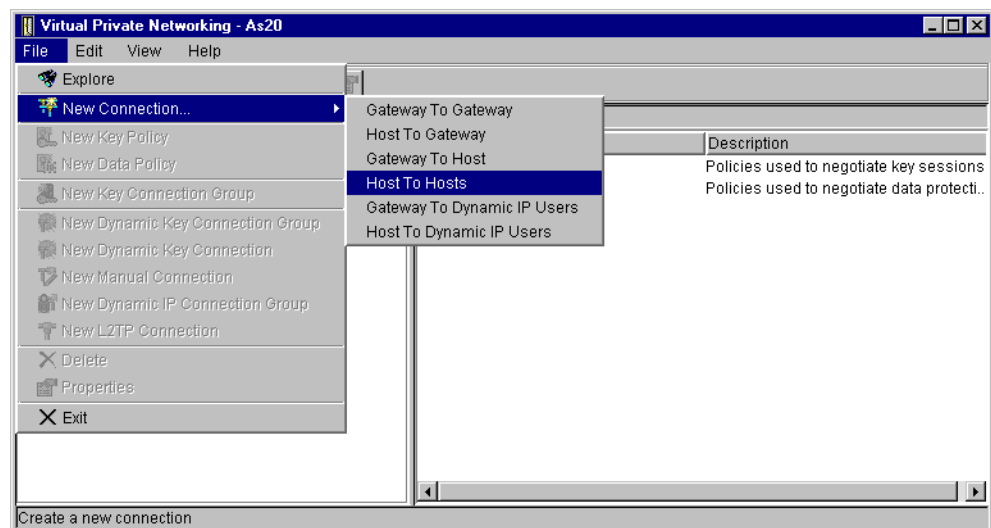


Figure 186. AS20 New Connection -> Host to hosts

2. Select **Host to Hosts**. This starts the New Connection Wizard for a host-to-host connection.
3. Click **Next** after reading the welcome window.
4. At the Connection Name window (Figure 187 on page 190), enter `HtoH20to14` for the Name of the connection group. This name is used for all objects that the wizard creates for this connection. It is case sensitive. Also enter a description of the configuration.

5. Click **Next**.

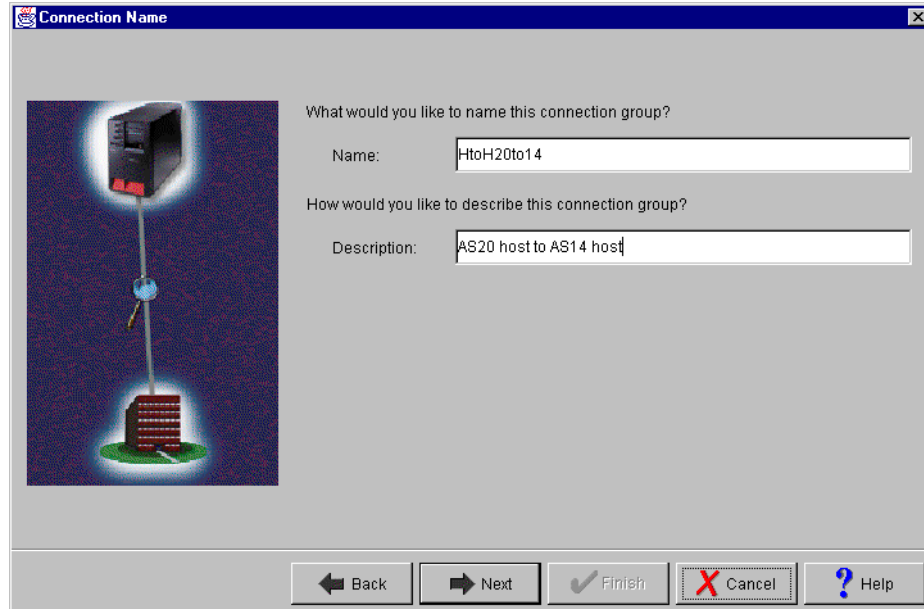


Figure 187. Connection Name window

6. At the Key Policy window (Figure 188), specify the level of authentication and encryption protection IKE uses during phase 1 negotiations. Phase 1 establishes the keys that protect the messages that flow during subsequent phase 2 negotiations. Phase 2 protects the data itself. Select **Highest Security, lowest performance** as specified on the worksheet. The wizard chooses the appropriate encryption and authentication algorithms based on the selection made here.

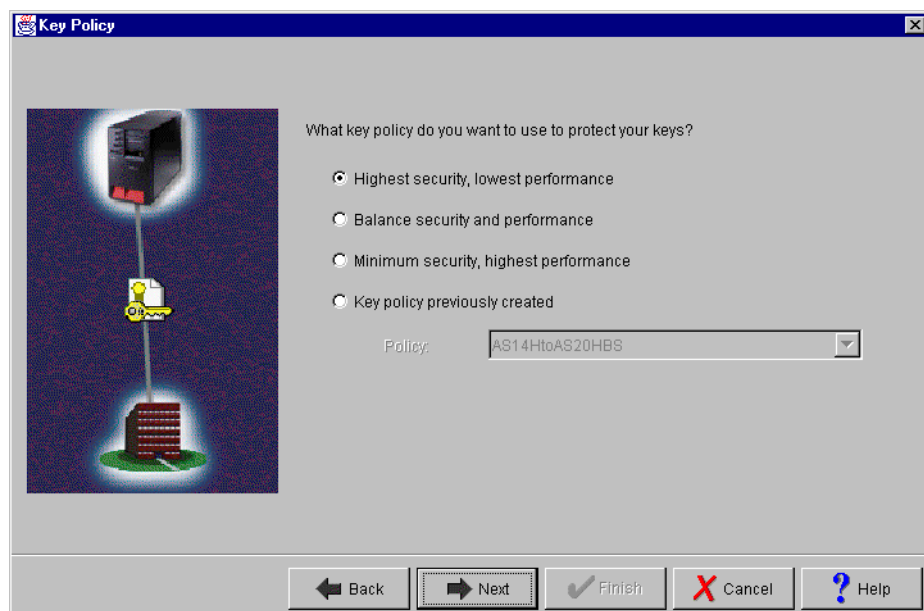


Figure 188. Key Policy window

7. Click **Next**.

- At the Local Identifier window (Figure 189), specify the identity of the local key server. Leave Identifier type as the default value **Version 4 IP address**. For the IP Address parameter, use the pull-down list to select the IP address of the interface that is connecting to the remote VPN host AS14. Refer back to the planning worksheets and to the network configuration in Figure 156 on page 165, for AS20 select **10.196.11.14**.

Note: Figure 189 shows various IP addresses, 10.70.21.1, 10.80.21.1, and so on, that we do not reference anywhere in this scenario. These interfaces are configured on AS20, but are used for other scenarios and projects and should be ignored here.

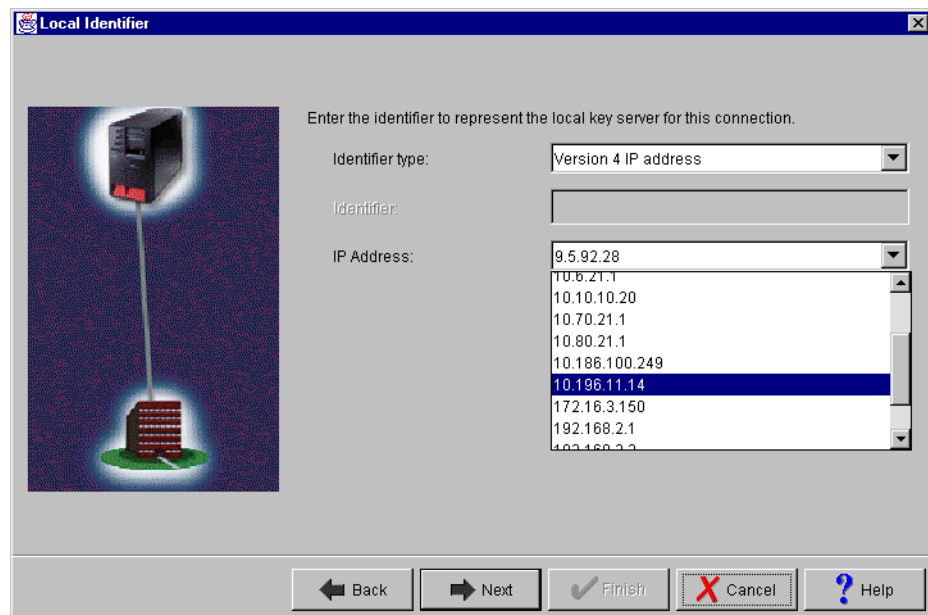


Figure 189. Local identifier window pull-down list

- Click **Next**.
- At the Remote Hosts window (Figure 190 on page 192), click **Add** to add a new remote identifier for AS14.

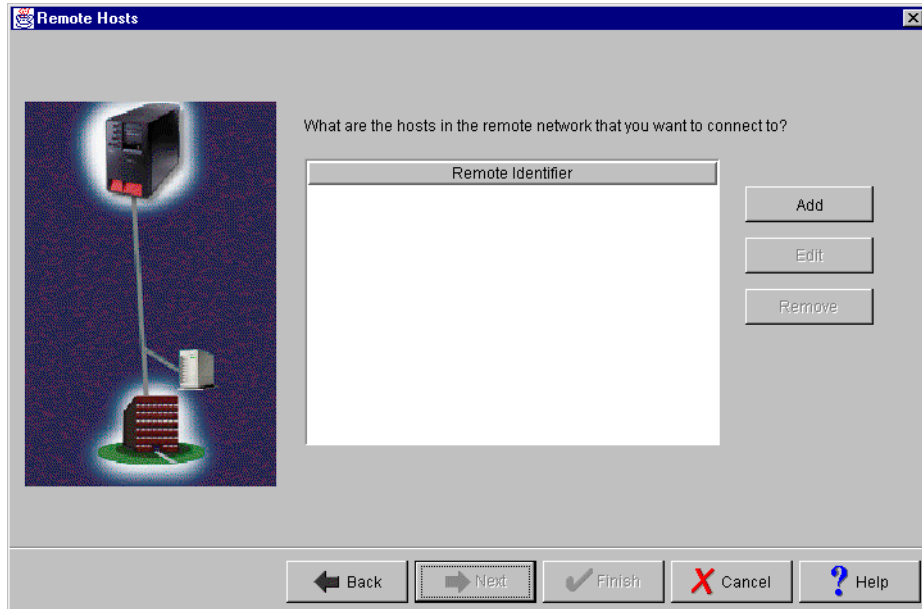


Figure 190. Remote Hosts window

11. At the Remote Identifier window (Figure 191), enter details about the remote key server, as well as the pre-shared key. The pre-shared key is the shared secret IKE uses to generate the actual keys for phase 1. The remote key server is AS14's IP Address, 10.196.11.1. Specify *AndrewBryan* in the Pre-shared key parameter. It is case sensitive. Remember, the same pre-shared key is entered when configuring VPN on the remote AS14 AS/400 system.

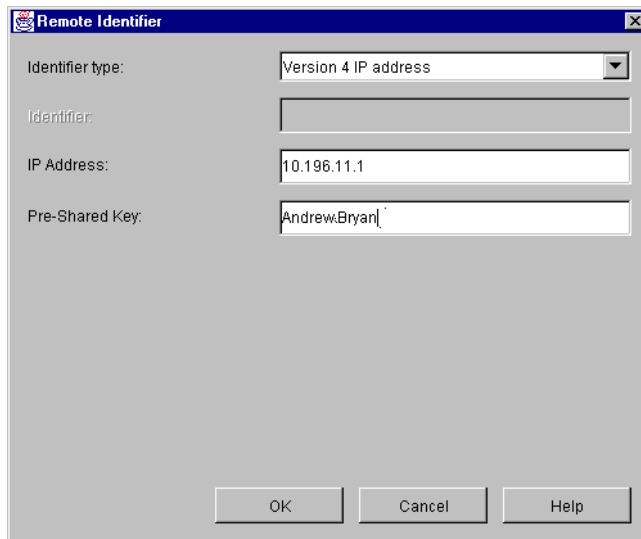


Figure 191. Remote Identifier window

12. Click **OK**.

13. Back at the Remote Hosts window (Figure 190), click **Next**.

14. Use the Data Policy window (Figure 192 on page 193) to specify the level of authentication and encryption that IKE uses to protect data flowing through

the host-to-host tunnel during phase 2 negotiations. For this example, select **Highest security, lowest performance** as specified on the worksheet in Table 16 on page 187.

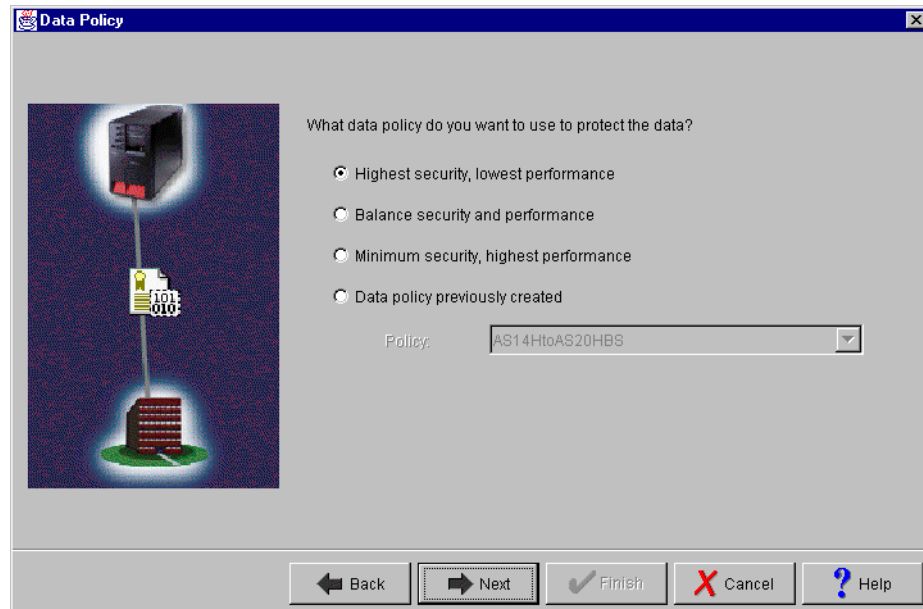


Figure 192. Data Policy window

15. Click **Next**.

16. The final window (Figure 193) summarizes the configuration values entered. Scroll down to see a list of the configuration objects that the wizard creates when you click Finish. Check the configuration values against the worksheets. If changes need to be made, click **Back**. Otherwise, click **Finish**.

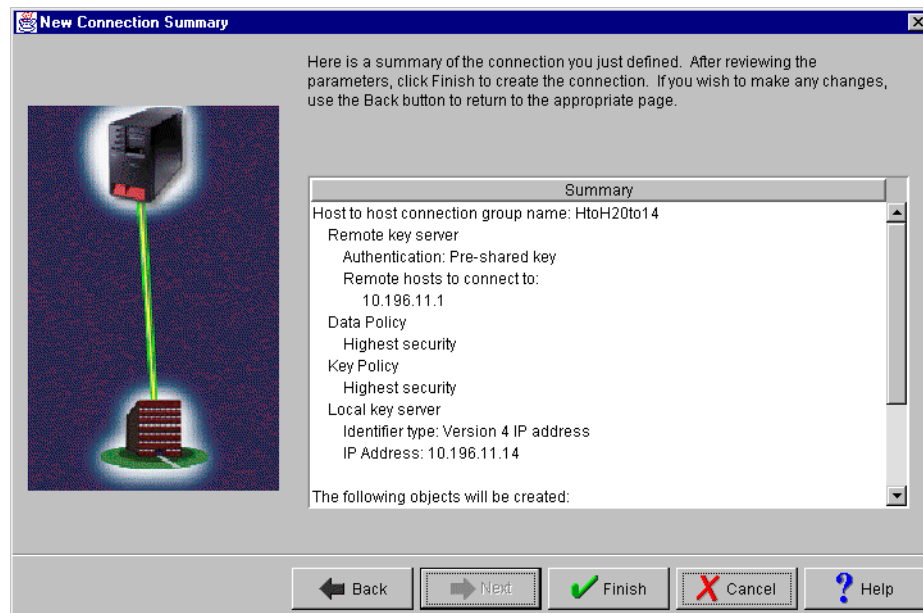


Figure 193. New Connection Summary window

The wizard creates the various objects that were configured for this VPN connection. After a short delay (and assuming there are no errors), the initial Virtual Private Networking GUI window is shown.

5.5.1 Customizing the VPN configuration created by the wizard on AS20

To configure AS20 to be the responder of the VPN connections in this scenario, perform the following steps:

1. At the Virtual Private Networking GUI, expand **Secure Connections**.
2. Expand **Data Connections**.
3. Expand **Dynamic Key Groups**.
4. Right-click the **HtoH20to14** Dynamic Key Group, and select **Properties**.
5. At the Dynamic Key Group Properties - General page (Figure 194), select **Only the remote system can initiate this connection** for the Initiation parameter.

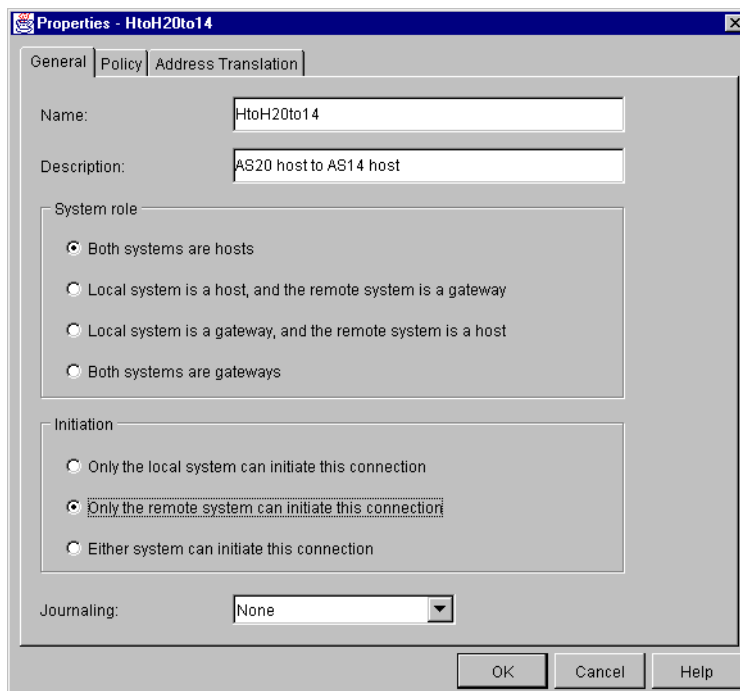


Figure 194. Dynamic Key Group Properties General page

6. Click **OK**.

This completes the VPN configuration customization for AS20.

5.5.2 Configuring IP packet security on AS20

To configure the required IP filters on AS20 for this scenario, repeat the steps described in 5.3.5, "Configuring IP packet security on AS14" on page 179, but swap IP addresses and use the connection group name configured on AS20 (HtoH20to14). Figure 195 on page 195 summarizes the filters configured on AS20 for this scenario.

```

IP Packet Security: All Security Rules
#Defined address for internal network
ADDRESS InternalNetwork IP = 192.168.1.0 MASK = 255.0.0.0 TYPE = TRUSTED
#Permit all traffic from and to internal network
FILTER SET VPNSET ACTION = PERMIT DIRECTION = * SRCADDR = InternalNetwork
    DSTADDR = InternalNetwork PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE
    JRN = OFF
#IKE filter rules
FILTER SET VPNSET ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 10.196.11.1
    DSTADDR = 10.196.11.14 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE
    JRN = OFF
FILTER SET VPNSET ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 10.196.11.14
    DSTADDR = 10.196.11.1 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE
    JRN = OFF
#IPSEC filter rule
FILTER SET VPNSET ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 10.196.11.14
    DSTADDR = 10.196.11.1 PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE
    JRN = OFF CONNECTION_DEFINITION = HtoH20to14
#Filter interface
FILTER_INTERFACE LINE = TRNLINE SET = VPNSET

```

Figure 195. AS20 IP filters configuration summary

5.6 Configuration cross-reference table

Table 18 summarizes the AS14 and AS20 configurations and provides a cross-reference list.

Table 18. AS14 and AS20 configuration cross-reference table

<u>AS14 AS/400</u>	<u>AS20 AS/400</u>
Key Policy	Key Policy
Name = HtoH14to20HS	Name = HtoH20to14HS
Initiator Negotiation = Agressive Mode (1)	Responder Negotiation = Agressive Mode (1)
Key Protection Transforms	Key Protection Transforms
Authentication Method = Pre-shared key (2)	Authentication Method = Pre-shared key (2)
Pre-shared key value = AndrewBryan (3)	Pre-shared key value = AndrewBryan (3)
Hash Algorithm = SHA (4)	Hash Algorithm = SHA (4)
Encryption Algorithm = 3DES-CBC (5)	Encryption Algorithm = 3DES-CBC (5)
Diffie-Hellman Group = Default 768-bit MODP (6)	Diffie-Hellman Group = Default 768-bit MODP (6)
Key Management	Key Management
Maximum key lifetime (minutes) = 180 (7)	Maximum key lifetime (minutes) = 180 (7)
Maximum size limit (kilobytes) = No size limit (8)	Maximum size limit (kilobytes) = No size limit (8)
Data Policy	Data Policy
Name = HtoH14to20HS	Name = HtoH20to14HS
Use Diffie-Hellman Perfect Forward Secrecy = Yes (9)	Use Diffie-Hellman Perfect Forward Secrecy = Yes (9)
Diffie-Hellman Group = Default 768-bit MODP (10)	Diffie-Hellman Group = Default 768-bit MODP (10)
Data Protection Proposals	Data Protection Proposals
Encapsulation mode = Transport (11)	Encapsulation mode = Transport (11)
Protocol = ESP (12)	Protocol = ESP (12)
Algorithms	Algorithms
Authentication Algorithm = HMAC-SHA (13)	Authentication Algorithm = HMAC-SHA (13)
Encryption Algorithm = 3DES-CBC (14)	Encryption Algorithm = 3DES-CBC (14)
Key Expiration	Key Expiration
Expire after (minutes) = 5 (15)	Expire after (minutes) = 5 (15)
Expire at size limit (kilobytes) = No size limit (16)	Expire at size limit (kilobytes) = No size limit (16)
Key Connection Group	Key Connection Group
Name = HtoH14to20	Name = HtoH20to14
Remote Key Server	Remote Key Server
Identifier Type = Version 4 IP address (17)	Identifier Type = Version 4 IP address (19)
IP address = 10.196.11.14 (18)	IP address = 10.196.11.1 (20)
Local Key Server	Local Key Server
Identifier Type = Version 4 IP address (19)	Identifier Type = Version 4 IP address (17)
IP address = 10.196.11.1 (20)	IP address = 10.196.11.14 (18)
Key Policy = HtoH14to20HS	Key Policy = HtoH20to14HS
Dynamic Key Group	Dynamic Key Group
Name = HtoH14to20	Name = HtoH20to14
System Role = Both systems are hosts (21)	System Role = Both systems are hosts (21)
Initiation = Only the local system can initiate this connection (22)	Initiation = Only the remote system can initiate this connection (22)
Policy	Policy
Data Management Security Policy = HtoH14to20HS	Data Management Security Policy = HtoH20to14HS
Connection Lifetime = 480 minutes	Connection Lifetime = Never Expires
Local addresses = Filter rule	Local addresses = Filter rule
Local ports = Filter rule	Local ports = Filter rule
Remote addresses = Filter rule	Remote addresses = Filter rule
Remote ports = Filter rule	Remote ports = Filter rule
Protocol = Filter rule	Protocol = Filter rule
Dynamic Key Connection	Dynamic Key Connection
Name = HtoH14to20:L1	Name = HtoH20to14:L1
Key Connection Group = HtoH14to20	Key Connection Group = HtoH20to14
Start when TCP/IP is started? = Yes	Start when TCP/IP is started? = No
Local Address = 10.196.11.1 (20)	Local Address = 10.196.11.14 (18)
Remote Address = 10.196.11.14 (18)	Remote Address = 10.196.11.1 (20)
IP Filters	IP Filters
Name = HtoHAsToAS.I3P	Name = HtoHAsToAS.I3P
IPSEC rule	IPSEC rule
Source address name = 10.196.11.1 (20)	Source address name = 10.196.11.14 (10)
Destination address name = 10.196.11.14 (18)	Destination address name = 10.196.11.1 (20)
Connection Name = HtoH14to20	Connection Name = HtoH20to14
Services	Services
Protocol = * (23)	Protocol = * (23)
Source port = * (24)	Source port = * (25)
Destination port = * (25)	Destination port = * (24)

5.7 Starting the VPN connection

For a complete description on activating IP filters and starting VPN connections, refer to 3.8, "VPN operations and management" on page 84.

The following list summarizes the steps you must perform to start the VPN connections:

1. Activate IP filters on both AS/400 systems (AS14 and AS20).
2. Start Virtual Private Networking on both AS/400 systems (AS14 and AS20).
3. On the initiator AS/400 system, AS14, start the dynamic key connections to AS20. In this scenario, start the connections **HtoH14to20:L1**.
4. At the Virtual Private Networking window, click **View**, and select **Active Connections**.

The Active Connections window (Figure 196) shows the host-to-host VPN connection running.

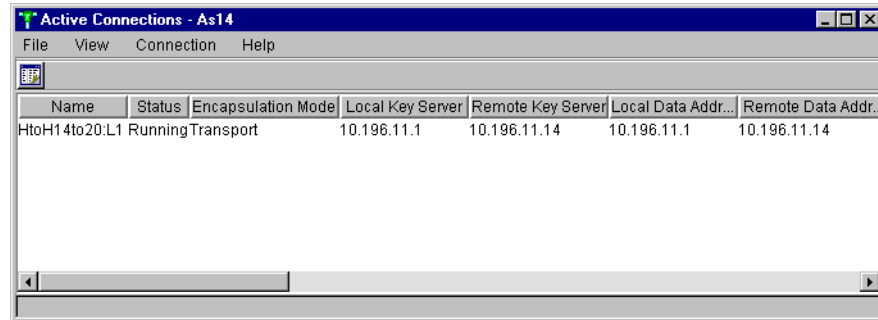


Figure 196. AS14 Active Connections window

5.8 Performing verification tests

After starting the VPN connection, perform the verification tests shown in Table 19. Use the IP addresses of the VPN data endpoint (10.196.11.*).

Table 19. Verifications tests - AS14 AS/400 host-to-AS20 AS/400 host scenario

	Start connection	PING	TELNET	FTP	SMTP
From AS14 to AS20	Yes	Yes	Yes	Yes	Yes
From AS20 to AS14	No	Yes	Yes	Yes	Yes

Chapter 6. Gateway-to-gateway VPN

A machine acting as a gateway usually connects systems in two separate networks at both sides of the gateway. The gateway system is not the data endpoint of the connection. Tunnel mode is used when at least one of the two systems participating in an IPSec tunnel is a gateway. Refer to 1.5.2, “AH transport and tunnel modes” on page 16, and 1.6.2, “ESP transport and tunnel modes” on page 20, for information on how the IP datagrams are processed in tunnel mode.

In a gateway-to-gateway VPN, a secure tunnel is established between the two gateway systems. Other hosts at both sides of the tunnel can use it to communicate securely between the two networks. The gateways or VPN servers perform the IKE negotiations and apply the IPSec protocols to the IP datagrams that flow through the secure tunnel. Other hosts using the tunnel don't need to support VPN functions.

This chapter introduces the concept of a gateway-to-gateway VPN, with AS/400 systems acting as VPN gateways, both directly attached to the Internet or intranet. For information on how to implement an AS/400 VPN gateway behind a firewall, refer to Chapter 12, “Don't forget a firewall: Protecting your VPN server” on page 515.

6.1 VPN gateways at the network boundaries: No firewall protection

This chapter explores scenarios where both gateways are connected directly to the intervening network. In other words, they are *border* or *edge* systems, which are not protected by firewalls. These examples serve as a useful introduction to the steps involved in setting up a VPN configuration and may also be a good solution in the following environments:

- Secure connection of subnets belonging to remote departments of a company across its private intranet. Examples of departments that may require secure communications include finance, human resources, and research and development (R&D).
- Secure connectivity extended to remote sites that are currently not connected. Some small, remote locations were not economically viable to connect to or had a remote controller that dialed-up the central office during some hours of the day. Now you can extend secure connectivity over the Internet to those remote sites by adding an AS/400 VPN gateway. Not only can the remote locations communicate with the corporate office, but they can also communicate with each other. The AS/400 systems on both networks are subject to rigorous security controls, including the implementation of native IP filtering. In this case, the AS/400 systems are most likely *not* running key production applications. Firewall functions such as SOCKS server and split DNS are *not* required and the customer's security policy permits such connections to the Internet. In most cases, filters *only* permit VPN connections over the public interface.

Figure 197 on page 200 shows an overview of the network presented in this chapter. XYZ Electronics has a pair of confidential research departments at different physical locations. The company's own private T1 network connects the two departments.

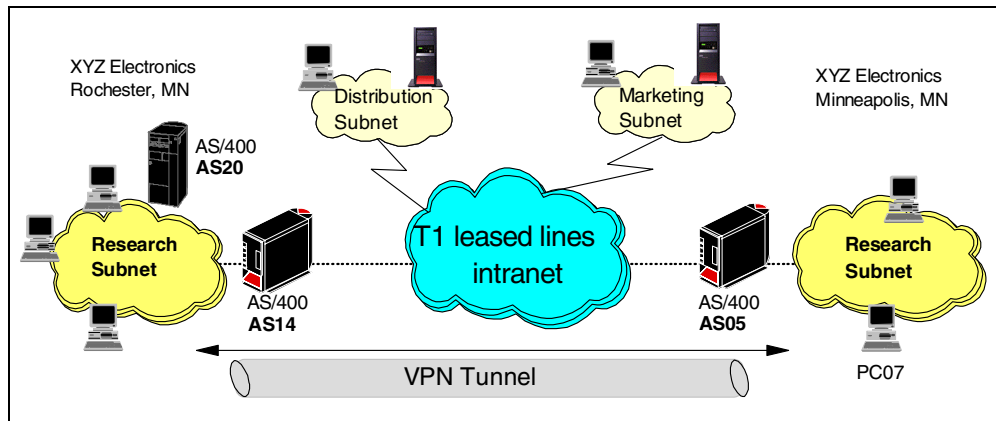


Figure 197. Gateway-to-gateway VPN - No firewall

6.1.1 Scenario characteristics

The main characteristics of this scenario are:

- The AS/400 systems, which are acting as a VPN gateway for the research subnets, are directly connected to the intervening network (no firewall protection).
- The gateway system has two physical interfaces: one line to connect it to the intervening network and a second line to connect the gateway to the internal subnet.
- The intervening network is a private network in this scenario. If the intervening network were the public Internet, the security controls applied to the AS/400 system acting as a gateway must be rigorous.

6.1.2 Scenario objectives

The objectives of this scenario are:

- All traffic between the research networks must be protected by a VPN tunnel.
- All traffic can flow in the clear inside the research intranets. Both networks belong to the same department, and there is strong physical security monitoring access to the premises. Therefore, only the VPN servers need to provide VPN functions.
- All clients and hosts on each network have full access to the partner's network, including all applications (Telnet, FTP, LPR/LPD, HTTP, etc.).
- Block all inbound traffic into the gateway AS/400 systems other than the VPN tunnel.
- Enable communications to and from applications on the gateway AS/400 systems themselves.

6.2 Implementing the Gateway to gateway: No firewall scenario

This section describes the tasks that you must perform to install and configure a gateway to gateway scenario with no intermediate firewalls. In this scenario, we allow client and server access from either partner subnet connected to the VPN tunnel. That is, we are not restricting the type of applications (TELNET, FTP, and so on), or the hosts that can use this tunnel. Anything on one partner subnet can talk to anything on the other partner subnet as though they were directly connected. As you will see later, this excludes applications running on the gateway AS/400 systems themselves.

6.2.1 Scenario network configuration

Figure 198 shows the network configuration for the *Gateway to gateway: No firewall* scenario. Each IP address is lettered, A to J. We use these letters to reference the interfaces and addresses in the following discussions.

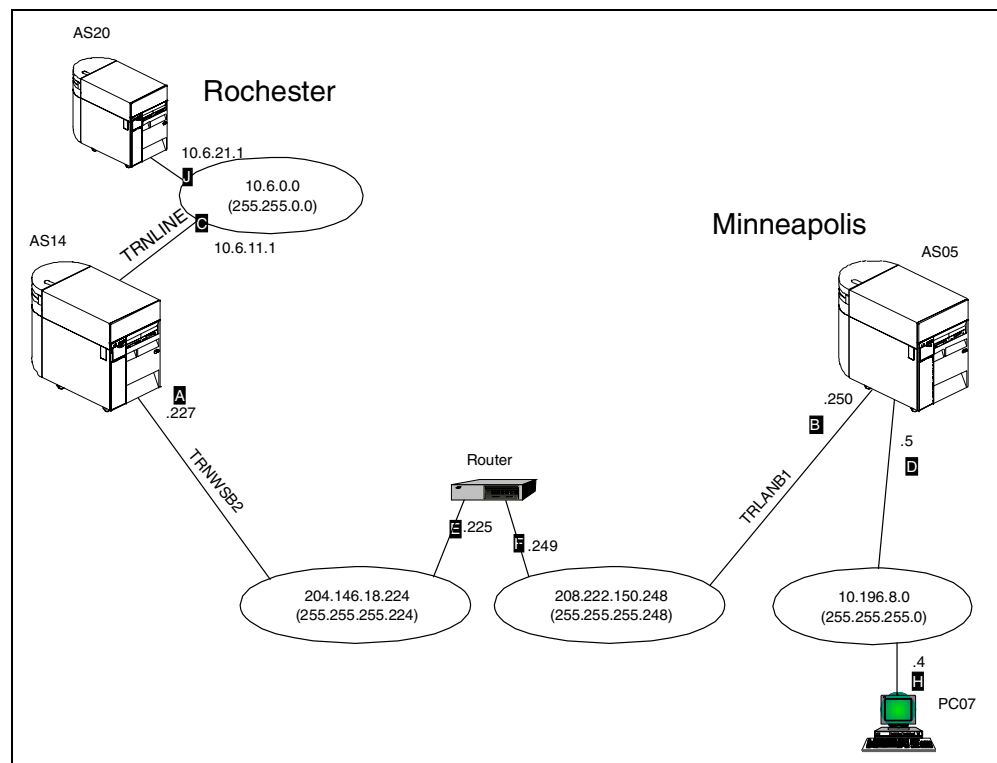


Figure 198. Gateway to gateway: No firewall scenario test network

The characteristics of the test network are:

- AS14 is an AS/400 system running OS/400 V4R4. AS14 represents the Rochester office VPN gateway.
- AS05 is an AS/400 system running OS/400 V4R4. AS05 represents the Minneapolis office VPN server.
- AS20 is an AS/400 system running standard TCP/IP applications. VPN functions are not configured on this system. It represents a generic TCP/IP host in the corporate network. For all practical purposes, it does not support VPN.

- PC07 represents a generic client (also referred to as a *host* in TCP/IP terminology) on the other remote subnet. PC7 will access the TCP/IP applications on AS20 through the VPN tunnel.
- At the Rochester office, the network administrator assigns a portion of a class C network to connect to the *Internet*. The corporate office Demilitarized Zone (DMZ) is assigned the network address 204.146.18.224, with subnet mask 255.255.255.224.
Note: In this context, Internet refers to the intervening network between the two VPN gateways.
- At the Minneapolis office, the network administrator assigns a portion of a class C network to connect to the Internet. The Minneapolis office DMZ is assigned the network address 208.222.150.248, with subnet mask 255.255.255.248.
- The Rochester office uses the subnet 10.6.0.0, with subnet mask 255.255.0.0 in its intranet. This subnet represents the data endpoint of the VPN tunnel at the Rochester office site.
- The Minneapolis office uses the subnet 10.196.9.0, with subnet mask 255.255.255.0 in its intranet. This subnet represents the data endpoint of the VPN tunnel at the Minneapolis office site.
- TRNWSB2 is the Token-Ring line description connecting AS14 to the Internet router in subnet 204.146.18.224.
- TRNLINE is the Token-Ring line description connecting AS14 to the corporate intranet subnet 10.6.0.0.
- TRLANB1 is the Token-Ring line description connecting AS05 to the Internet router in subnet 208.222.150.248.

6.2.2 Implementation task: Summary

This section summarizes the tasks that you need to perform to implement the *Gateway to gateway: No firewall* scenario:

Complete the following tasks to implement the *Gateway to gateway: No firewall* scenario:

1. Verify TCP/IP routing so that:
 - The gateway AS/400 systems can communicate to each other across the intervening Internet or intranet.
 - Hosts on each subnet are routed to their respective gateway for access to the remote subnet.
2. Complete the VPN checklists and planning worksheets for both AS/400 gateways.
3. Configure VPN on the Rochester gateway AS/400 system (AS14).
4. Configure IP filtering on AS14 referring to the VPN *connection group* configured in the previous step.
5. Configure VPN on the Minneapolis gateway AS/400 system (AS05).
6. Configure IP filtering on AS05 referring to the VPN connection group configured in the previous step.
7. Activate filters, and start VPN servers on both AS/400 gateways.

8. Start the VPN connection from one AS/400 system.
9. Test communications between the two remote subnets, and (optionally) use the AS/400 communications trace to verify that secure protocols are being used.
10. Add host-to-gateway connection groups to allow applications on the AS/400 gateways to talk to each other and to the remote subnets.

6.2.3 Verifying TCP/IP routing

Defining basic TCP/IP routing is beyond the scope of this redbook. However, it is vital that routing be configured and tested before attempting to implement a VPN connection. If you cannot establish normal TCP/IP communications between the required endpoints, the VPN will not work. Because you will likely use data encryption under VPN (which, by design, means line traces cannot be fully interpreted), problem determination is more difficult once the datagrams are encrypted. The recommendation is to sort out all routing and communication problems *before* implementing the VPN tunnel.

In the case of the Internet, your gateway AS/400 systems must be able to communicate to each other using public addresses. However, if you are using private network addresses on your local networks, these, by definition, will not route across the Internet. Therefore, you must configure local routing so that any request for the remote network routes to the gateway AS/400 system.

For example, Table 20 shows the routing configuration on AS14, and Table 21 shows the routing information for AS20.

Table 20. VPN gateway AS14 routes

Destination network	Next hop
10.196.8.0	204.146.18.225 - the "Internet" router
208.222.150.248	204.146.18.225 - the "Internet" router

Table 21. 'Generic' host AS20 routes

Destination network	Next hop
10.196.8.0	10.6.11.1 - AS14

Note: Rather than adding routing information to all hosts (including PC clients) that use the VPN tunnel, it may be possible to make the VPN gateway AS/400 system the default TCP/IP gateway. Alternatively, if you use routers on the local network, you may only need to add the necessary routing information once to a suitable router.



6.3 Configuring the Rochester AS/400 VPN gateway (AS14)

The following sections take you step-by-step through the configuration of the VPN and filters on the AS/400 VPN gateway in the Rochester network.

6.3.1 Planning worksheets for the the AS14 gateway

Complete the planning worksheets to gather the information you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 22 shows the planning worksheet for this scenario from the perspective of the VPN gateway at the Rochester network (AS14 in Figure 198 on page 201).

Table 22. AS14 New Connection Wizard planning worksheet - Gateway-to-gateway VPN

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	GtoG14toO5
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	204.146.18.227 
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	208.222.150.250 
What is the pre-shared key?	bdcfhhnprotvqa
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

We completed this planning worksheet (Table 22) from the perspective of AS14. The wizard selects IPSec protocols to balance security and performance for protecting both key and data information. The main configuration object, the *connection group*, is named *GtoG14toO5*, and the pre-shared key is a string of characters, *bdcfhhnprotvqa*.

To complete the VPN configuration, you must configure IP filters. Table 23 on page 205 shows the planning worksheet for the IP filters configured in this scenario.

Table 23. AS14 Planning worksheet - IP filters configuration

This is the information you need to create your IP filters to support your VPN	Scenario answers
<p>Is <i>your</i> VPN server acting as a host or gateway? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.</p>	Gateway
<p>Is the <i>remote</i> VPN server acting as a host or gateway?</p>	Gateway
<p>What name do you want to use to group together the set of filters that will be created?</p>	VPNIFC
<p>If <i>your</i> server is acting as a gateway... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.</p>	10.6.0.0 (see note) 255.255.0.0 AS14subnets
<p>If the <i>remote</i> server is acting as a gateway... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.</p>	10.196.0.0 (see note) 255.255.0.0 AS05subnets
<p>What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host.</p>	204.146.18.227 A
<p>What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host.</p>	208.222.150.250 B
<p>What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?</p>	TRNWSB2
<p>What other IP addresses, protocols and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i>!</p>	

Note: The actual subnet behind AS05 is 10.196.8.0, with a subnet mask of 255.255.255.0. By specifying a subnet of 10.196.0.0 and a subnet mask of 255.255.0.0, you are allowing any other networks subsequently added to AS05 and beginning with 10.196.*.* to use this VPN tunnel. Make sure that when you create the matching filter set on AS05, you also specify a subnet of 10.196.0.0 and a subnet mask of 255.255.0.0.

We completed the IP filter rules planning worksheet (Table 23) from the perspective of AS14. The filter rules allow traffic between any 10.6.*.* address on

the local network and any 10.196.*.* address on the remote network. To configure the filter rules, you need to give each of these address ranges a name. In this example, specify *AS14subnets* and *AS05subnets* respectively. You also need to choose a filter set name, *VPNIFC*, so you can group all your rules together and apply them to an interface. The interface is *TRNWSB2*. This is the Token-Ring line description used to connect to the 204.146.18.224 network. You are not going to permit any other traffic through *TRNWSB2*. When you activate these filter rules, they allow only the VPN gateway-to-gateway tunnel through *TRNWSB2*.

6.3.2 Configuring the gateway-to-gateway VPN on AS14

Perform the following steps to configure the gateway-to-gateway VPN on AS14:

1. Start Operations Navigator from your desktop.
2. Expand your AS/400 system, in this case, **AS14**. Sign on when prompted.
3. Expand **Network**.
4. Double-click **IP Security** (Figure 199) to reveal two server names in the right window: IP Packet Security and Virtual Private Networking. You must configure both of these, but start with Virtual Private Networking.

Note

At this stage, Virtual Private Networking may already have a status of *Started*, since the default is for the server to automatically start when TCP/IP starts. The server can be either *started* or *stopped* during the following steps.

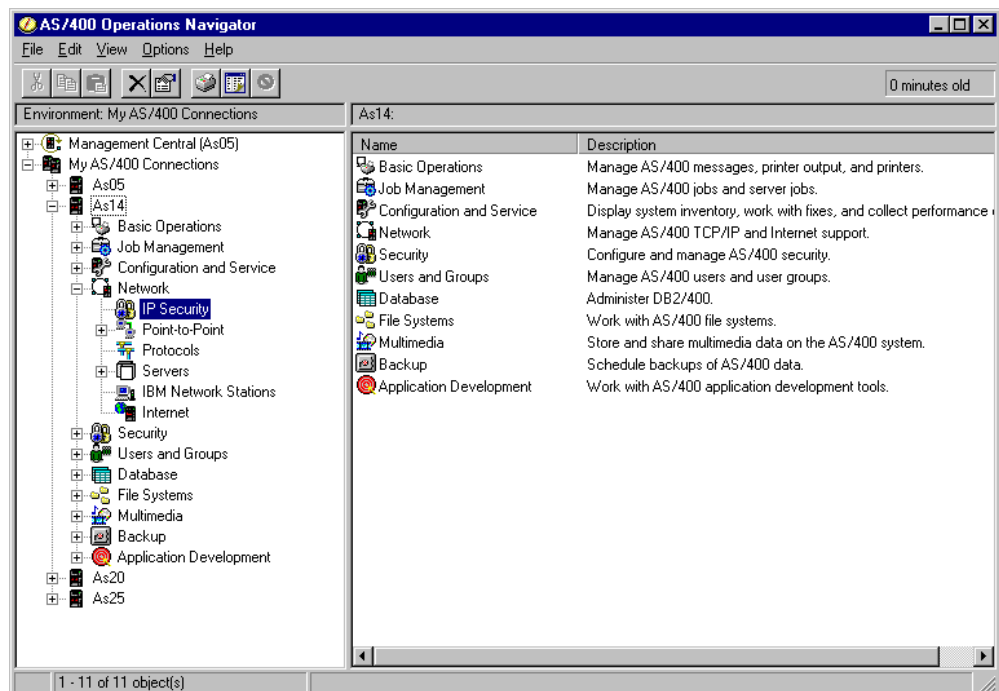


Figure 199. Operations Navigator - IP Security

5. Double-click **Virtual Private Networking** to start the VPN GUI (Figure 200).

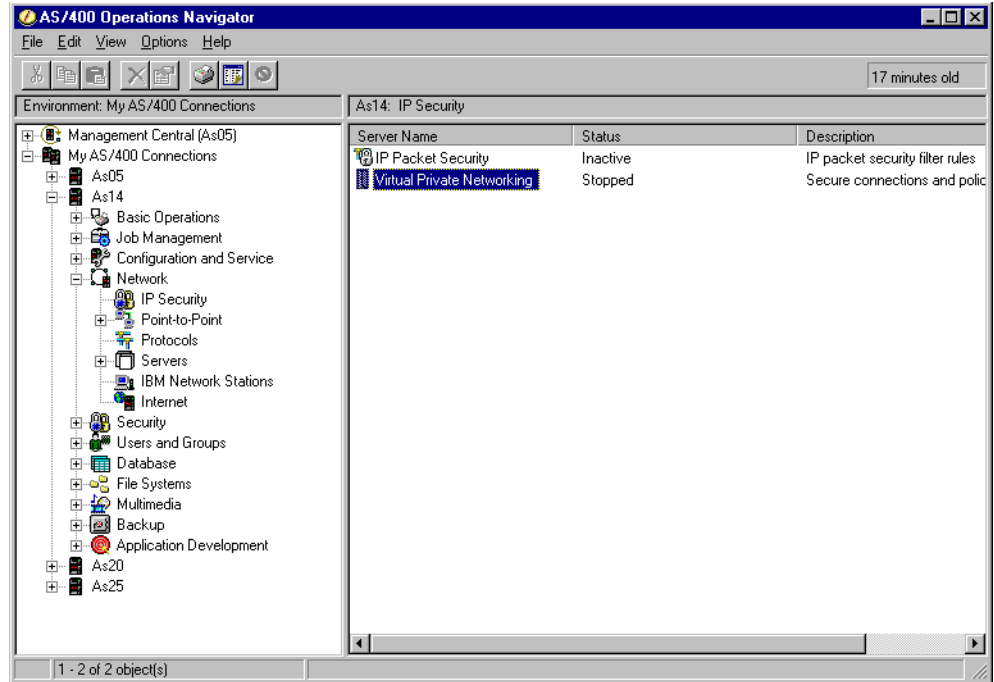


Figure 200. Operations Navigator - Starting VPN configuration GUI

The Virtual Private Networking window is displayed (Figure 201).

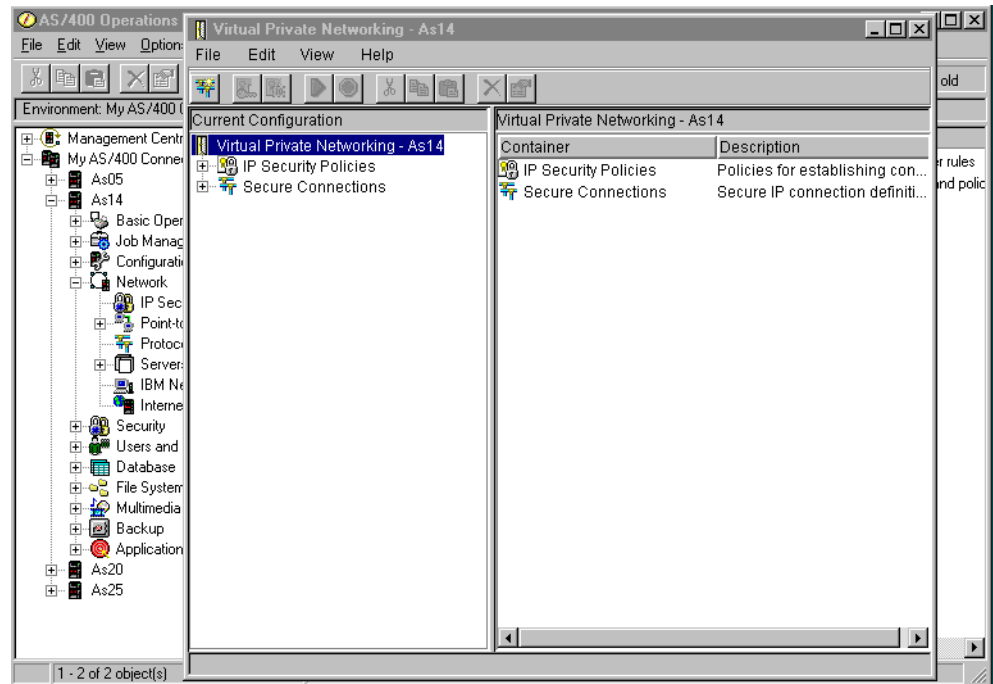


Figure 201. VPN GUI configuration interface

6. Select **File->New Connection**.
7. Select **Gateway To Gateway** from the pull-down menu (Figure 202 on page 208).

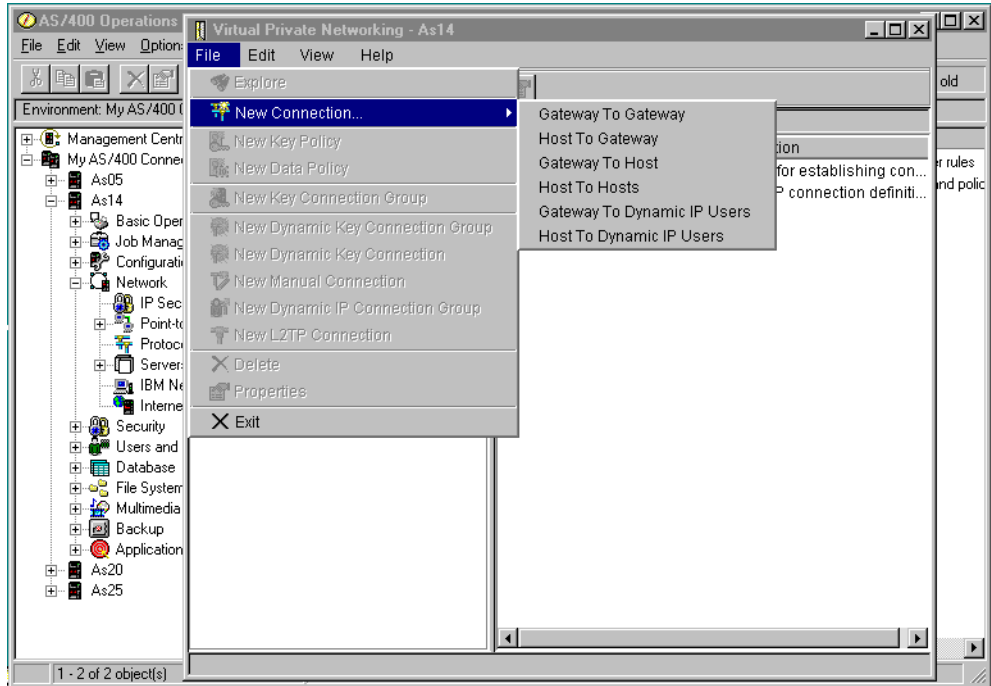


Figure 202. New Connection->Gateway to Gateway

This starts the New Connection Wizard for a gateway-to-gateway connection (Figure 203).

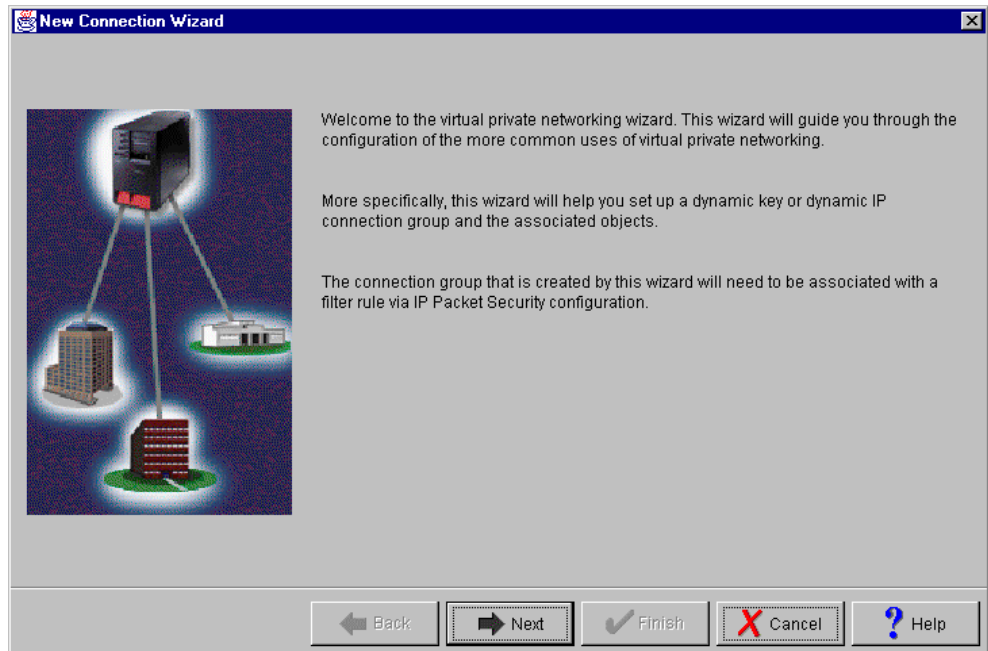


Figure 203. New Connection Wizard welcome window

Note 1: Read the New Connection Wizard welcome page. The wizard can only be used to configure dynamic key or dynamic IP connections. You must configure a *manual* connection, for example, if you are connecting to a remote system that does not support the Internet Key Exchange (IKE) protocols.

Note 2: The welcome screen also indicates that you must associate the connection group that the wizard creates with a filter rule by using the IP packet security configuration. The wizard does not create filter rules. You must always create these manually.

8. Click **Next** after reading the Welcome window.
9. At the Connection Name window (Figure 204), enter the name `GtoG14to05` for the connection group. Remember that `GtoG14to05` is the name from the planning worksheet in Table 22 on page 204. The name that you specify here is the name for all objects that the wizard creates for this particular connection. It is case sensitive. Also, enter a description of the configuration that you are creating.

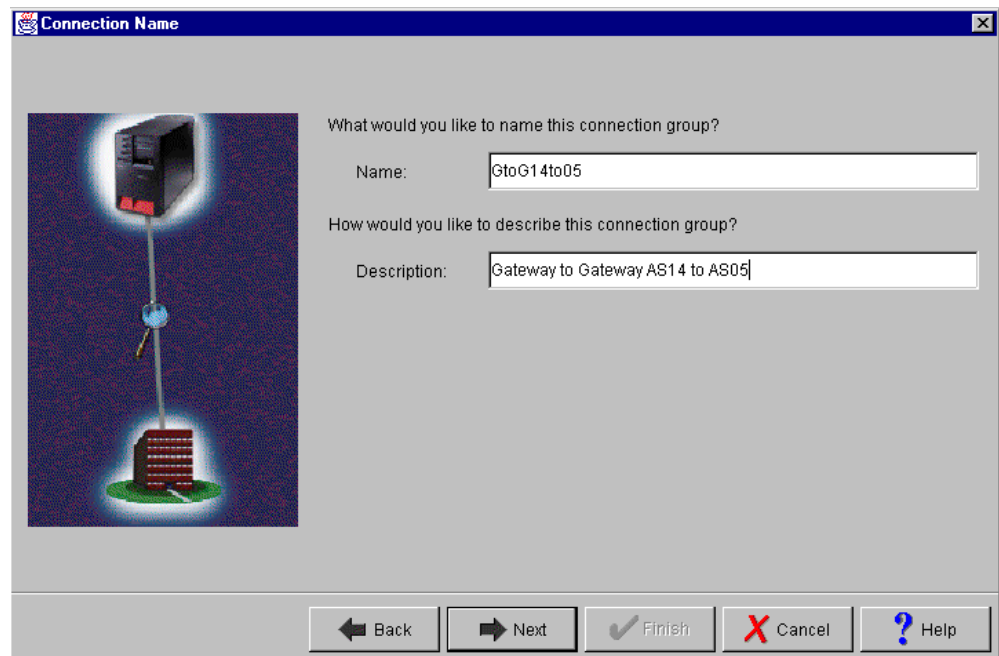


Figure 204. Connection Name window

10. Click **Next**.
11. On the Key Policy window (Figure 205 on page 210) specify the level of authentication or encryption protection that IKE uses during phase 1 negotiations. Phase 1 negotiations establish the keys that protect the messages that flow during subsequent phase 2 negotiations. Phase 2 negotiations establish the keys that protect the data itself. For the purposes of this example, select **Balance security and performance** as specified on the worksheets. The wizard chooses the appropriate encryption and authentication algorithms based on the selection you make here.

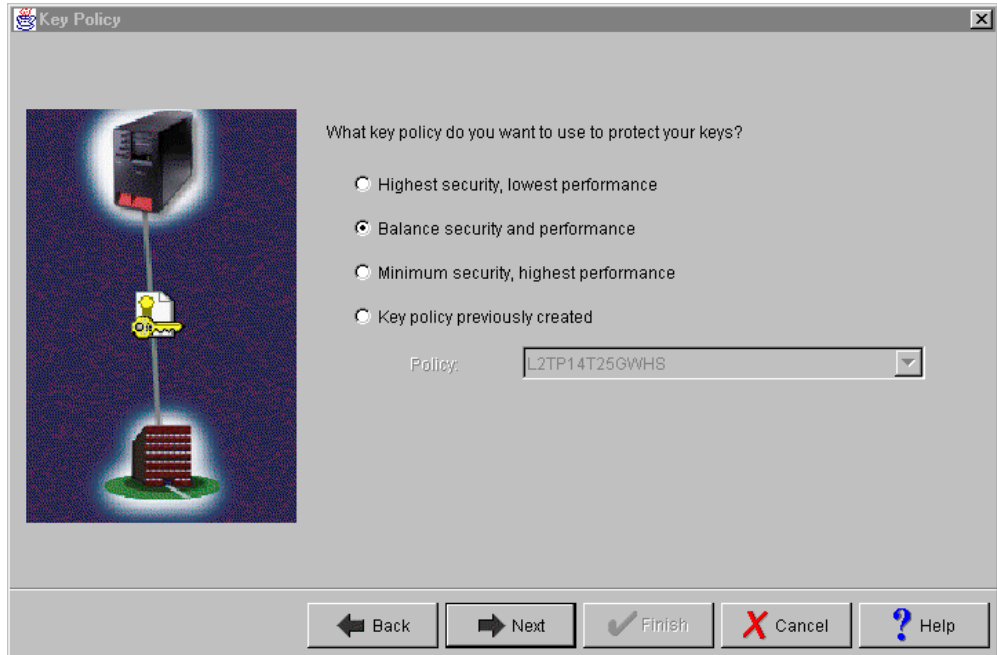


Figure 205. Key Policy window

12. On the Local Identifier window (Figure 206), specify the identity of the local key server. In other words, specify the local AS/400 system that acts as the VPN gateway, which, in this case, is AS14. Leave Identifier type as the default value, Version 4 IP address. For the IP Address, use the pull-down list to select the IP address of the interface that is connecting to the remote gateway AS/400 system (AS05). Refer to the planning worksheet (Table 22 on page 204). For AS14, the IP address is 204.146.18.227 (interface A in Figure 198 on page 201).

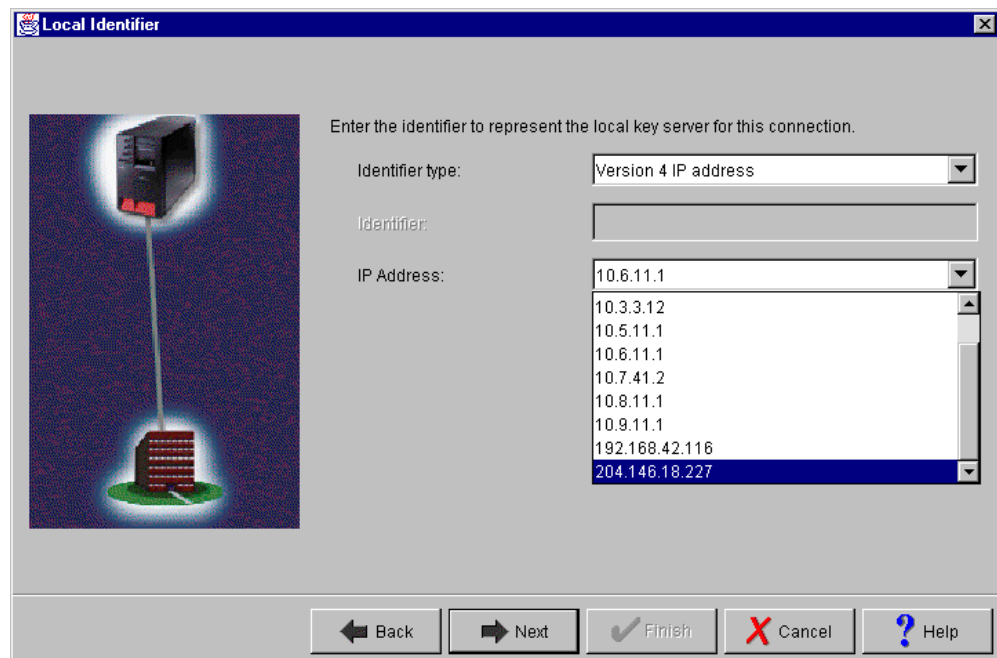


Figure 206. Local Identifier window pull down

Note: Figure 206 on page 210 shows various IP addresses, such as 10.1.1.14, 10.3.3.12, and so on, that we do not reference anywhere in this scenario. These interfaces are configured on AS14. Although they are used for other scenarios and projects, they should be ignored here.

Figure 207 shows the completed Local Identifier window.

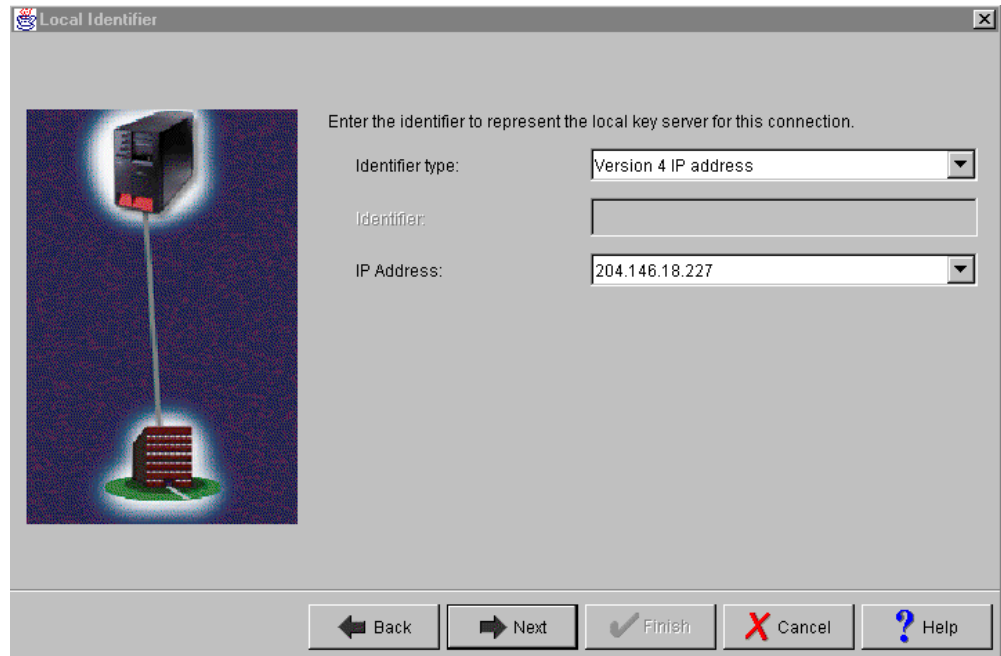


Figure 207. Local Identifier window

13. Click **Next**.

14. On the Remote Network window (Figure 208 on page 212), enter details about the remote key server, as well as the *pre-shared key*. The pre-shared key is the shared secret IKE uses to generate the actual keys for phase 1. The remote key server is AS05 with IP Address 208.222.150.250 (interface **E** in Figure 198 on page 201). Specify `bdcfhhnprotvqa` in the Pre-shared key field. Remember, the same pre-shared key must be entered when configuring VPN on the remote AS/400 VPN gateway.

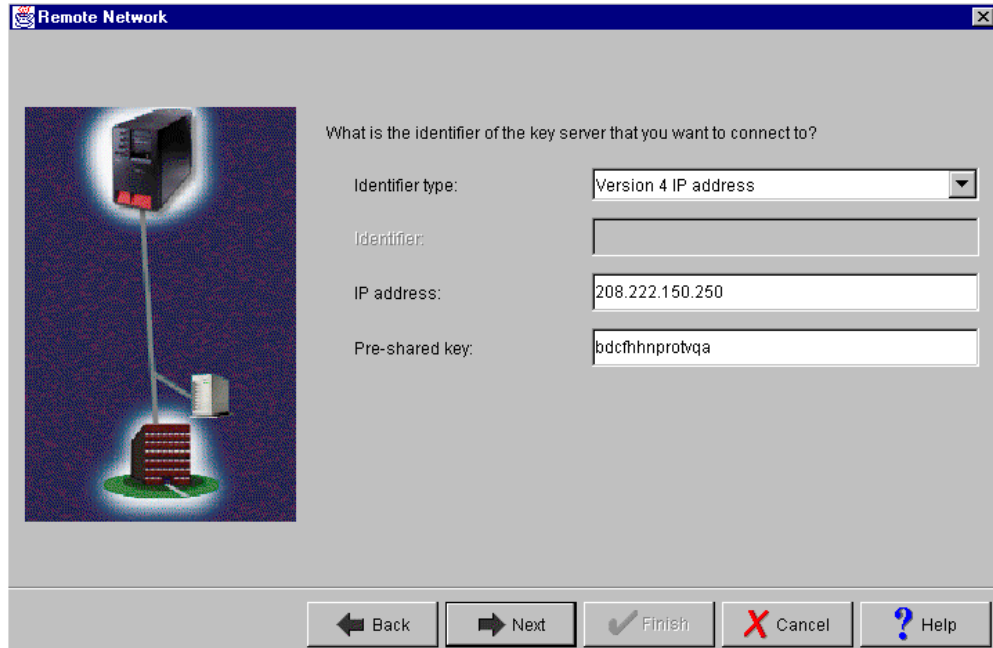


Figure 208. Remote Network window

15. Click **Next**.

16. On the Data Policy window (Figure 209), specify the level of authentication or encryption IKE uses to protect data flowing through the gateway-to-gateway tunnel during phase 2 negotiations. For this example, select **Balance security and performance** as specified on the worksheet.

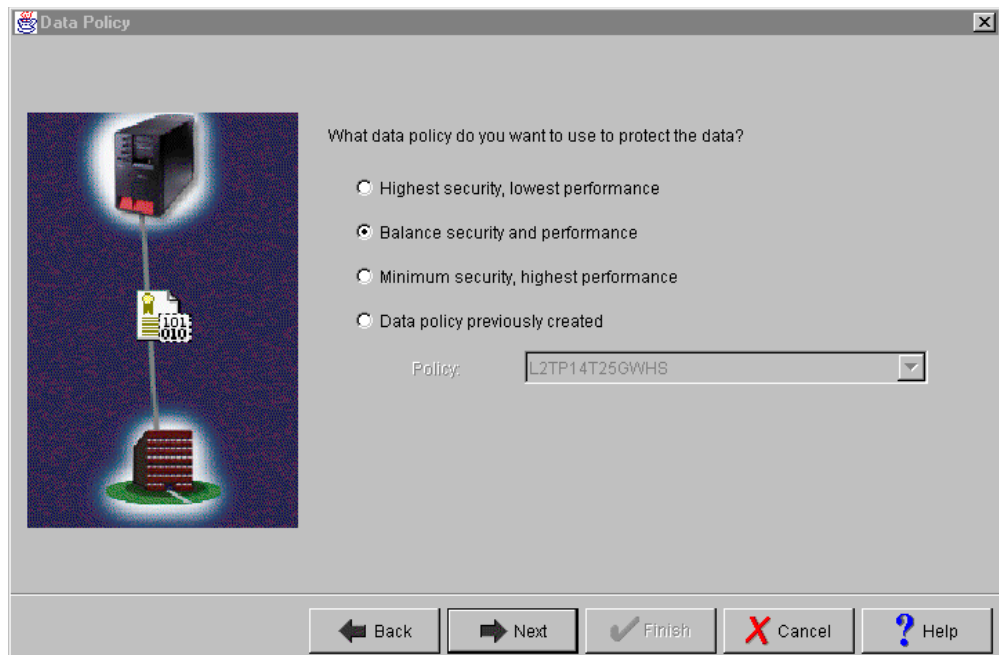


Figure 209. Data Policy window

17. Click **Next**.

18. The New Connection Summary window (Figure 210) summarizes the configuration values you entered. Scroll down to see a list of the configuration objects that the wizard creates when you click the Finish button. Check the configuration values against the worksheets. If you need to make changes, click **Back**. Otherwise, click **Finish**.

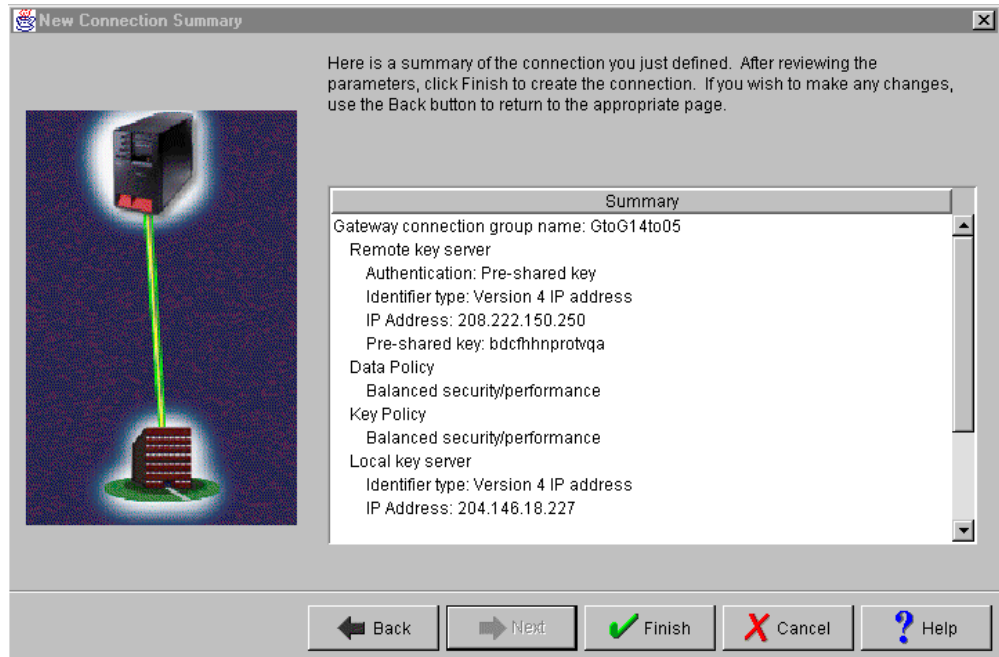


Figure 210. AS14 New Connection Summary window

The wizard now creates the various objects you configured for this VPN connection. After a short delay (and assuming there are no errors), you return to the initial VPN GUI Configuration window (Figure 201 on page 207).

6.3.2.1 Reviewing the objects created by the VPN configuration wizard

As a result of the information you provided through the VPN configuration wizard, the wizard creates the objects needed for the VPN gateway-to-gateway configuration.

Briefly review all the configuration objects that the wizard creates. These include:

- Key Policy
- Data Policy
- Key Connection Group
- Dynamic Key Connection Group
- Dynamic Key Connection

Should you need to fine tune or extend your configuration, you can view and update each of these objects by using the VPN Configuration GUI. To review the objects created by the wizard, follow these steps:

1. Expand all the subfolders on the VPN Configuration GUI interface (Figure 211 on page 214).

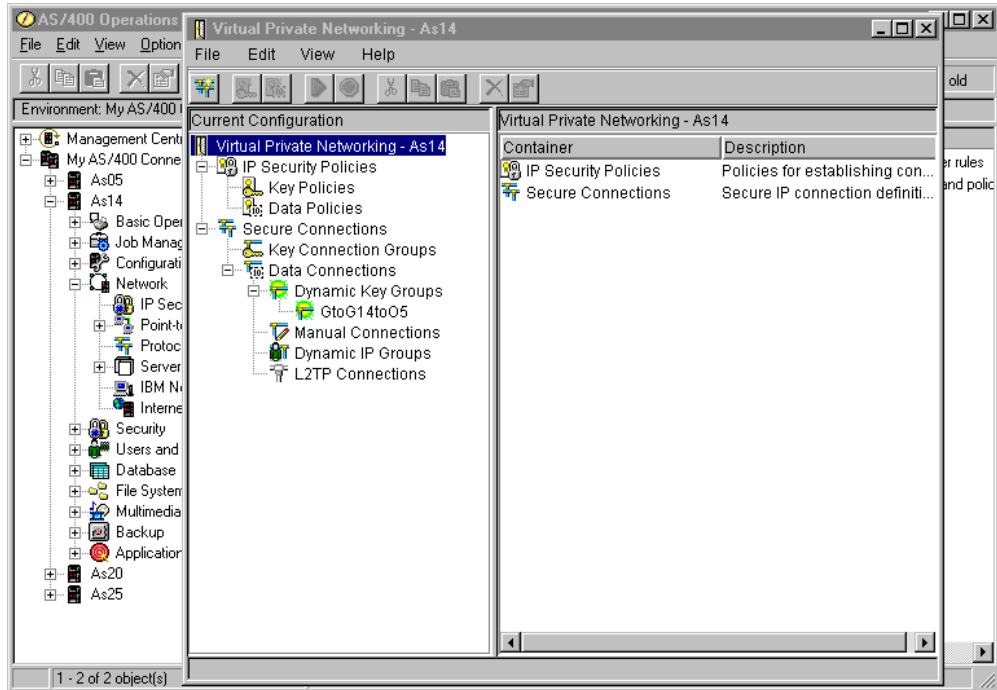


Figure 211. VPN GUI configuration interface expanded

2. Double-click **Key Policies** (Figure 212 on page 215) to display the list of key policies, including the one you just created. The key policy name is the connection group name you entered on the wizard, followed by a two letter suffix. In this example, the suffix is *BS* because you requested *Balanced security and performance* for the key policy. Selecting *Highest security, lowest performance* for the key policy results in *HS* as the suffix. Selecting *Minimum security, highest performance*, results in *HP* as the suffix. This is a convention followed by the wizard that you do not need to adopt if you create your own objects through the configuration GUI (not using the wizard).

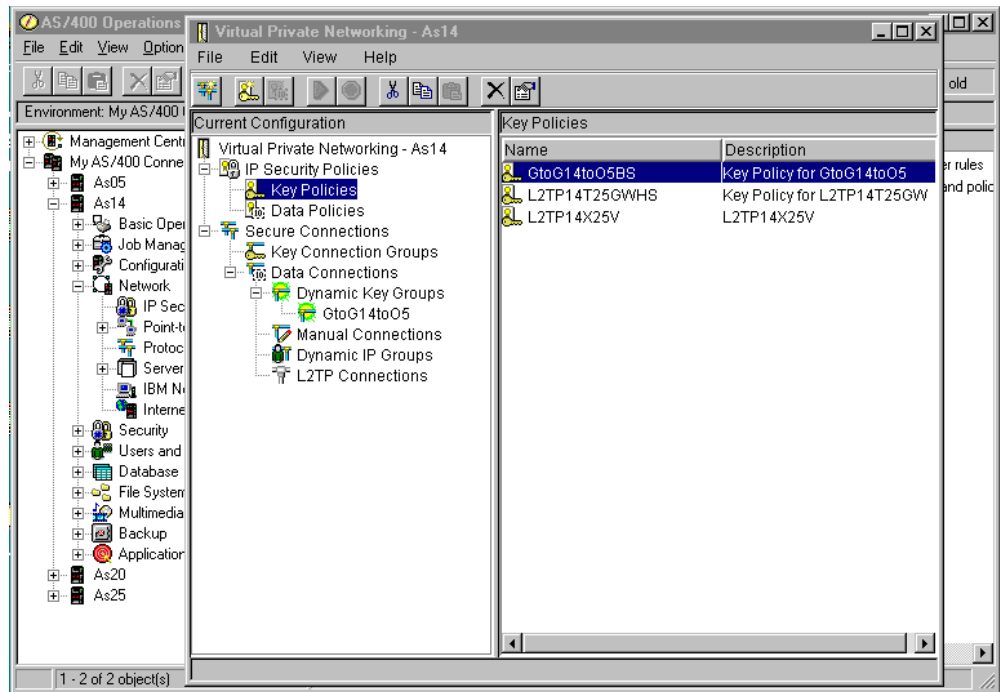


Figure 212. VPN Key Policies

3. Double-click **Data Policies** (Figure 213) to review the data policy you created for this connection. The data policy name is the connection group name that you entered on the wizard, followed by BS (for Balanced Security).

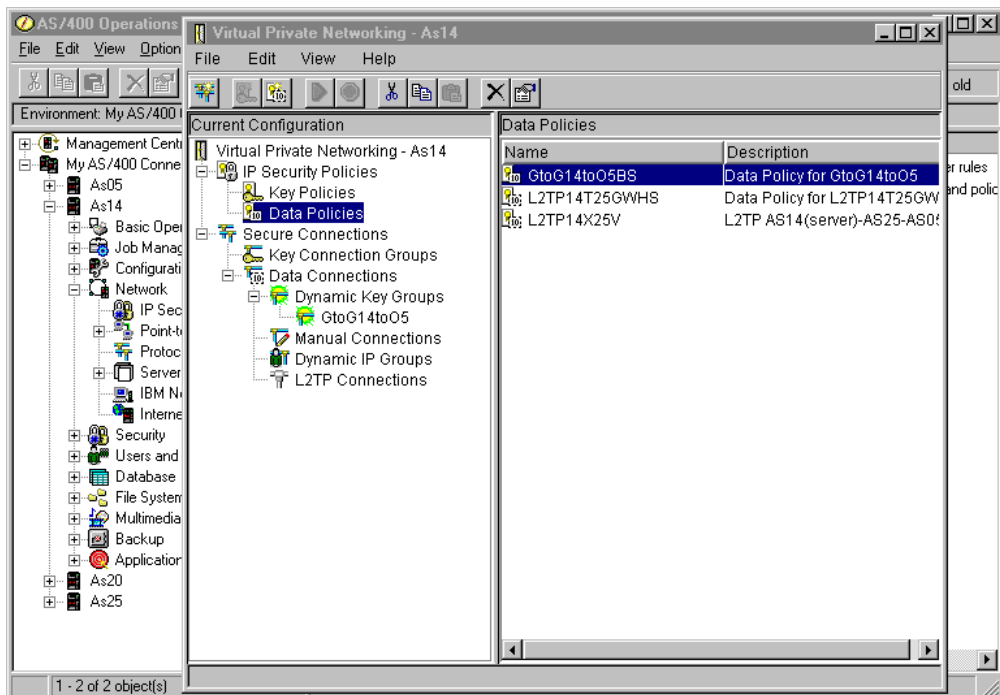


Figure 213. VPN Data Policies

4. Double-click **Key Connection Groups** (Figure 214 on page 216) to display the key connection group created by the wizard, GtoG14toO5. The key connection

group name does not have a BS suffix because the actual security level that the VPN uses is held in the key and data policies, not here.

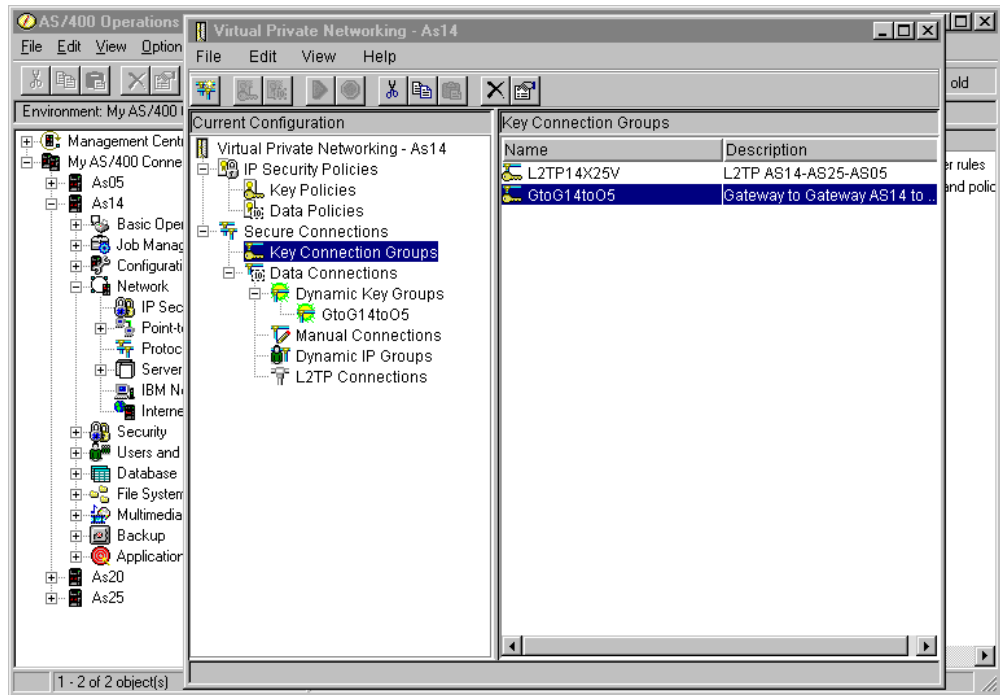


Figure 214. VPN Key Connection Groups

- Expand **Dynamic Key Groups** under Data Connections (Figure 214). A dynamic key group is a type of *data connection* that uses the IKE protocol for dynamic key exchanges. Contrast this to a *manual connection*, where keys are configured and exchanged manually. The actual *connection group* object created by the wizard is listed here.
- Double-click the connection group **GtoG14to05**. A list of *connections* within the connection group is shown (Figure 215 on page 217). The wizard creates only one connection here, which is called *GtoG14to05:L1*.

Note: You cannot change connection names. They are always the connection group name followed by :L1, :L2, and so on.

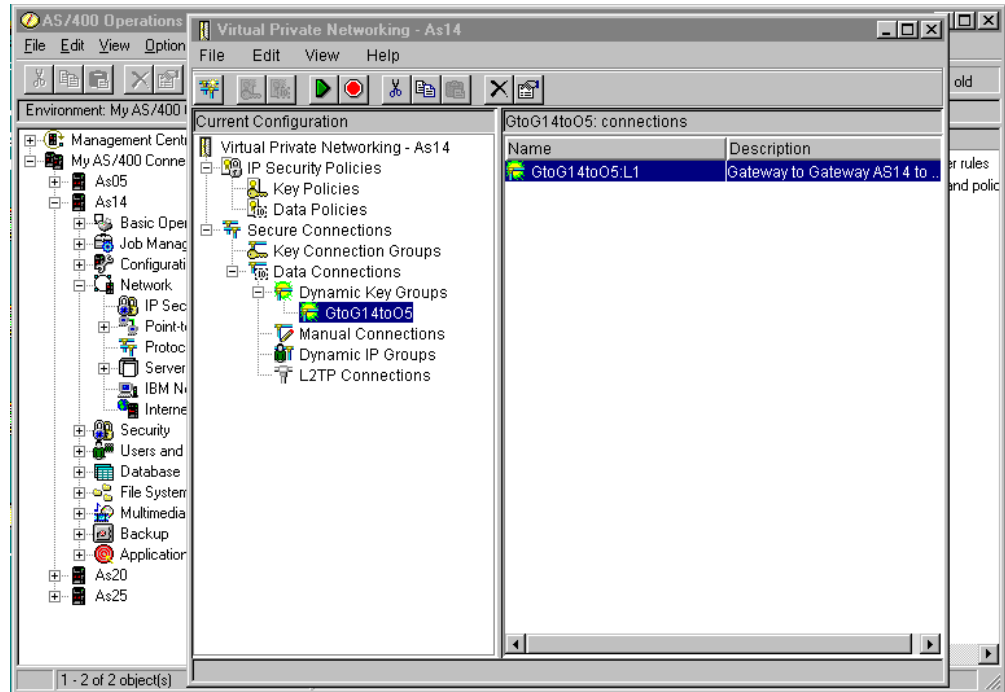


Figure 215. VPN Dynamic Key Groups

You have now completed the VPN configuration for AS14. Configure AS/400 IP filtering in the next task.

6.3.3 Configuring IP filters on the AS14

The wizard does *not* configure IP filtering. You must complete this task manually by using Operations Navigator. In this example, no filters currently exist. However, if IP filtering is already configured and active, the active filters must be stopped and any new filters must be integrated with those already in existence.

Complete the following steps:

1. From Operations Navigator, double-click **IP Packet Security** (Figure 216 on page 218).

This takes you into the GUI for configuring IP Packet Security, which includes IP filtering and Network Address Translation support. You will configure IP filtering, but not Network Address Translation, since it is not compatible with VPN. VPN has its own NAT function, which is Virtual Private Network Address Translation.

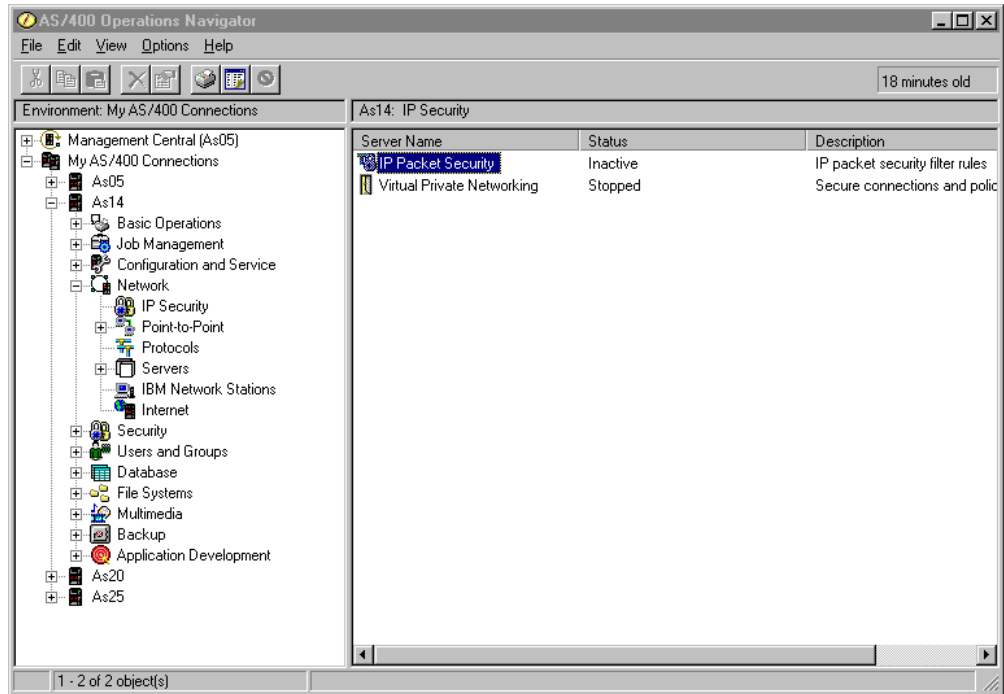


Figure 216. IP Packet Security

In this scenario, we are starting a new IP packet security configuration. All Security Rules displays an empty window (Figure 217).

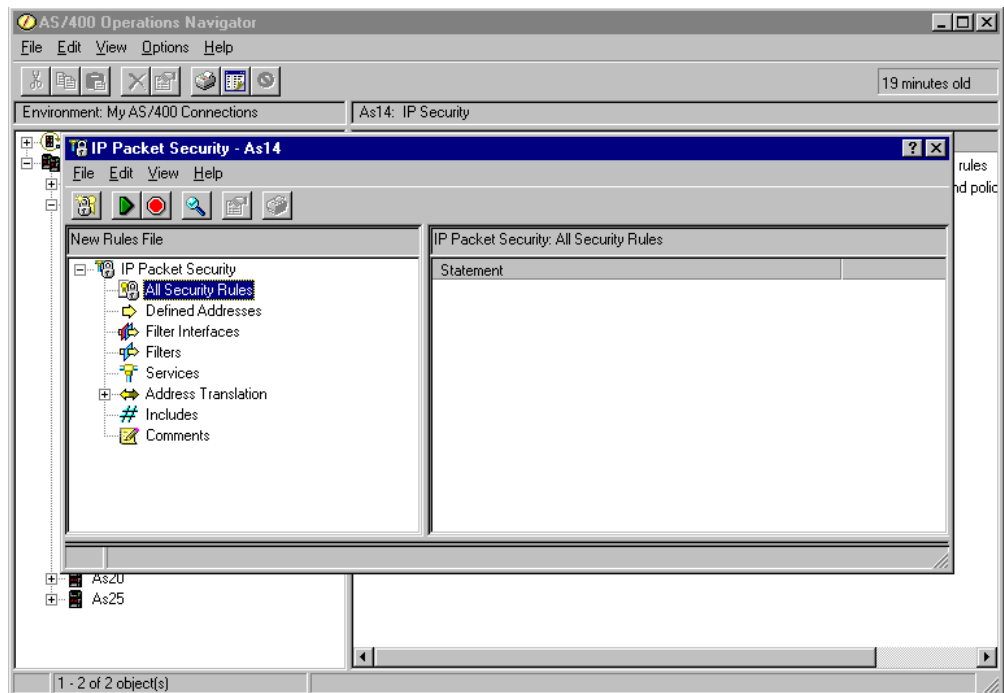


Figure 217. All Security Rules empty

2. Configure the subnets that can use the VPN tunnel. Right-click **Defined Addresses**, and select **New Defined Address** (Figure 218 on page 219).

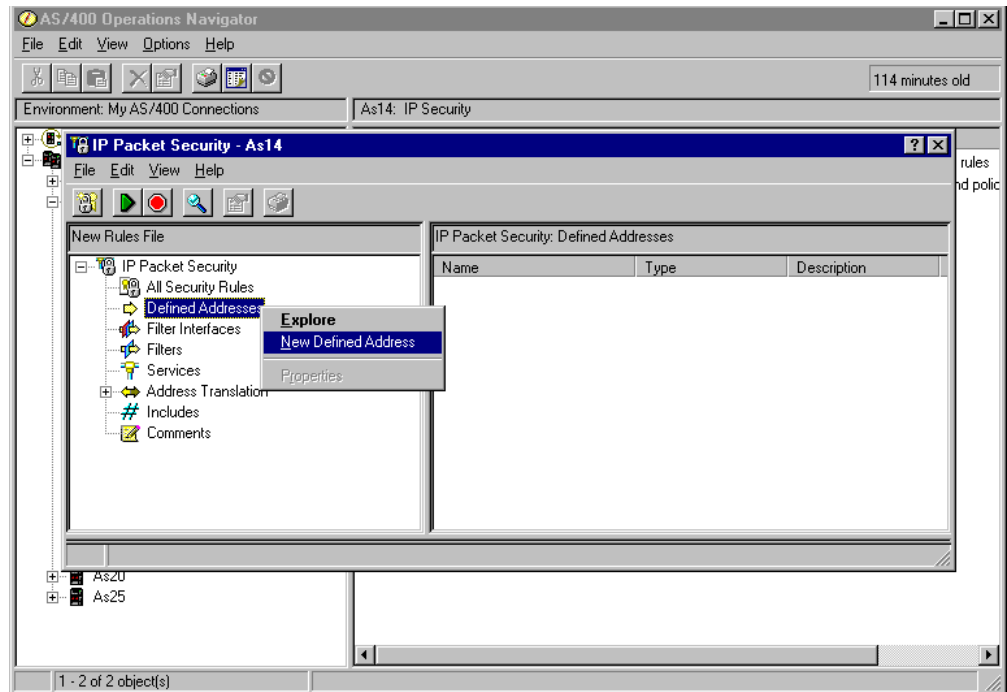


Figure 218. Configuring subnets - New Defined Address

The New Defined Address window is displayed (Figure 219 on page 220).

3. The *Address name* is referenced by other rules using this defined address. You are creating a subnet. Therefore, select **IP specification**, and enter a subnet mask.
4. Click **Add**, and enter the IP address of the subnet. You can optionally add a description to document the rules file that you are creating (Figure 219 on page 220).

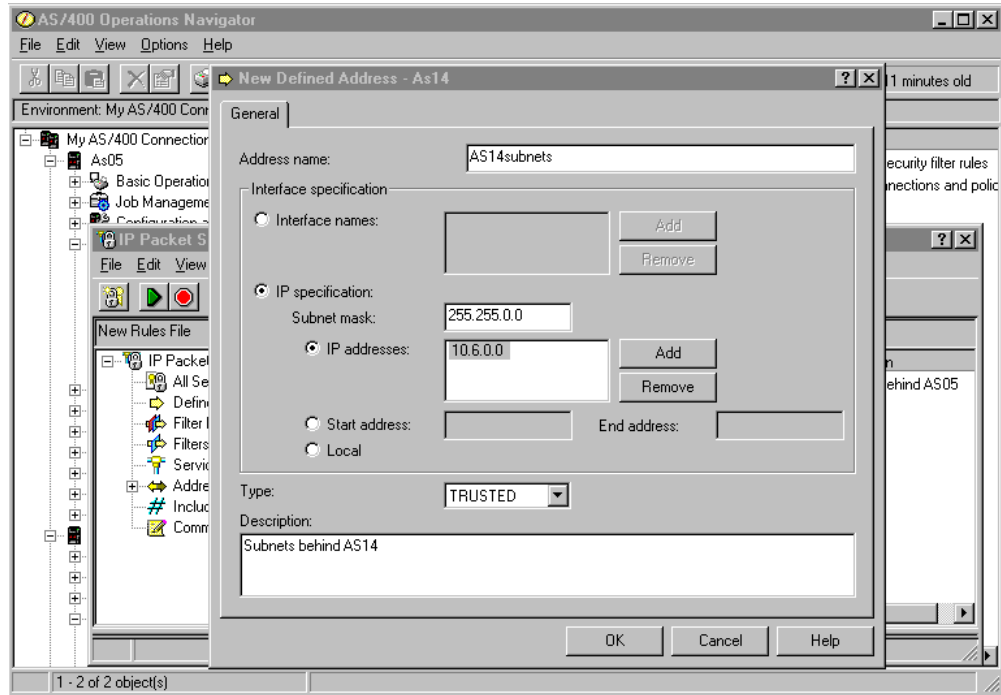


Figure 219. Defined address AS14 subnets

Refer to the worksheet for AS14 in Table 23 on page 205 for the appropriate address name for this subnet. These addresses define the subnet that you are allowing to use the VPN tunnel. In this case, the subnet is 10.6.0.0 with a subnet mask of 255.255.0.0. Since this subnet is the local network to AS14, select the default for Type:, which is **TRUSTED**. Complete the remaining fields.

5. Click **OK**.
6. Repeat step 2 on page 218 through step 5 on page 220 to create a defined address for the subnet behind the remote VPN gateway (Figure 220 on page 221). In our example, the address name is AS05subnets with subnet 10.196.0.0 and subnet mask 255.255.0.0. Because this is the remote subnet, select **UNTRUSTED** for Type: Don't be confused by the term "UNTRUSTED." In this gateway-to-gateway scenario, the remote network is part of the same organization and has full access to hosts and applications on the local network.

Note: The actual subnet behind AS05 is 10.196.8.0, with a subnet mask of 255.255.255.0. By specifying 10.196.0.0 and 255.255.0.0, you are allowing any other networks subsequently added to AS05 and beginning with 10.196.*.* to use this VPN tunnel. Make sure that when you create the matching filter set on AS05, you also specify 10.196.0.0 and 255.255.0.0.

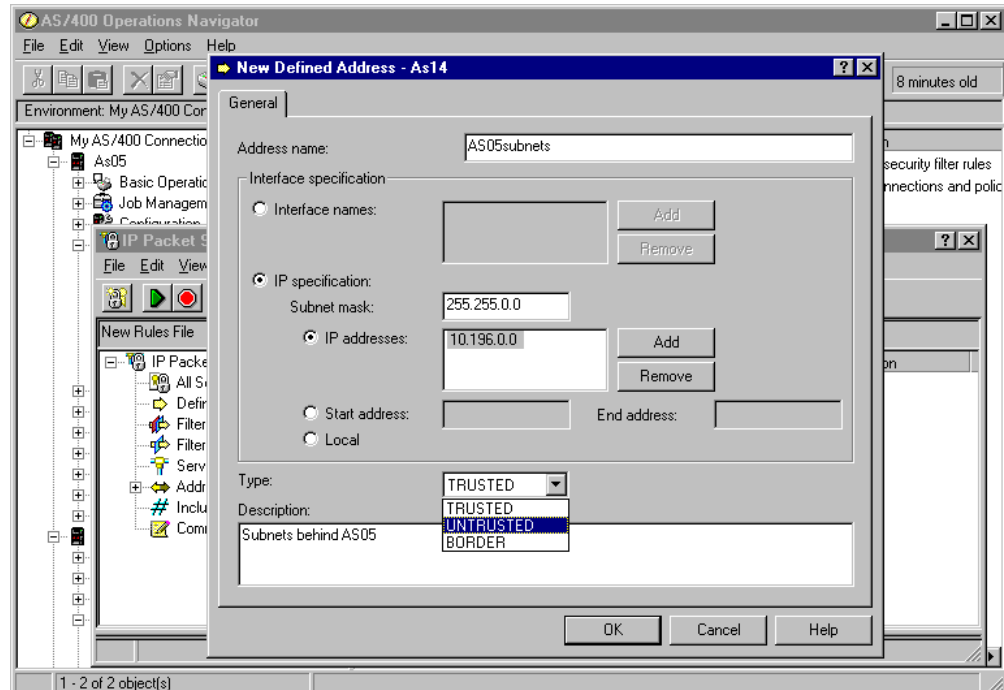


Figure 220. Defined addresses AS05 subnets

- Right-click **Filters**, and select **New Filter**. All associated filter rules (for example, all rules for one interface) should have the same *Set name*. In this example, we use `VPNIFC` for the Set Name.

You need to add two rules to allow Internet Key Exchange (IKE) traffic to flow into and out of the AS/400. Select **PERMIT** for Action and, for the first rule, select **OUTBOUND** for Direction. Specify the local AS/400 system address `204.146.18.227` in the Source address name field, and the remote AS/400 system address `208.222.150.250` in the Destination address name field.

Leave the other fields on the General page set to their defaults (Figure 221 on page 222).

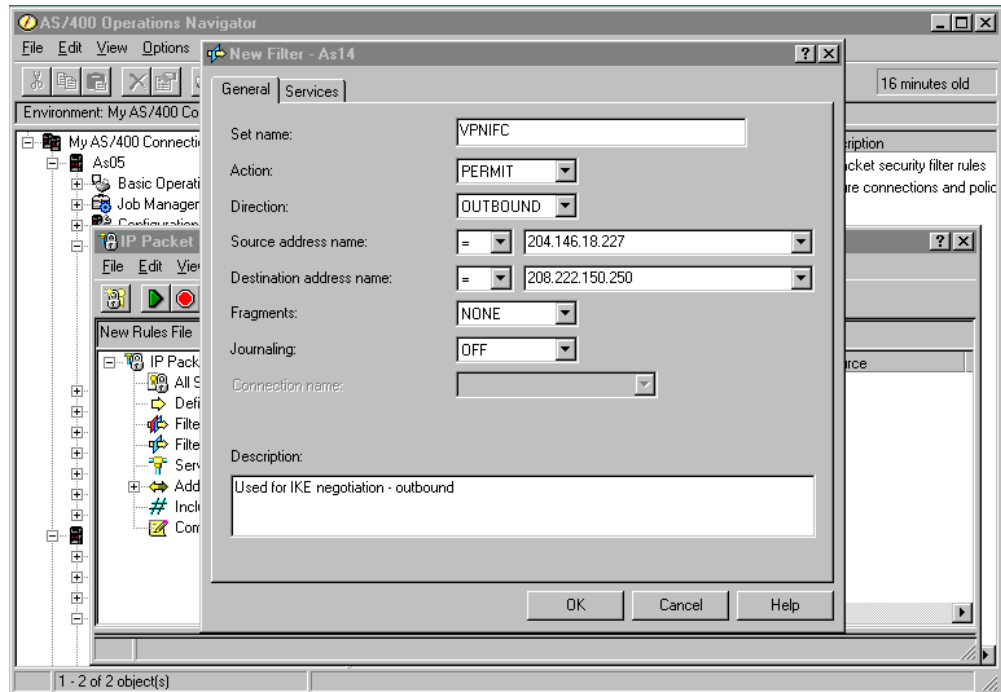


Figure 221. AS14 Outbound IKE filter rule

8. Click the **Services** tab to display the Services window (Figure 222).

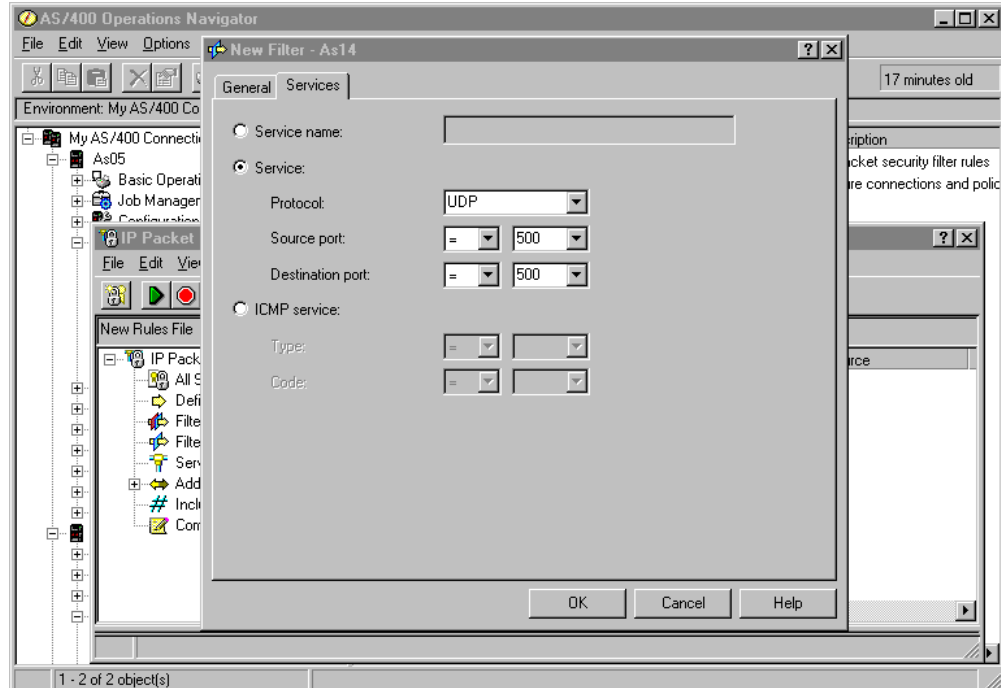


Figure 222. AS14 Outbound IKE filter rule services

9. Select the **Services** tab. In the Protocol field, select **UDP**. In the Source and Destination port fields, enter 500. IKE uses the UDP protocol with a source port of 500 and a destination port of 500.

10. Click **OK**.

11.Repeat step 7 on page 221 through step 10 on page 222 for the *INBOUND* IKE filter rule. Remember to *reverse* the Source and Destination address names. Refer to Figure 223 and Figure 224.

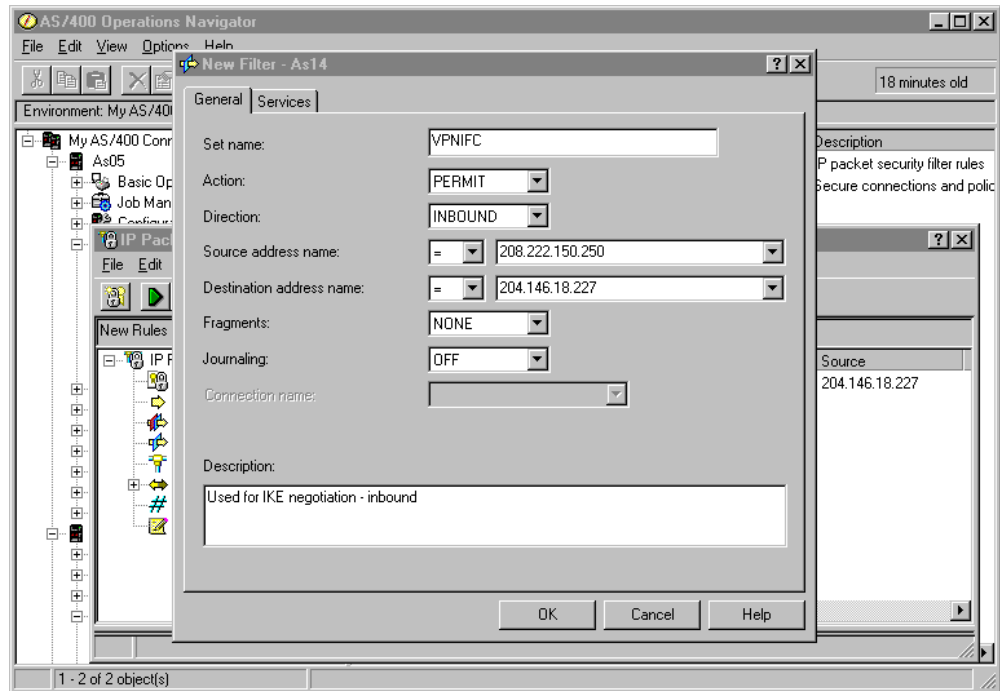


Figure 223. AS14 Inbound IKE filter rule

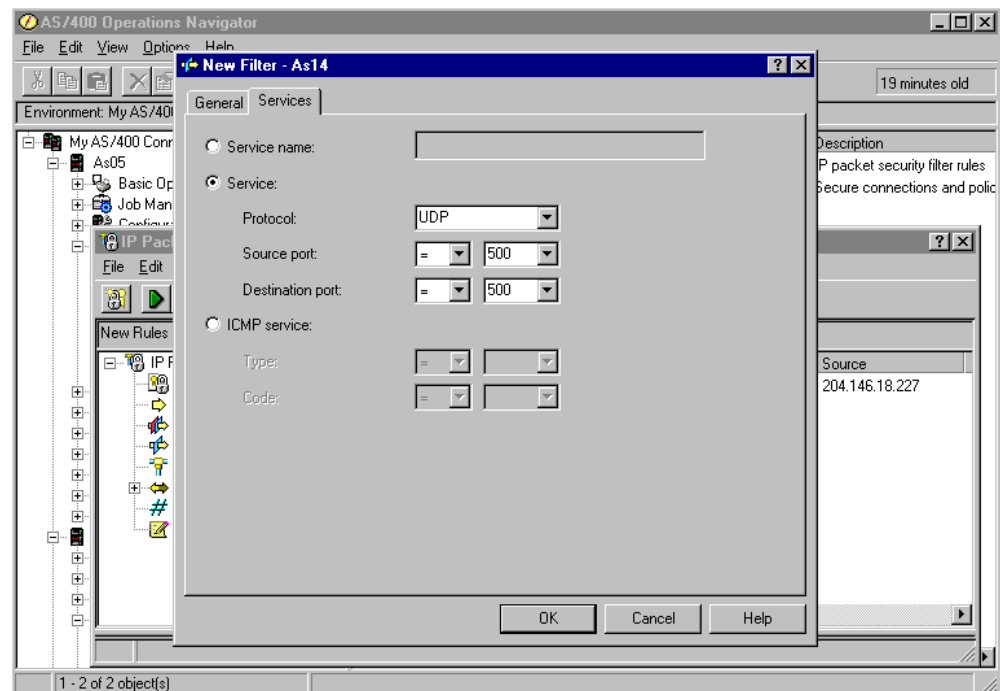


Figure 224. AS14 - Inbound IKE filter rule services

12.Create a new filter rule that allows data traffic to use the VPN tunnel. Use the same filter Set name, *VPNIFC*, but select **IPSEC** in the Action field. With an

IPSEC filter rule, Direction is always set to OUTBOUND and grayed out. In the Source and Destination address name fields, enter the defined address names you created earlier, which, in this example, is AS14subnets and AS05subnets. Make sure that the source and destination addresses are in the correct direction. The source address is for the local subnets connected directly to the local AS/400 system (AS14 in this configuration).

Key step

At this stage, you tie your IP filters back to the VPN configuration that you built in the previous task. The *Connection name* is the data connection, which, in this case, is a dynamic key connection *group*. Use the pull-down list to view all the data connection names that have been configured on this system, and select the one required. In this example, select **GtoG14to05**.

Because IP filters refer to the VPN data connection name, the VPN connection must be created before configuring the filters.

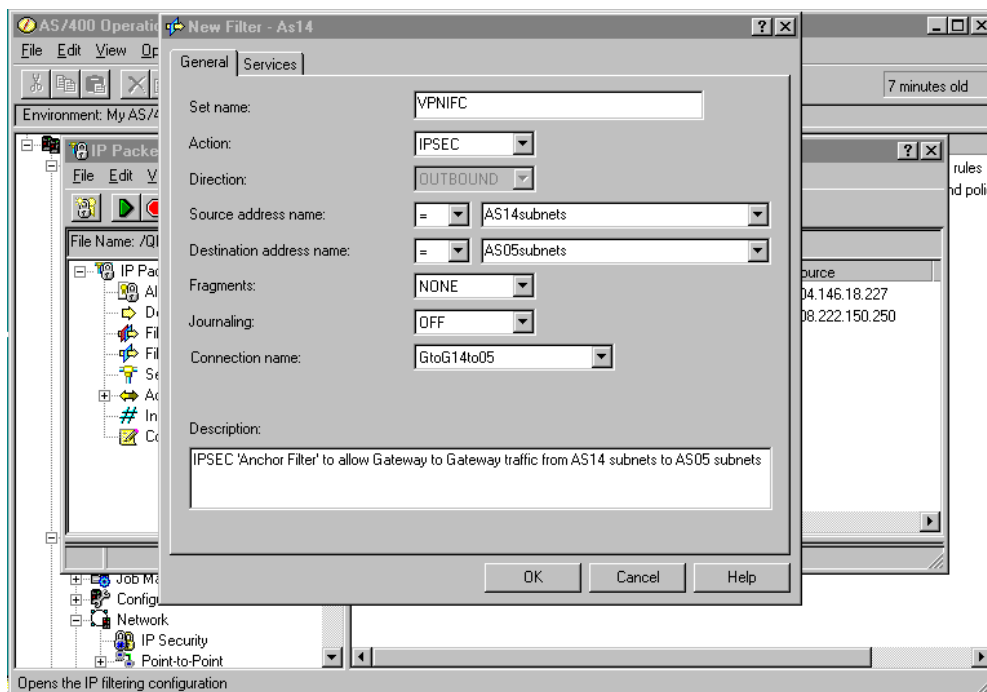


Figure 225. AS14 IPSEC filter rule

13. Click the **Services** tab.

14. Select **Service** and select the wildcard (*) for the Protocol, Source port, and Destination port fields. This allows any protocol using any port to use this filter rule and, therefore, the VPN tunnel.

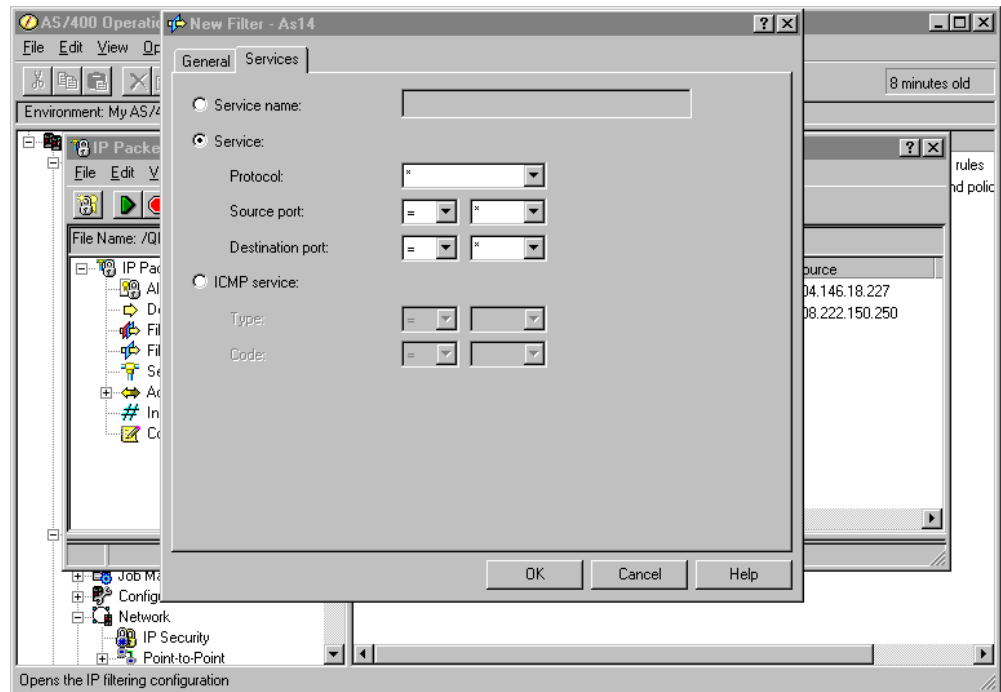


Figure 226. IPSEC filter rule services

15. Click **OK**.

16. The final rule you must create is a *Filter Interface* rule, which ties the filter rules that you just created to the physical interface. Right-click **Filter Interfaces**, and select **New Filter Interface**. Select **Line name**, and use the pull-down menu to view a list of all the AS/400 line descriptions on the system (for example, created by CRTLINTRN or CRTLINETH). Select the line description that connects *out* to the remote gateway AS/400 system across the Internet or intranet. For this example, select **TRNWSB2**.

Note: This is the line that connects the gateway to the Internet. This is *not* the line that connects the gateway to the internal subnet.

17. Click **Add** to add the filter set name of the filter rules you created previously, which, in this example, is **VPNIFC** (Figure 227 on page 226).

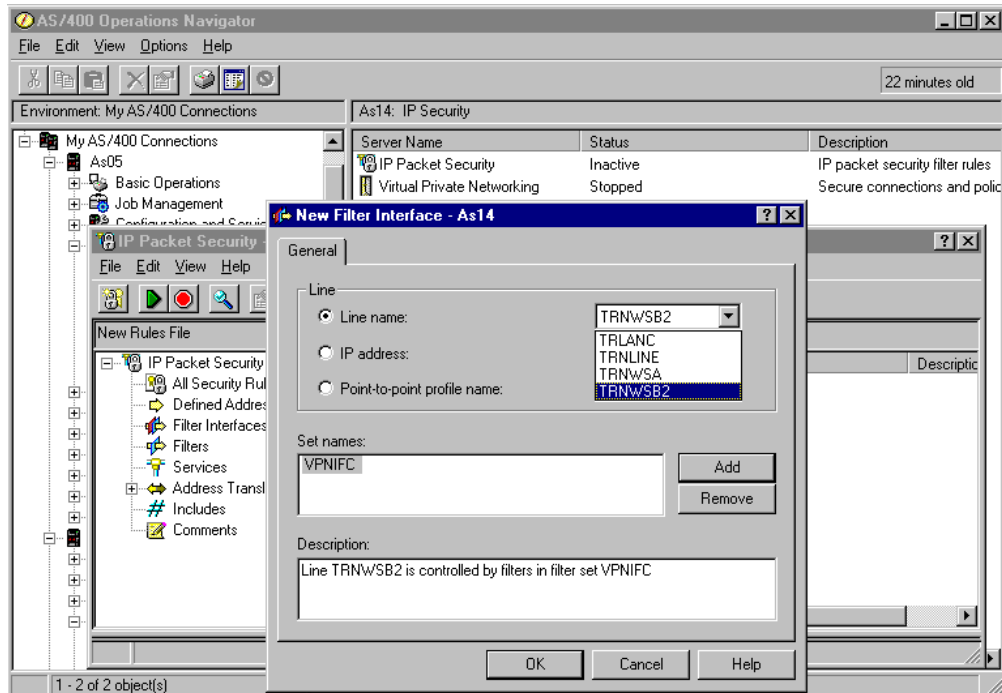


Figure 227. Filter interface rule

Tip

Whenever you add any filter rules for an AS/400 line description, the system automatically adds a default DENY ALL for that line. This means any traffic not explicitly permitted is denied. You cannot see, nor change, this rule. As a result, you may find that connections, which previously worked, mysteriously fail once you activate your filter rules. From a security viewpoint, this is a sound policy, particularly if the AS/400 system is directly connected to the Internet. However, in a worst case scenario, you may accidentally restrict access to the line you use for Operations Navigator and not be able to deactivate IP filtering. In this case, use the `RMVTCPTBL *ALL` command to deactivate all filter rules.

If you want to allow traffic other than VPN on the line, you must add explicit Permit rules to do so.

- To document your filter rules file, you can add comment lines. Right-click **Comment**, and select **New Comment** to add a comment line (Figure 228 on page 227).

toolbar. Notice the message area at the bottom of the IP Packet Security window. If necessary, drag the edges of the window to see more of the filter rules and the verify messages. If the filter rules are syntactically correct, you will see the message: The rules file was successfully verified (Figure 230).

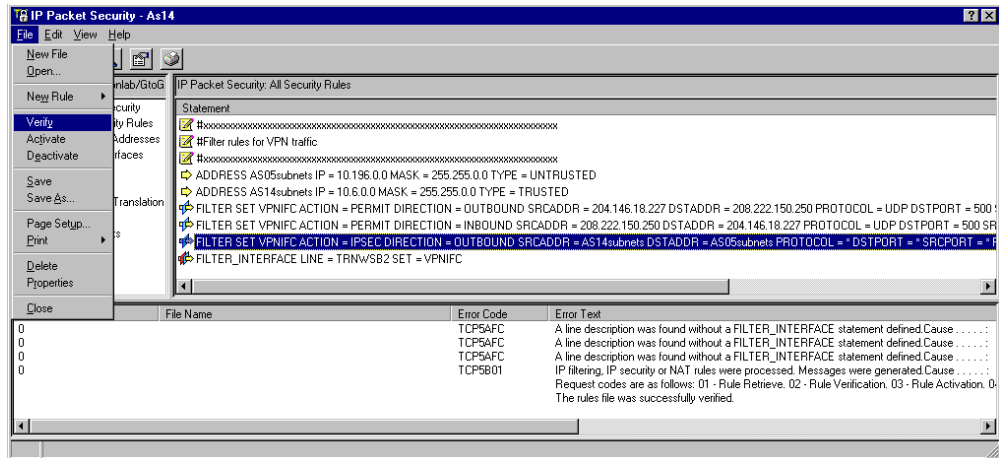


Figure 230. Verifying filter rules

20. You can now activate the rules file. Select **File** from the main menu, and then select **Activate** (Figure 231). Alternatively, there is an activate icon (a green triangle) on the toolbar. Look for the message: The rules file was successfully activated.

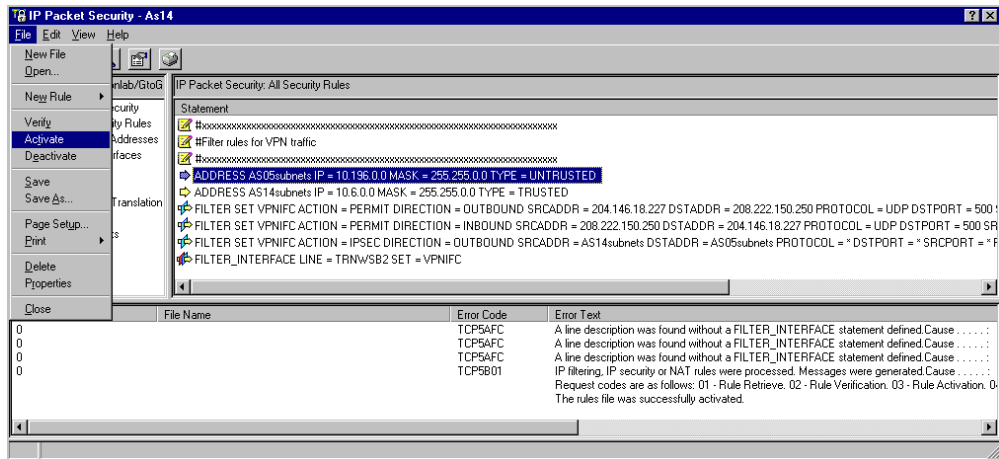


Figure 231. Activating filter rules

21. Save your filter rules file. Select **File** from the main menu, and then select **Save** (Figure 232 on page 229). The file is saved into the IFS with an extension of *i3p*. In this example, we created a subdirectory, *vpnlab*, under the directory *QIBM*. Save the filter rules as *GtoGfilter1.i3p* into */QIBM/vpnlab*.

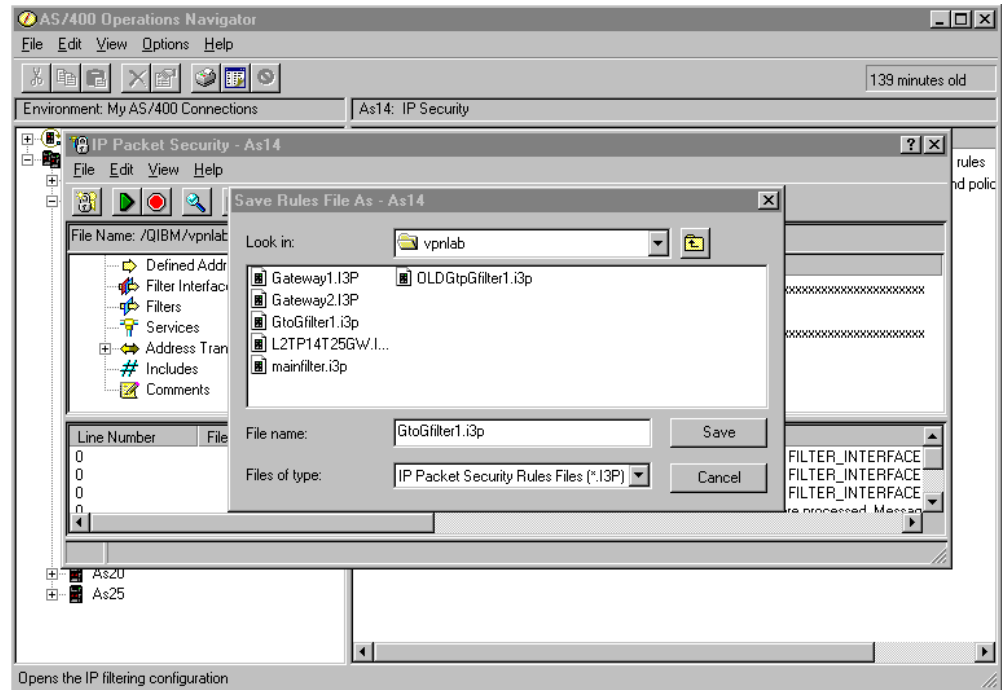


Figure 232. Saving the filter rules file

Tip

Do *not* save your file into the /QIBM/UserData/OS400/TCPIP/CONFIGURATION directory.

If you use the RMVTCPTBL *ALL command to deactivate IP filtering, the command will delete *all* files within this directory.

6.4 Configuring the Minneapolis AS/400 VPN gateway (AS05)

The following sections take you step-by-step through the configuration of the VPN and filters on the AS/400 VPN gateway in the Minneapolis network.

6.4.1 Planning worksheets for the AS05 gateway

Complete the planning worksheets to gather the information you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 24 on page 230 shows the planning worksheet for this scenario from the perspective of the VPN gateway at the Minneapolis network (AS05 in Figure 198 on page 201).

Table 24. AS05 New Connection Wizard planning worksheet - Gateway-to-gateway VPN

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	GtoG05to14
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	208.222.150.250 B
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	204.146.18.227 A
What is the pre-shared key?	bdcfhhnprotvqa
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

We completed this planning worksheet (Table 24) from the perspective of AS05. The level of key and data protection must match AS14. The wizard does *not* support multiple data protection *proposals* for negotiation with the remote VPN server. The pre-shared key must also match. The connection group is named *GtoG05to14*.

To complete the VPN configuration, you must configure IP filters. Table 25 shows the planning worksheet for the IP filters configured in this scenario.

Table 25. AS05 Planning worksheets - IP filters configuration

This is the information you need to create your IP filters to support your VPN	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ?	gateway
Is the <i>remote</i> VPN server acting as a host or gateway ?	gateway
What name do you want to use to group together the set of filters that will be created?	VPNIFC
If <i>your</i> server is acting as a gateway ... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	10.196.0.0 255.255.0.0 AS05subnets
If the <i>remote</i> server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	10.6.0.0 255.255.0.0 AS14subnets
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	208.222.150.250 B
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on IPSEC filter if the remote server is acting as a host .	204.146.18.227 A
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRLANB1
What other IP addresses, protocols and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

We also completed an IP filter rules planning worksheet (Table 25) for AS05. Addresses are essentially the reverse of those we specified for AS14. We use the same names for address ranges (AS14subnets and AS05subnets), and the filter set (VPNIFC), but these do not necessarily have to match between the two systems. The Token-Ring line name on AS05 is to which the filters apply TRLANB1.

6.4.2 Configuring the gateway-to-gateway VPN on AS05

Repeat the steps described in 6.3.2, "Configuring the gateway-to-gateway VPN on AS14" on page 206, but use the configuration values specified in Table 24 on page 230.

Figure 233 shows the New Connection Summary window that the wizard presents at the end of the AS05 configuration. Compare it with the equivalent window for AS14 in Figure 210 on page 213.

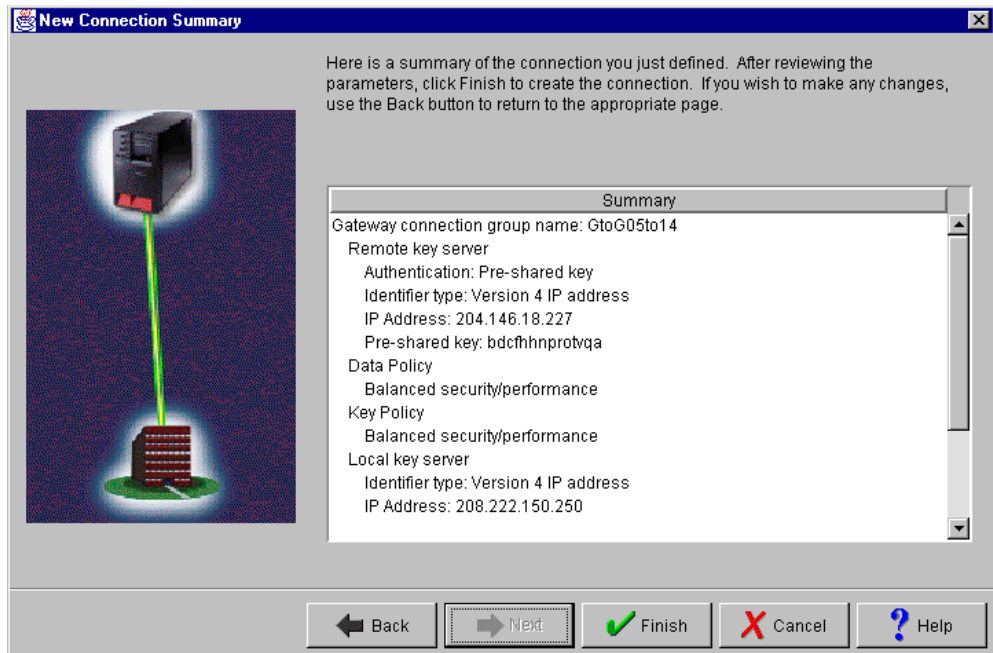


Figure 233. AS05 New Connection Summary window

6.4.3 Configuring IP filters on AS05

Repeat the steps described in 6.3.3, “Configuring IP filters on the AS14” on page 217, but use the configuration values specified in Table 25 on page 231.

Figure 234 on page 233 shows the IP Packet Security - All Security Rules window. This window is displayed when you select All Security Rules under IP Packet Security. You can see this option in Figure 229 on page 227.

Tip

The addresses and subnet masks should match exactly. For example, on AS14, you specified that the subnet behind AS05 was 10.196.0.0, with a subnet mask of 255.255.0.0. In the AS05 filter rules, you must also specify 10.196.0.0, with a mask of 255.255.0.0. Subnet 10.96.8.0, with a mask of 255.255.255.0, will not match, and the VPN connection will not start.

There is a graceful way to avoid this restriction. Change the IP address granularity of the connection group that is associated with the filter rule for 10.196.0.0 to *connection* (instead of *filter rule*). For example, if the AS14 rule is written as 10.196.0.0 and the AS05 rule is written as 10.196.8.0, change the AS14 GtoG14to05 connection group granularity for remote IP address to *connection*. Then, initiate the connection from AS05 (start GtoG05to14:L1). If you want to initiate from AS14, change the AS14 connection (GtoG14to05:L1) to indicate a remote address of 10.196.8.0 with a mask of 255.255.255.0.

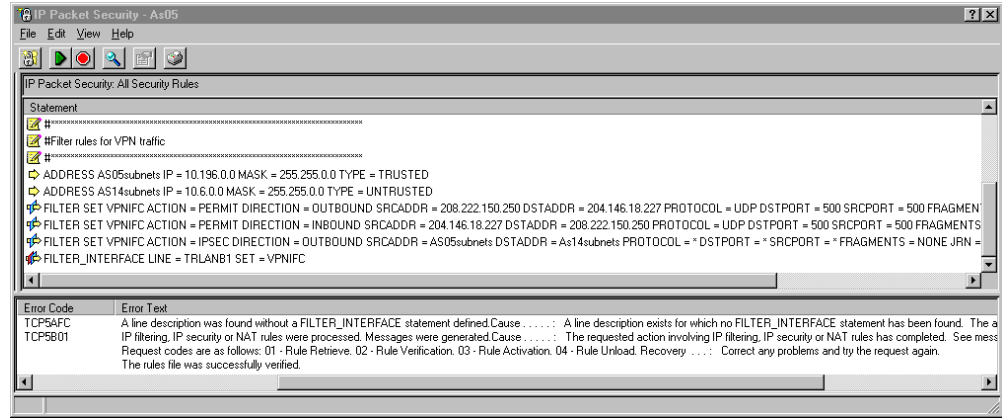


Figure 234. AS05 All security rules

To print your filter rules file, select **File** from the main menu, and then select **Print**. A sample filter rules printout is shown in Figure 235.

```

#*****
#Filter rules for VPN traffic
#*****
ADDRESS AS05subnets IP = 10.196.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
ADDRESS AS14subnets IP = 10.6.0.0 MASK = 255.255.0.0 TYPE = UNTRUSTED
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 208.222.150.250
    DSTADDR = 204.146.18.227 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 204.146.18.227
    DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS05subnets DSTADDR = As14subnets
    PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = GtoG05to14
FILTER_INTERFACE LINE = TRLANB1 SET = VPNIFC

```

Figure 235. Print of AS05 filter rules

6.4.4 Starting the gateway-to-gateway VPN connection

To start VPN on both AS/400 systems, complete the following steps:

1. Use Operations Navigator to check the status of IP Packet Security and Virtual Private Networking on both AS/400 systems (Figure 236 on page 234).

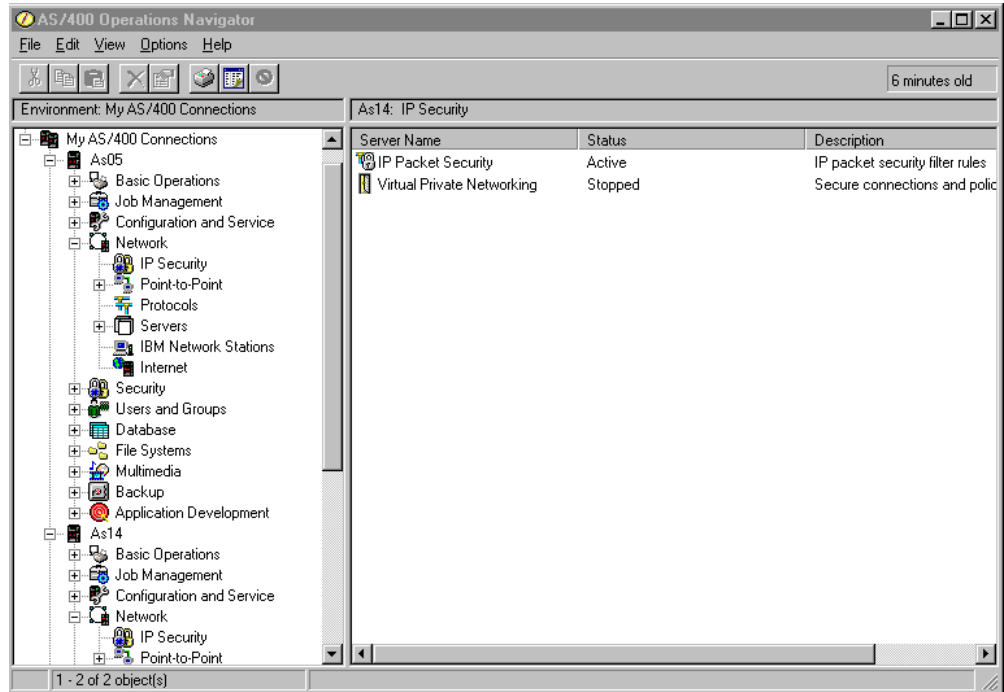


Figure 236. Status of IP Packet Security and Virtual Private Networking

2. If IP Packet Security is not *Active*, activate your filter rules file as described previously.
3. If Virtual Private Networking is not *Started*, right-click on it, and select **Start**.

Note

IP Packet Security must be active with the correct filter rules before a specific VPN *connection* can be successfully started. However, the Virtual Private Networking server jobs can start without IP Packet Security being active.

One of the VPN partners must be the initiator of the connection while the other one is the responder. By default, either system can initiate the connection. In this scenario, start the connection from the Rochester AS/400 system AS14.

4. Double-click **Virtual Private Networking** to open the VPN Configuration GUI.
5. Expand **Secure Connections->Data Connections->Dynamic Key Groups**.
6. Click the Dynamic Key Group **GtoG14to05**. This displays the associated connection (or connections), which, in this case, is GtoG14to05:L1 (Figure 237 on page 235).

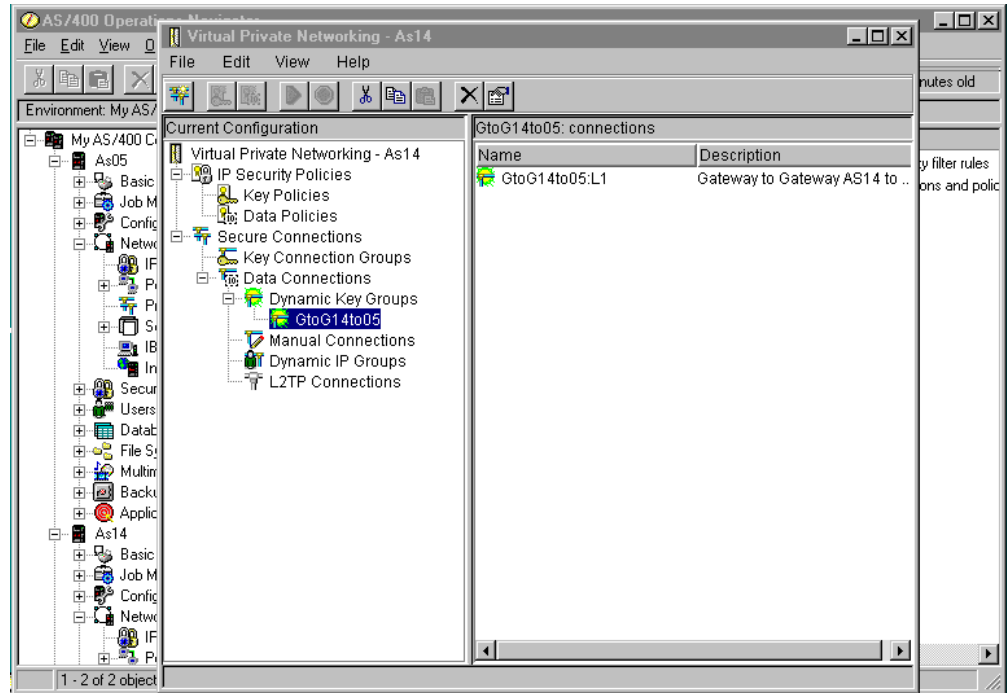


Figure 237. Displaying connections within dynamic key group

- Right-click **GtoG14to05:L1**, and select **Start** to start the connection. Alternatively, select **GtoG14to05:L1** with the left mouse button, and then click on the start icon (a green triangle) on the toolbar (Figure 238).

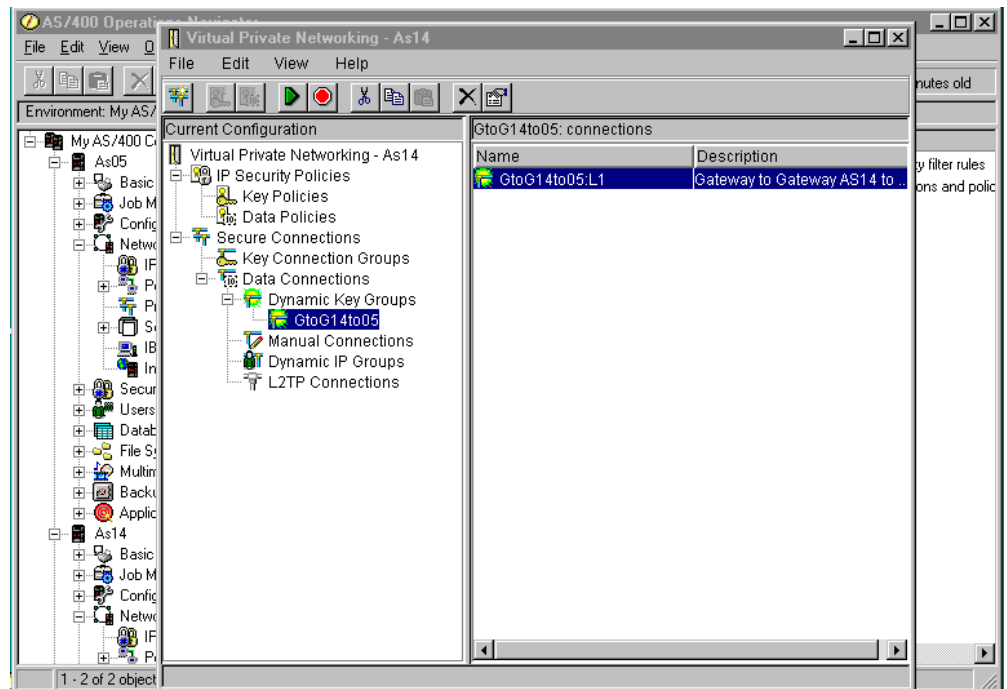


Figure 238. Starting the connection

After a short delay, the connection starts. No messages appear unless a problem occurs.

- To display the active connections, select **View** from the main menu, and then select **Active Connections** (Figure 239).

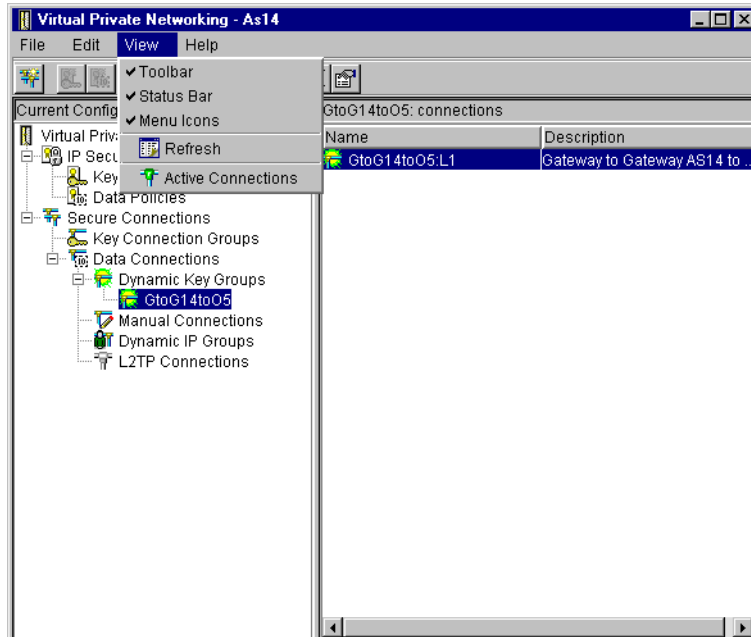


Figure 239. View -> Active Connections

Figure 240 shows that the connection is successfully started with a status of Running.

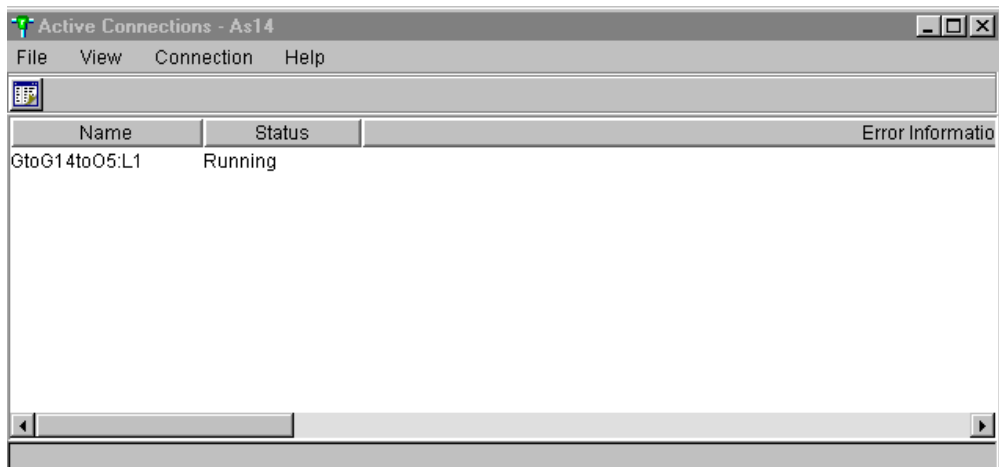


Figure 240. AS14 Active Connections windows

- Display the Active Connections window for AS05, as shown in Figure 241 on page 237. Notice that there are additional columns in this window. You can select which columns to view by selecting **View** from the main menu and then selecting **Preferences**. Click the **Columns** tab to view a list of columns you can display.

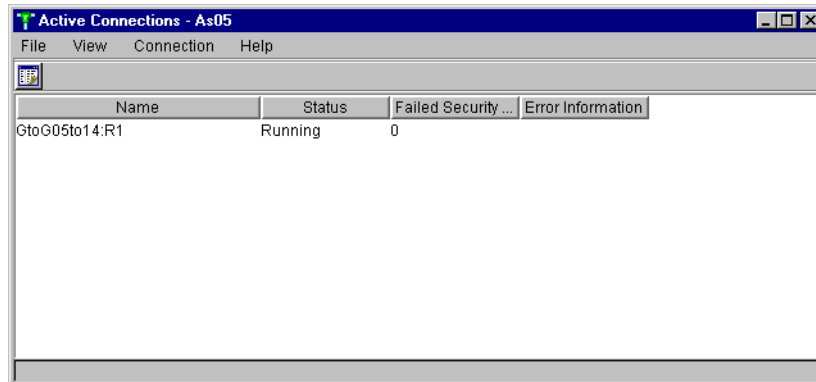


Figure 241. AS05 Active Connections window

6.4.5 Verification tests

At this stage, you should test communications through the VPN tunnel. Table 26 shows a summary of the verification tests that were run and the results after implementing the gateway-to-gateway VPN in this scenario. Refer to Figure 198 on page 201.

Table 26. Gateway-to-gateway VPN - Verification tests

From	To	To IP address	Application	Success
AS20	PC07	10.196.8.4 (H)	PING	Yes
AS20	AS05	10.196.8.5 (D)	PING	Yes
AS20	AS05	10.196.8.5 (D)	FTP	Yes
AS20	AS05	10.196.8.5 (D)	TELNET	Yes
PC07	AS20	10.6.21.1 (J)	TELNET	Yes
PC07	AS20	10.6.21.1 (J)	Client Access PC5250	Yes
PC07	AS20	10.6.21.1 (J)	Operations Navigator	Yes
PC07	AS20	10.6.21.1 (J)	FTP	Yes
PC07	AS14	10.6.11.1 (C)	FTP	Yes
AS20	AS05	208.222.150.250 (B)	PING	No
AS14	AS05	208.222.150.250 (B)	PING	No
AS14	AS05	10.196.8.5 (D)	PING (default source address)	No
AS14	PC07	10.196.8.4 (H)	PING	No
AS05	AS20	10.6.21.1 (J)	PING	No

The tests in Table 26 were performed in our example network to validate a selection of TCP/IP applications and IP addresses. Notice that some connections involving AS14 and AS05 did not work. This is to be expected. Refer to 6.5, “Adding host-to-gateway and gateway-to-host connection groups” on page 238, for more information about these special cases.

To verify that a secure VPN tunnel is in place between AS14 and AS05, run a communication trace on AS14 for traffic between it and AS05. For example, you can follow these steps:

1. Delete any existing trace data for the line that you are about to trace using the Delete Communication Trace (`DLTCMNTRC`) command:

```
DLTCMNTRC CFGOBJ(TRNWSB2) CFGTYPE(*LIN)
```

2. Start the trace by using the Start Communication Trace (`STRCMNTRC`) command. Because you are collecting data for a short period, select the option to stop the trace if it gets full. However, collect the maximum amount of user data from each frame since encapsulated (tunnelled) frames can be quite long:

```
STRCMNTRC CFGOBJ(TRNWSB2) CFGTYPE(*LIN) MAXSTG(2M) TRCFULL(*STOPTRC)
USRDTA(*MAX) TEXT('IPSEC trace to AS05')
```

3. Start any TCP/IP application between the data endpoints to force datagrams through the tunnel.

4. End the trace by using the End Communication Trace (`ENDCMNTRC`) command:

```
ENDCMNTRC CFGOBJ(TRNWSB2) CFGTYPE(*LIN)
```

5. Print the trace by using the Print Communication Trace (`PRTCMNTRC`) command. Format the TCP/IP data but do not print broadcast data:

```
PRTCMNTRC CFGOBJ(TRNWSB2) CFGTYPE(*LIN) CODE(*ASCII) FMTTCP(*YES)
FMTBCD(*NO)
```

Figure 242 shows an excerpt from a `PRTCMNTRC` report with a single IP datagram. Notice that the protocol is ESP. Therefore, the data is unintelligible and encrypted. You can use this technique to verify that the traffic between endpoints is funneled through the tunnel as expected.

```
R      101      3250.6          402233445534  C02211222111  LLC   UI          OFF  AA  AA
Routing Info . : 0270
          Frame Type : IP          TOS: NORMAL          Length: 96 Protocol: ESP
Datagram ID: 6A01
          Src Addr: 208.222.150.250  Dest Addr: 204.146.18.227  Fragment Flags:
DON'T, LAST
          SNAP Header: 0000000800
          IP Header : 450000606A0140001D32AC1CD0DE96FACC9212E3
          IP Options : NONE
          ESP header : SPI: '92F9D73E'X SNF: 35
Data . . . :E693A3E175A8F800 CD2E5FA60887FDD7 5549D4DB4B664B1D BCA586A3077B23E7
*****U**.*_*.***UI**KFK*****.{***
          106A780EF71144B9 E731C4A9E3305B5A 9F60DEF0A6BE68D0 1B22E9FCDFC60A27
* .JX.*.D**1***0φZ*.***H*."*****.'*
          27A138D3
*
* * * 8 *
*
```

Figure 242. Excerpt from the `PRTCMNTRC` report - Encrypted datagram through the tunnel

6.5 Adding host-to-gateway and gateway-to-host connection groups

The gateway-to-gateway VPN configured in the previous sections of this chapter allows any host or client on subnet 10.6.0.0 to talk to any host or client on subnet 10.196.0.0 and vice versa. Assume an application on AS14 needs to communicate with an application on AS05. For example, a user in AS14 needs to initiate a Telnet session to the Telnet server on AS05 as shown in Figure 243.

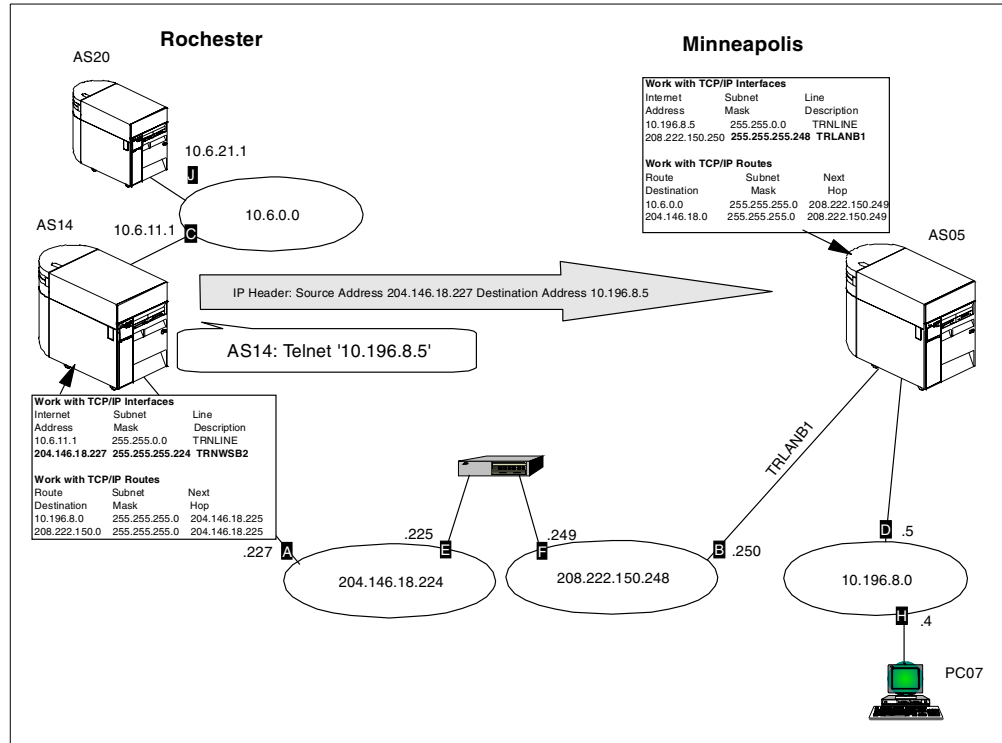


Figure 243. Telnet client on AS14 to Telnet server on AS05

AS14 has an address on the 10.6.0.0 network, which is 10.6.11.1 **C**. AS05 has an address on the 10.196.8.0 network, which is 10.196.8.5 **D**. When they begin communicating with each other, by default they use the source address from the interface used for routing, which, in this case, is 204.146.18.227 **A** on AS14 or 208.222.150.250 **B** on AS05. Very few AS/400 TCP/IP applications allow you to override the source IP address. PING is one exception that allows you to override the source IP address by using the parameter local Internet address (LCLINTNETA). The IPSEC filter rules configured for the gateway-to-gateway VPN only support source and target addresses in either the AS14subnets (10.6.0.0) or AS05subnets (10.196.0.0). Therefore, connections with a 204.*.*.* or 208.*.*.* source (or destination) IP address are not allowed to enter the gateway-to-gateway tunnel. Refer to the test results shown in Table 26 on page 237 for an illustration of this.

Note

For more information, refer to 6.3.3, “Configuring IP filters on the AS14” on page 217, and 6.4.3, “Configuring IP filters on AS05” on page 232).

One solution to this problem is to create a separate *host-to-host* connection between 204.146.18.227 and 208.222.150.250 that runs alongside the existing *gateway-to-gateway* connection. This allows AS14 and AS05 to talk to each other by using their public addresses. Assume that AS05 needs to establish a session with AS20. In this case, the data endpoints are 208.222.150.250 and 10.6.21.1. The host-to-host connection does not support this, since it only supports the source and target addresses of 204.146.18.227 and 208.222.150.250.

You can simplify and minimize the number of connections you need to configure if any-to-any communications are required between the hosts shown in Figure 243 on page 239. Simply create two sets of *host-to-gateway* and matching *gateway-to-host* connections between AS14 and AS05. You must configure each connection on both systems. In other words, you need to add a total of four new dynamic key connection groups, each with a dynamic key connection, for example:

- On AS14:
 - Host-to-gateway with data endpoints 204.146.18.227 and 10.196.0.0
 - Gateway-to-host with data endpoints 10.6.0.0 and 208.222.150.250
- On AS05:
 - Host-to-gateway with data endpoints 208.222.150.250 and 10.6.0.
 - Gateway-to-host with data endpoints 10.196.0.0 and 204.146.18.227

The existing key and data policies you defined for the initial gateway-to-gateway connection can be shared with the new data connection groups. In this case, you will use the VPN configuration GUI, but *not* the VPN configuration wizard to configure the additional connection.

Note that a conflict can occur if you use the wizard for this configuration example, because you have already associated pre-shared keys with the remote key server addresses.

6.5.1 Configuring a host-to-gateway VPN on AS14

To configure a host-to-gateway VPN to satisfy the communications requirements of AS14 subnets (204.146.18.227) and AS05 subnets (10.196.0.0) as data endpoints, perform the following steps:

1. Start the VPN configuration GUI. Right-click **Dynamic Key Groups**, and select **New Dynamic Key Connection Group** (Figure 244 on page 241).

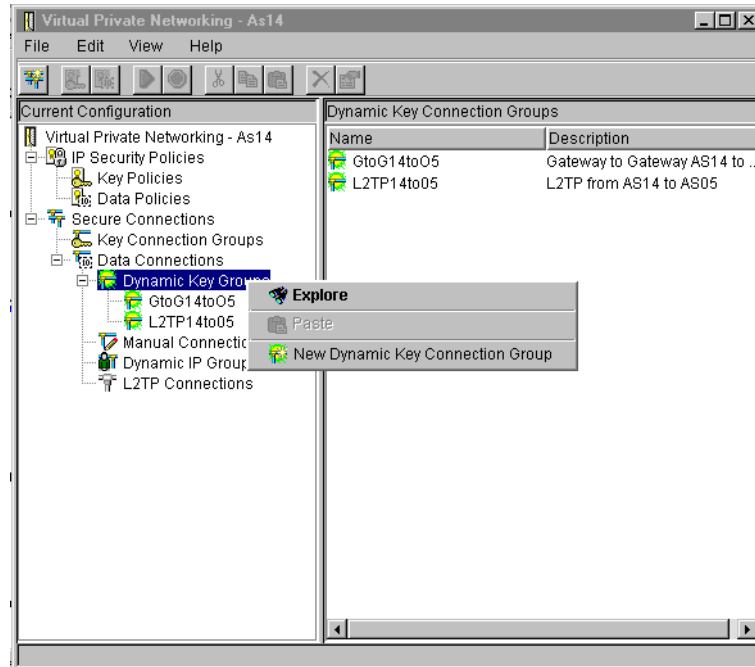


Figure 244. AS14 Creating a new dynamic key connection group

2. Enter a name for the connection group, which here is `HtoG14to05`, and a description. For System role, select **Local system is a host, and the remote system is a gateway**. Allow Initiation to default so that either system can initiate the connection (Figure 245).

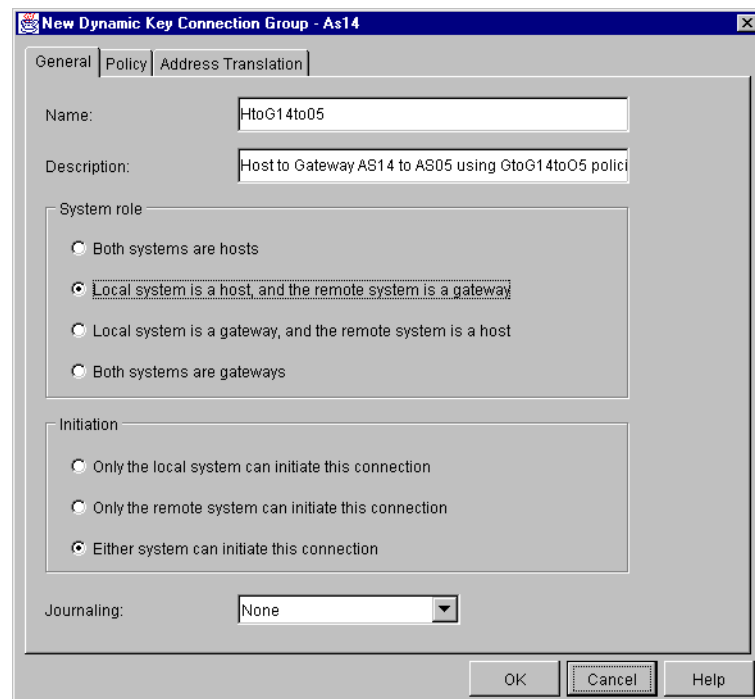


Figure 245. AS14 New Dynamic Key Connection Group - General HtoG14to05

3. Click the **Policy** tab.

4. Select the data management security policy that you created for the gateway-to-gateway connection, which is **GtoG14toO5BS**. This means that IKE uses the same authentication and encryption protocols to protect the data during phase 2 negotiations as it does in the gateway-to-gateway configuration (Figure 246).

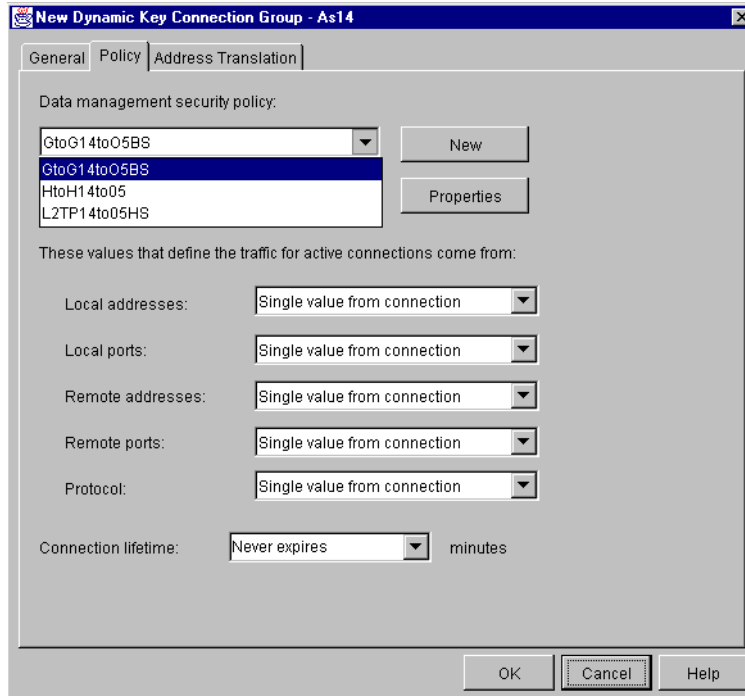


Figure 246. AS14 New Dynamic Key Connection Group - Policy HtoG14to05

5. For the values that define the traffic for active connections, select **Filter rule** for the address, port, and protocol fields. This indicates that the addresses, ports and protocols that can use this connection are defined by the IPSEC filter rule you will configure later (Figure 247 on page 243).

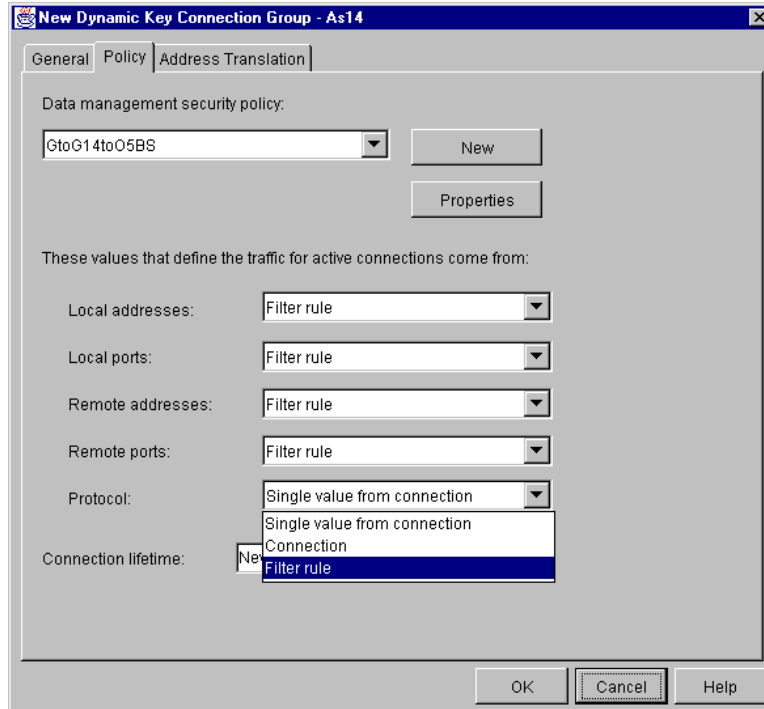


Figure 247. AS14 New Dynamic Key Connection Group - Policy for HtoG14to05

6. Click **OK** to create the host-to-gateway data connection group HtoG14to05.
7. The new data connection group, HtoG14to05, should now be under Dynamic Key Groups. Right-click on it, and select **New Dynamic Key Connection** to add an individual connection to the group (Figure 248).

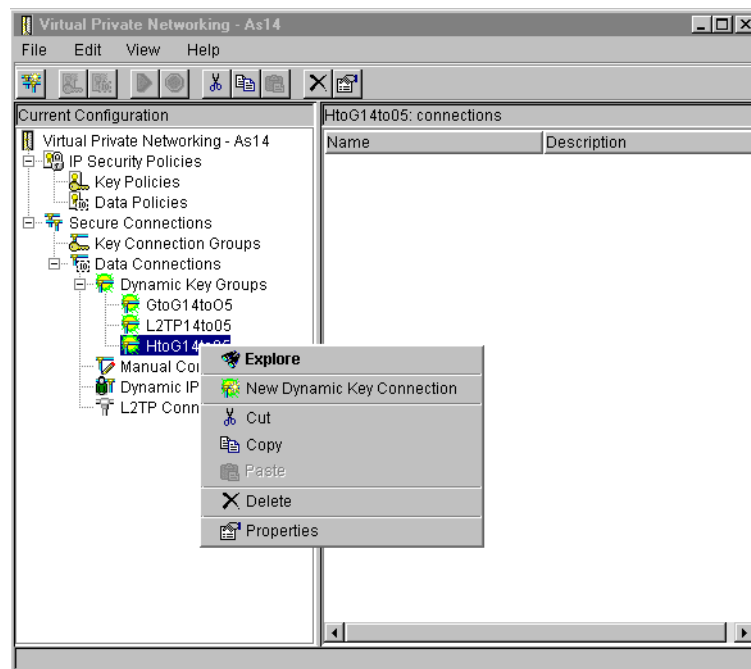


Figure 248. AS14 New dynamic key connection HtoG14to05

8. Enter a description of the connection. Then, select the Key connection group **GtoG14toO5**, which you created for your gateway-to-gateway connection. This means that IKE uses same protocols for authentication and encryption as the previous configuration. The IP address of the remote key server, 208.222.150.250 **B**, is automatically selected for you (Figure 249).

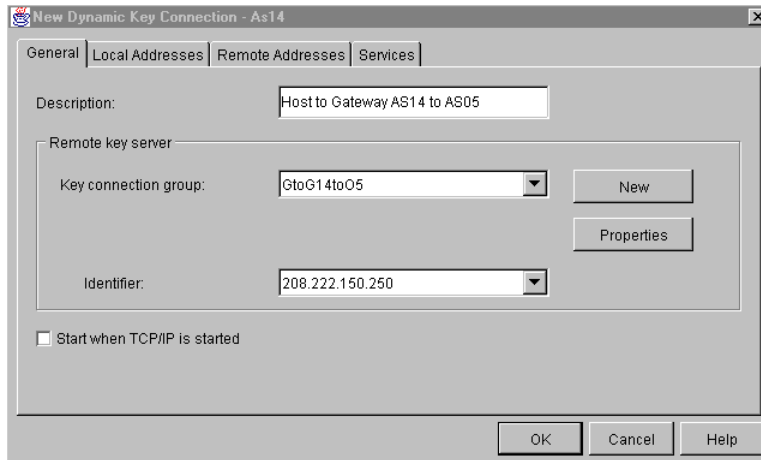


Figure 249. AS14 New Dynamic Key Connection - General HtoG14toO5

9. Click the **Local Addresses** tab.
10. Even though you specified *filter rules* when you created the Dynamic Key Connection Group, you must still enter an IP address for the local interface. This is not used in this case. For completeness, enter the correct address, 204.146.18.227 **A** (Figure 250).

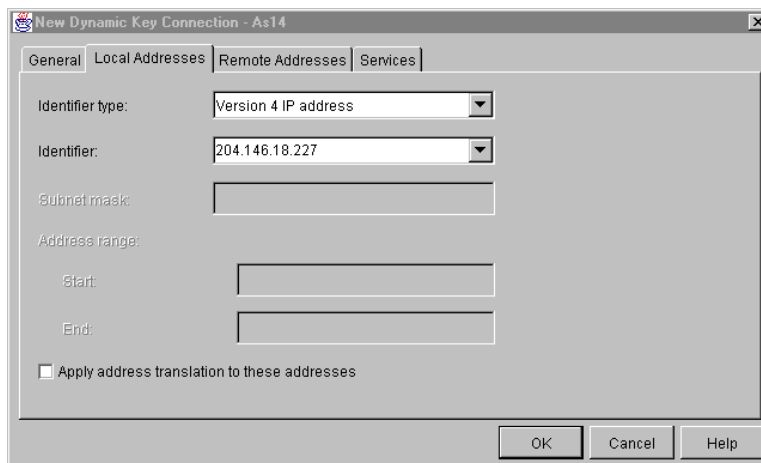


Figure 250. AS14 New Dynamic Key Connection - Local addresses HtoG14toO5

11. Click the **Remote Addresses** tab.
12. Enter an identifier for the remote subnet that can use this data connection. Because this is a host-to-gateway configuration, select **IP version 4 subnet** for Identifier type. Enter 10.196.0.0 for Identifier (the IP address of the remote subnet) and 255.255.0.0 for the Subnet mask (Figure 251 on page 245).

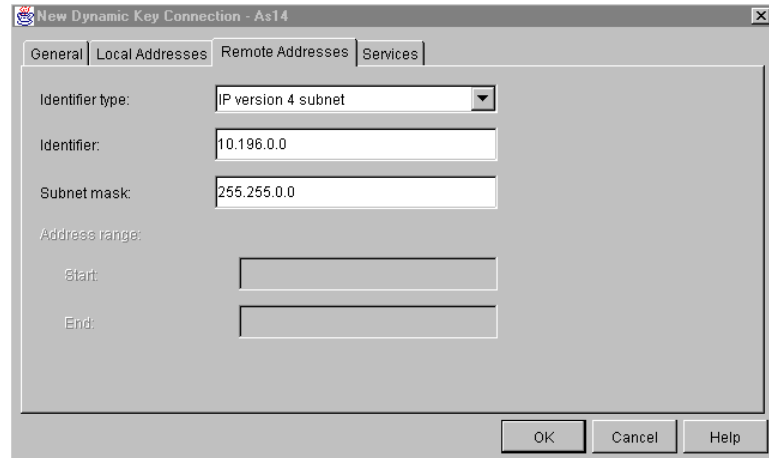


Figure 251. AS14 New Dynamic Key Connection - Remote addresses HtoG14to05

Note

In this scenario, we configure the values that define the traffic for the connection in the filter rules (Figure 247 on page 243). Therefore, the local and remote addresses actually come from the IPSEC filter rule associated with this connection.

13. Click the **Services** tab.

14. Review the Services parameters, but remember that these values come from the filter rules.

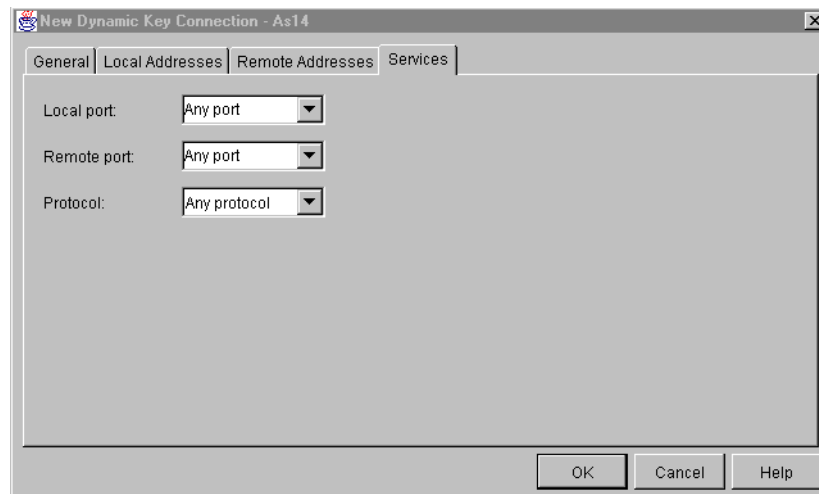


Figure 252. AS14 New Dynamic Key Connection - Services HtoG14to05

15. Click **OK** to create the new dynamic key connection.

This completes the configuration of the host-to-gateway connection for AS14.

6.5.2 Configuring a gateway-to-host VPN on AS14

Repeat step 1 on page 240 through step 15 on page 245 to create a gateway-to-host connection on AS14.

Note the following points:

- This time, the System role is *Local system is a gateway, and the remote system is a host* (Figure 253).

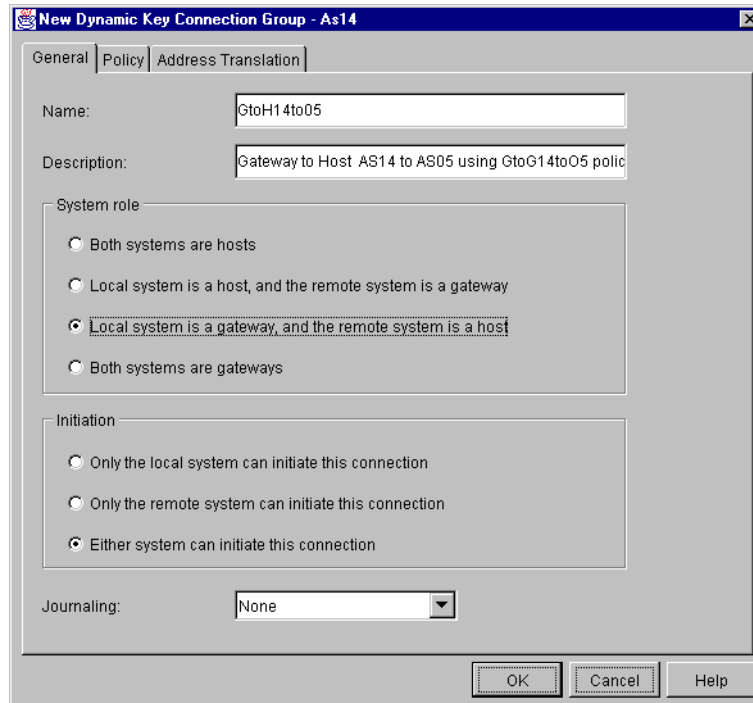


Figure 253. New Dynamic Key Connection Group - General GtoH14to05

- Select the same Data management security policy, **GtoG14to05BS**, as you specified for the gateway-to-gateway and host-to-gateway configuration (Figure 254 on page 247).

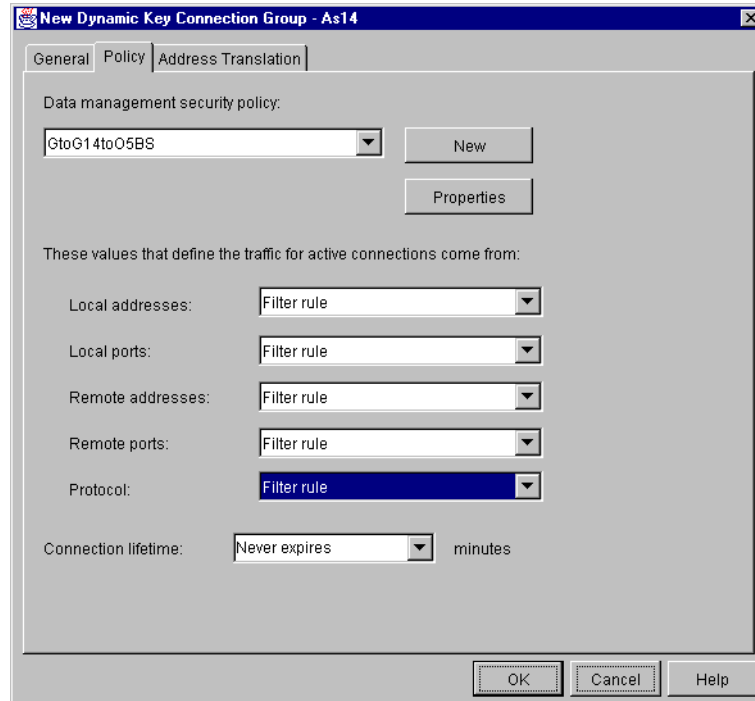


Figure 254. New Dynamic Key Connection Group - Policy GtoH14to05

- Add a connection to the GtoH14to05 key connection group (Figure 255).

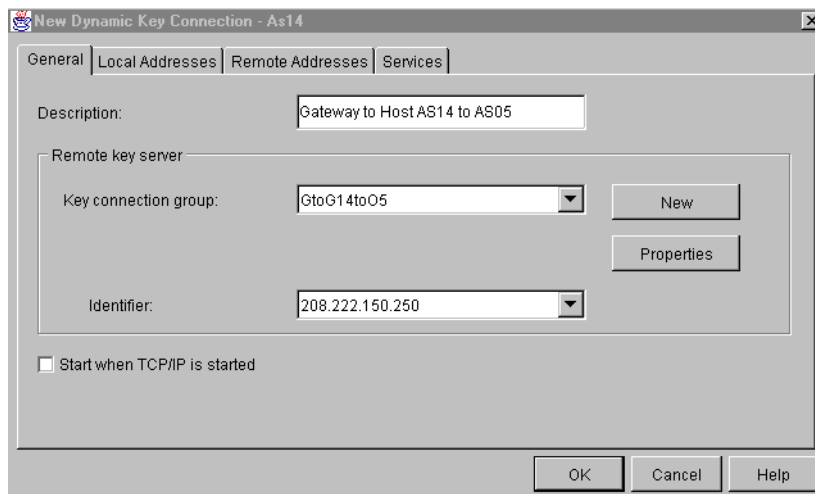


Figure 255. New Dynamic Key Connection - General GtoH14to05

- This is a gateway-to-host connection. Therefore, the local data endpoint (local addresses) is a subnet (Figure 256 on page 248).

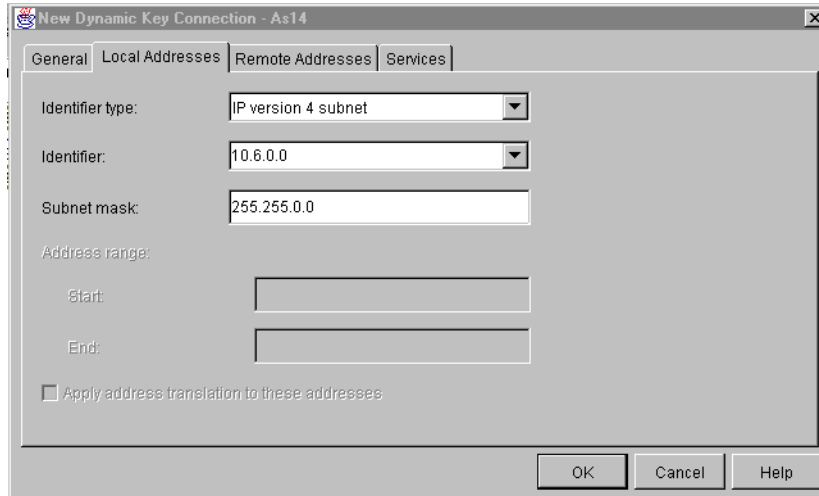


Figure 256. New Dynamic Key Connection - Local addresses GtoH14to05

- The remote data endpoint IP address is the address of the AS05 host (Figure 257).

Note

In this scenario, we configure the values that define the traffic for the connection in the filter rules (Figure 254 on page 247). Therefore, the local and remote addresses actually come from the IPSEC filter rule associated with this connection.

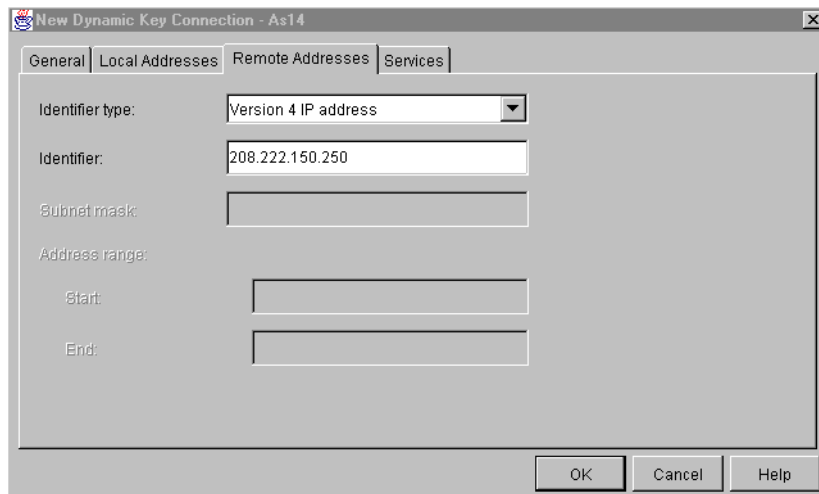


Figure 257. New Dynamic Key Connection - Remote addresses GtoH14to05

This ends the configuration of the gateway-to-host connection.

6.5.3 Adding IPSEC filter rules

To complete the configuration of the host-to-gateway VPN configured in 6.5.1, “Configuring a host-to-gateway VPN on AS14” on page 240, and the gateway-to-host VPN configured in 6.5.2, “Configuring a gateway-to-host VPN on

AS14” on page 246, you must configure the IPSEC filter rules associated with those connections.

Perform the following steps to add new filter rules to the existing GtoGfilter1.i3p IP filter file created in 6.3.3, “Configuring IP filters on the AS14” on page 217:

1. Return to Operations Navigator, and double-click **IP Packet Security**.
2. Select **File->Open** (Figure 258). Select the file you created earlier in this example, **GtoGfilter1.i3p**, to open it.

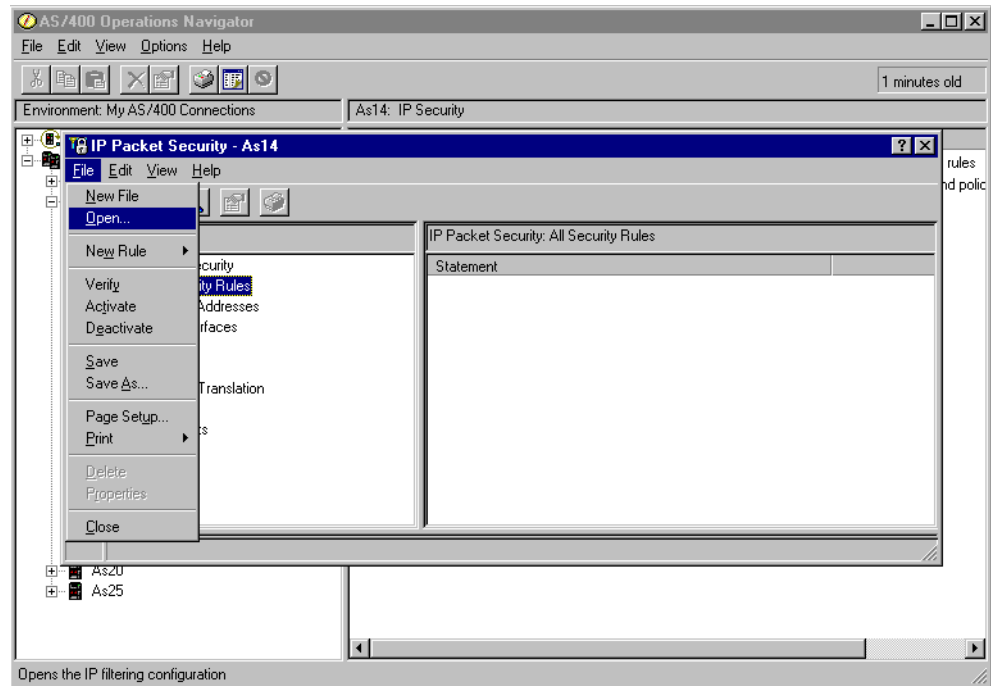


Figure 258. Open existing filter rules file

3. Right-click **Filters**, and select **New Filter**.
4. Add a new filter to the existing file using the same set name, VPNIFC, as you used for the other filter rules. Select **IPSEC** for Action and enter the source and destination addresses that are allowed to use this host-to-gateway connection. In this example, AS14’s interface, 204.146.18.227, is the Source address name, and AS05subnets (created earlier to represent the 10.196.0.0 subnet) is the Destination address name. Select **HtoG14to05** from the Connection name pull-down menu. This is the dynamic key connection created in 6.5.1, “Configuring a host-to-gateway VPN on AS14” on page 240. See Figure 259 on page 250.

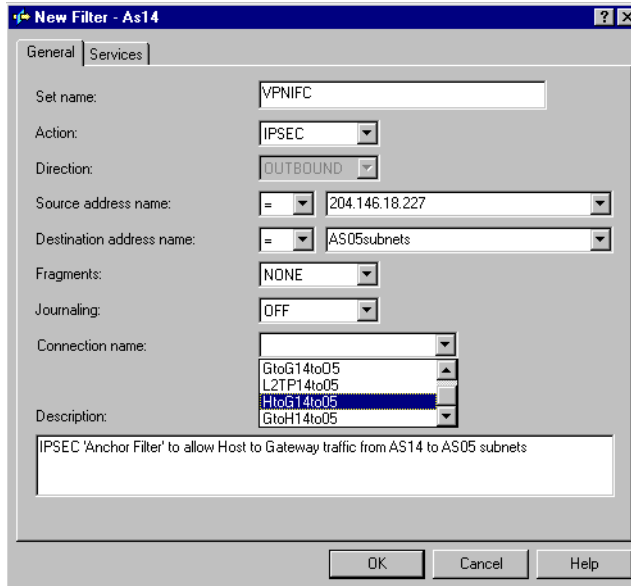


Figure 259. IPSEC filter rule for the host-to-gateway connection HtoG14to05

Tip

You can only use one connection name per IPSEC filter rule. A filter rules file that contains duplicate connection names fails verification. If you need multiple IPSEC rules, separate connection groups must be created for each one.

5. Click the **Services** tab.
6. Select **Service**, and use the pull-downs to enter a wildcard (*) in the Protocol, Source port, and Destination port fields.
7. Click **OK**.
8. Repeat step 3 on page 249 through step 7 on page 250 to add an IPSEC filter rule for the gateway-to-host connection group created in 6.5.2, “Configuring a gateway-to-host VPN on AS14” on page 246. This is GtoH14to05 between the source address AS14subnets and the destination address 208.222.150.250 **B**. See Figure 260 on page 251.

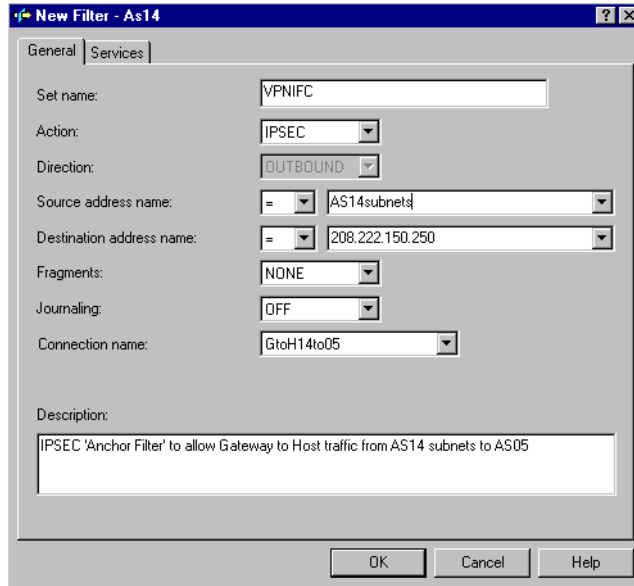


Figure 260. IPSEC filter rule for the gateway-to-host connection GtoH14to05

9. Verify and save the modified filter rules file as you did before.

Tip

Before *activating* a new or modified filter rule file, you should stop all active VPN connections. Activating a new set of filter rules automatically causes the currently active set to deactivate. VPN connections require the filter rules to be active. Therefore, a filter rules file cannot be activated or deactivated until VPN connections are stopped.

10. Stop any active connections from one of the VPN partners AS/400 systems. From the Active Connections window, select **Connection->Stop** (Figure 261).

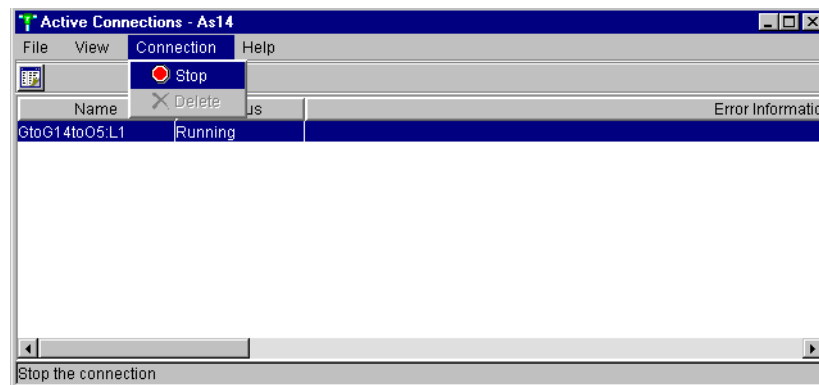


Figure 261. Stop Active Connections

Figure 262 on page 252 shows the modified filter rules file successfully activated. Notice that there are three IPSEC filter rules associated with the three dynamic key connection groups configured in this chapter.

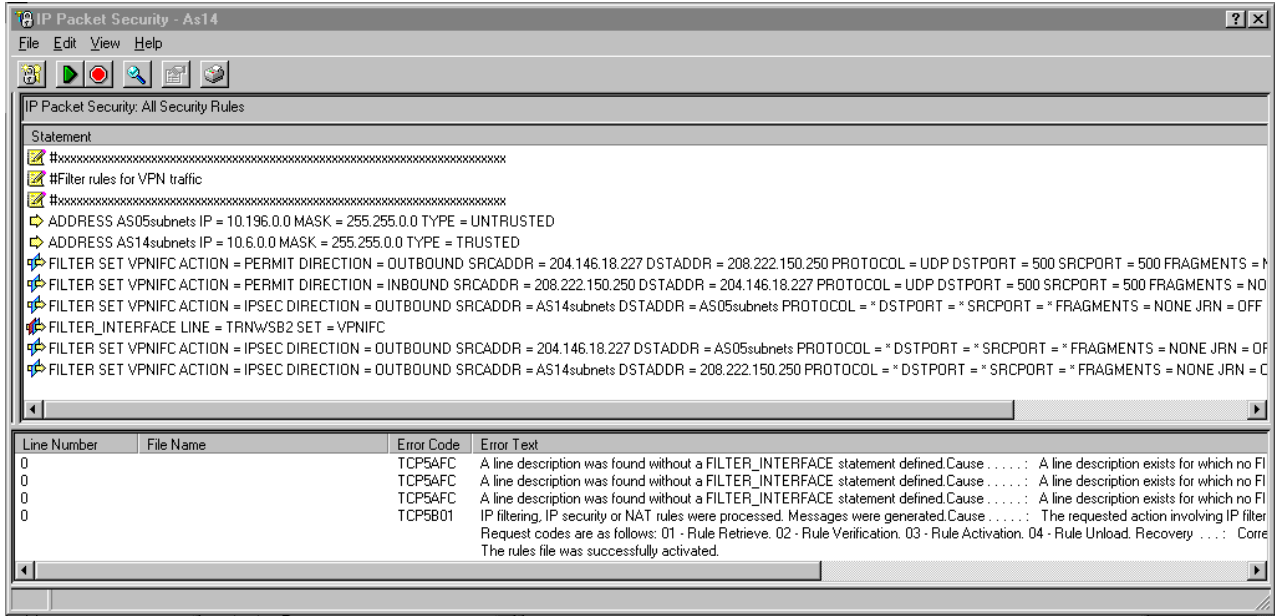


Figure 262. AS14 Activate updated filter rules file

6.5.4 Configuring host-to-gateway and gateway-to-host VPNs on AS05

Repeat the host-to-gateway and gateway-to-host configuration on the Minneapolis AS/400 system, AS05. Create two matching dynamic key connection groups, each with a dynamic key connection. In this example, the connection groups are called *HtoG05to14* and *GtoH05to14*.

Note: As an alternative to creating two new dynamic key connection groups, you can use the VPN configuration GUI *copy* and *paste* functions.

To copy a dynamic key connection group, right-click on it, and select **Copy** as shown in Figure 263 on page 253.

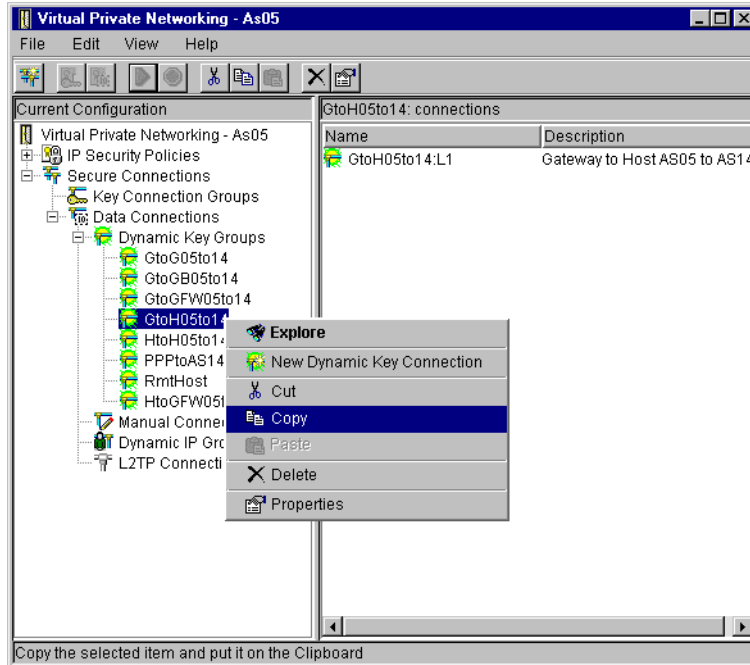


Figure 263. VPN configuration GUI - Copy

To paste the copy, right-click on **Dynamic Key Groups**, and select **Paste** as shown in Figure 264.

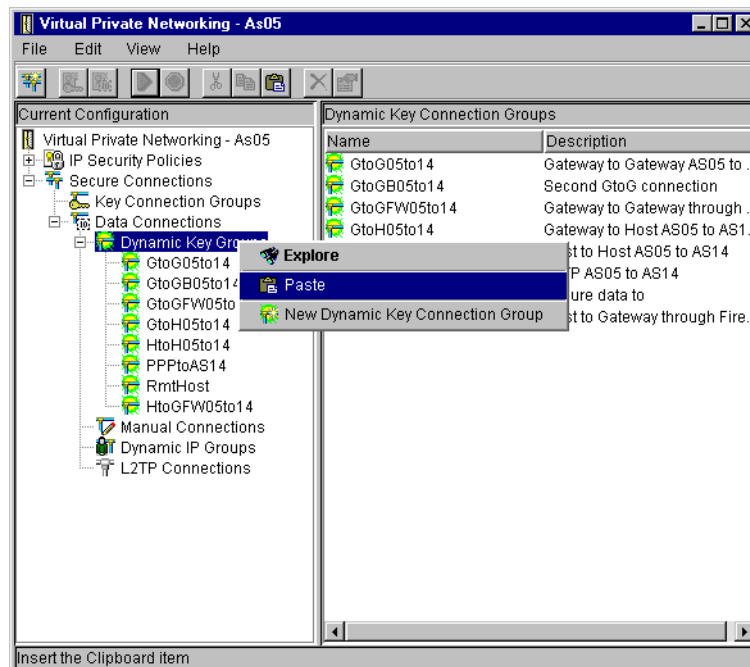


Figure 264. VPN configuration GUI - Paste

This creates a duplicate of the dynamic key connection group, including the connection within it. The properties can then be edited as required.

You must also create a pair of matching IPSEC filter rules on AS05. Ensure that source and target addresses are reversed on the remote system. Figure 265 shows an updated printout of all the filter rules that you configured for AS05.

```

*****
#Filter rules for VPN traffic
*****
ADDRESS AS05subnets IP = 10.196.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
ADDRESS AS14subnets IP = 10.6.0.0 MASK = 255.255.0.0 TYPE = UNTRUSTED
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 208.222.150.250
  DSTADDR = 204.146.18.227 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 204.146.18.227
  DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS05subnets DSTADDR = AS14subnets
  PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
  CONNECTION_DEFINITION = GtoG05to14
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 208.222.150.250 DSTADDR = AS14subnets
  PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
  CONNECTION_DEFINITION = HtoG05to14
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS05subnets DSTADDR = 204.146.18.227
  PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
  CONNECTION_DEFINITION = GtoH05to14
FILTER_INTERFACE LINE = TRLANB1 SET = VPNIFC

```

Figure 265. AS05 Updated IP filters file - Summary

When complete, activate the modified filter rules file as shown in Figure 266.

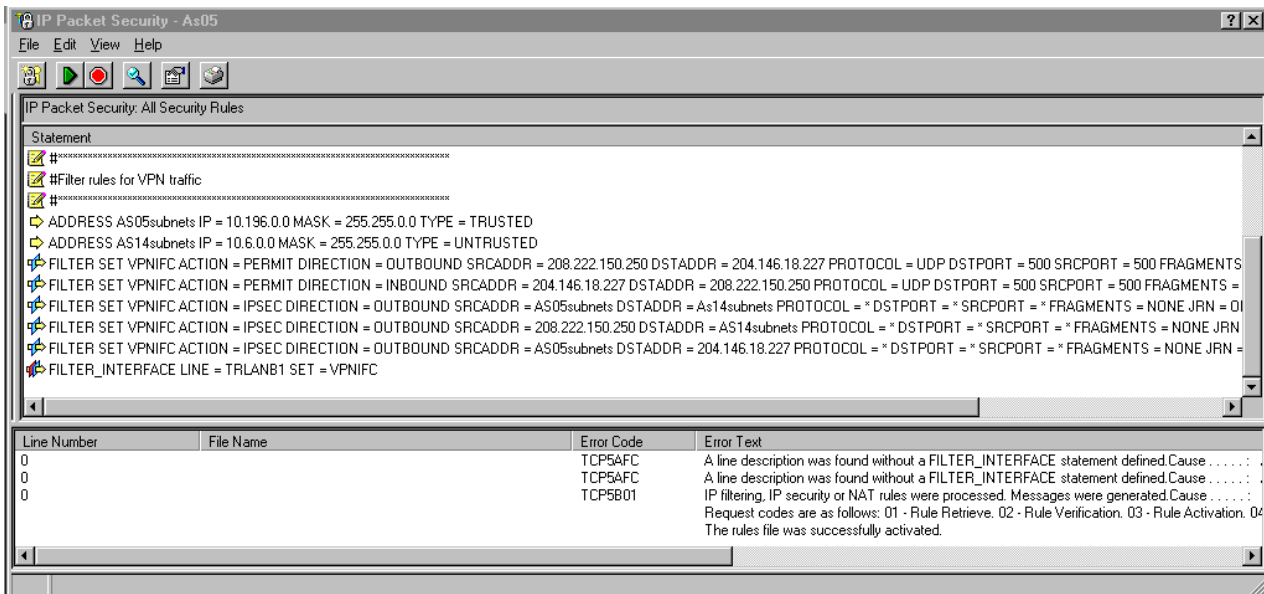


Figure 266. AS05 Activate updated filter rules file

6.5.5 Starting host-to-gateway and gateway-to-host VPN connections

You are now ready to start the new host-to-gateway and gateway-to-host connections. In this scenario, we are not restricting the system that can be the initiator. Either VPN server can initiate the connection. As an example, start the three connections from AS14. Perform the following steps:

1. From the VPN configuration GUI, select the gateway-to-gateway connection **GtoG14toO5:L1** (Figure 267). Click the green triangle on the toolbar to start this connection.

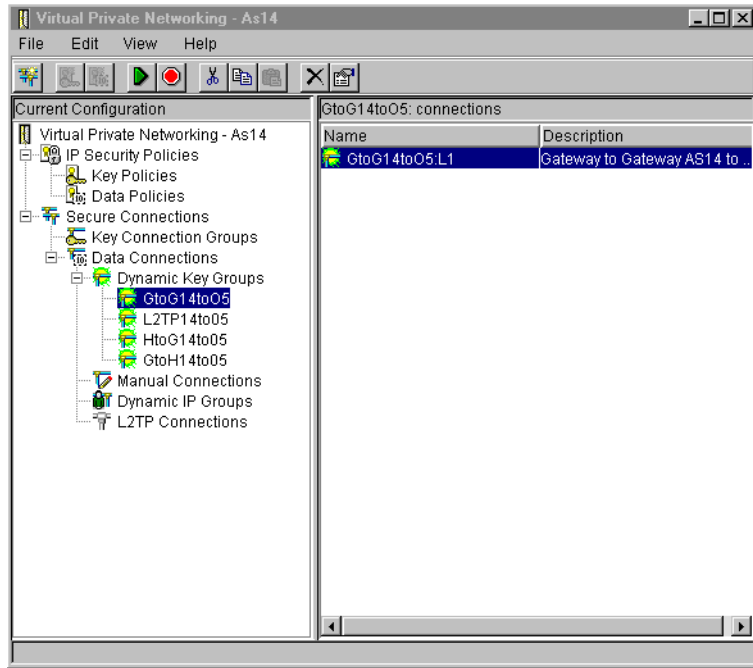


Figure 267. Start gateway to gateway connection GtoG14toO5:L1

2. Repeat step 1 for both the host-to-gateway (HtoG14to05:L1) and the gateway-to-host (GtoH14to05) connections.
3. View the connections status on both systems from the Active Connections window as shown in Figure 268 and Figure 269 on page 256.

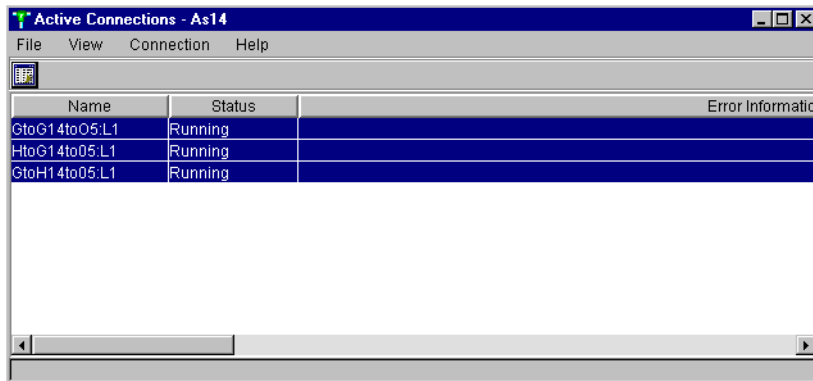


Figure 268. AS14 View active connections

Name	Status	Failed Security...	Error Information
GtoG05to14:R2	Running	0	
GtoH05to14:L1	Running	0	
HtoG05to14:L1	Running	0	

Figure 269. AS05 View active connections

6.5.6 Tracing the VPN tunnels

This section includes excerpts of communication traces taken on datagrams in the gateway-to-gateway, host-to-gateway, and gateway-to-host tunnels. The communication trace was run on AS14, tracing the public interface TRNWSB2.

We modified the data policy to use the AH protocol, rather than ESP, to avoid encryption and, therefore, make the trace readable. A simpler way to disable encryption is to select encryption NULL for ESP.

6.5.6.1 Tracing the gateway-to-gateway connection

Figure 270 shows a datagram in the gateway-to-gateway connection as a result of a PING (echo) request from AS20 (Src Addr 10.6.21.1) to PC07 (Dest Addr 10.196.8.4).

```

S      333      4865.3          402211222111  C02233445534  LLC   UI          OFF  AA  AA
Routing Info . : 0270
      Frame Type : IP          TOS: NORMAL          Length:  328  Protocol: AH
Datagram ID: C4BF
      Src Addr: 204.146.18.227  Dest Addr: 208.222.150.250  Fragment
Flags: MAY ,LAST
  SNAP Header: 0000000800
  IP Header  : 45000148C4BF00003E336F75CC9212E3D0DE96FA
  IP Options : NONE
  AH header  : Next header: IP          Length:  4  SPI: 'ECD2E46E'X  SNF:    11
  AH data . . : 0BF222A0F020788D0DDDB55CD
      Frame Type : IP          TOS: NORMAL          Length:  284  Protocol: ICMP
Datagram ID: C4BF
      Src Addr: 10.6.21.1          Dest Addr: 10.196.8.4          Fragment
Flags: MAY ,LAST
  IP Header  : 4500011CC4BF00003E0185530A0615010AC40804
  IP Options : NONE

```

Figure 270. Gateway to gateway - Ping request from 10.6.21.1 (AS20) to 10.196.8.4 (PC07)

Figure 271 on page 257 shows a datagram in the gateway-to-gateway connection as a result of a PING (echo) response from PC07 (Src Addr 10.196.8.4) to AS20 (Dest Addr 10.6.21.1).


```

R      333      4865.3              402233445534 C02211222111 LLC   UI              OFF  AA  AA
Routing Info . : 0270
      Frame Type : IP              TOS: NORMAL              Length: 328 Protocol: AH
Datagram ID: 5A06
      Src Addr: 208.222.150.250 Dest Addr: 204.146.18.227 Fragment
Flags: MAY ,LAST
      SNAP Header: 0000000800
      IP Header : 450001485A0600001D33FB2ED0DE96FACC9212E3
      IP Options : NONE
      AH header : Next header: IP      Length: 4 SPI: '68C311FC'X SNF: 11
      AH data . . : 16696DE2AF73129AD94CB9C7
      Frame Type : IP              TOS: NORMAL              Length: 284 Protocol: ICMP
Datagram ID: 5A06
      Src Addr: 10.196.8.4 Dest Addr: 10.6.21.1 Fragment Flags:

```

Figure 271. Gateway to gateway - Ping response from PC07 (10.196.8.4) to AS20 (10.6.21.1)

Notice that the outer IP header has the source and destination addresses of the VPN servers, 204.146.18.227 and 208.222.150.250. Then, notice that there is an AH protocol header and within the AH frame another IP frame with a second IP header. The source and destination addresses for this tunnelled IP frame are 10.6.21.1 and 10.196.8.4.

Compare these trace records with the ESP example in Figure 242 on page 238. Notice that with ESP DES encryption, the private IP addresses in the inner (tunnelled) IP frame cannot be seen.

6.5.6.2 Tracing the host-to-gateway connection

Figure 272 shows a datagram in the host-to-gateway connection as a result of a PING (echo) request from AS14 (Src Addr 204.146.18.227) to AS05 (Dest Addr 10.196.8.5).

```

S      333      4878.2              402211222111 C02233445534 LLC   UI              OFF  AA  AA
Routing Info . : 0270
      Frame Type : IP              TOS: NORMAL              Length: 328 Protocol: AH
Datagram ID: A95E
      Src Addr: 204.146.18.227 Dest Addr: 208.222.150.250 Fragment
Flags: MAY ,LAST
      SNAP Header: 0000000800
      IP Header : 45000148A95E00003F3389D6CC9212E3D0DE96FA
      IP Options : NONE
      AH header : Next header: IP      Length: 4 SPI: '8A31CC12'X SNF: 11
      AH data . . : 1AE491D758E493AF439F1345
      Frame Type : IP              TOS: NORMAL              Length: 284 Protocol: ICMP
Datagram ID: A95E
      Src Addr: 204.146.18.227 Dest Addr: 10.196.8.5 Fragment

```

Figure 272. Host to gateway - Ping request from 204.146.18.227 (AS14) to 10.196.8.5 (AS05)

Figure 273 on page 258 shows a datagram in the host-to-gateway connection as a result of a PING (echo) response from AS05 (Src Addr 10.196.8.5) to AS14 (Dest Addr 204.146.18.227).

```

R      333      4878.2                402233445534 C02211222111 LLC   UI                                OFF  AA  AA
Routing Info . : 0270
      Frame Type : IP                TOS: NORMAL                Length: 328 Protocol: AH
Datagram ID: FD5A
      Src Addr: 208.222.150.250  Dest Addr: 204.146.18.227  Fragment
Flags: MAY ,LAST
      SNAP Header: 0000000800
      IP Header : 45000148FD5A00003E3336DAD0DE96FACC9212E3
      IP Options : NONE
      AH header : Next header: IP      Length: 4 SPI: '07DE949B'X SNF: 11
      AH data . . : 89979828FE72A81DF35F9725
      Frame Type : IP                TOS: NORMAL                Length: 284 Protocol: ICMP
Datagram ID: FD5A
      Src Addr: 10.196.8.5          Dest Addr: 204.146.18.227  Fragment

```

Figure 273. Host to gateway - Ping response from AS05 (10.196.8.5) to 204.146.18.227 (AS14)

Tracing datagrams in the host-to-gateway VPN shows that the outer IP addresses are still those of the VPN key servers. However, the inner addresses are now the AS14 host IP address (204.146.18.227) and the AS05 IP address in the AS05 subnets (10.196.8.5).

6.5.6.3 Tracing the gateway-to-host connection

Figure 274 shows a datagram in the gateway to host connection as a result of a PING (echo) request from AS05 (Src Addr 208.222.150.250) to AS20 (Dest Addr 10.6.21.1).

```

R      333      4886.4                402233445534 C02211222111 LLC   UI                                OFF  AA  AA
Routing Info . : 0270
      Frame Type : IP                TOS: NORMAL                Length: 328 Protocol: AH
Datagram ID: FD84
      Src Addr: 208.222.150.250  Dest Addr: 204.146.18.227  Fragment
Flags: MAY ,LAST
      SNAP Header: 0000000800
      IP Header : 45000148FD8400003E3336B0D0DE96FACC9212E3
      IP Options : NONE
      AH header : Next header: IP      Length: 4 SPI: '71FC6E69'X SNF: 11
      AH data . . : EA769F0F065A680E86BF584E
      Frame Type : IP                TOS: NORMAL                Length: 284 Protocol: ICMP
Datagram ID: FD84
      Src Addr: 208.222.150.250  Dest Addr: 10.6.21.1      Fragment

```

Figure 274. Gateway to host - Ping request from 208.222.150.250 (AS05) to 10.6.21.1 (AS20)

Figure 274 shows a datagram in the gateway-to-host connection as a result of a PING (echo) response from AS20 (Src Addr 10.6.21.1) to AS05 (Dest Addr 208.222.150.250).

```

S      333      4886.4          402211222111 C02233445534 LLC   UI          OFF  AA  AA
Routing Info . . : 0270
      Frame Type : IP          TOS: NORMAL          Length: 328 Protocol: AH
Datagram ID: C67E
      Src Addr: 204.146.18.227  Dest Addr: 208.222.150.250 Fragment
Flags: MAY ,LAST
      SNAP Header: 0000000800
      IP Header : 45000148C67E00003E336DB6CC9212E3D0DE96FA
      IP Options : NONE
      AH header : Next header: IP          Length: 4 SPI: '2BAEA773'X SNF: 11
      AH data . . : FC4D906B34551CEDA5B48FDF
      Frame Type : IP          TOS: NORMAL          Length: 284 Protocol: ICMP
Datagram ID: C67E
      Src Addr: 10.6.21.1      Dest Addr: 208.222.150.250 Fragment

```

Figure 275. Gateway to host - Ping response from AS20 (10.6.21.1) to AS05 (208.222.150.250)

The outer IP addresses are again those of the VPN servers. However, the inner addresses are now the IP address of AS05 host (208.222.150.250) and the IP address of AS20 on the AS14subnets (10.6.21.1).

Note that in all of these figures, the Security Parameter Index (SPI) fields are different. This is because each tunnel uses a unique SPI for each direction. This indicates that different Security Associations (SA) have been created for each tunnel, even though they share the same key and data policies. For more information about SPI and SA concepts, refer to 1.9, “IPSec configuration concepts” on page 29.

6.6 Additional TCP/IP configuration information

This section shows additional TCP/IP configuration information for the systems used in the scenarios of this chapter.

6.6.1 AS14 TCP/IP interfaces and routes configuration

Figure 276 shows the TCP/IP interfaces on AS14 that are relevant to this scenario.

```

Work with TCP/IP Interfaces
System: AS14
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  9=Start  10=End

  Internet      Subnet      Line      Line
  Opt  Address      Mask      Description  Type
  ....
  10.6.11.1     255.255.0.0  TRNLIN    *TRLAN
  ....
  127.0.0.1     255.0.0.0   *LOOPBACK *NONE
  204.146.18.227 255.255.255.224 TRNWSB2   *TRLAN

```

Figure 276. AS14 TCP/IP interfaces - Gateway to gateway: No firewall

Figure 277 on page 260 shows the TCP/IP routes on AS14 that are relevant to this scenario.

```

Work with TCP/IP Routes
System: AS14
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display
Route      Subnet      Next      Preferred
Opt  Destination  Mask      Hop      Interface
....
10.196.8.0  255.255.255.0  204.146.18.225  *NONE
....
208.222.150.0  255.255.255.0  204.146.18.225  *NONE

```

Figure 277. AS14 TCP/IP routes

6.6.2 AS05 TCP/IP interfaces and routes configuration

Figure 278 shows the TCP/IP interfaces on AS05 that are relevant to this scenario.

```

Work with TCP/IP Interfaces
System: AS05
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  9=Start  10=End
Internet  Subnet      Line      Line
Opt  Address      Mask      Description  Type
....
10.196.8.5  255.255.255.0  TRLANC  *TRLAN
127.0.0.1  255.0.0.0  *LOOPBACK  *NONE
....
208.222.150.250  255.255.255.248  TRLANB1  *TRLAN

```

Figure 278. AS05 TCP/IP Interfaces - Gateway to gateway: No firewall

Figure 279 shows the TCP/IP routes on AS05 that are relevant to this scenario.

```

Work with TCP/IP Routes
System: AS05
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display
Route      Subnet      Next      Preferred
Opt  Destination  Mask      Hop      Interface
....
10.6.0.0  255.255.0.0  208.222.150.249  *NONE
204.146.18.0  255.255.255.0  208.222.150.249  *NONE

```

Figure 279. AS05 TCP/IP routes

6.6.3 AS20 TCP/IP interfaces and routes configuration

Figure 280 on page 261 shows the TCP/IP interfaces on AS20 that are relevant to this scenario.

```

Work with TCP/IP Interfaces
System: AS20
Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

Opt  Internet      Subnet      Line      Line
     Address      Mask        Description Type
     ....
     10.6.21.1     255.255.0.0 TRNLINE  *TRLAN
     ....
     127.0.0.1     255.0.0.0  *LOOPBACK *NONE

```

Figure 280. AS20 TCP/IP interfaces - Gateway to gateway: No firewall

Figure 281 shows the TCP/IP routes on AS20 that are relevant to this scenario.

```

Work with TCP/IP Routes
System: AS20
Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display

Opt  Route      Subnet      Next      Preferred
     Destination Mask        Hop        Interface
     ....
     10.196.8.0  255.255.255.0 10.6.11.1 *NONE
     208.222.150.250 *HOST        10.6.11.1 *NONE

```

Figure 281. AS20 TCP/IP routes

6.6.4 Router configuration

The router that connects both networks has an interface on each Demilitarized Zone (DMZ). In a real life environment, two routers would be used: one router to connect the Rochester network to the *intervening network*, and a second router to connect the Minneapolis network to the *intervening network*. Refer to Figure 198 on page 201.

Router interface **E** (204.146.18.225) represents the router that connects the Rochester network to the Internet. This router must route IP datagrams to AS14 public interface **A** (204.146.18.227). Since interfaces **E** and **A** are in the same subnet, no additional routes need to be configured in the router.

Router interface **F** (208.222.150.249) represents the router that connects the Minneapolis network to the Internet. This router must route IP datagrams to AS05 public interface **B** (208.222.150.250). Since interfaces **F** and **B** are in the same subnet, no additional routes need to be configured in the router.

6.6.5 PC07 TCP/IP configuration

The TCP/IP properties on PC07 are defined here:

- IP address: 10.196.8.4
- Subnet mask: 255.255.255.0
- Default gateway: 10.196.8.5

Chapter 7. L2TP host-to-gateway voluntary tunnel

In voluntary tunneling, a tunnel is created by the user, typically through the use of a tunneling client. A tunneling client is one that features L2TP Access Concentrator support such as the AS/400 system in V4R4. As a result, the L2TP client, also known as *initiator*, sends L2TP packets to the ISP, which forwards them to the corporate office gateway. The corporate office gateway performs the role of L2TP Network Server (LNS) or terminator of the L2TP tunnel. Note that in a voluntary tunnel, the ISP does not need to support L2TP, and the L2TP tunnel initiator effectively resides on the same machine as the remote client.

In this model, an L2TP-enabled client establishes a Point-to-Point Protocol (PPP) session to an ISP and then launches an L2TP session directly to the main office gateway without any involvement from the ISP. The client must first establish an L2TP tunnel with its corporate office gateway using a globally routable (registered) IP address. Once the L2TP tunnel is established, the client and the corporate office gateway negotiate the PPP session. They set up protocols and allocate network addresses for communications with hosts in the corporate network.

In voluntary tunneling, the client implementation is more complex, but it offers more flexibility in enabling multiple access. It also eliminates the need to establish secure tunnels with ISPs and corporate office gateways.

Refer to Chapter 2, "Introduction to Layer 2 Tunneling Protocol (L2TP)" on page 33, for general information on L2TP voluntary tunnel.

7.1 Branch office to main office connection using L2TP voluntary tunnel

This chapter presents a branch office AS/400 system (AS25b) connected to the corporate office network through a gateway AS/400 system (AS05) in an L2TP tunnel protected by IPsec. Figure 282 shows an overview of the network presented in this chapter.

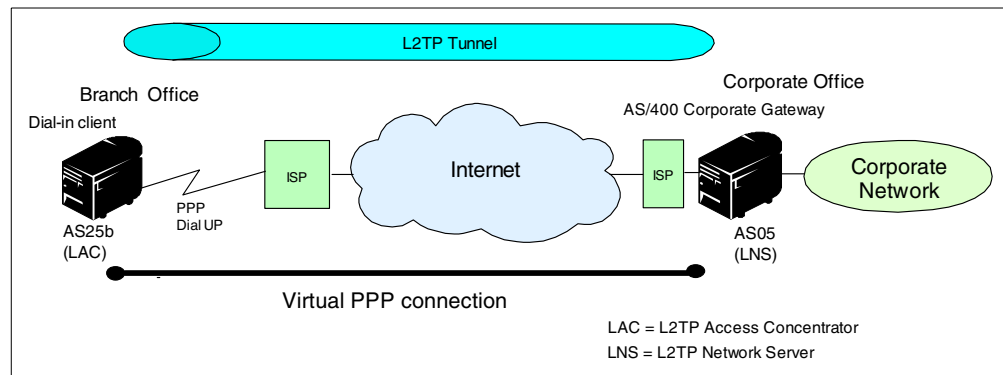


Figure 282. Host-to-corporate network connection - L2TP voluntary tunnel network overview

Important Note

All the scenarios in this redbook show the AS/400 security gateway at the corporate office directly connected to the Internet. The absence of a firewall in these redbook scenarios is meant to simplify the VPN examples. It does *not* imply that the use of a firewall is not necessary. For information about how the AS/400 security gateway interacts with a firewall, refer to Chapter 12, “Don’t forget a firewall: Protecting your VPN server” on page 515.

7.1.1 Scenario characteristics

The main characteristics of this scenario are:

- The AS/400 system at the branch office (AS25b) is the initiator of the connection.
- The AS/400 system at the remote branch office (AS25b) is the only system at the branch office network that needs access to the corporate network. In other words, its role is that of a host, not a gateway, for the branch office network.
- The AS/400 system at the corporate office (AS05) is the gateway into the corporate office network.
- The AS/400 system at the branch office connects to the corporate office through the Internet backbone by dialing up an ISP using a dial-up PPP connection. The ISP randomly assigns a globally routable IP address to the dial-in client (AS25b).
- The client AS/400 system at the branch office (AS25b) supports L2TP. Therefore, there is no need for the ISP to provide LAC support.

7.1.2 Scenario objectives

The objectives of this scenario are:

- The AS/400 system at the branch office (AS25b) must be able to access TCP/IP applications in all systems in the corporate network and vice versa.
- The AS/400 system at the branch office (AS25b) must be regarded as a system in the corporate office network. To achieve this objective, the LNS (AS05) assigns to AS25b an IP address in the corporate office address space from a pool of addresses.
- There are no requirements for the ISP to provide LAC services. Therefore, the dial-in client (AS25b) must be configured to provide L2TP support.
- There is no requirement for hosts in the corporate network to support IPsec (other than the corporate gateway AS05).
- The L2TP tunnel between the branch office AS/400 system (AS25b) and the LNS (AS05) must be protected with IPsec ESP encryption and authentication. The IPsec tunnel must be established before the L2TP tunnel. To achieve this objective, and since the IP address assigned to AS25b by the ISP is unknown, configure a gateway-to-dynamic IP users on the LNS (AS05). Configure an L2TP connection on the remote client (AS25b).

7.1.3 Scenario network configuration

Figure 283 shows the test network used in this scenario.

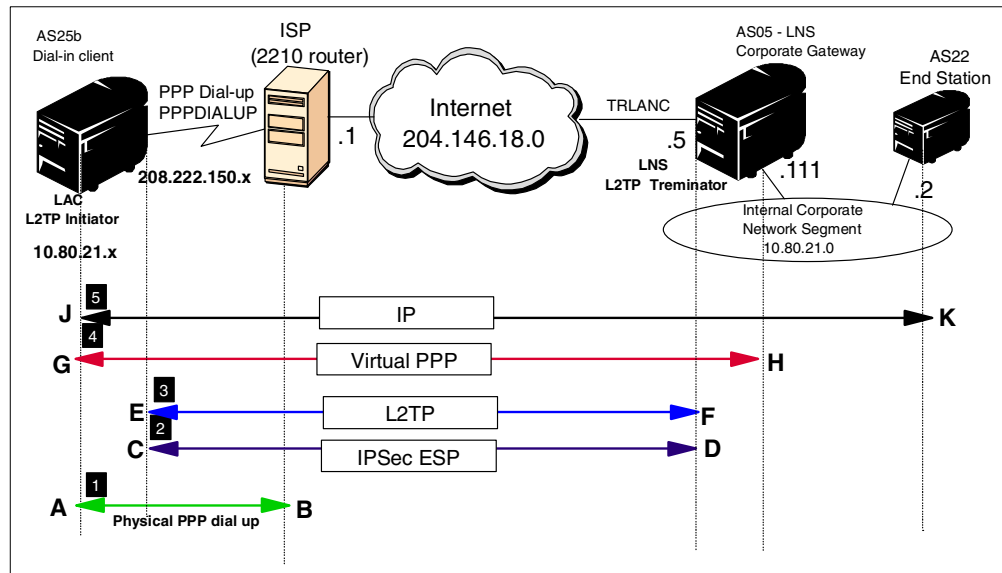


Figure 283. L2TP voluntary tunnel with IPsec test network

The timeline of events that takes place to establish an L2TP voluntary tunnel protected by IPsec is as follows (refer to Figure 283):

- 1 The PPP client (AS25b) dials the ISP and establishes a PPP dial-up session (A-B) between the dial-in client and the ISP. The ISP randomly assigns a globally routable IP address to the client. In our test scenario, the IP address is one in the address pool 208.222.150.x.
- 2 The client (AS25b) initiates the IPsec tunnel to the responder corporate office gateway (AS05). The key server identifiers are the fixed globally routable IP addresses at the LNS (D) and a key identifier at the remote client (C).
- 3 The client (AS25b) establishes an L2TP tunnel with the corporate office gateway (AS05) by using the globally routable IP address assigned to it by the ISP (E-F).
- 4 Once the L2TP tunnel has been established, the client (AS25b) and the corporate office gateway (AS05) negotiate the virtual PPP connection (G-H). The LNS assigns the client an IP address in the corporate office address space (10.80.21.x).
- 5 IP traffic flows between AS25b (J) and any system in the corporate network, for example AS22 (K). Since AS25b has an IP address in the corporate office address space (10.80.21.x), the AS05 interface 10.80.21.111 performs proxy ARP for packets destined for AS25b. Interface 10.80.21.111 is the associated local interface for 10.80.21.x.

7.1.4 Implementation tasks: Summary

You need to perform the following summary of tasks to implement this L2TP voluntary tunnel protected by IPsec in this scenario:

1. LNS configuration (AS05)
 - a. Configure the IPsec ESP tunnel that protects the L2TP tunnel to the client (Host to Dynamic IP Users).
 - b. Configure the L2TP terminator profile.
 - c. Configure the IP filters.
2. L2TP initiator client (AS25b)
 - a. Configure a PPP dial-up connection to the ISP.
 - b. Configure the IPsec ESP tunnel that protects the L2TP tunnel to the LNS (L2TP connection).
 - c. Configure the IP filters.
 - d. Configure the L2TP initiator profile.
3. Start connections
4. Verify communications

7.2 Configuring the LNS in a voluntary tunnel protected by IPsec (AS05)

The following sections take you step-by-step through the configuration of the VPN, L2TP network server (terminator profile), and filters in AS05.

7.2.1 Configuring IPsec tunnel to the client: Host to Dynamic IP Users

To protect the L2TP tunnel between the LNS and the client, configure a VPN. This is the IPsec ESP tunnel at the terminator end (AS05) shown as **D** in Figure 283 on page 265. This VPN has the following characteristics:

- Protocol must be ESP with both authentication and encryption. It is important to authenticate the client and hide the data exchanged between the client and the corporate network.
- The VPN configuration is Host to Dynamic IP Users. The ISP randomly assigns global IP addresses to the client. For that reason, we selected a Host to Dynamic IP Users configuration. Keep in mind that this VPN protects the L2TP tunnel only. That is the reason why the LNS is a *host* and not a gateway from this VPN tunnel perspective.
- The local key server identifier for the corporate gateway is the global IP address, 204.148.18.5 (**D**).
- The remote key server identifier (client) is a key identifier known by both key servers.
- The filters must be applied to the physical LAN interface (TRLANC).

Table 27 summarizes the configuration values you must enter at the VPN configuration wizard.

Table 27. AS05 New Connection Wizard planning worksheet - Host to Dynamic IP Users to ISP

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Gateway to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Dynamic IP User
What will you name the connection group?	AS25btoAS05
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest security, lowest performance
How will you identify your local server?	IP address
What is the IP address of your local server?	204.146.18.5
How will you identify the remote server to which you are connecting?	Key identifier
What is the identifier of the remote server?	AS25b
What is the pre-shared key?	4208182
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balance security and performance

7.2.1.1 Using the wizard to configure a Host to Dynamic IP Users VPN

To configure a Host to Dynamic IP Users VPN with the wizard, perform the following steps:

1. At the Virtual Private Networking window, select **File->New Connection**.
2. Select **Host to Dynamic IP Users** from the pull-down menu. This starts the New connection Wizard as shown in Figure 284 on page 268.

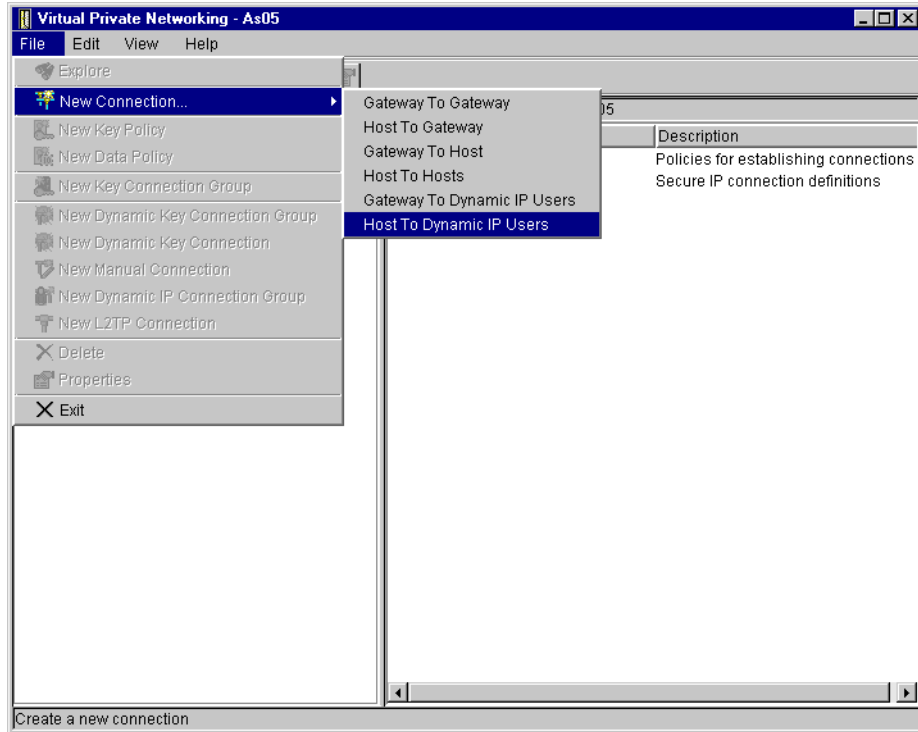


Figure 284. AS05 New Connection -> Host to Dynamic IP Users

3. Click **Next** after reading the welcome window as shown in Figure 285.

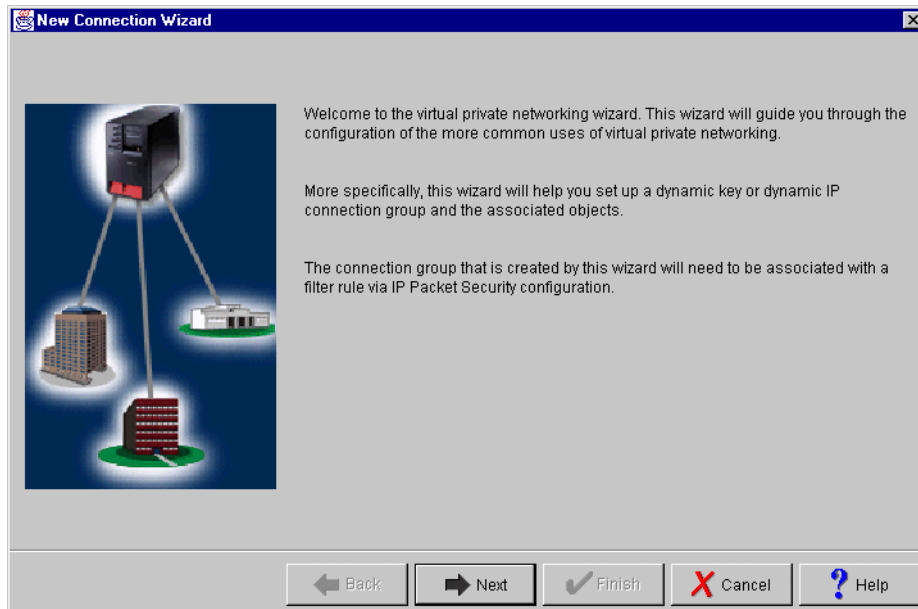


Figure 285. AS05 New Connection Wizard welcome window

4. Enter the name, AS25btoAS05, for the connection group and enter a description, L2TP from AS25b to AS05 (DynamicIP), as shown in Figure 286 on page 269.

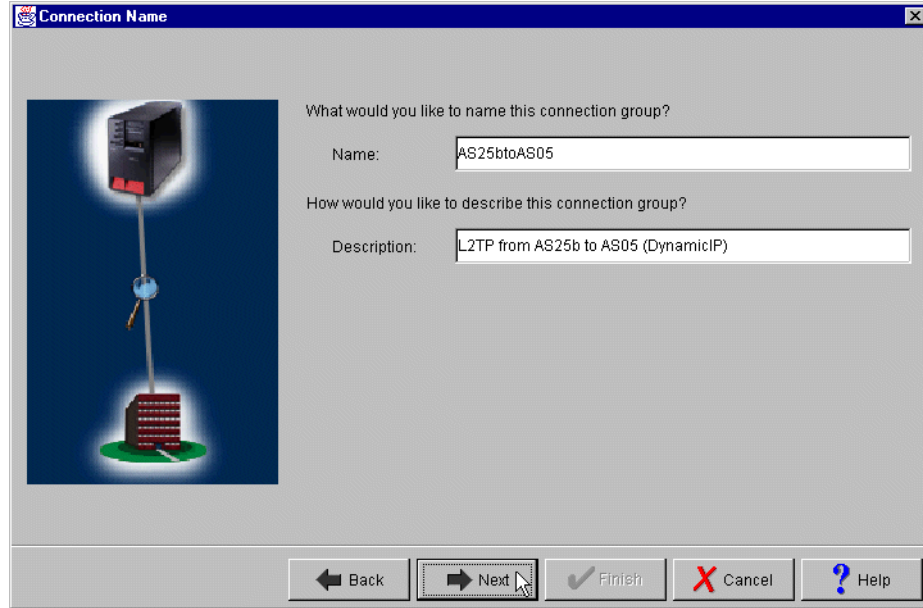


Figure 286. AS05 Connection name and description window

5. Click **Next**.
6. On the Key Policy window (Figure 287), specify the level of authentication or encryption protection that IKE uses during Phase 1 negotiations. Select **Highest Security, Lowest performance** for this VPN. The wizard selects SHA as the hash algorithm and 3-DES (if 5769-AC3 is installed) or DES (if 5769-AC2 is installed) as the encryption algorithm for this option.



Figure 287. AS05 Key Policy window

7. Click **Next**.
8. On the Local identifier window (Figure 288 on page 270), specify the identity of the local key server. This is the globally routable IP address of the corporate

gateway (AS05). Leave Identifier type as the default value, **Version 4 IP address**. For the IP address, use the pull-down list to select the IP address for the interface, **204.146.18.5**. Refer to Figure 283 on page 265 and to the planning worksheet Table 27 on page 267. This is the key server IP address which is shown as **(D)** in Figure 283 on page 265.

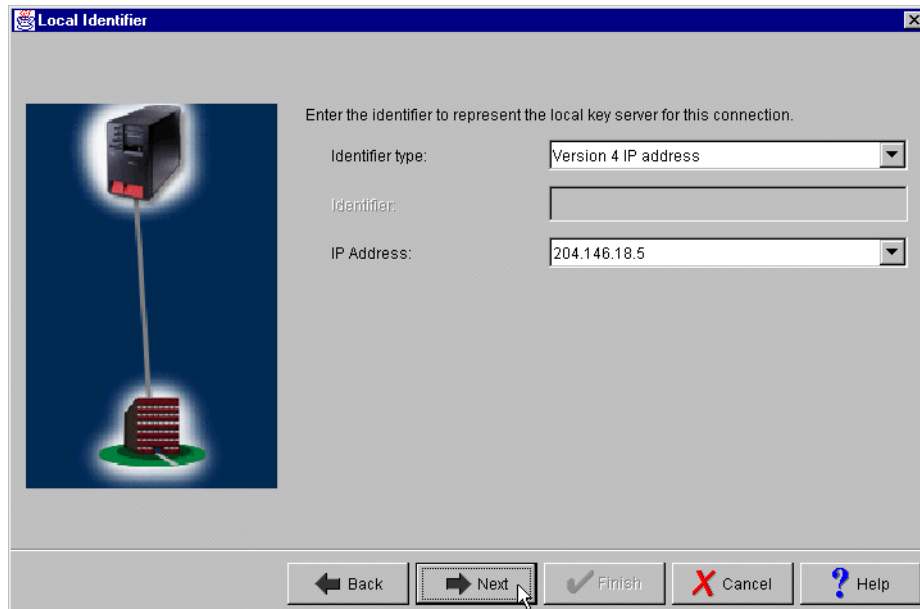


Figure 288. AS05 Local key server identifier window

9. Click **Next**.
10. Enter the client identifier in the Users window. Leave the default value in the identifier type, **Key identifier** (Figure 289 on page 271).
11. Click **Add**.
12. Enter `AS25b` as the Identifier.
13. Press the **Tab** key, and enter `4208182` as the value for the Pre-shared key. Refer to Figure 289 on page 271.



Figure 289. AS05 Remote user identification

14. Click **Next**.

15. On the Data Policy window (Figure 290), specify the level of authentication or encryption protection that IKE uses during phase 2. Select **Balance Security and Performance** for this VPN. The wizard selects the authentication algorithm HMAC-MD5 and the encryption algorithm DES for this option.

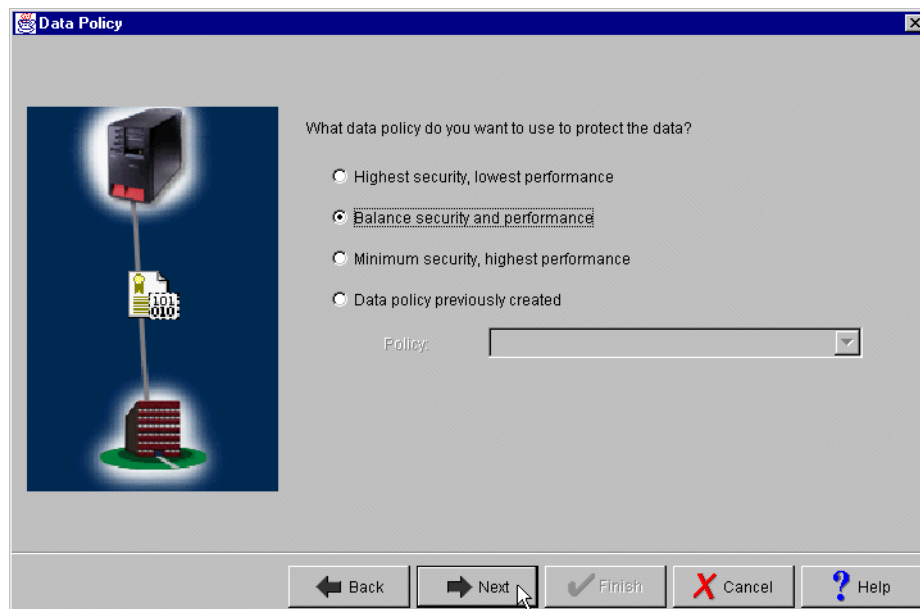


Figure 290. AS05 Data Policy window

16. Click **Next**.

17. The final window summarizes the configuration values that you entered as shown in Figure 291 on page 272. If you scroll down, you can also see a list of the configuration objects that the wizard creates when you click Finish. Check

the configuration values against your worksheet (Table 27 on page 267). If you need to make changes, click **Back**.

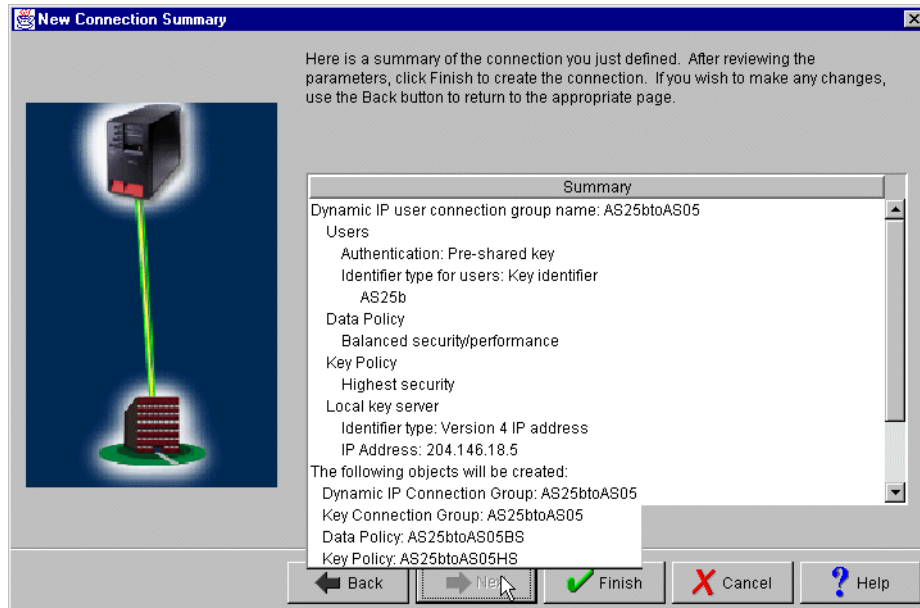


Figure 291. AS05 New Connection Summary window

18. Click **Finish**.

7.2.1.2 Modifying the policy values for active connections (AS05)

You can modify the values that define the traffic for active connections by performing the following steps:

1. At Virtual Private Networking window, expand **Secure Connections->Data Connections**.
2. Click **Dynamic IP Groups**.
3. On the right panel, double-click **AS25btoAS05** to open its properties (Figure 292).

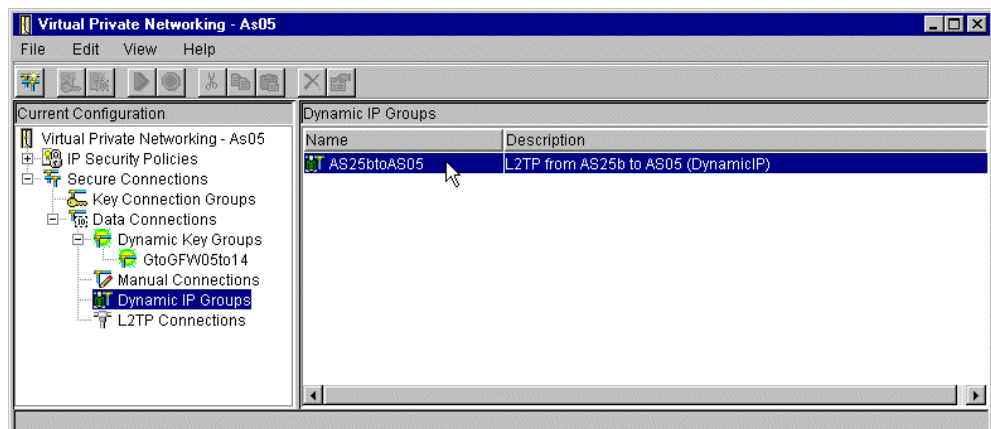


Figure 292. AS05 Opening the Dynamic IP Group

4. Click the **Policy** tab.

- Change Local addresses, Local ports, Remote addresses, Remote ports, and Protocol parameters to **Connection** by using the pull-down menu on each field. Refer to Figure 293. As you configure the responder end of the connection (D in Figure 283 on page 265), changing the value to Connection in this page means that the responder (AS05) will accept the values proposed by the initiator (AS25b) as long as the values are within the limits set by the IPsec rules. Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for more information.

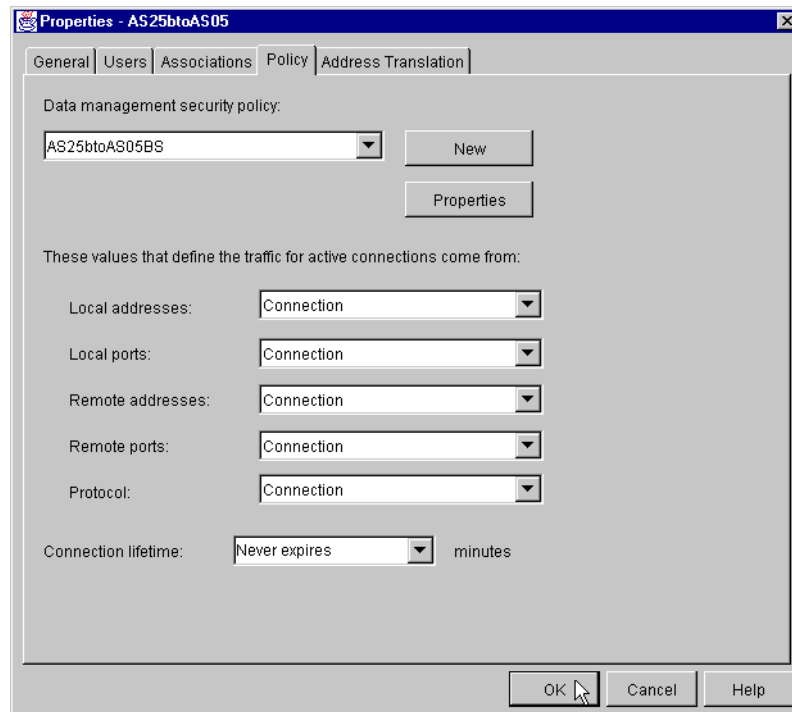


Figure 293. AS05 Policy connection values

- Click **OK**.

7.2.2 Configuring the L2TP terminator profile (AS05)

This section explains how to configure the LNS end of the L2TP tunnel. This is represented by F in Figure 283 on page 265.

Table 28 provides an overview of the most important parameters in the PPP connection profile that you must consider when configuring the L2TP terminator in a voluntary tunnel. Refer to Figure 283 on page 265 for the scenario values.

Table 28. AS05 L2TP terminator profile - Parameter summary

PPP configuration parameter	Scenario value	Comment
Name	AS25bTERM	Virtual PPP terminator profile
Line connection type	Virtual line (L2TP)	Physical line is Token Ring LAN (TRLANC)
Mode type	Terminator (network server)	AS05 is LNS

PPP configuration parameter	Scenario value	Comment
Local tunnel endpoint IP address	204.146.18.5	Local L2TP tunnel endpoint is the globally known IP address.
Local IP address	10.80.21.111 (Token Ring)	Interface on the internal network. This interface performs an proxy ARP on behalf of the PPP client in the voluntary tunnel. It is the associated local interface associated with the IP address assigned to the remote PPP client (AS25).
Remote IP address Defined address pool: Number of addresses	10.80.21.115 10	Pool of IP addresses to be assigned to remote PPP clients that are <i>not</i> in the Caller User list.
Routing	Dynamic routing: None Static routing: None	No special routing configuration in the PPP connection profile.
Allow IP forwarding	Allow (check box)	Allow to route traffic from or to the remote PPP client and the internal network.

Perform the following steps to create the virtual PPP connection on the L2TP terminator, AS05 for a voluntary L2TP tunnel:

1. From Operations Navigator, expand the **AS05** AS/400 system.
2. Click **Network->Point-to-Point**.
3. Right-click **Connection profiles**, and select **New Profile** from the menu (Figure 294).

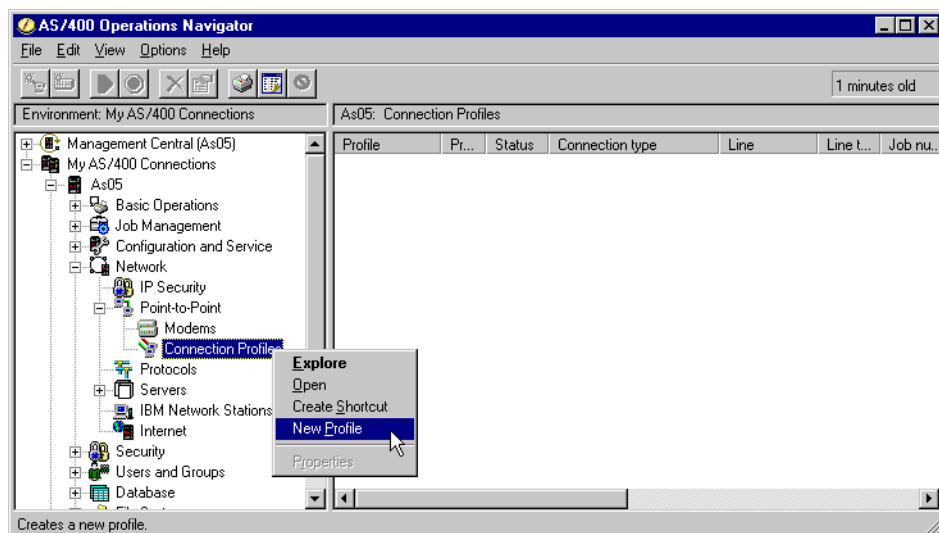


Figure 294. AS05 Creating a virtual PPP connection on the L2TP terminator

Ensure the General tab is selected since the settings on this page affect the rest of the pages.

4. Enter `AS25bTERM` as the Name of the virtual PPP profile.

5. Enter **L2TP AS25b (initiator) to AS05 (terminator) link** or similar for Description.
6. Select **PPP** as the Type of connection.
7. Select **Virtual line (L2TP)** for the Mode parameter.
8. Select **Terminator (network server)** for the Mode - Line connection type parameter (Figure 295).

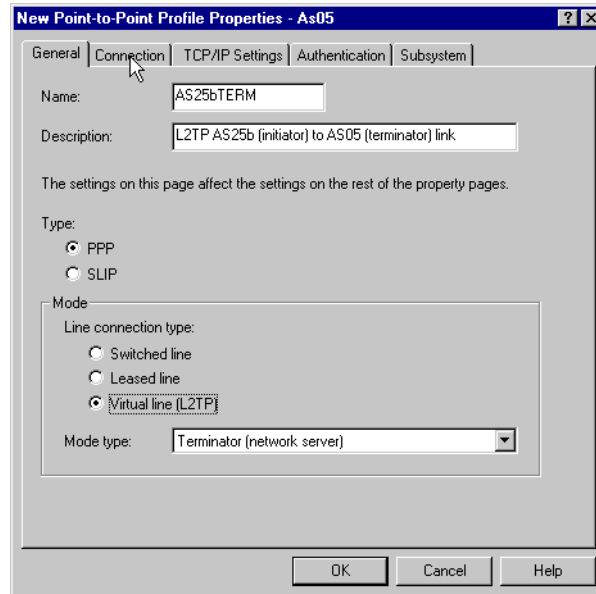


Figure 295. AS05 Creating the virtual PPP line

9. Click the **Connection** tab.
10. For the Local tunnel endpoint IP address, select **204.146.18.5** from the pull-down menu.
11. Enter **AS25bL2TP** for the Virtual line name parameter.
12. Click **New**. Refer to Figure 296 on page 276.

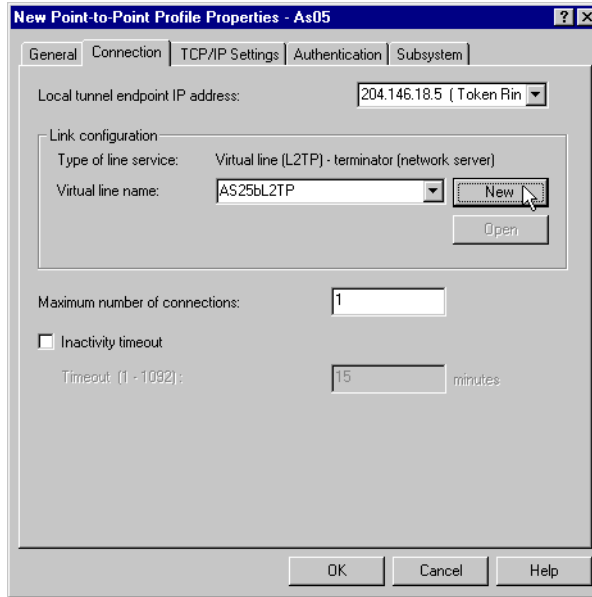


Figure 296. AS05 Defining the virtual PPP connection parameters

13. Enter AS25b to AS05 L2TP connection or similar as the Description (Figure 297).

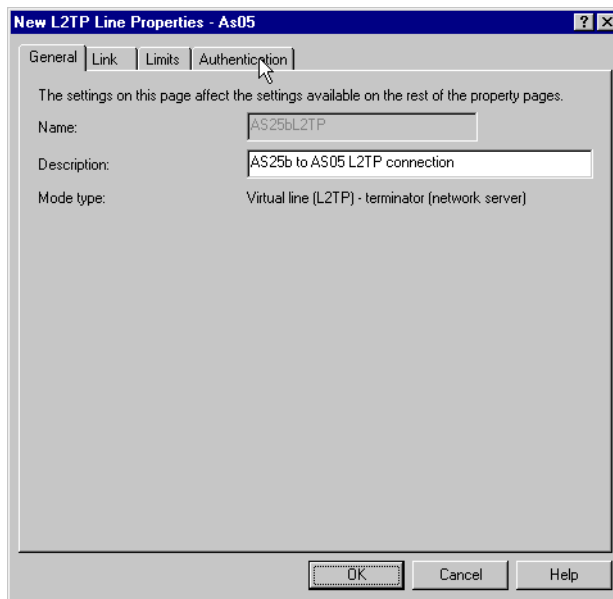


Figure 297. AS05 Entering the virtual PPP description

14. Click the **Authentication** tab.

15. Enter AS05 as the **Local host name** (Figure 298 on page 277).

Note: We chose not to require authentication in our test environment. However, as an additional level of security, PPP authentication, is recommended.

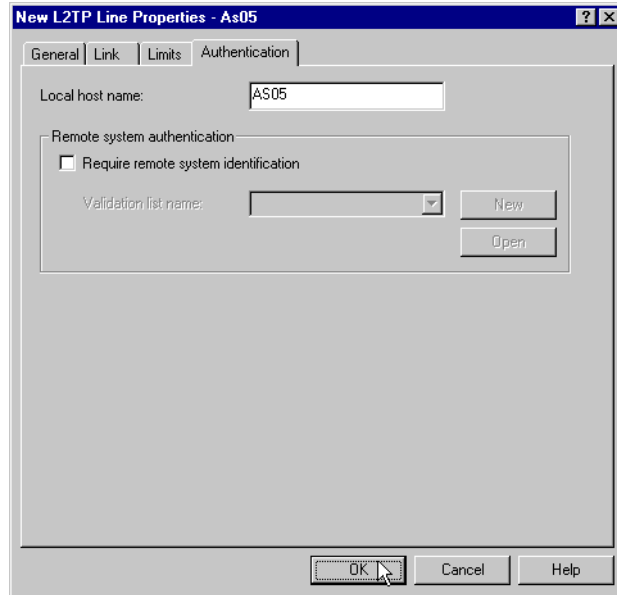


Figure 298. AS05 Virtual PPP authentication page

16. Click **OK**.
17. Select the **TCP/IP Settings** tab.
18. For the Local IP address parameter, ensure **IP address** is selected, and select **10.80.21.111** from the pull-down menu (**H** in Figure 283 on page 265).
19. For the Remote IP address parameter, select **Define address pool**.
20. Enter 10.80.21.115 as the Starting IP address (**G** in Figure 283 on page 265).
21. Enter 10 for the number of addresses to give from this pool. This value depends on the number of remote clients.
22. Click **Allow IP forwarding** to select this function. IP forwarding must be enabled for the corporate gateway to forward traffic between the remote client and the corporate network. Refer to Figure 299 on page 278.

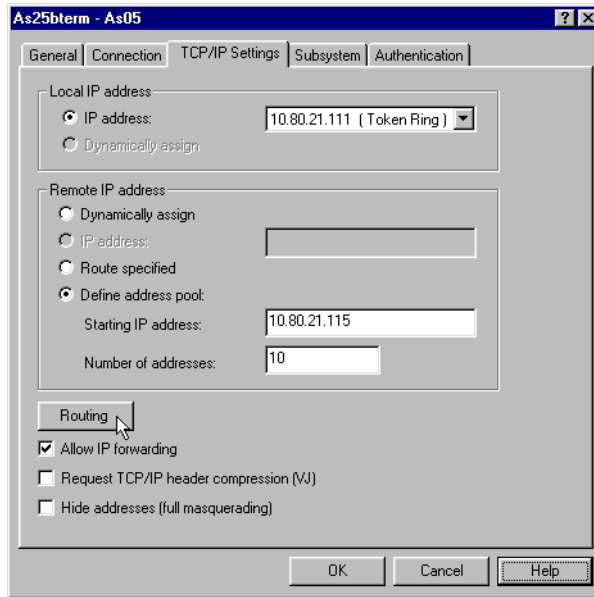


Figure 299. AS05 TCP/IP settings on the virtual PPP link

23. Click the **Routing** button.

24. Leave Dynamic routing (RouteD) and Static routing set to **None** (Figure 300).

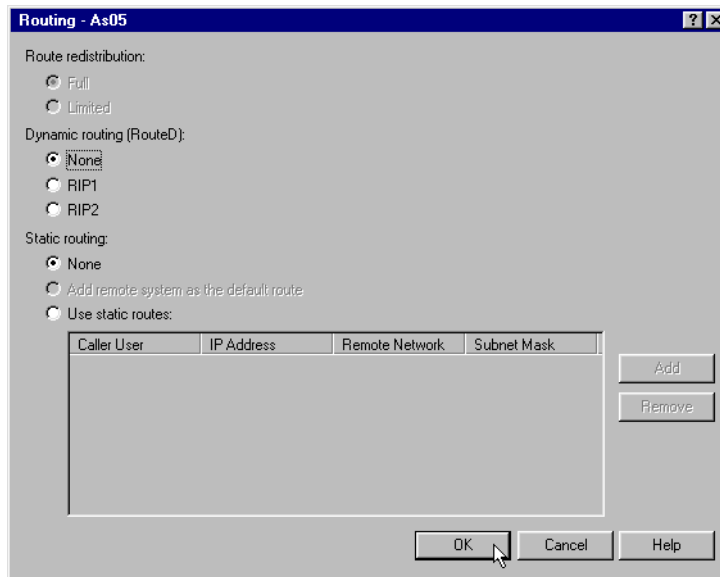


Figure 300. AS05 Routing configuration

Note

There is no need to define a static route on this link since AS05 will perform the proxy ARP functions for AS25b.

25. Click **OK**.

26. Click **OK** again. It is not necessary to modify the settings on the Subsystem and Authentication pages.

Next, configure the IP packet filtering rules as described in the following section.

7.2.3 Configuring IP filters in the LNS AS/400 system (AS05)

As usual, you must configure filters to complete the VPN configuration. To implement this scenario, four filter rules are required:

- Two filter rules to allow IKE negotiations.
- One IPSEC filter rule associated with the connection created in 7.2.1, “Configuring IPSEC tunnel to the client: Host to Dynamic IP Users” on page 266. Notice that, in this scenario, the IPSEC tunnel encapsulates the L2TP tunnel as shown in Figure 283 on page 265. Therefore, you can restrict the services to protocol UDP, with source and destination port 1701 in the IPSEC filter rule.
- One filter interface associated with the filter rules. This is the physical LAN line TRLANC in this scenario.

Note

The filter rules presented throughout this redbook are *limited* to those required to enable the services in the proposed scenario. If you want to enable other services beyond those in the scenario, you need to configure additional rules. Exercise extreme caution when doing so and always take security into account.

Table 29 summarizes the configuration values to create the IP filters associated with the IPSEC tunnel to the client.

Table 29. AS05 Planning worksheet - IP filter rules

This is the information you need to create your IP filters to support VPN	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.	Host
Is the <i>remote</i> VPN server acting as a host or gateway ?	Host
What name do you want to use to group together the set of filters that will be created?	L2TPSet
If <i>your</i> server is acting as a gateway ... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	

This is the information you need to create your IP filters to support VPN	Scenario answers
If the <i>remote</i> server is acting as a gateway ... <ul style="list-style-type: none"> – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter. 	
What is the IP address of <i>your</i> VPN server? <ul style="list-style-type: none"> – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host. 	204.146.8.5
What is the IP address of the remote VPN server? <ul style="list-style-type: none"> – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host. 	Dynamic IP (*)
What is the name of the interface (for example, the Token-Ring, Ethernet, or PPP connection profile) to which these filters will be applied?	TRLANC
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

Using the values in the planning worksheet, create the following filters:

1. Start the Operations Navigator.
2. Select the system **AS05**, and sign on as required.
3. Expand **Network**.
4. Click **IP Security**.
5. In the right-hand window, right-click on **IP Packet Security**, and select **Configuration**. See Figure 301 on page 281.

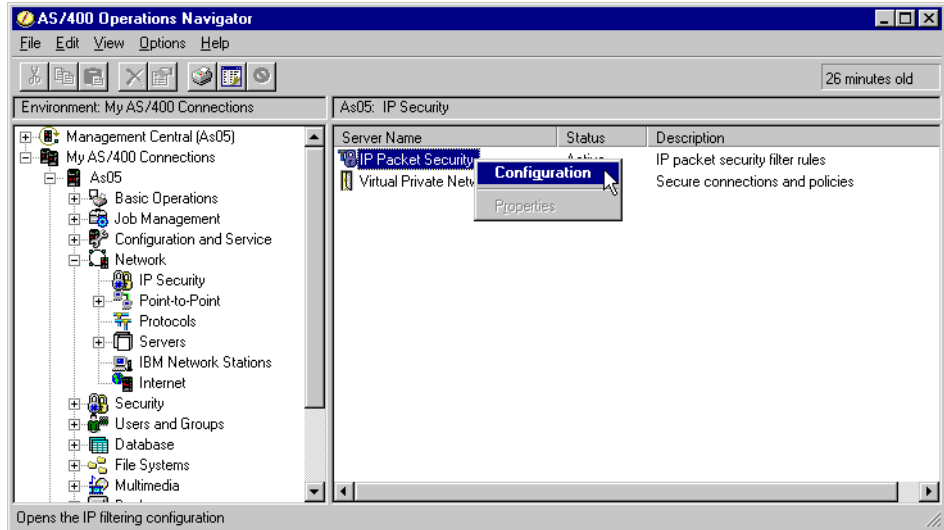


Figure 301. AS05 Starting the IP packet security configuration

6. Right-click on **Filters->New Filter** (Figure 302).

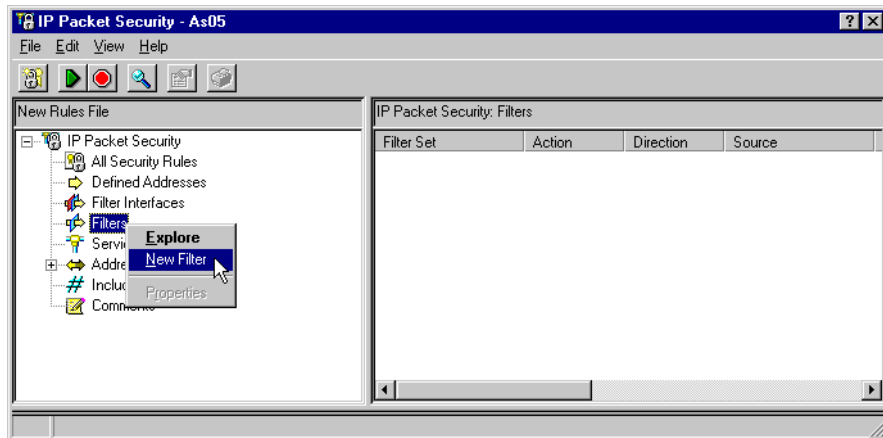


Figure 302. AS05 Creating a new IP packet filter rule

- Configure the outbound IKE filter rule to permit IKE negotiations (Figure 303 on page 282). The following values apply:
 - Source address name:** Local key server IP address (204.146.18.5).
 - Destination address:** Wildcard. Remote key server IP address is dynamic (randomly assigned by the ISP).

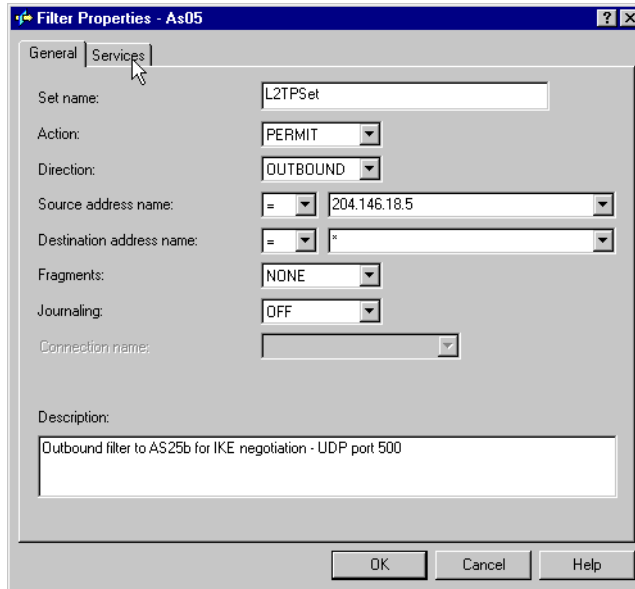


Figure 303. AS05 Outbound IKE filter rule

8. Click the **Services** tab.
9. IKE negotiations use protocol UDP, with source and destination port 500. Enter the values as shown in Figure 304.

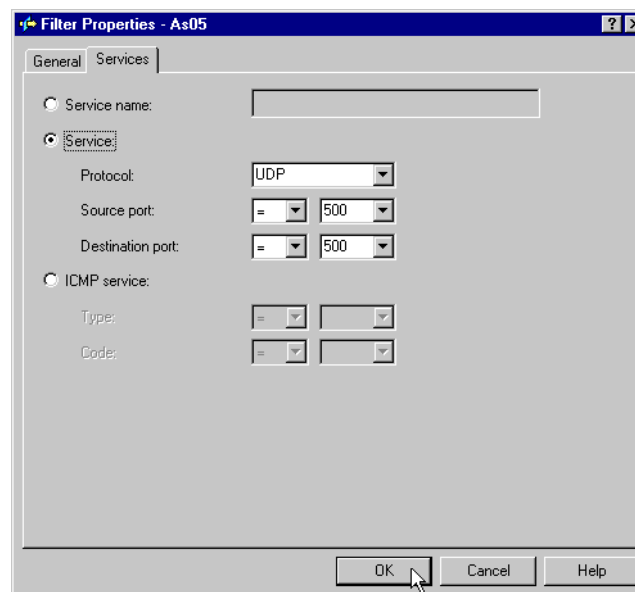


Figure 304. AS05 Outbound IKE filter rule - Services configuration

10. Click **OK** to add the filter rule.
11. Repeat the previous four steps for the *inbound* filter rule. Remember to reverse the Source and Destination address names. Complete the Services window as you did for the outbound rule as shown in Figure 305 and Figure 306 on page 283.

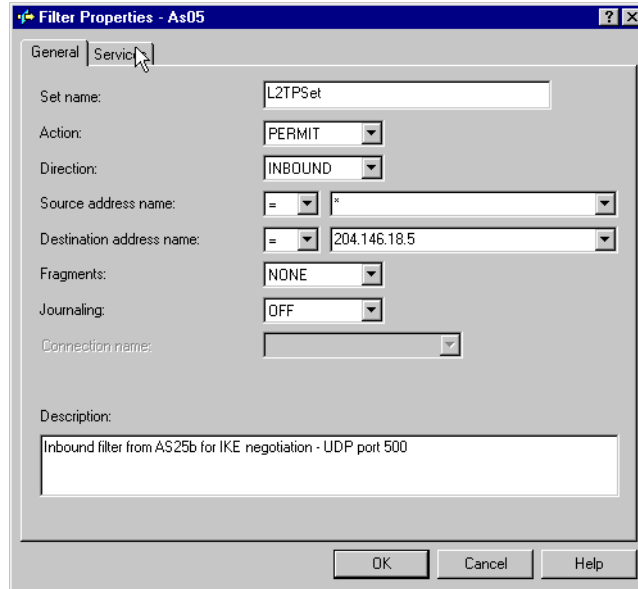


Figure 305. AS05 Inbound IKE filter rule

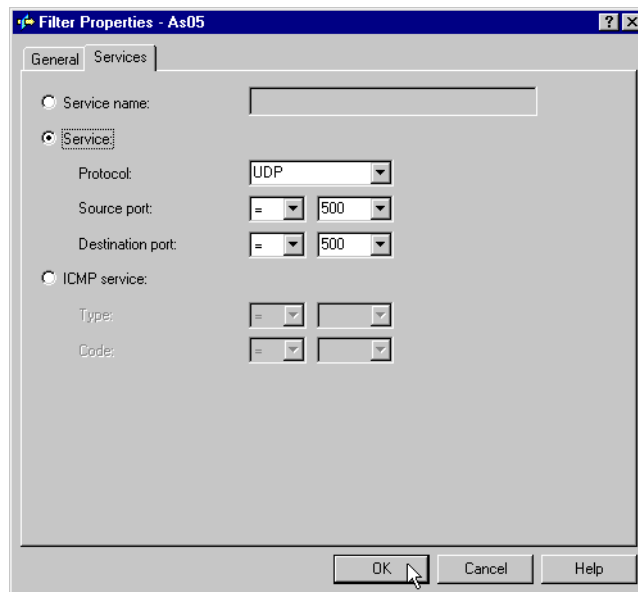


Figure 306. AS05 Inbound IKE filter rule - Services configuration

12. Click **OK** to add the second rule.
13. Configure the IPSEC filter rule that allows data traffic to use the VPN tunnel . Use the same filter Set name, L2TPSet, but specify IPSEC in the Action field. With an IPSEC filter rule, Direction is always set to OUTBOUND and grayed out. In the Source and Destination address name fields, enter the globally routable IP address of AS05, 204.146.18.5, and a wildcard (*) for the destination address as shown in Figure 307 on page 284. Since the Destination is not identified by a fixed IP address, select **DYNAMICIP** for the Connection name field. Refer to Figure 307.

Note

The source and destination IP addresses in the IPSEC filter rule define the data endpoints of the IPsec tunnel. Notice that in this scenario, data flows between AS25b (10.80.21.115, **J** in Figure 283 on page 265) and the corporate network (10.80.21.0, **K** in Figure 283 on page 265). The IPsec tunnel in this scenario protects the L2TP tunnel and ends at 204.146.18.5 on TRLANC (**D** in Figure 283 on page 265). Through proxy ARP, traffic that is destined for AS25b is routed from the corporate network by AS05. AS05 replies to ARP requests on behalf of AS25b and routes the data straight to AS25b through the virtual PPP connection. Likewise, the routing configuration on AS25b directs the traffic destined for the corporate network (10.80.21.0) through the L2TP tunnel.

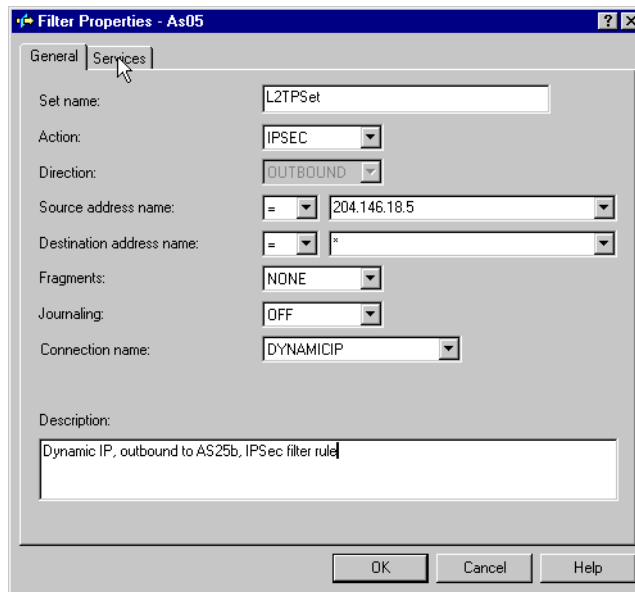


Figure 307. AS05 IPSEC filter rule

14. Click the **Services** tab.

15. Enter `UDP` in the Protocol field. Enter `1701` for the Source port field. Enter `1701` in the Destination port fields. This allows only L2TP traffic to use this filter rule and, therefore, the VPN tunnel. See Figure 308 on page 285.

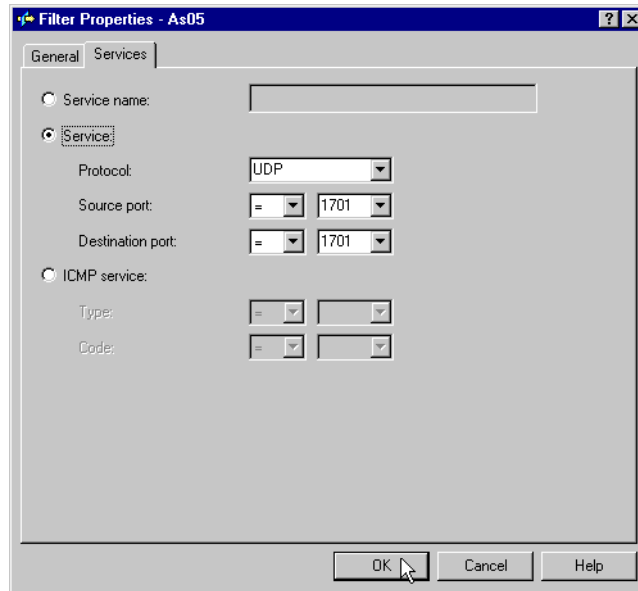


Figure 308. AS05 IPSEC filter rule - Services configuration

16. Click **OK**.

17. The final rule you must create is a Filter Interface rule, which ties the filter rules you just created to the required interface. Right-click on **Filter Interfaces**, and select **New Filter Interface** as shown in Figure 309.

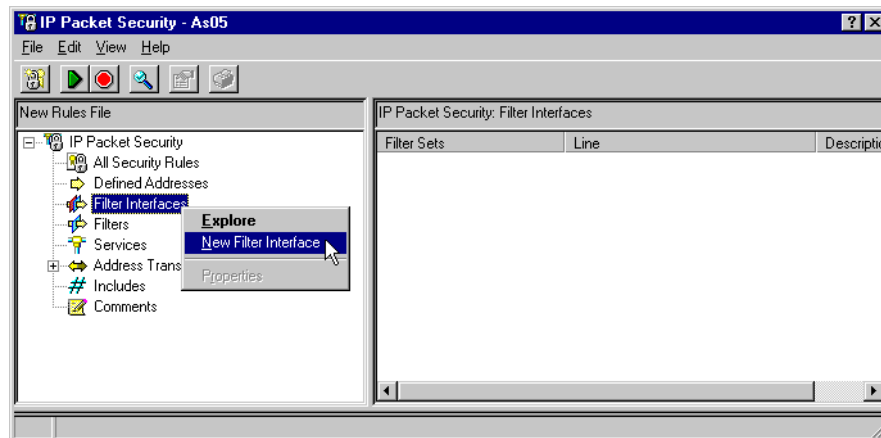


Figure 309. AS05 Defining a filter interface for the IP filter rules

18. Select **Line name** for the Line radio box, and select **TRLANC** from the pull-down menu.

19. Click **Add** to add the filter set name of the filter rules you created previously, which, in this scenario, is **L2TPSet**. See Figure 310 on page 286.

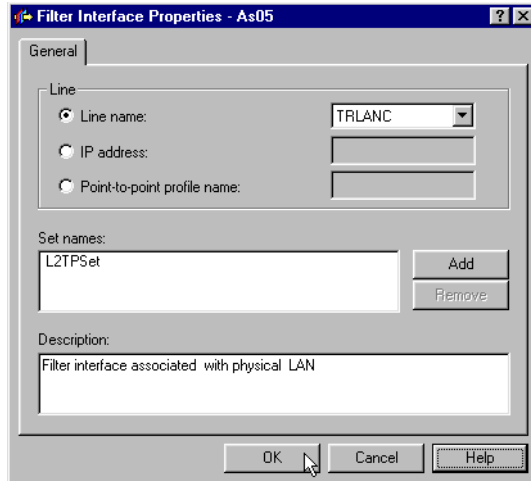


Figure 310. AS05 Filter interface

20. Click **OK** to create the filter interface.
21. Click **File->Save as...**, and name the file `main.i3p`. Ensure that you use the extension `.i3p` since this is the default.
22. Select **File->Activate** to activate the new filter rules.

Figure 311 shows a summary of the filters configured in the LNS (AS05).

```

IP Packet Security: Filter Interfaces
FILTER_INTERFACE LINE = TRLANC SET = L2TPSet
#IKE Rules - IKE negotiation
FILTER SET L2TPSet ACTION = PERMIT DIRECTION = OUTBOUND
SRCADDR = 204.146.18.5 DSTADDR = *
PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET L2TPSet ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = 204.146.18.5
PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC rule - IPsec tunnel encapsulates L2TP tunnel
FILTER SET L2TPSet ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 204.146.18.5
DSTADDR = * PROTOCOL = UDP DSTPORT = 1701 SRCPORT = 1701 FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = DYNAMICIP

```

Figure 311. AS05 Filters summary at the LNS in voluntary tunnel

7.3 Configuring the L2TP client in a voluntary tunnel protected with IPsec

The following sections take you step-by-step through the configuration of the PPP dial-up connection to the ISP, L2TP client (initiator), VPN, and filters in AS25b.

7.3.1 Configuring the PPP dial-up connection to the ISP (AS25b)

The configuration of the PPP dial-up connection on AS25b (**A** and **B** in Figure 283 on page 265) is much like any regular PPP connection.

Table 30 shows the parameters that are relevant to the PPP connection profile to the ISP.

Table 30. AS25b - PPP dial-up connection profile to ISP

PPP configuration parameter	Scenario value	Comment
Profile name	PPPDIALUP	
Line connection type	Switched line	Dial-up to ISP
Mode type	Dial	
Remote phone number	56109	ISP phone number
Type of line service	Analog	
Link name	PPPDIALUP	
Local IP address	Dynamically assigned	This is the IP address randomly assigned by the ISP.
Remote IP address	Dynamically assigned	LNS local IP address
Routing	Add remote system as the default route	Link to the ISP <i>must</i> be default route
Local system identification User name Password	Enable local system identification CHAP only as400 xxxx	Must match authentication required by ISP

Note: The following process does *not* contain the complete list of steps that you need to perform to configure a PPP dial-up connection profile. Log on to: <http://www.as400.ibm.com/infocenter> for a description of how to configure a PPP connection.

- In the General window, ensure that Type is **PPP** and Line connection type is **Switched line**. See Figure 312 on page 288.

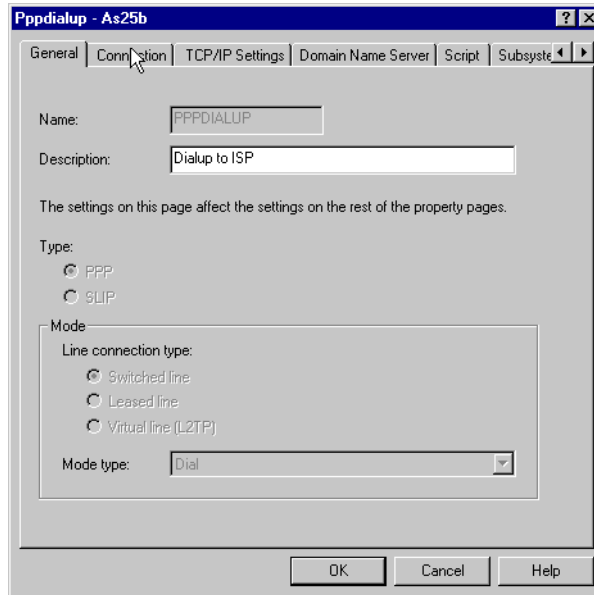


Figure 312. AS25b Physical PPP connection general configuration

- In the Connection window, enter the phone number of your ISP. Create a new link configuration, PPPDIALUP, in our example (Figure 313).

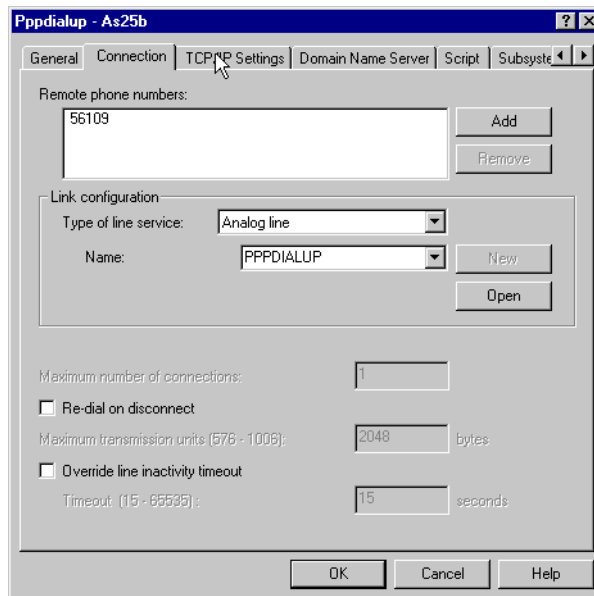


Figure 313. AS25b Physical PPP connection configuration

- In the TCP/IP Settings window, select **Dynamically assign** for both Local and Remote IP addresses (Figure 314 on page 289).

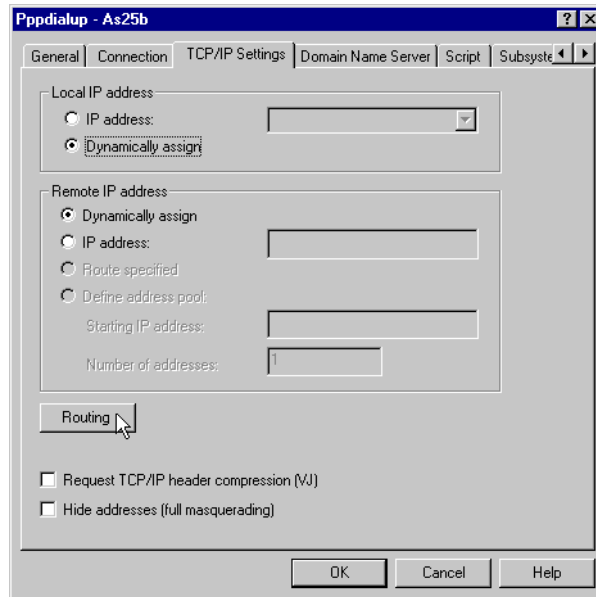


Figure 314. AS25b Physical PPP connection TCP/IP configuration

- Select **Add remote system as the default route** for the Static routing field. This option configures these PPP connections to the ISP as the default route for AS25b (Figure 315).

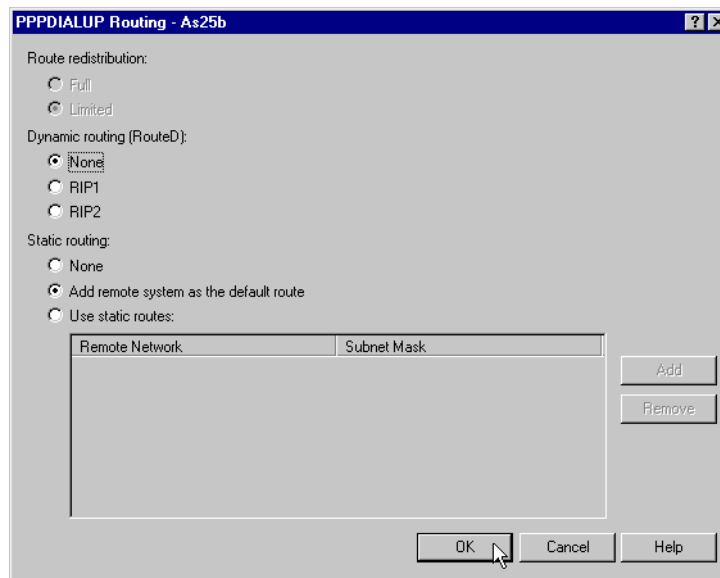


Figure 315. AS25b Physical PPP connection routing configuration

- In the Authentication window, check **Enable local system identification**, and select **CHAP only**. Enter the user name and password that the ISP will use to authenticate the connection (Figure 316 on page 290).

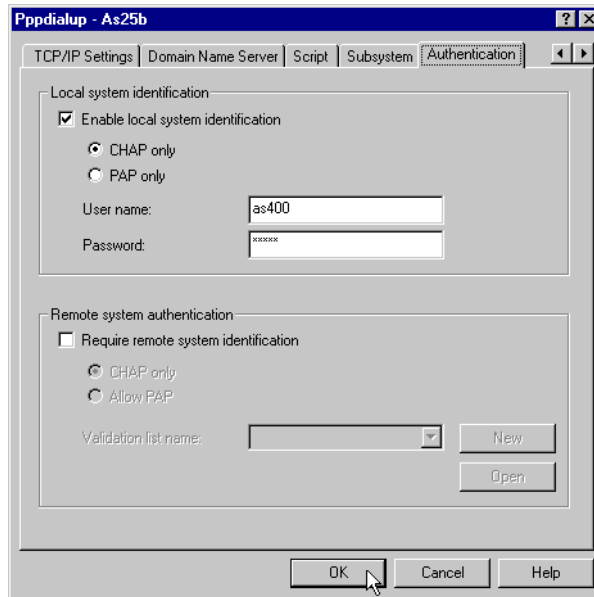


Figure 316. AS25b Physical PPP connection authentication configuration

- Select the hardware resource on your system (Figure 317).

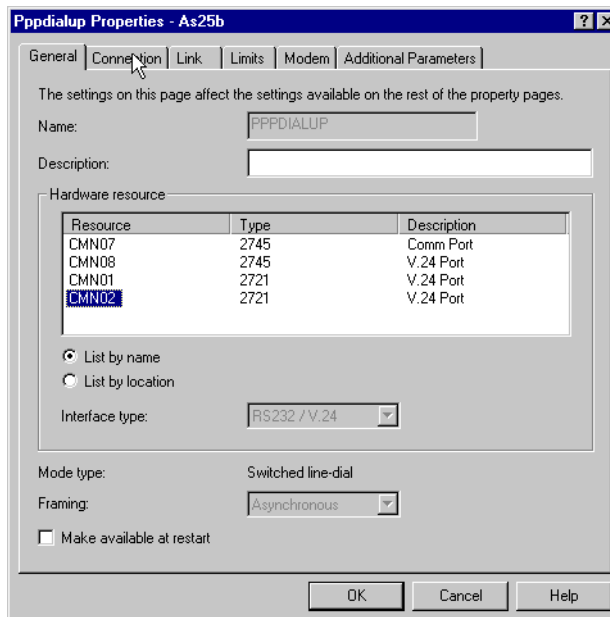


Figure 317. AS25b Physical PPP connection configuration

- Select the correct modem type for your connection (Figure 318 on page 291).

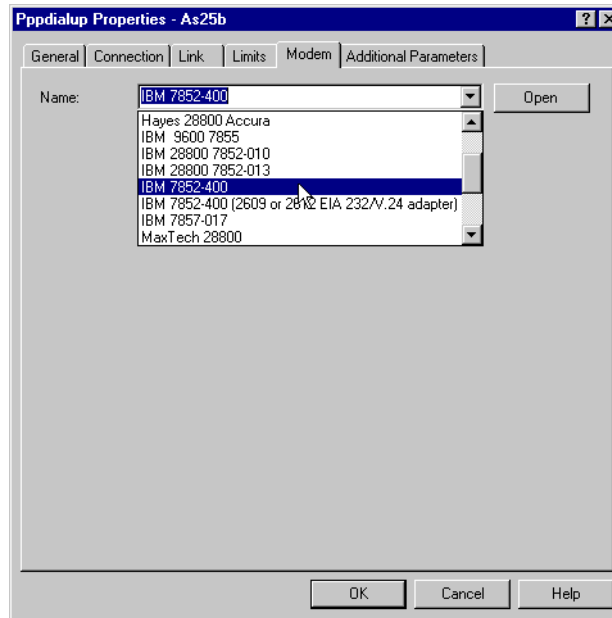


Figure 318. AS25b Physical PPP connection modem selection

7.3.2 Configuring the L2TP VPN connection on the initiator (AS25b)

To protect the L2TP tunnel between the corporate gateway (LNS) and the client, configure a VPN. This is the IPsec ESP tunnel at the client end (AS25b), which is shown as **C** in Figure 283 on page 265. This VPN has the following characteristics:

- The VPN configuration at the client is an L2TP connection. There is no VPN configuration wizard provided for this connection type.
- Protocol must be ESP with both authentication and encryption. It is important to authenticate the client and hide the data exchanged between the client and the corporate network.
- The remote key server identifier for the corporate gateway is the global IP address 204.146.18.5 (**D** in Figure 283 on page 265).
- The local key server identifier (client) is a key identifier.
- The filters must be applied to the physical PPP connection profile (PPPDIALUP).

To configure an L2TP connection on the client (AS25b), perform the following steps:

1. Start Operations Navigator.
2. Select the system **AS25b**, and sign on as required.
3. Expand **Network**.
4. Click **IP Security**.
5. Right-click **Virtual Private Networking**, and select **Configuration** from the menu (Figure 319 on page 292).

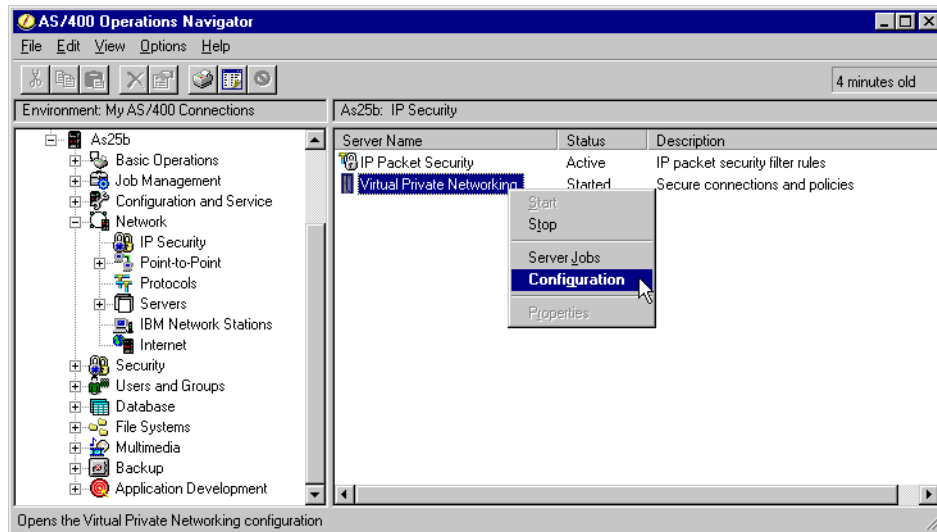


Figure 319. AS25b Starting the VPN configuration

6. From the Virtual Private Networking window, expand **Secure Connection-> Dynamic Key Groups**.
7. Right-click **L2TP Connection**, and select **New L2TP connection** from the pull-down menu (Figure 320).

Tip

Even though you cannot use the wizard to create this connection configuration, selecting **New L2TP connection** leads you through all of the objects you need to create this configuration. In the following steps, we show you how to follow the path.

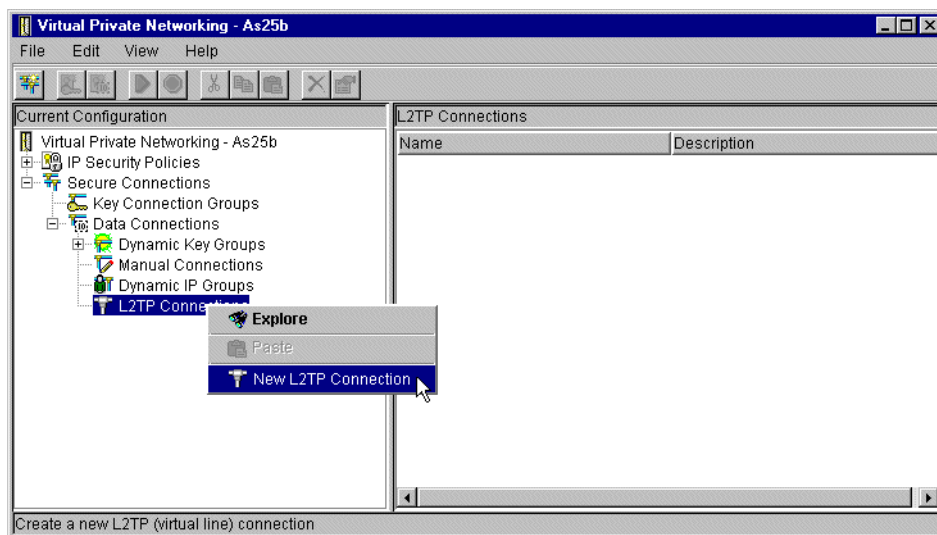


Figure 320. AS25b Creating a new L2TP connection

8. Enter AS25bt.oAS5 as the name of the L2TP profile.

9. Enter AS25b (initiator) to AS05 (terminator) or similar for the Description.
10. At the Remote key server - Key connection group parameter, click **New** to create a new key connection group (Figure 321).

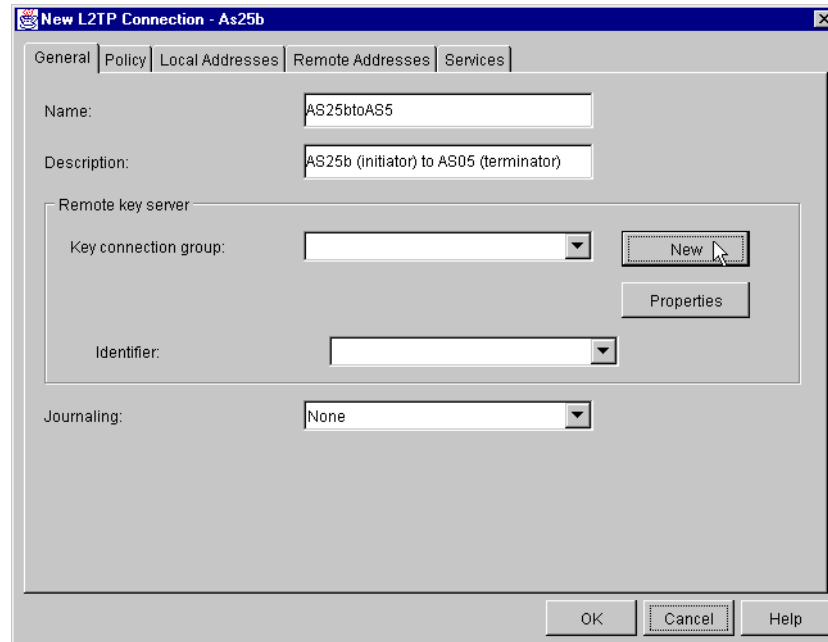


Figure 321. AS25b Defining general definitions for the L2TP initiator

11. At the New Key Connection Group window, enter the name AS25btoAS5 and Description Key connection between AS25b (init) and AS05 (term) or similar.
12. Click **Add** to add the remote server identifier. See Figure 322 on page 294.

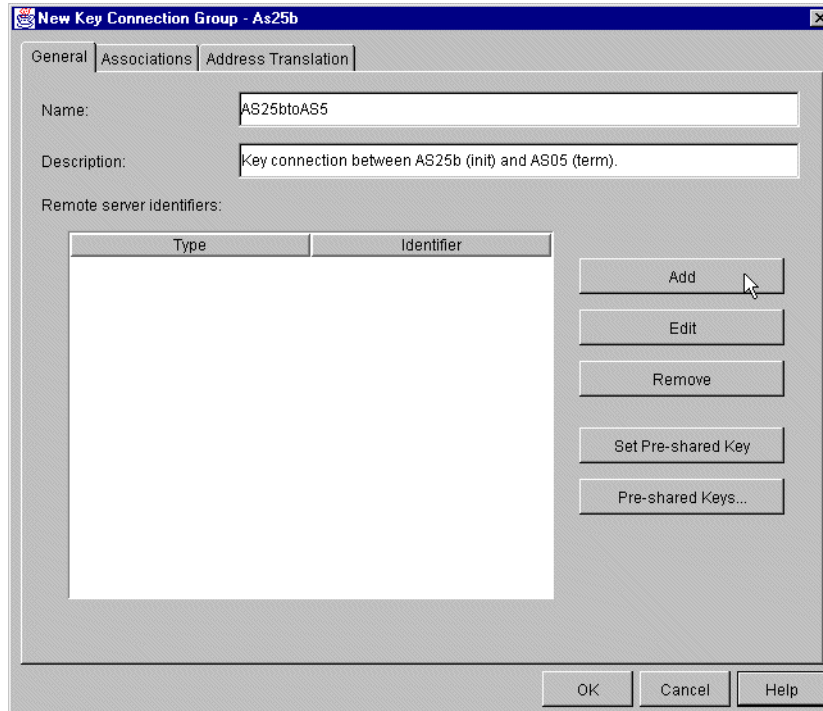


Figure 322. AS25b Configuring a new key connection group

13. Select **Version 4 IP address** from the pull-down menu for the Identifier type.

14. Enter 204.146.18.5 in the IP address field (Figure 323).

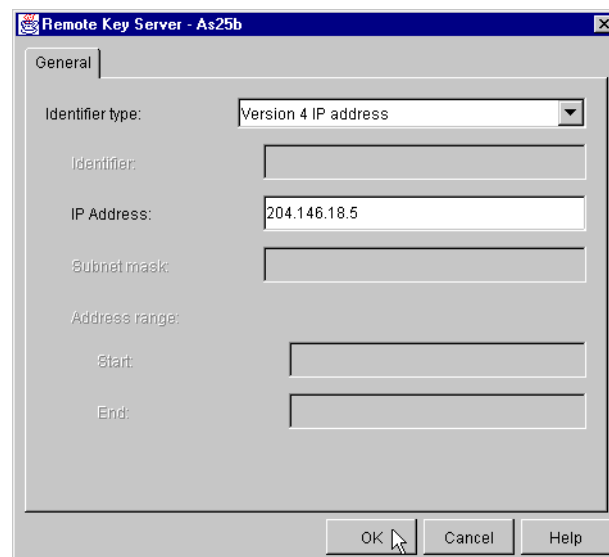


Figure 323. AS25b Configuring the remote key server identifier

15. Click **OK**.

16. Click **Set Pre-shared key**.

17. Enter 4208182 in the Set pre-shared key dialog box. See Figure 324 on page 295.

The pre-shared key must match on both key server (AS05 and AS25b) configurations.

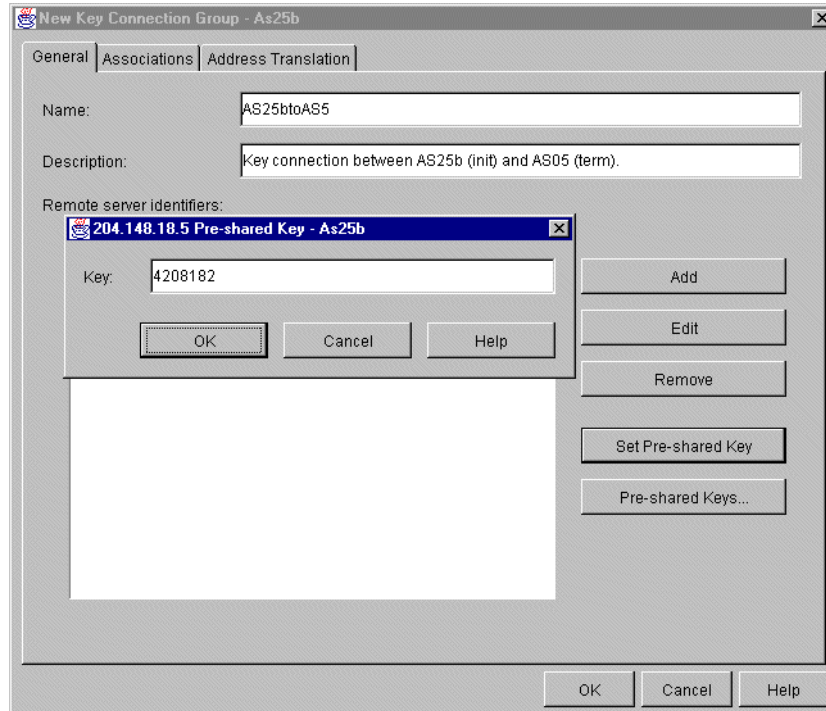


Figure 324. AS25b Setting the pre-shared key

18. Click on **OK**.
19. Click the **Associations** tab.
20. Click **New** to create a new Key Policy (Figure 325 on page 296).

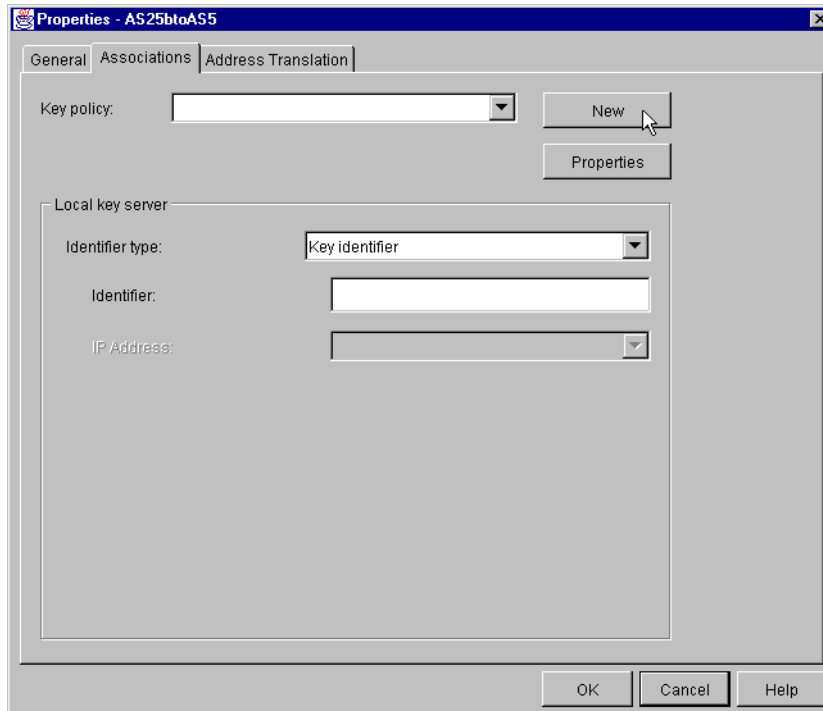


Figure 325. Configuring a new key management policy

21. At the New Key Management Policy window, enter the name `AS25btoAS05` and the description `AS25b and AS05 Max. Security Key policy`.

22. Do *not* select Initiator negotiation - Identity protection.

23. Select Responder negotiation - **Do not allow identity protection** (Figure 326).

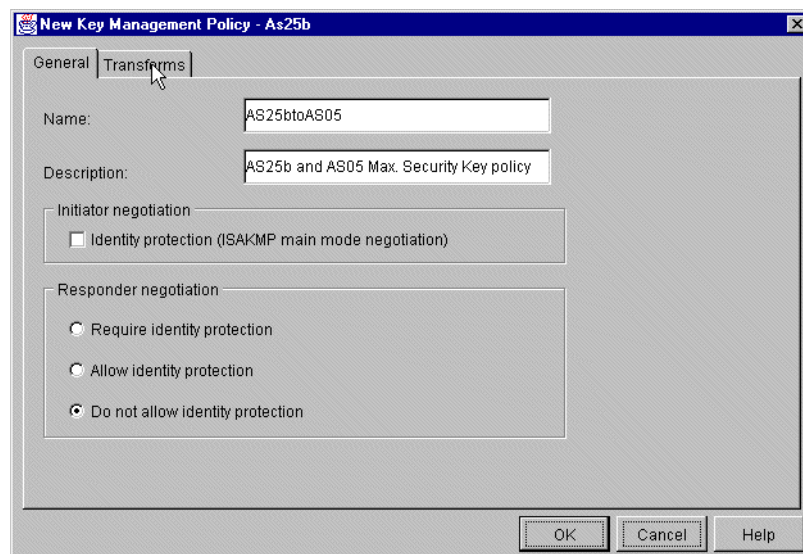


Figure 326. AS25b Configuring a new key management policy

24. Click the **Transforms** tab.

25. Click **Add** (Figure 327 on page 297).

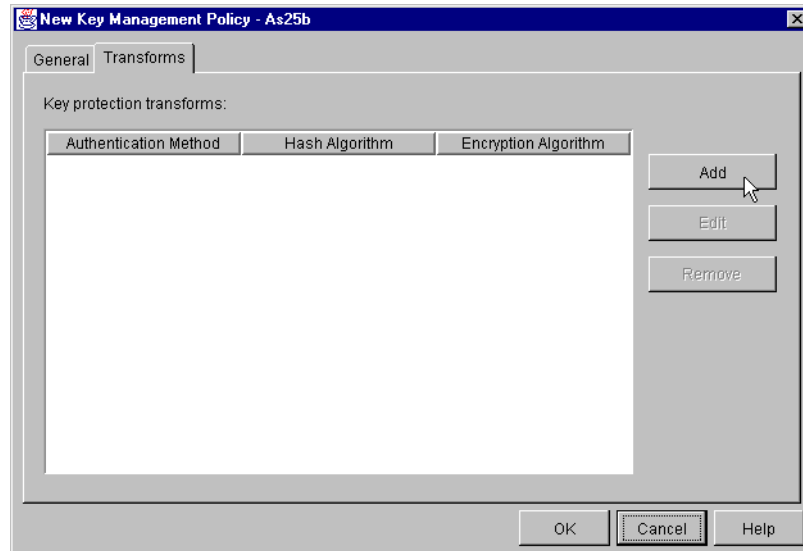


Figure 327. AS25b Configuring key management policy transforms

26. Leave the Authentication method set to **Pre-shared key**.
27. Select **MD5** for the Hash Algorithm parameter.
28. Select **3DES-CBC** for the Encryption Algorithm parameter.
29. Select **Default 768-bit MODP** for the Diffie-Hellman group parameter.
30. Set the Maximum key lifetime to **120** minutes.
31. Leave the Maximum size limit set to **No size limit**. See Figure 328.

Note

The settings in the key transform page (Figure 328) must match those which are configured on the terminator AS05.

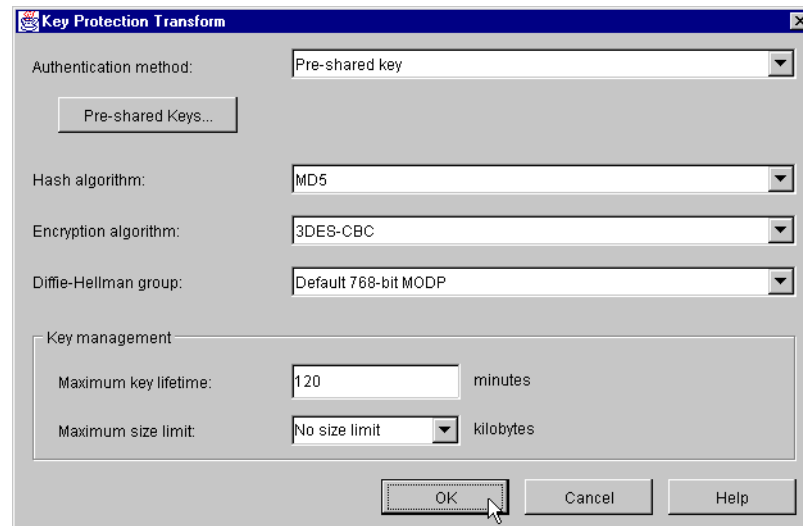


Figure 328. AS25b Configuring the key protection transform

32. Click **OK**.
33. Click **OK** again.
34. Select **Key Identifier** for the Local key server - Identifier type.
35. Enter `AS25b` in the Identifier field (Figure 329). This parameter must match the remote key server identifier configured on the responder (AS05) in 7.2.1, “Configuring IPsec tunnel to the client: Host to Dynamic IP Users” on page 266.

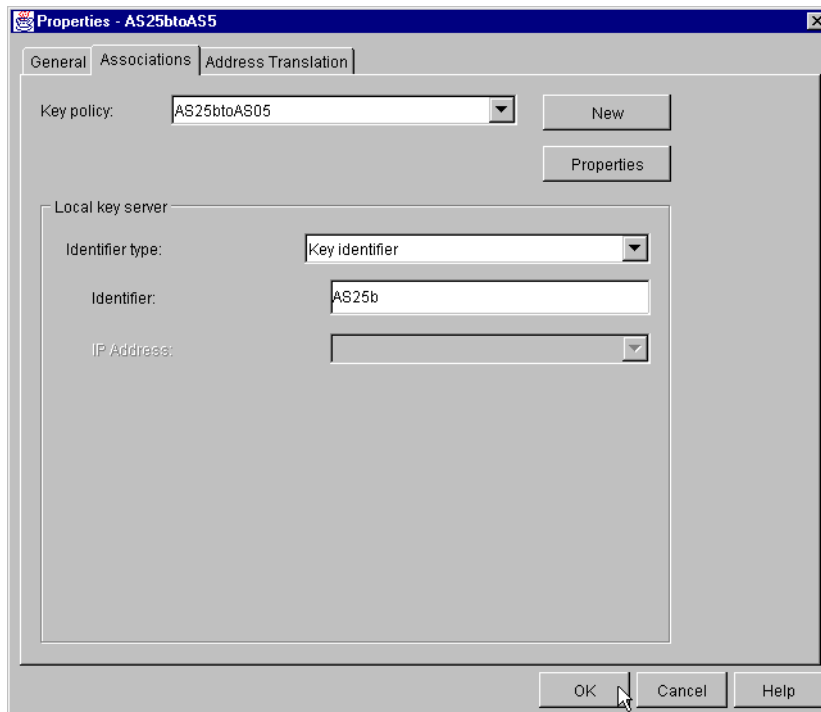


Figure 329. Configuring the local key server identifier

36. Click **OK**.
At this point, you are back at the New L2TP Connection window. See Figure 330 on page 299. You have already configured the key connection group and the key management policy.

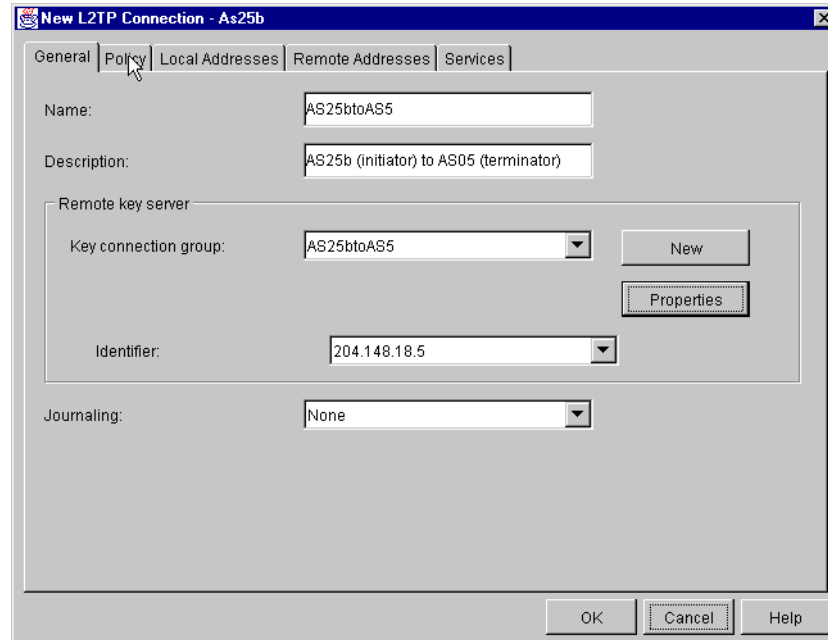


Figure 330. AS25b New L2TP connection after configuring key connection group and key policy

37. Click the **Policy** tab.

38. Set the Local addresses field to **Single value from connection**.

39. Set the Local ports field to **Single value from connection**.

40. Set the Remote addresses field to **Single value from connection**.

41. Set the Remote ports field to **Filter rule**.

42. Set the Protocol field to **Single value from connection**.

43. Set the Connection lifetime field to **Never expires**. See Figure 331 on page 300.

Note

The IPsec tunnel configured here is meant to protect the L2TP tunnel. That is the reason why the VPN is a host to host (point to point) and the values in the Policy window are *Single value from connection*. These values can also be *Filter rule* if you prefer to define them in the IPSEC filter rule.

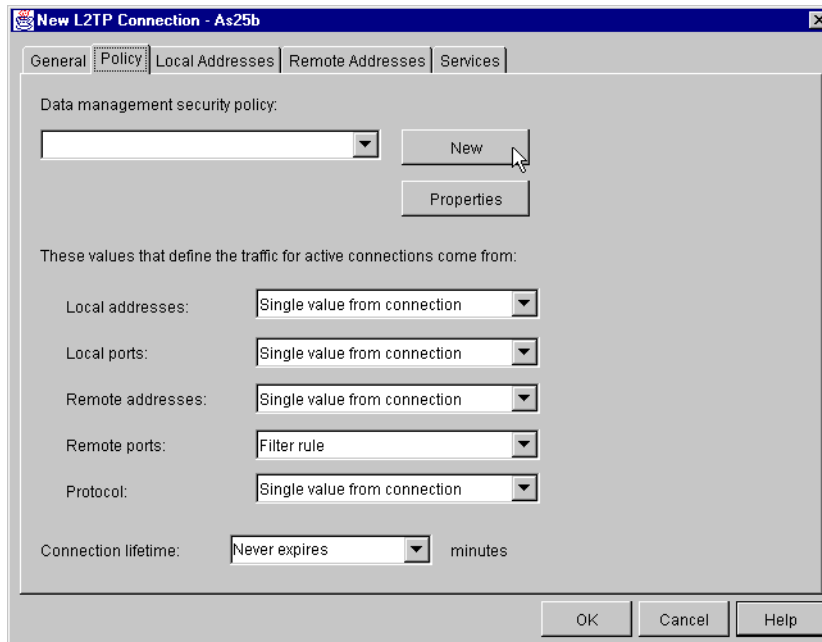


Figure 331. AS25b Configuring values for the traffic in active connections

44. Click **New** to create a new data management security policy.

45. Enter AS25btoAS05 as the data policy Name.

46. Enter Medium Security Data Policy or similar for the Description (Figure 332).

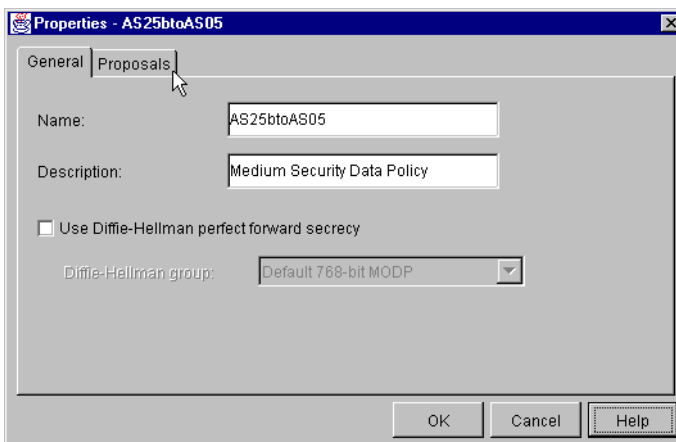


Figure 332. AS25b Configuring a new data management policy

47. Click the **Proposals** tab.

48. Click **Add** to add a new data management proposal.

49. Click **Add** again to add a new transform.

50. Select **Encapsulating security payload (ESP)** for the Protocol parameter.

51. Select **HMAC-MD5** for the Authentication algorithm.

52. Select **DES-CBC** for the Encryption algorithm (Figure 333 on page 301).

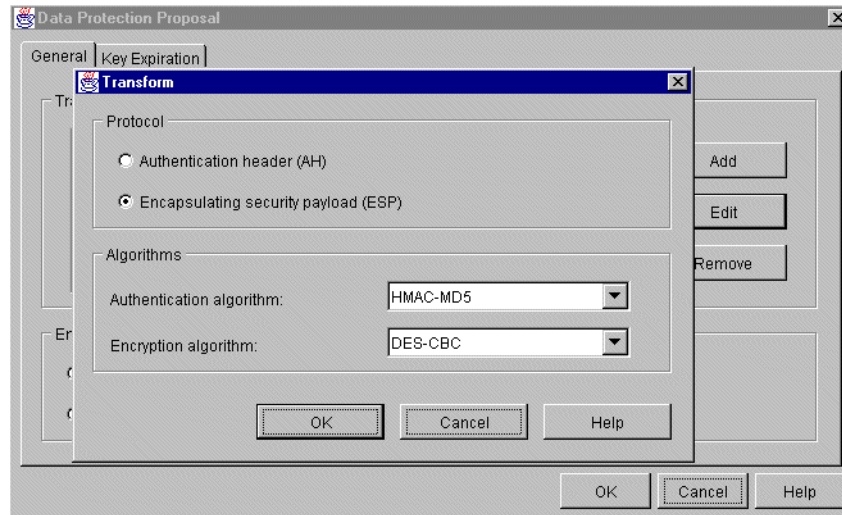


Figure 333. AS25b Configuring the data transform policy

53. Click **OK**.

54. Set the Encapsulation mode to **Transport** (Figure 334).

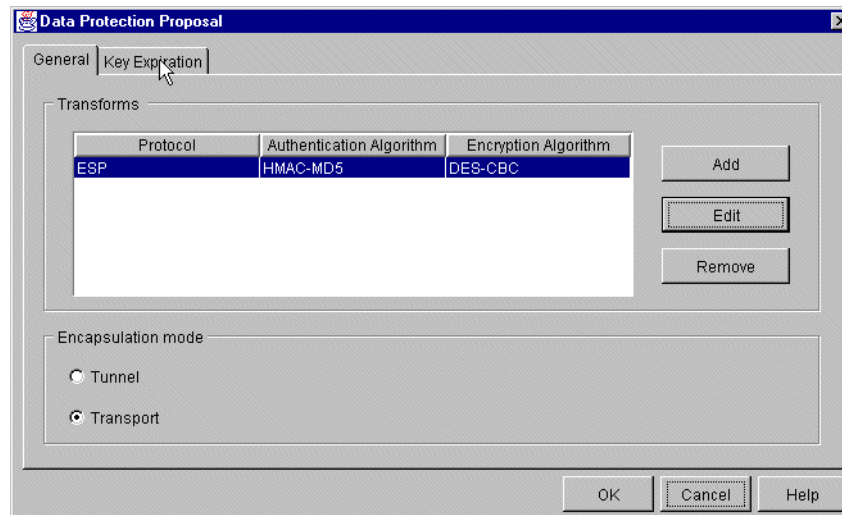


Figure 334. AS25b Selecting transport mode on the data protection proposal

55. Click the **Key Expiration** tab.

56. Enter the value 60 as the number of minutes for Key expiration - Expire after.

57. Leave the Expire at size limit parameter as **No size limit**. See Figure 335 on page 302.

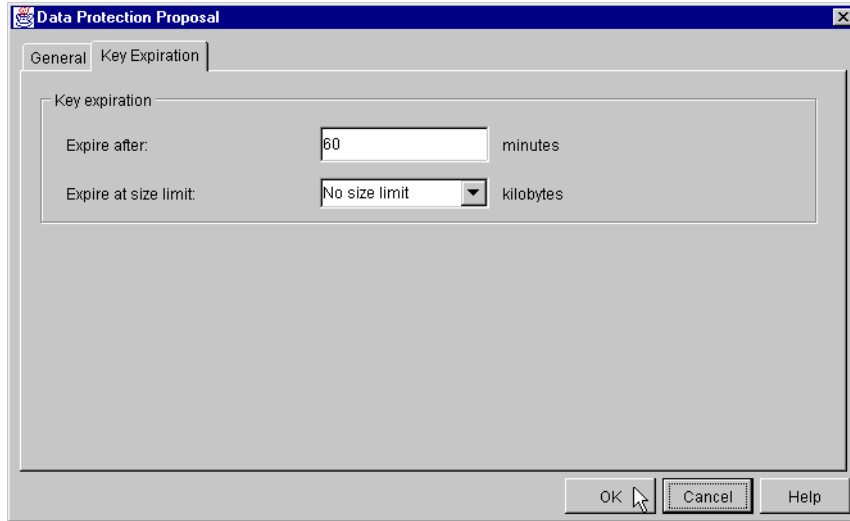


Figure 335. AS25b Setting the key expiration values

58. Click **OK**.
59. Click **OK** again to return to the Policy page of the L2TP connection window.
60. Click the **Local Addresses** tab.
61. Select **Point-to-Point profile** as the Identifier type from the pull-down menu.
62. Select **AS05TERM** as the Identifier from the pull-down menu (Figure 336 on page 303).

Note

The local address configured here is the local data endpoint for the VPN. In the IPsec tunnel that protects the L2TP tunnel presented in this scenario, this is defined by the virtual PPP connection configured in 7.3.4, “Configuring a virtual PPP connection on the L2TP initiator (AS25b)” on page 311. If you follow the sequence of steps in this chapter, the virtual PPP connection does not exist yet. Complete the virtual PPP connection configuration and return to this step to define the Local Addresses.

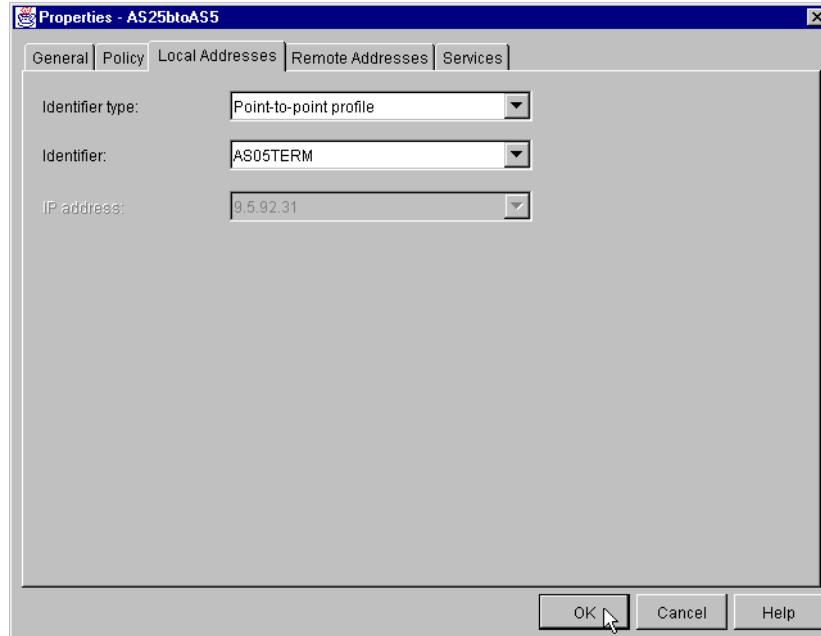


Figure 336. AS25b Configuring the local data endpoint address

63. Click the **Remote Addresses** tab.

64. Select **Version 4 IP address** from the Identifier type pull-down menu.

65. Enter 204.146.18.5 for the IP address parameter (Figure 337).

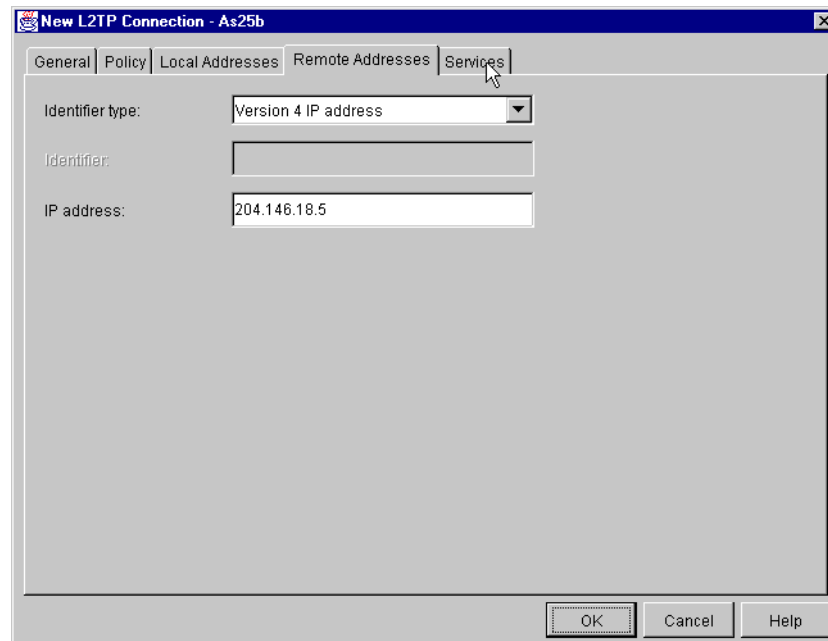


Figure 337. AS25b Configuring the remote data endpoint address

66. Click the **Services** tab.

Review the Services window. It should appear like the one shown in Figure 338 on page 304.

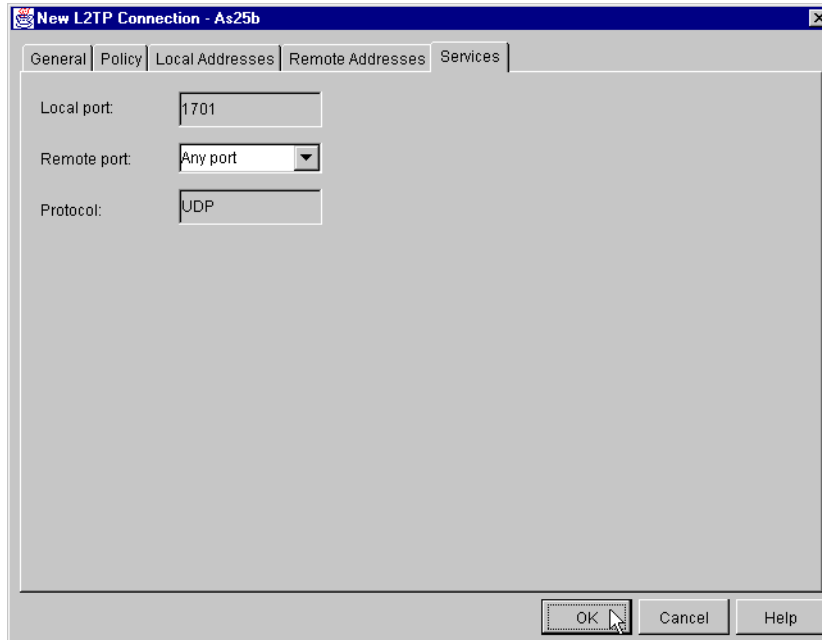


Figure 338. AS25b L2TP connection services

67. Click **OK**

This completes the configuration of the IPsec tunnel that protects the L2TP tunnel. You must also configure the filters as described in 7.3.3, “Configuring IP filters in the L2TP client AS/400 system (AS25b)” on page 304.

7.3.3 Configuring IP filters in the L2TP client AS/400 system (AS25b)

As usual, you must configure filters to complete the VPN configuration. To implement this scenario, four filter rules are required:

- Two filter rules to allow IKE negotiations.
- One IPSEC filter rule associated with the connection created in 7.3.2, “Configuring the L2TP VPN connection on the initiator (AS25b)” on page 291. Notice that, in this scenario, the IPsec tunnel encapsulates the L2TP tunnel as shown in Figure 283 on page 265. Therefore, you can restrict the services to protocol UDP, with source and destination ports 1701 in the IPSEC filter rule.
- One filter interface associated with the filter rules. This is the physical PPP connection profile PPPDIALUP.

Note

The filter rules presented throughout this redbook are *limited* to those required to enable the services in the proposed scenario. If you want to enable other services beyond those in the scenario, you need to configure additional rules. Exercise extreme caution when doing so and always take security into account.

Table 31 summarizes the configuration values to create the IP filters associated with the IPsec tunnel to the client.

Table 31. AS25b Planning worksheet - IP filter rules

This is the information you need to create your IP filters to support VPN	Scenario answers
<p>Is <i>your</i> VPN server acting as a host or gateway? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.</p>	Host
<p>Is the <i>remote</i> VPN server acting as a host or gateway?</p>	Host
<p>What name do you want to use to group together the set of filters that will be created?</p>	L2TPSet
<p>If <i>your</i> server is acting as a gateway...</p> <ul style="list-style-type: none"> – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter. 	
<p>If the <i>remote</i> server is acting as a gateway...</p> <ul style="list-style-type: none"> – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter. 	
<p>What is the IP address of <i>your</i> VPN server?</p> <ul style="list-style-type: none"> – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host. 	Dynamic IP (*)
<p>What is the IP address of the remote VPN server?</p> <ul style="list-style-type: none"> – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host. 	204.146.8.5
<p>What is the name of interface (for example, the Token-Ring, Ethernet, or PPP connection profile) to which these filters will be applied?</p>	PPPDIALUP
<p>What other IP addresses, protocols, and ports do you wish to permit on this interface?</p> <p>Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i>!</p>	

Perform the following steps to create the filters:

1. Start the Operations Navigator.
2. Select the system **AS25b** and sign on as required.
3. Expand **Network**.
4. Click on **IP Security**.
5. In the right hand window, right-click on **IP Packet Security** and select **Configuration** (Figure 339).

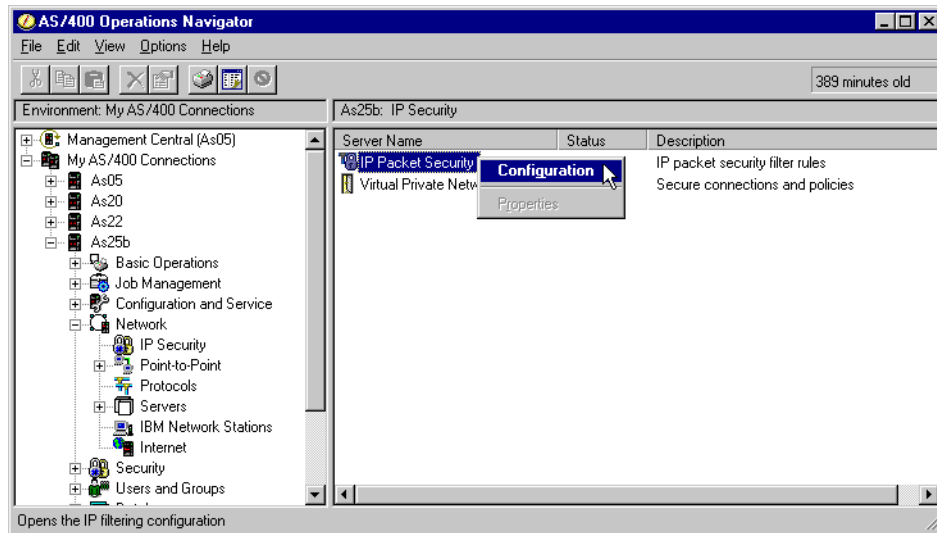


Figure 339. AS25b Starting the IP packet security configuration

6. Right-click on **Filters**, and select **New Filter** (Figure 340).

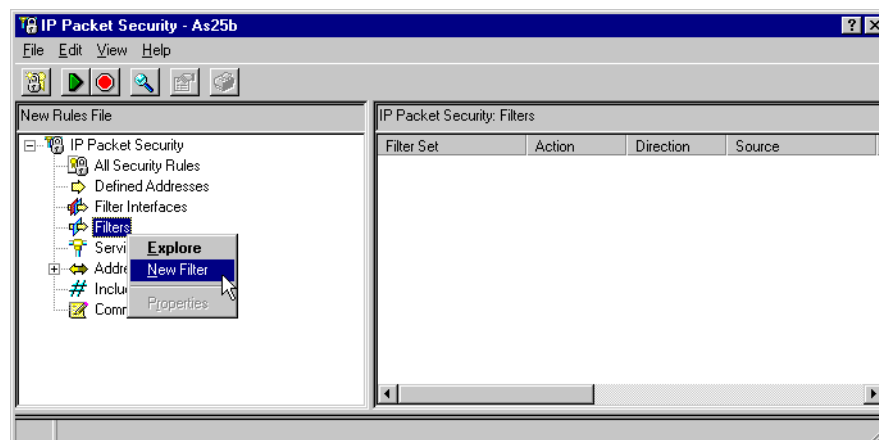


Figure 340. AS25b Creating a new IP filter rule

7. Configure the outbound IKE filter rule to permit IKE negotiations (Figure 341 on page 307). The following values apply:

- **Source address name:** Wildcard. The local key server IP address is dynamic (randomly assign by ISP).
- **Destination address name:** 204.146.18.5

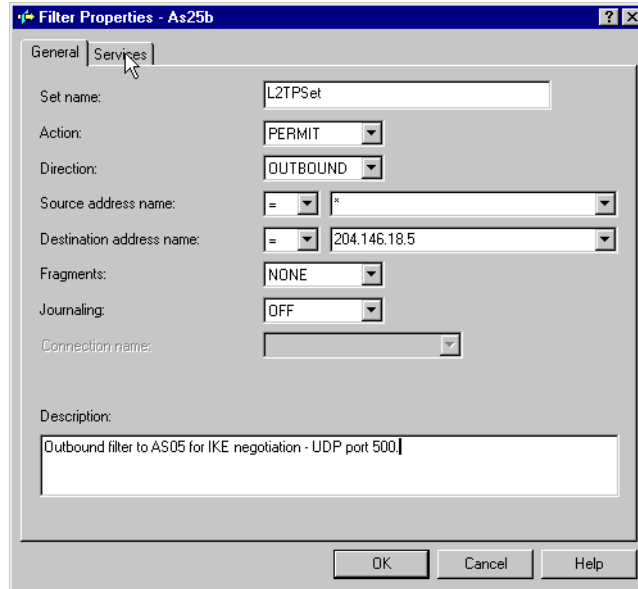


Figure 341. AS25b IKE outbound filter rule - General window

8. Click the **Services** tab.
9. IKE negotiations use protocol UDP, with source and destination port 500. Enter the values as shown in Figure 342.

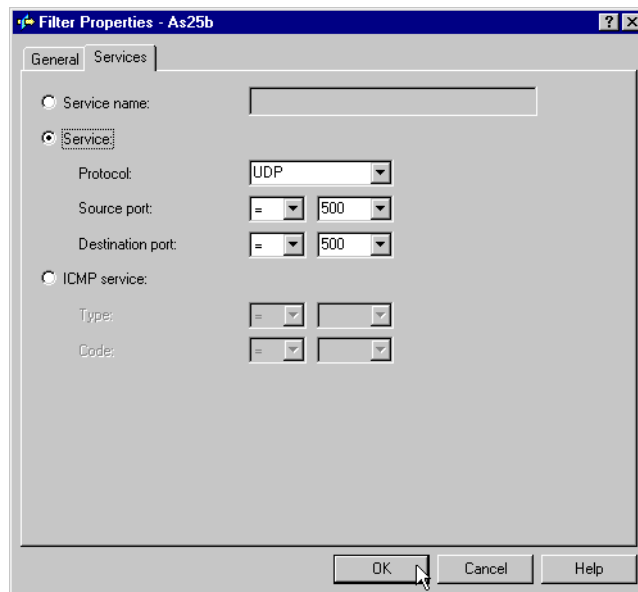


Figure 342. AS25b IKE outbound filter rule - Services window

10. Click **OK** to add the filter rule.
11. Repeat the previous four steps for the *inbound* filter rule. Remember to reverse the Source and Destination address names. Complete the Services window as you did for the outbound rule as shown in Figure 343 and Figure 344 on page 308.

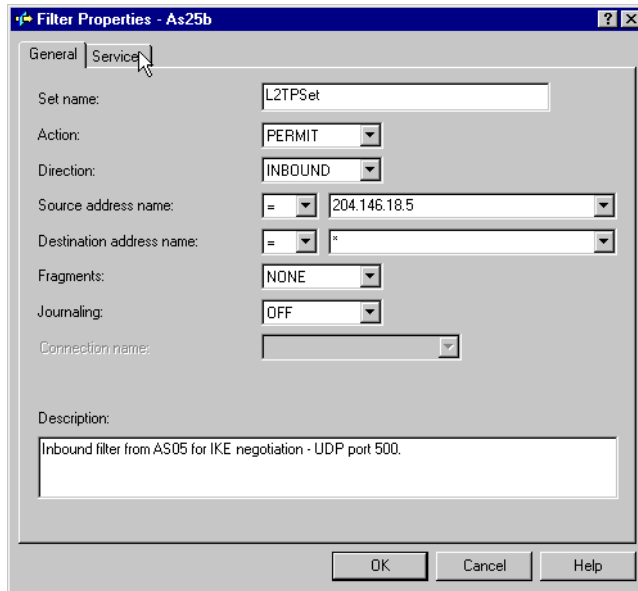


Figure 343. AS25b IKE inbound filter rule - General window

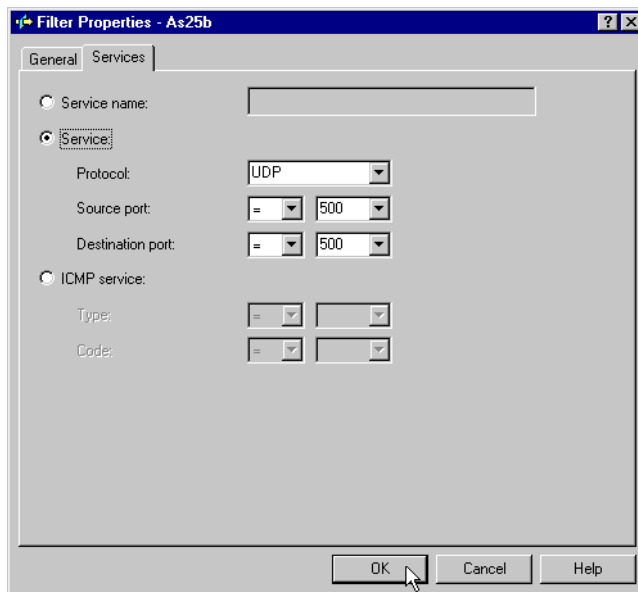


Figure 344. AS25b IKE inbound filter rule - Services window

12. Click on **OK** to add the second rule.

13. Configure the IPSEC filter rule that allows data traffic to use the VPN tunnel. Use the same filter Set name, L2TPSet, but specify **IPSEC** in the Action field. With an IPSEC filter rule, Direction is always set to **OUTBOUND** and grayed out. In the Source address name field, enter wildcard (*). In the Destination address name field, enter the globally routable IP address of AS05, 204.146.18.5, as shown in Figure 345 on page 309. Select **AS25btoAS5** for the connection name field. This is the VPN connection created in 7.3.2, “Configuring the L2TP VPN connection on the initiator (AS25b)” on page 291. See Figure 345 on page 309.

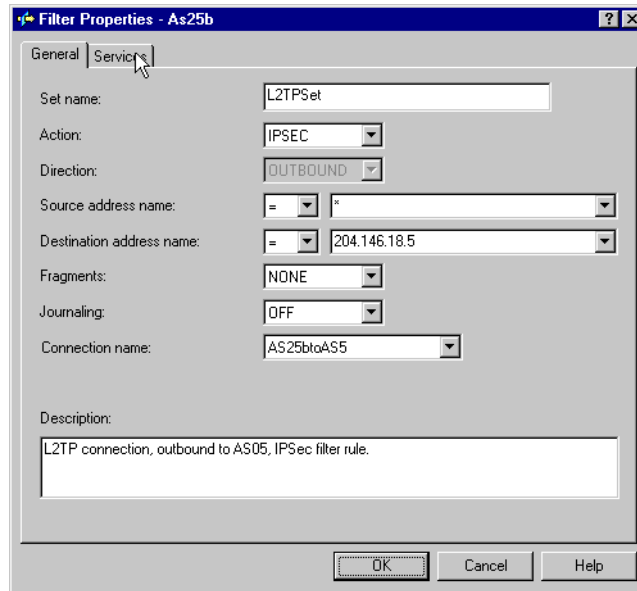


Figure 345. AS25b IPSEC filter rule

14. Click the **Services** tab.

15. Enter **UDP** in the Protocol field. Enter **1701** for the Source port field. Enter **1701** in the Destination port fields. This allows only L2TP traffic to use this filter rule and, therefore, the VPN tunnel. See Figure 346.

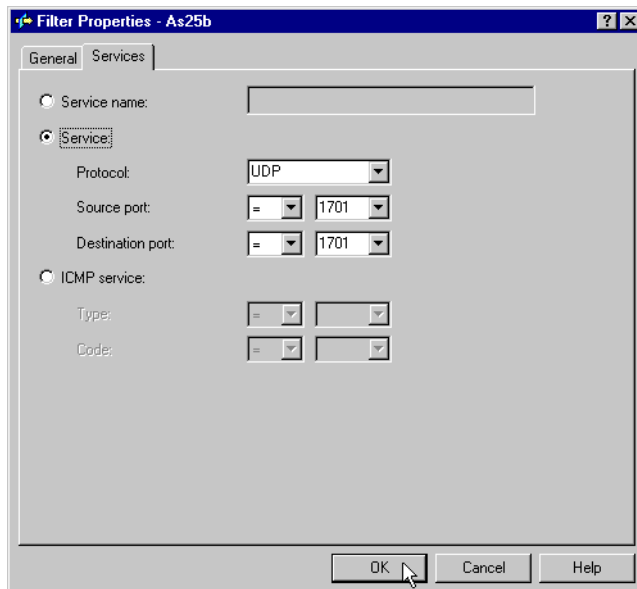


Figure 346. AS25b IPSEC filter rule - Services configuration

16. Click **OK**.

17. The final rule you must create is a Filter Interface rule that ties the filter rules you just created to the required interface. Right-click **Filter Interfaces**, and select **New Filter Interface** as shown in Figure 347 on page 310.

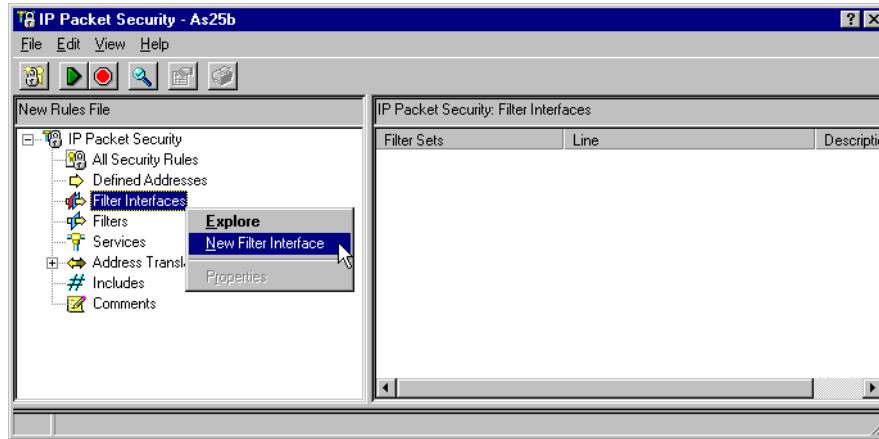


Figure 347. AS25b Defining a filter interface for the IP filter rules

18. Select **Point-to-point profile name** for the Line, and select **PPPDIALUP** from the pull-down menu.
19. Click **Add** to add the filter set name of the filter rules you created previously, which, in this scenario, is L2TPSet (Figure 348).

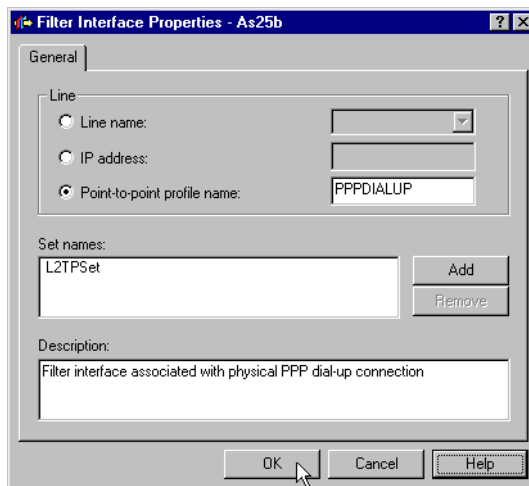


Figure 348. AS25b Filter interface

20. Click **File->Save as...**, and name the file `main.i3p`. Ensure that you use the extension `.i3p` since this is the default.
21. Select **File->Activate** to activate the new filter rules.

Figure 349 on page 311 shows a summary of the filter rules configured in the L2TP client (AS25b).

```

IP Packet Security: All Security Rules
FILTER_INTERFACE INTERFACE = PPPDIALUP SET = L2TPSet
#IKE rules
FILTER SET L2TPSet ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = *
DSTADDR = 204.146.18.5 PROTOCOL = UDP DSTPORT = 500
SRCPORT = 500 FRAGMENTS = NONE JRN = OFF

FILTER SET L2TPSet ACTION = PERMIT DIRECTION = INBOUND
SRCADDR = 204.146.18.5 DSTADDR = * PROTOCOL = UDP DSTPORT = 500
SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC Rule
FILTER SET L2TPSet ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = *
DSTADDR = 204.146.18.5 PROTOCOL = UDP DSTPORT = 1701
SRCPORT = 1701 FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = AS25btoAS5

```

Figure 349. AS25b IP filters summary at the L2TP client in voluntary tunnel

7.3.4 Configuring a virtual PPP connection on the L2TP initiator (AS25b)

To enable the L2TP support on the initiator of the voluntary tunnel, you must configure a virtual PPP connection (G in Figure 283 on page 265). Notice that the physical dial-up PPP connection that you configured in 7.3.1, “Configuring the PPP dial-up connection to the ISP (AS25b)” on page 286, only represents the physical link to the ISP. This physical connection could be a LAN link (since it is on the LNS or terminator end of the L2TP tunnel in AS05) or a leased PPP connection profile.

Perform the following steps to configure a virtual PPP connection on AS25b.

1. Open Operations Navigator, and select system **AS25b**. Sign on as required.
2. Expand **Network->Point-to-Point**.
3. Right-click on **Connection Profiles**, and select **New Profile** (Figure 350).

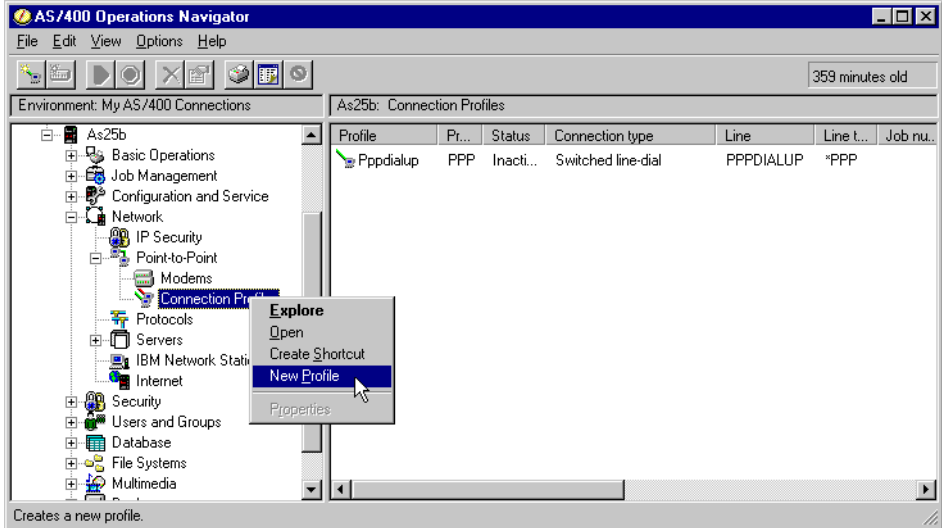


Figure 350. AS25b Creating a new virtual PPP connection profile

Ensure that the General tab is selected since the settings on this page affect the rest of the pages.

4. Enter `AS05TERM` as the Name of the virtual PPP profile.
5. Enter `L2TP AS25b (initiator) to AS05 (terminator) link` or similar for the Description.
6. Select **PPP** as the Type of connection.
7. Select **Virtual line (L2TP)** for the Mode-Line connection type parameter.
8. Select **Initiator** for the Mode type parameter (Figure 351).

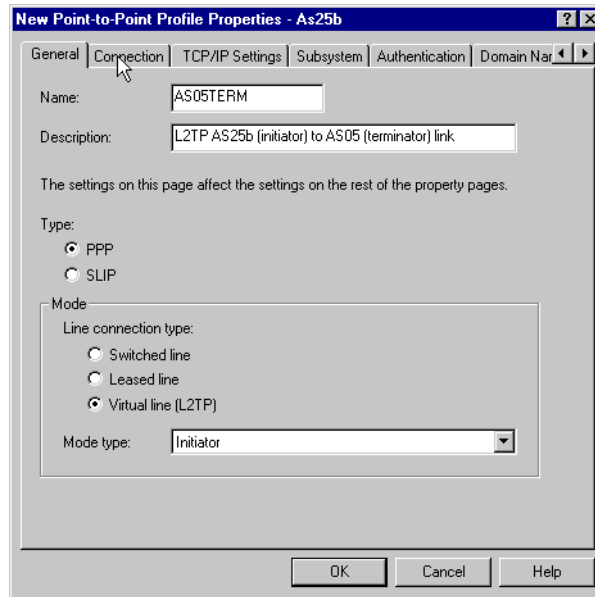


Figure 351. AS25b Creating the virtual PPP link

9. Click the **Connection** tab.
10. For the Remote tunnel endpoint IP address, enter `204.146.18.5` from the pull-down menu.
11. Enter `AS05L2TP` for the Virtual line name parameter.
12. Click the checkbox **Requires IPsec Protection** to start the IPsec tunnel when the virtual PPP connection starts.
13. Select **AS25btoAS5** as the Connection group name from the pull-down menu. This is the L2TP connection (IPsec tunnel) that you created in 7.3.2, "Configuring the L2TP VPN connection on the initiator (AS25b)" on page 291.
14. Click **New** to create a virtual line. See Figure 352 on page 313.

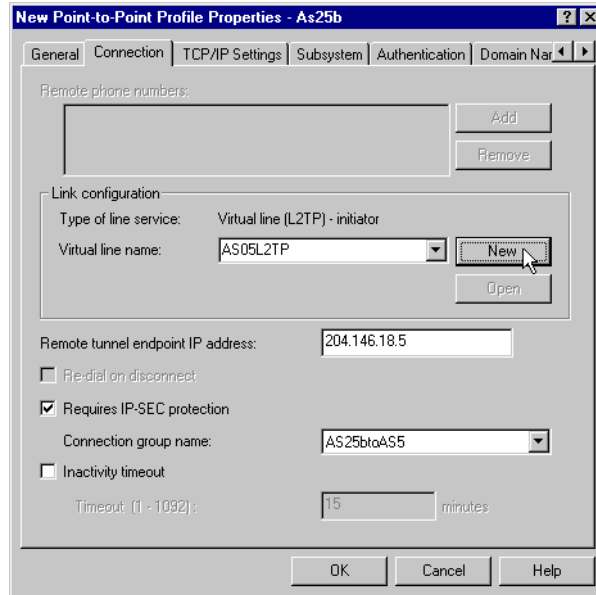


Figure 352. AS25b Defining the virtual PPP connection parameters

15. Enter AS25b to AS05 L2TP connection or similar as the Description (Figure 353).

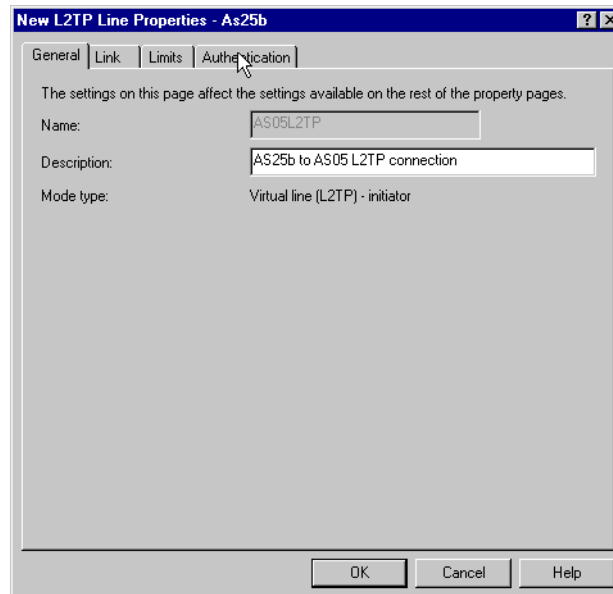


Figure 353. AS25b Entering the virtual PPP line description

16. Click the **Authentication** tab.

17. Enter AS25b as the Local host name. See Figure 354 on page 314.

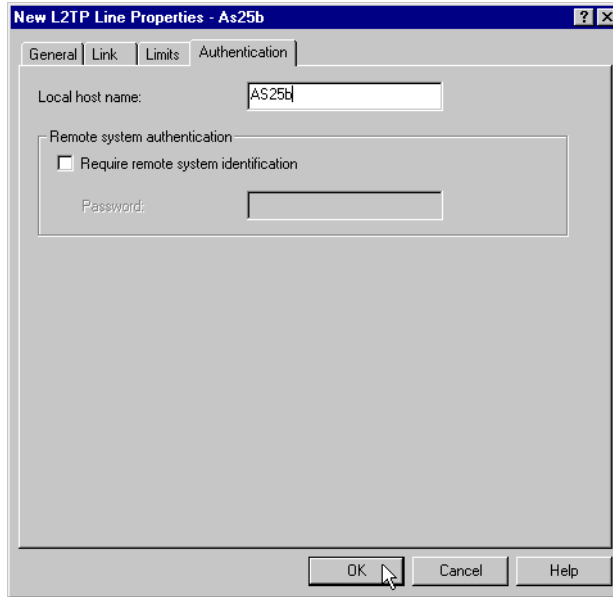


Figure 354. AS25b Virtual PPP authentication page

Note: We are not using PPP authentication in this example.

18. Click on **OK**.

19. Select the **TCP/IP Settings** tab.

20. Select **Dynamically assign** for Local IP address.

21. Select **Dynamically assign** for Remote IP address (Figure 355).

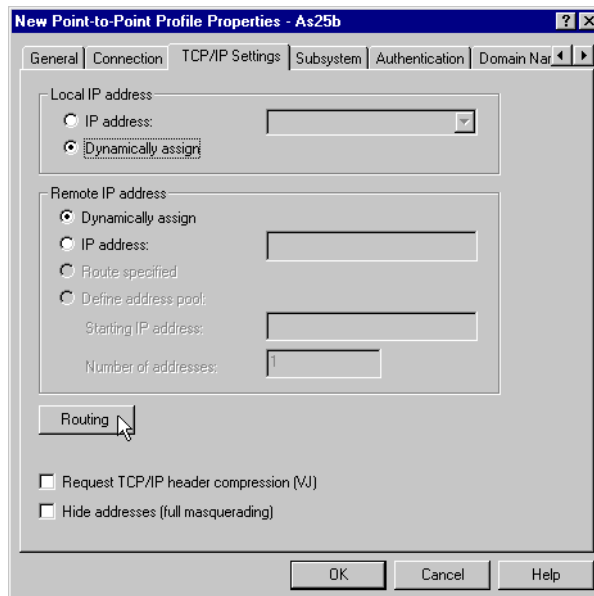


Figure 355. AS25b TCP/IP settings on the virtual PPP link

22. Click the **Routing** button.

23. Select **None** for Dynamic routing (RouteD).

24. Select **Use static routes** for Static routing.

25. Click **Add** to add a route to the corporate network (10.80.21.0).

26. Enter 10.80.21.0 for the Remote network parameter.

27. Enter 255.255.255.0 for the Subnet mask parameter.

A route to the corporate network must be defined in the virtual PPP profile. When the virtual PPP link is activated, the route can be viewed with the `NETSTAT *RTE` command. This route ensures that traffic destined for the corporate network travels over the virtual PPP link.

28. Click **OK** (Figure 356).

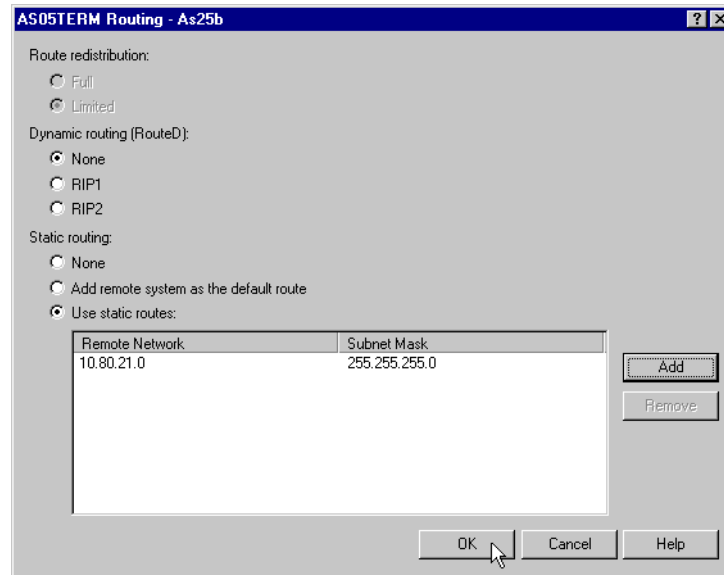


Figure 356. AS25b Defining a route to the corporate network in the virtual PPP profile

29. Click **OK** to create the connection profile.

It is not necessary to modify the settings on the Subsystem, Authentication, or Domain name server pages.

Note: At this point, return to the VPN L2TP connection configuration step 61 on page 302 to update the Local Addresses parameter with the point-to-point profile just created.

7.4 Starting the connections in an L2TP voluntary tunnel with IPSec

This section provides a summary of the tasks you need to perform to start all the required connections in an L2TP voluntary tunnel protected by IPSec.

7.4.1 Starting the LNS in an L2TP voluntary tunnel (AS05)

To start the functions needed in the LNS (AS05), perform the following tasks:

1. Start the filters.
2. Start Virtual Private Networking.

3. Start the L2TP terminator profile by following these steps:
 - a. Expand **Network**.
 - b. Expand **Point-to-Point**, and click **Connection Profiles** as shown in Figure 357.

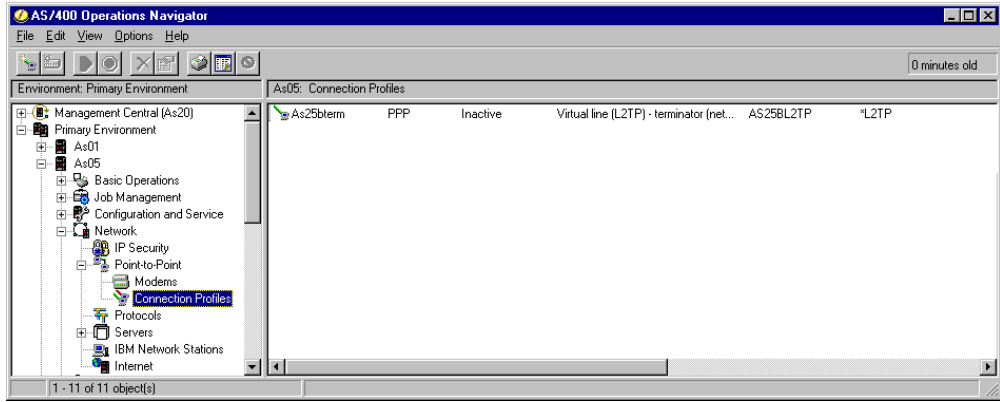


Figure 357. AS05 Starting the virtual PPP connection profile

3. Right-click the virtual line (L2TP) terminator profile **AS25bterm** in this scenario. Select **Start** from the pull-down menu. Alternatively, there is an activate icon (a green triangle) on the toolbar. Once the profile has started, it will be in a `Waiting for connection requests` status. See Figure 358. The job `QTPPPL2TP` starts in the subsystem `QSYSWRK`.

Tip

If you experience problems with the PPP connection, check the job log of the job `QTPPPL2TP`, which runs in subsystem `QSYSWRK`. Alternatively you can access the PPP job log by entering `WRKTCPPPTP` and typing `14` beside the profile `AS05term`.

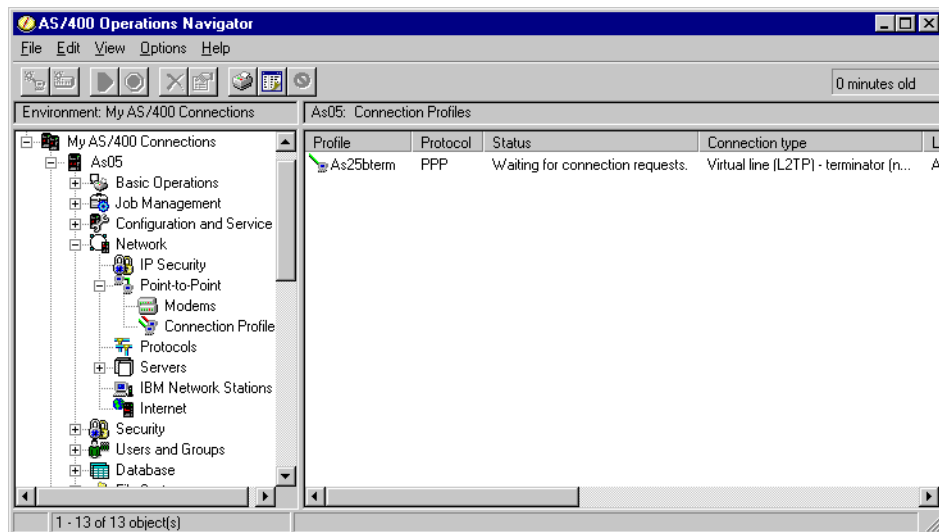


Figure 358. AS05 Starting the virtual PPP terminator profile

7.4.2 Starting the L2TP initiator in an L2TP voluntary tunnel (AS25b)

To start all the functions needed in the L2TP initiator or LAC (AS25b), perform the following tasks:

1. Start the filters.
2. Start Virtual Private Networking.
3. Start the physical PPP dial-up connection (PPPDIALUP) to the ISP:
 - a. From Operations Navigator, expand **Network->Point-to-Point**.
 - b. Click **Connection profiles**.
 - c. Right-click the physical PPP profile **PPPDIALUP**, and select **Start** from the pull-down menu.
4. Start the L2TP initiator profile by following these steps:
 - a. From Operations Navigator, expand **Network->Point-to-Point**.
 - b. Click **Connection profiles**.
 - c. Right-click the virtual PPP L2TP initiator profile **AS05term**, and select **Start** from the pull-down menu.

This activates the L2TP tunnel and starts the VPN L2TP connection on the initiator automatically.

7.5 Verifying interfaces and routes

This section reviews the interfaces and routes in the LNS (AS05) and the L2TP client (AS25b).

7.5.1 Verifying interfaces and routes in the LNS (AS05)

Figure 359 on page 318 shows the results of the `NETSTAT OPTION(*IFC)` command in AS05. Notice that the IP address assigned to the remote L2TP client (10.80.21.115) is listed as a local interface associated with the line description `L20CB70001`.

```

Work with TCP/IP Interface Status
System: AS05
Type options, press Enter.
5=Display details 8=Display associated routes 9=Start 10=End
12=Work with configuration status 14=Display multicast groups

Internet      Network      Line      Interface
Opt Address      Address      Description Status
5  10.80.21.111  10.80.21.0   ITSCRNO   Active
   10.80.21.115  10.80.21.115 L20CB70001 Active
   127.0.0.1     127.0.0.0   *LOOPBACK Active
   204.146.18.5  204.146.18.0 TRLANC    Active

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F11=Display line information  F12=Cancel
F13=Sort by column  F24=More keys

```

Figure 359. AS05 TCP/IP interfaces

The L2TP terminator (LNS) performs proxy ARP for the remote client through the associated local interface 10.80.21.111. You can verify it by entering 5 (Display details) by the IP address assigned to the remote client 10.80.21.115, as shown in Figure 359. Then, the screen shown in Figure 360 on page 319 appears. The client appears as a local interface in the LNS. When hosts in the corporate network broadcast ARP requests with IP address 10.80.21.115, AS05 recognizes that it is a local interface and sends back the MAC address corresponding to the associated local interface 10.80.21.111. Once the packet reaches AS05, it knows how to route it to the remote L2TP client.

```

                                Display TCP/IP Interface Status
                                System:  AS05
Interface host name . . . . . :
Internet address . . . . . : 10.80.21.115
  Subnet mask . . . . . : 255.255.255.255
  Network address . . . . . : 10.80.21.115
  Host address . . . . . : *
  Directed broadcast address . . . . . : *NONE

Interface status . . . . . : Active
Change date/time . . . . . : 07/15/99 17:08:37
Line description . . . . . : L20CB70001
Line type . . . . . : *NOTFND
Associated local interface . . . . . : 10.80.21.111
Type of service . . . . . : *NORMAL
Maximum transmission unit . . . . . : 2046
Automatic start . . . . . : *NO

Press Enter to continue.

F3=Exit  F6=Print  F12=Cancel  F22=Display entire field

```

Figure 360. AS05 Remote L2TP client IP address and associated local interface

Notice the line name, L20CB70001, assigned by the system to internally created L2TP lines (L2 followed by four hexadecimal characters). Notice the Line type *NOTFND, indicating that it is a virtual line.

Figure 361 shows the TCP/IP route information in AS05 after entering the NETSTAT OPTION(*RTE) command.

```

                                Display TCP/IP Route Information
                                System:  AS05
Type options, press Enter.
  5=Display details

  Route          Subnet          Next          Route
  Opt  Destination  Mask           Hop           Available
  5    10.80.21.115  *HOST         *DIRECT      *YES
      10.80.21.0   255.255.255.0 *DIRECT      *YES
      127.0.0.0    255.0.0.0     *DIRECT      *YES
      204.146.18.0 255.255.255.0 *DIRECT      *YES
      *DFTRROUTE  *NONE         204.146.18.1 *YES

                                Bottom

F3=Exit  F5=Refresh  F6=Print list  F9=Command line
F11=Display route type  F12=Cancel  F13=Sort by column  F24=More keys

```

Figure 361. AS05 Routing information

Note: The *DFTRROUTE points to the ISP router. The remote L2TP client appears as a *HOST with a direct route to it.

Figure 362 on page 320 shows the details of the route to the remote L2TP client (10.80.21.115).

A point of interest here is that the *Next hop* and *Route type* are set to **DIRECT*, even though we know this connection traverses the Internet. The Local interface information shows that this is one single network of one host.

```

                                Display TCP/IP Route Details
                                System:  AS05

Route information:
Route destination . . . . . : 10.80.21.115
Subnet mask . . . . . : *HOST
Next hop host name . . . . . :
Next hop . . . . . : *DIRECT
Type of service . . . . . : *NORMAL
Route available . . . . . : *YES
Route type . . . . . : *DIRECT
Route source . . . . . : *CFG
Change date/time . . . . . : 07/15/99 17:08:38
Route maximum transmission unit . . . . . : 2046
Reference count . . . . . : 0

Local interface information:
Internet address . . . . . : 10.80.21.115
Subnet mask . . . . . : 255.255.255.255
Network address . . . . . : 10.80.21.115
More...

Press Enter to continue.

F3=Exit F6=Print F12=Cancel F22=Display entire field

```

Figure 362. AS05 Routing information for the L2TP connection

7.5.2 Verifying interfaces and routes in the L2TP client (AS25b)

Figure 363 on page 321 shows the result of the `NETSTAT OPTION(*IFC)` command in AS25b. Notice that the IP address assigned to the L2TP client (10.80.21.115) is listed as a local interface associated with the L2TP line L244790001. The IP address randomly assigned by the ISP (208.222.150.10) is associated with the physical PPP connection profile (PPPDIALUP).


```

Work with TCP/IP Interface Status
System: AS25B

Type options, press Enter.
5=Display details 8=Display associated routes 9=Start 10=End
12=Work with configuration status 14=Display multicast groups

Internet      Network      Line      Interface
Opt Address      Address      Description Status
10.80.21.115  10.80.21.115 L244790001 Active
127.0.0.1     127.0.0.0    *LOOPBACK Active
208.222.150.10 208.222.150.10 PPPDIALUP Active

Bottom
F3=Exit F4=Prompt F5=Refresh F11=Display line information F12=Cancel
F13=Sort by column F24=More keys

```

Figure 363. AS25b TCP/IP interfaces

Figure 364 shows the details for the interface 10.80.21.115.

```

Display TCP/IP Interface Status
System: AS25B

Interface host name . . . . . :
Internet address . . . . . : 10.80.21.115
Subnet mask . . . . . : 255.255.255.255
Network address . . . . . : 10.80.21.115
Host address . . . . . : *
Directed broadcast address . . . . . : *NONE

Interface status . . . . . : Active
Change date/time . . . . . : 07/15/99 17:09:18
Line description . . . . . : L244790001
Line type . . . . . : *NOTFND
Associated local interface . . . . . : *NONE
Type of service . . . . . : *NORMAL
Maximum transmission unit . . . . . : 2046
Automatic start . . . . . : *NO

Press Enter to continue.

F3=Exit F6=Print F12=Cancel F22=Display entire field

```

Figure 364. AS25b TCP/IP interface details

Figure 365 on page 322 shows the TCP/IP route information in AS25b after entering the NETSTAT OPTION(*RTE) command.

Notice the *HOST route to the remote LNS, 10.80.21.111 (AS05) through the local interface 10.80.21.115.

The routing to the corporate subnet is through the associated local interface in the LNS 10.80.21.111.

*DFTRROUTE is the route to the ISP through the physical PPP dial-up connection (PPPDIALUP). This is the result of adding the remote system as the default route in the Static routing of the PPP configuration (see Figure 315 on page 289).

```

                                Display TCP/IP Route Information
                                System:  AS25B
Type options, press Enter.
  5=Display details

  Route      Subnet      Next      Route
Opt  Destination  Mask      Hop      Available
  10.80.21.115 *HOST     *DIRECT   *YES
  10.80.21.111 *HOST     10.80.21.115 *YES
  10.80.21.0    255.255.255.0 10.80.21.115 *YES
  127.0.0.0    255.0.0.0    *DIRECT   *YES
  208.222.150.10 *HOST     *DIRECT   *YES
  208.222.150.1 *HOST     208.222.150.10 *YES
  *DFTRROUTE   *NONE      208.222.150.10 *YES

                                Bottom
F3=Exit  F5=Refresh  F6=Print list  F9=Command line
F11=Display route type  F12=Cancel  F13=Sort by column  F24=More keys

```

Figure 365. AS25b Routing table information

7.6 Verification tests

Table 32 presents a summary of the verification tests run after the L2TP voluntary tunnel protected by IPSec was implemented. Notice that the source and destination IP addresses used in the tests are the IP interfaces in the corporate address space (10.80.21.x).

Table 32. Host-to-gateway L2TP voluntary tunnel verification tests

From/to system	PING	TELNET	FTP
AS25b to AS05	Yes	Yes	Yes
AS25b to AS22	Yes	Yes	Yes
AS22 to AS25b	Yes	Yes	Yes
AS25b to AS22	Yes	Yes	Yes

Chapter 8. L2TP gateway-to-gateway voluntary tunnel

This chapter expands the scenario discussed in Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263. It shows how the AS/400 system L2TP client at the remote branch office can perform as a gateway for the branch office network.

The L2TP principles and configurations presented in the previous chapter remain the same. This chapter explores how to use routing, transparent subnetting, and proxy Address Resolution Protocol (ARP) to expand the host-to-gateway scenario presented in Chapter 7, to a gateway-to-gateway configuration.

8.1 Branch office network to corporate network connection with L2TP

This chapter presents a branch office network (network A) connected to the corporate office network (network B) through a gateway AS/400 system (AS25b) in an L2TP tunnel protected by IPSec. The corporate office gateway (AS05) is the L2TP Network Server (LNS) or terminator of the L2TP tunnel. The branch office gateway (AS25b) is the L2TP access concentrator (LAC) or initiator of the L2TP tunnel. The scenario in this chapter is the same as in Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263. The only difference is that now all systems in the branch office network can communicate with all systems in the corporate network using the L2TP tunnel protected by IPSec over the Internet. Figure 366 shows an overview of the network presented in this chapter.

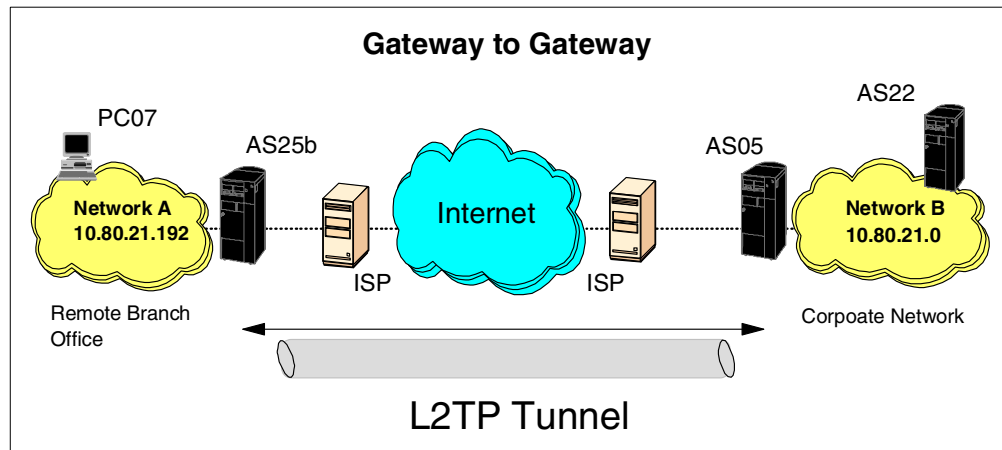


Figure 366. Branch office network to corporate network connection - L2TP voluntary tunnel

Important note

All scenarios in this redbook show the AS/400 security gateway at the corporate office directly connected to the Internet. The absence of a firewall in these scenarios is meant to simplify the VPN examples. It does *not* imply that the use of a firewall is not necessary. For information about how the AS/400 security gateway interacts with a firewall, refer to Chapter 12, “Don’t forget a firewall: Protecting your VPN server” on page 515.

8.1.1 Scenario characteristics

The main characteristics of this scenario are:

- The address space of the branch office network (network A, 10.80.21.192) is a subnet of the corporate network's address space (network B 10.80.21.0).
- AS25b is the gateway between all hosts in network A and the corporate office network.
- AS05 is the gateway between all hosts in network B and the remote branch office network.
- Due to the IP addressing scheme selected for both networks, transparent subnetting and proxy ARP are enabled. Hosts on network A appear to be directly connected to network B and vice versa, even when they are not.
- Network A and network B fully trust each other.

8.1.2 Scenario objectives

The objectives of the scenario are almost the same as in the Chapter 7, "L2TP host-to-gateway voluntary tunnel" on page 263. Refer to 7.1.2, "Scenario objectives" on page 264, for a complete list of objectives.

In this scenario, all systems in the branch office network must be able to communicate with all systems in the corporate office network and vice versa. This objective is accomplished by connecting both sites through an L2TP tunnel protected with IPSec. Transparent subnetting, proxy ARP, and routing make it possible to view both networks as a larger network so that hosts in both networks can talk to each other.

8.1.3 Scenario network configuration

Figure 367 on page 325 shows the test network used in this scenario.

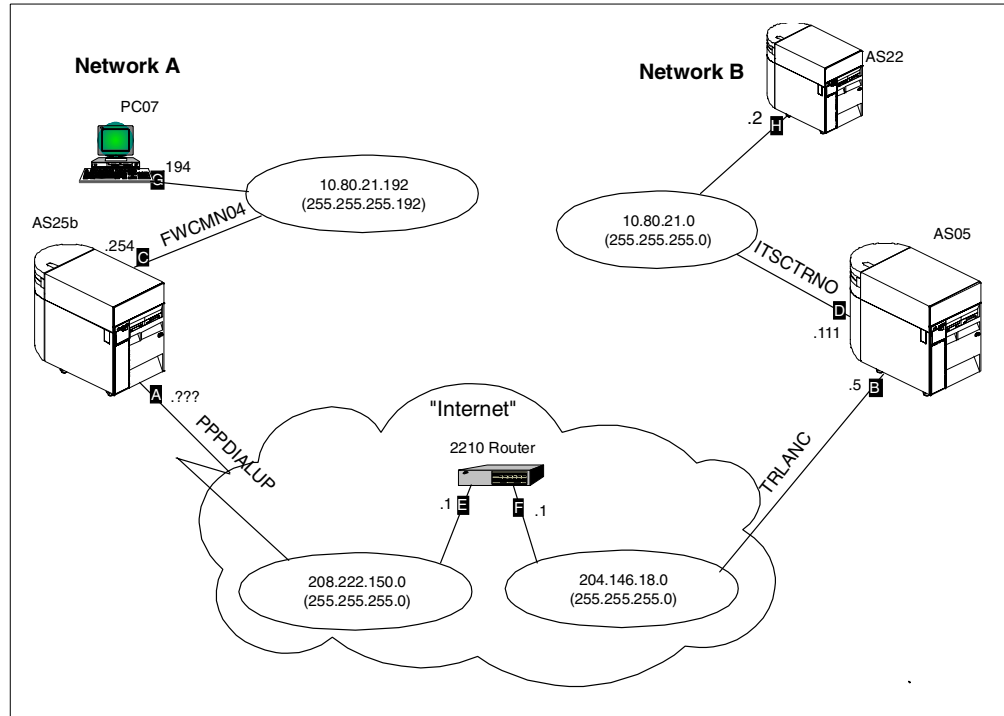


Figure 367. L2TP gateway-to-gateway voluntary tunnel - Scenario test network

The main points to note about the test network are:

- The address space of the branch office network (network A) is a subnet of the corporate office address space (network B).
- AS05 is the corporate gateway, the L2TP terminator or LNS, and the responder in the VPN that protects the L2TP tunnel.
- AS25 is the branch office gateway, the L2TP initiator or LAC, and the initiator in the VPN that protects the L2TP tunnel.
- The 2210 router and subnets 208.222.150.0 and 204.146.18.0 represent the "Internet" in our test environment.
- PC07 represents *any* system in the branch office network. It is not required for hosts in network A to support IPSec except for the gateway system (AS25b).
- AS22 represents *any* system in the corporate office network. It is not required for hosts in network B to support IPSec, except for the gateway system (AS05).

8.1.4 Implementation tasks: Summary

You need to perform the following tasks to implement this L2TP voluntary tunnel protected by IPSec in this scenario:

1. Plan the network's IP addressing and routing scheme.
2. LNS configuration (AS05)
 - a. Configure the IPSec ESP tunnel that protects the L2TP tunnel to the client (Host to Dynamic IP Users).
 - b. Configure the L2TP terminator profile.

- c. Configure IP filters.
3. L2TP initiator client (AS25b)
 - a. Configure a PPP dial-up connection to the ISP.
 - b. Configure the IPsec ESP tunnel that protects the L2TP tunnel to the LNS (L2TP connection).
 - c. Configure IP filters.
 - d. Configure the L2TP initiator profile.
4. Start connections
5. Verify communications

Notice that most of the tasks are identical to those discussed in the implementation of Chapter 7, "L2TP host-to-gateway voluntary tunnel" on page 263. The main difference is the configuration of network A and network B to use transparent subnetting (proxy ARP).

8.1.5 Planning the networks IP addressing and routing scheme

This scenario shows you how to connect two subnets (network A and network B) using transparent subnet masking and appropriate routing. It is beyond the scope of this redbook to discuss the basic concepts of transparent subnetting and proxy ARP. Refer to RFC1027, "Using ARP to Implement Transparent Subnet Gateways", *TCP/IP Addressing*, written by Buck Graham, and the redbook *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147, for more information on these concepts.

The term *transparent subnet masking* is slightly misleading. Another way to describe it is with the term *IP address grouping*. Using different masks over the same network ID, you can segment or group contiguous ranges of IP addresses together to use for remote LANs attached to the AS/400 gateways. The transparency part comes into play when proxy ARP is enabled, which happens automatically when the hosts on the network share the same network ID. In effect, the subnetting within your network is transparent because a router or gateway is not required to join the subnets.

Transparent subnetworking allows remote clients that are on separate LANs to communicate with one another as if they were on the same physical network. To accomplish transparent subnetworking, you must carve branch office subnets from the corporate office address space. This is done by using a common network ID (10.80.21.x in our sample network) and choosing subnet masks that partition the corporate office address space in blocks of contiguous IP addresses.

In our sample network, the corporate office address space is the class C network 10.80.21.0, subnet 255.255.255.0. We divided this address space of 256 hosts into four partitions of 62 hosts each by using the subnet mask 255.255.255.192 in the branch offices. Notice that, even when it appears that 256 addresses can be divided into four blocks of 64 addresses each, all "0" and all "1" host addresses are not allowed.

Note: In our sample network with only one branch office, one block of 62 hosts is assigned to the branch office, while the rest remain part of the corporate office address space.

The IP address deployment and routing characteristics of our sample network are:

- The corporate address space (network B) is the whole class C network 10.80.21.0, with subnet mask 255.255.255.0.
- The branch office address space (network A) is a subset of 62 hosts carved out of the corporate address space using subnet mask 255.255.255.192. The block of IP addresses assigned to network A is 10.80.21.193 - 10.80.21.254, with subnet mask 255.255.255.192.
- The corporate office gateway (AS05) performs proxy ARP for the systems in the branch office network. This way, hosts on network B view hosts on network A as locally attached to network A.
- The LNS (AS05) assigns the L2TP client (AS25b) an IP address in the block carved out for the branch office network. This is accomplished by adding a static route in the virtual PPP terminator profile based on the AS25b caller user name. This configuration also provides AS05 with the necessary routing information to forward IP packets destined for network A.
- The virtual PPP initiator profile in AS25b includes a static route to the corporate network 10.80.21.0, with subnet mask 255.255.255.0.
- The default route for the branch office gateway (AS25b) is the physical PPP connection to the ISP.
- The default route for the corporate office gateway (AS05) is the ISP router IP address.
- The default route for all hosts in network A point to the branch office gateway (AS25b).
- The default route for all hosts in network B point to the corporate office gateway (AS05).

8.2 Configuring the LNS in a voluntary tunnel protected by IPsec (AS05)

The following sections take you step-by-step through the configuration of the VPN, L2TP network server (terminator profile), and filters on AS05.

8.2.1 Configuring IPsec tunnel to the client: Host to Dynamic IP users

This is exactly the same VPN configuration as the one described in 7.2.1, “Configuring IPsec tunnel to the client: Host to Dynamic IP Users” on page 266.

8.2.2 Configuring the L2TP terminator profile (AS05)

This section explains how to configure the LNS end of the L2TP tunnel. To configure the LNS terminator profile on AS05, complete the following steps:

1. Start Operations Navigator from your desktop.
2. Expand the AS/400 system, which, in this case, is **AS05**. Sign on when prompted.
3. Expand **Network**.
4. Expand **Point-to-point**.
5. Right-click **Connection profiles**, and select **New profile** as shown in Figure 368.

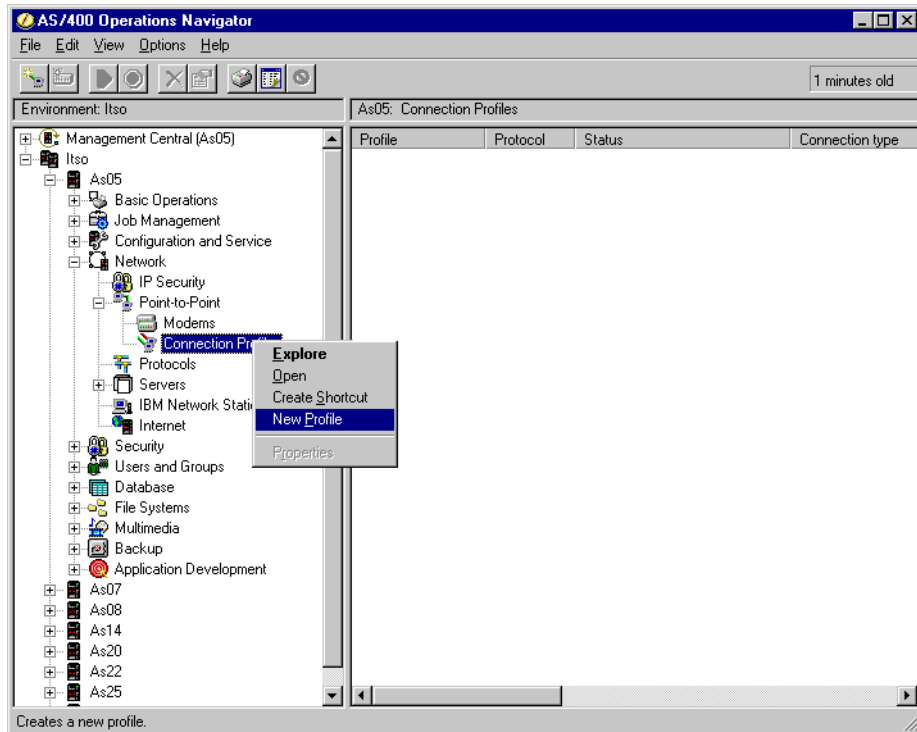


Figure 368. Operations Navigator - Connection Profiles -> New Profile

6. Enter the name `GtoGterm` for the profile name, and enter a description.
7. Select Mode-Line connection type **Virtual Line (L2TP)**
8. Select Mode type **Terminator (network server)** (Figure 369).

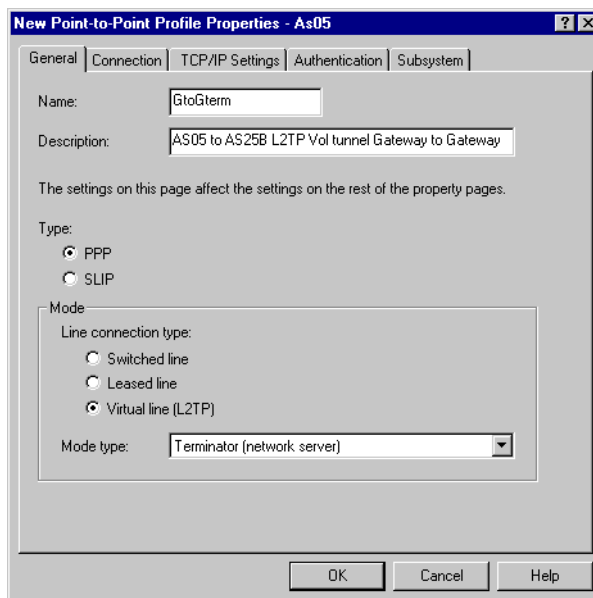


Figure 369. AS05 Virtual PPP terminator profile - General window

9. Click the **Connection** tab.

10. For the Local tunnel endpoint IP address, specify the globally routable IP address for this AS/400 system, AS05. In this scenario, select **204.146.18.5** from the pull-down box.
11. In this configuration, we are re-using the line description **AS25bL2TP** created in 7.2.2, “Configuring the L2TP terminator profile (AS05)” on page 273. See Figure 370.

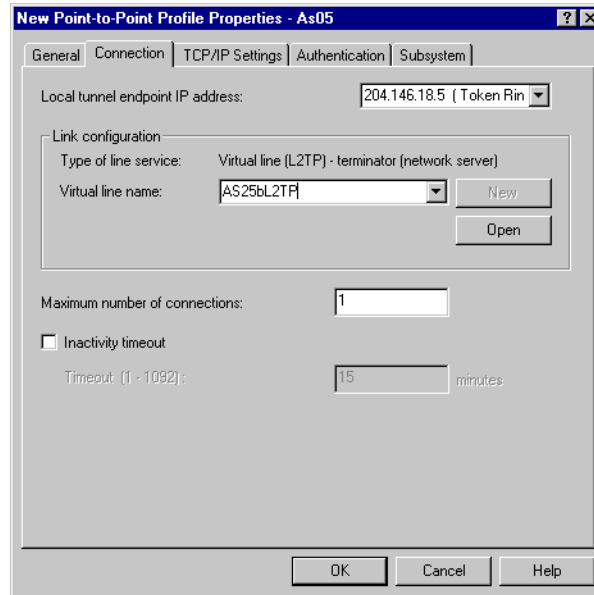


Figure 370. AS05 Virtual PPP terminator profile - Connection window

12. Click the **TCP/IP Settings** tab.
13. For the local IP address, select the IP address of the LNS system (AS05) on the corporate network (**10.80.21.111**). This is the IP address that performs proxy ARP in the corporate subnet for the remote branch office.
14. Select **Route specified** for the remote IP address.
15. Select **Allow IP forwarding** since this system is acting as a gateway for IP packets between the branch and corporate offices (Figure 371 on page 330).

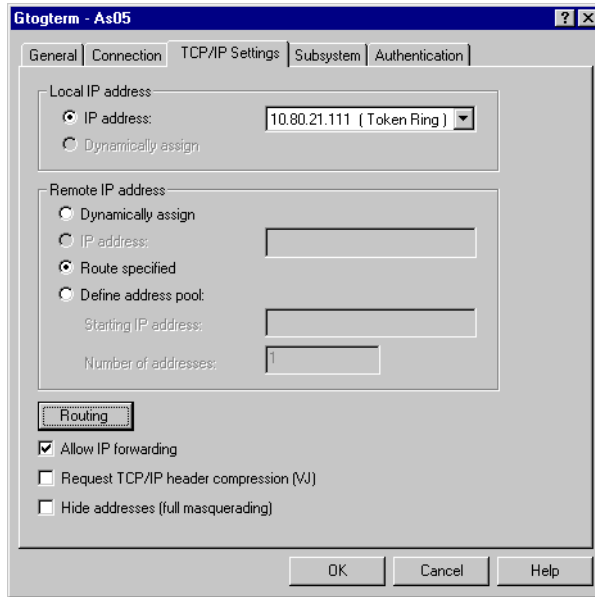


Figure 371. AS05 TCP/IP settings on the virtual PPP link

16. Click **Routing**.

17. Click **Add** to add a static route for the L2TP client AS25b as shown in Figure 372.

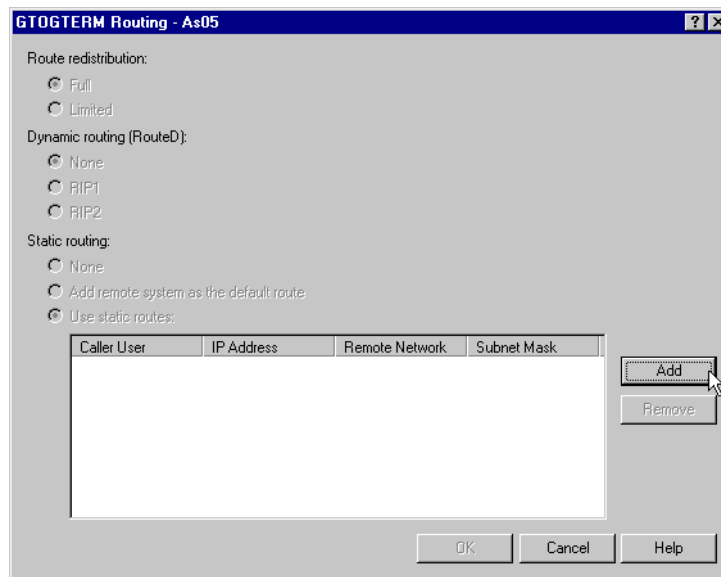


Figure 372. Clicking Add on the point-to-point profile routing window

18. Fill in the Add Routes for the PPP Answer Parameters - AS05 window. Caller user name is the identification that the remote client sends during authentication. For this scenario, it is **AS25B**. In the IP address field, enter the IP address that the LNS will assign to the client after successful authentication. In this example, enter the IP address as 10.80.21.193, and the Subnet mask as 255.255.255.192. Notice that this is the first IP address in the block of 62 IP addresses assigned to the branch office to enable proxy ARP

and transparent subnetting as discussed in 8.1.5, “Planning the networks IP addressing and routing scheme” on page 326. See Figure 373.

Note

In this gateway-to-gateway scenario, you must configure a static route to the branch office network in the virtual PPP terminator profile as shown in the current step. Contrast this configuration with the one in the previous chapter, in which AS05 performs proxy ARP for a single host, not for a network as it does in this chapter.

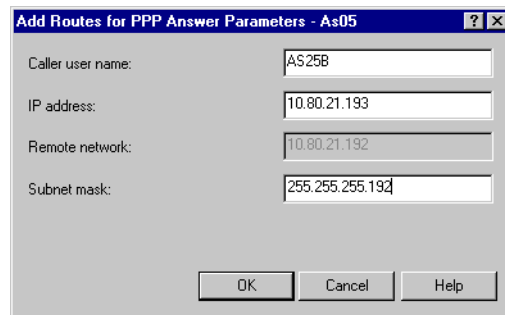


Figure 373. Adding a route to the L2TP client

19. Click **OK**. The route should be added as shown in Figure 374.

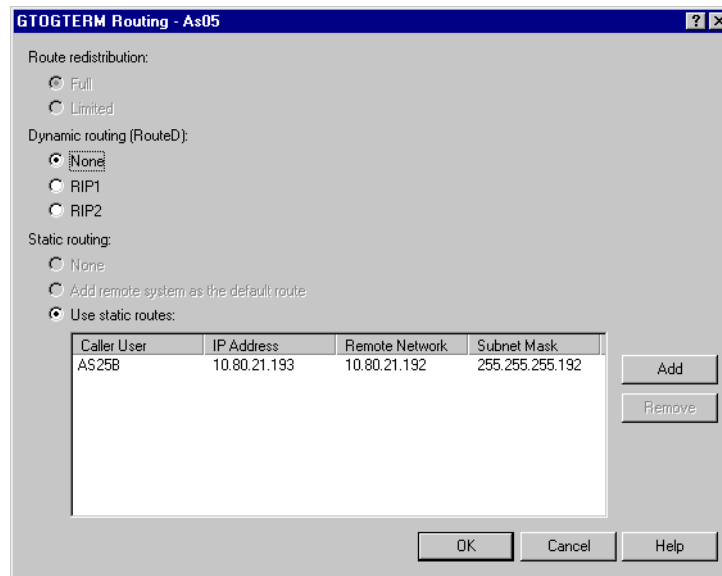


Figure 374. AS05 Point-to-point profile routing to remote network

20. Click **OK**.

21. Click the **Authentication** tab.

22. For Remote system authentication, select **Require remote system identification** and **CHAP only**.

23. Enter the Validation list name `GTOGVOL` (in our example).

24. Click **New** to create a new validation list as shown in Figure 375 on page 332.

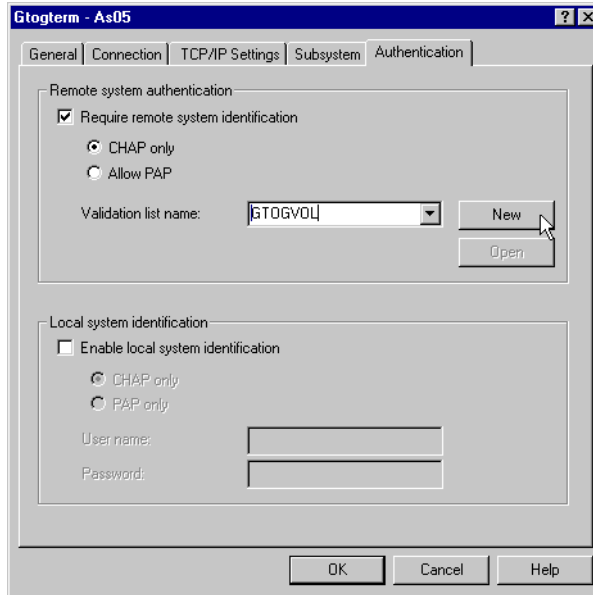


Figure 375. AS05 Remote system authentication

25. A new window appears. Click **Add** to add an entry to the validation list as shown in Figure 376.

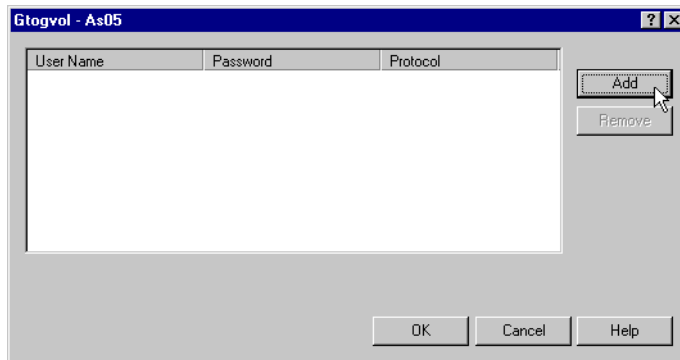


Figure 376. AS05 Adding entries to the validation list

26. Select **CHAP only**.

27. Enter the client User name as AS25B and the Password as shown in Figure 377.

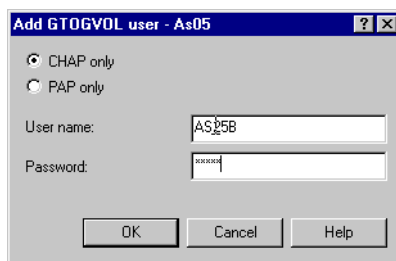


Figure 377. AS05 Adding remote user authentication information to the validation list

28. Click **OK**.

29. Confirm the password when prompted to do so (Figure 378).

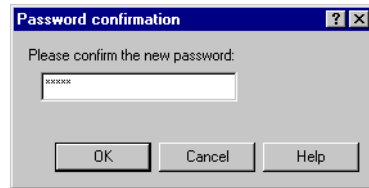


Figure 378. Password confirmation window

30. Click **OK**.

31. Click **OK** to create the new PPP profile.

8.2.3 Configuring IP filters in the LNS AS/400 system (AS05)

This is exactly the same IP filter configuration as the one described in 7.3.3, “Configuring IP filters in the L2TP client AS/400 system (AS25b)” on page 304.

8.3 Configuring the L2TP client in a voluntary tunnel protected with IPsec

The following sections take you step-by-step through the configuration of the PPP dial-up connection to the ISP, L2TP client (initiator), VPN, and filters in AS25b.

8.3.1 Configuring the PPP dial-up connection to the ISP (AS25b)

The configuration of the PPP dial-up connection on AS25b to the ISP is much like any regular PPP connection. This is exactly the same PPP configuration as the one described in 7.3.1, “Configuring the PPP dial-up connection to the ISP (AS25b)” on page 286.

8.3.2 Configuring the L2TP VPN connection on the L2TP initiator

To protect the L2TP tunnel between the corporate gateway (LNS) and the client, configure a VPN. This is exactly the same VPN configuration as the one described in 7.3.2, “Configuring the L2TP VPN connection on the initiator (AS25b)” on page 291.

8.3.3 Configuring IP filters in the L2TP client AS/400 system (AS25b)

As usual, you must configure filters to complete the VPN configuration. This is exactly the same IP filter configuration as the one described in 7.3.3, “Configuring IP filters in the L2TP client AS/400 system (AS25b)” on page 304.

8.3.4 Configuring a virtual PPP connection on the L2TP initiator (AS25b)

To enable the L2TP support on the initiator of the voluntary tunnel, you must configure a virtual PPP connection. Notice that the physical dial-up PPP connection to the ISP configured in 8.3.1, “Configuring the PPP dial-up connection to the ISP (AS25b)”, only represents the physical link to the ISP. This physical connection could be a LAN link (since it is on the LNS or terminator end of the L2TP tunnel in AS05) or a leased PPP connection profile.

Perform the following steps to configure a virtual PPP connection on AS25b:

1. Start Operations Navigator.
2. Expand the AS/400 system, in this case, **AS25B**.
3. Expand **Network**.
4. Expand **Point-to-Point**.
5. Right-click **Connection Profiles**, and select **New Profile** as shown in Figure 379.

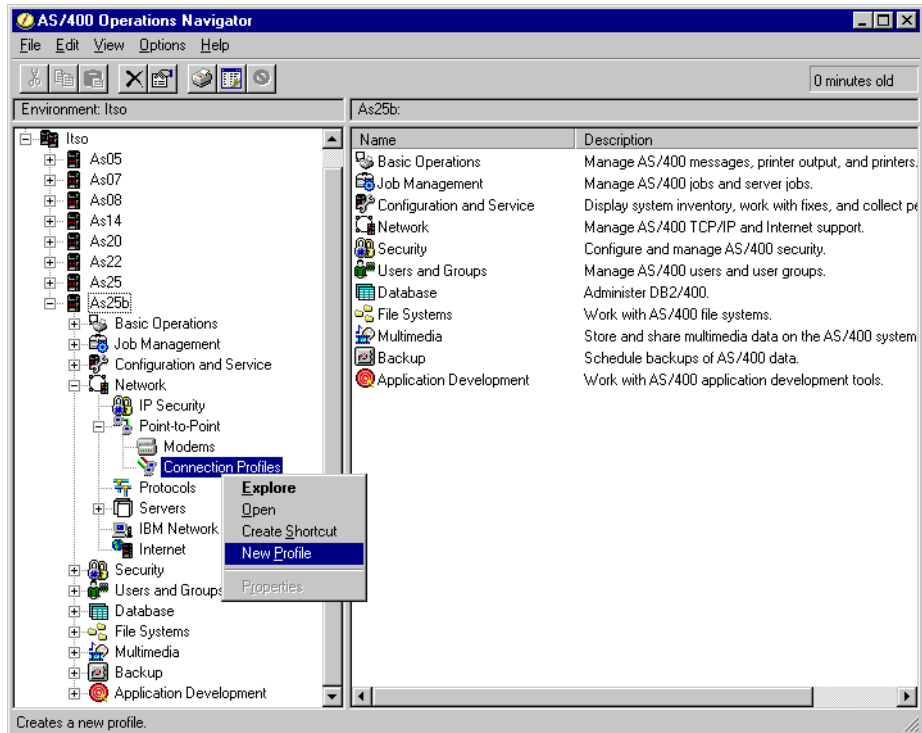


Figure 379. Operations Navigator - Connection Profiles -> New Profile

6. Enter the name `Gtoginit` for the profile name, and enter a description.
7. Select Mode-Line connection type **Virtual Line (L2TP)**
8. Select Mode type **Initiator**. See Figure 380 on page 335.

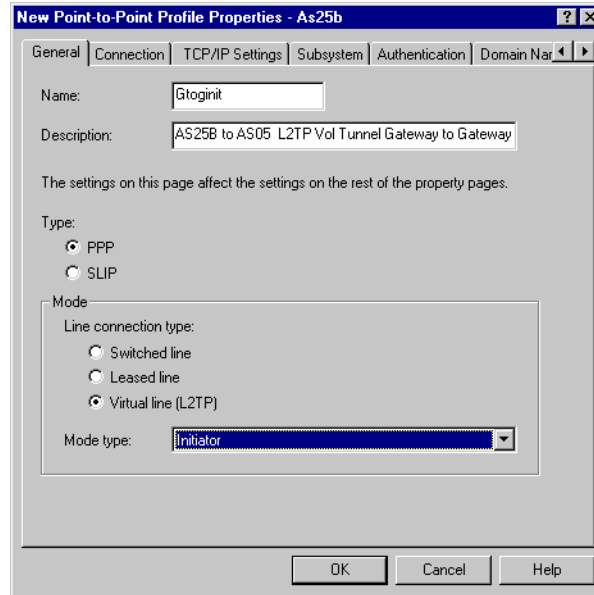


Figure 380. AS25b New point-to-point connection profile - General window

9. Click the **Connection** tab.
10. For the Virtual line name, we are re-using the line description AS05L2TP created in 7.3.4, "Configuring a virtual PPP connection on the L2TP initiator (AS25b)" on page 311.
11. For the Remote tunnel endpoint IP address, specify the globally routable IP address of the LNS, **204.146.18.5**.
12. Click **Requires IPsec Protection** to start the IPsec tunnel when the virtual PPP connection starts.
13. Select **AS25btoAS5** as the Connection group name from the pull-down menu. This is the L2TP connection (IPSec tunnel) that you created in 8.3.2, "Configuring the L2TP VPN connection on the L2TP initiator" on page 333.

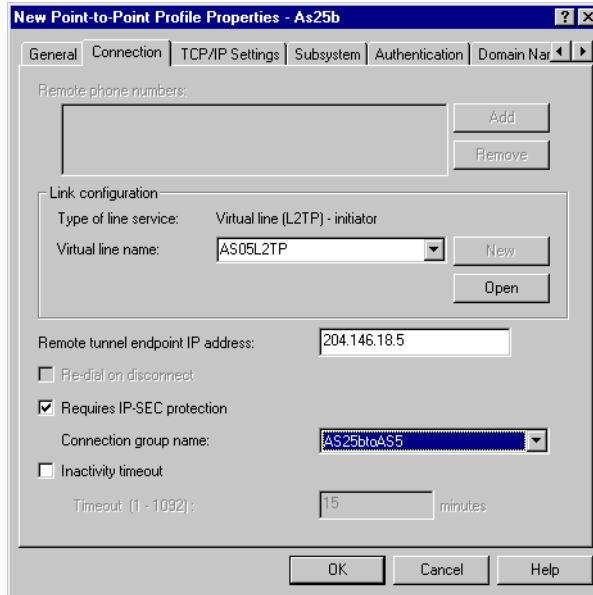


Figure 381. AS25b L2TP initiator profile - Connection window

14. Click the **TCP/IP Settings** tab.

15. Select **Dynamically assign** for Local IP address and Remote IP address as shown in Figure 382.

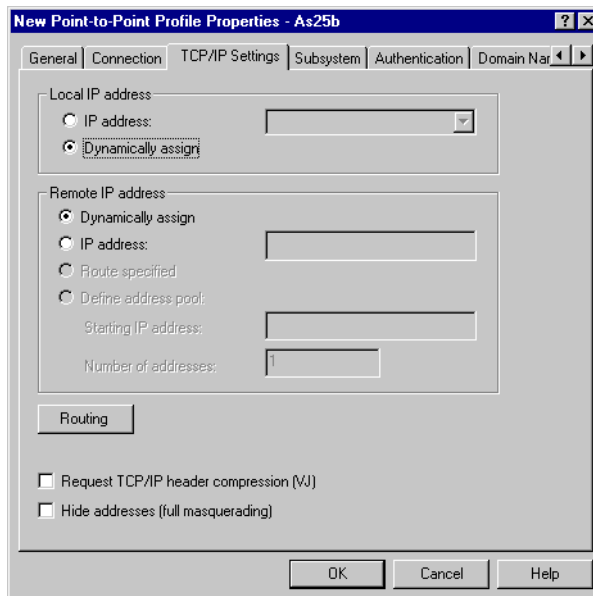


Figure 382. AS25b TCP/IP settings on the virtual PPP link

16. Click the **Routing** button.

17. Select Static routing - **Use static routes**.

18. Click **Add** to add a route to the corporate network as shown in Figure 383 on page 337.

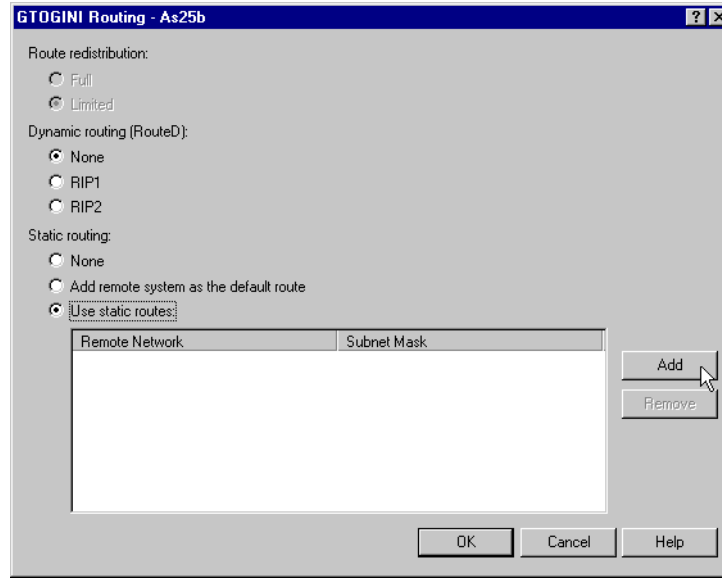


Figure 383. AS25b Adding a static route to the corporate network

19. Fill in the Add Routes for PPP Dial Parameters pointing to the corporate network subnet as shown in Figure 384. For this scenario, Remote network is 10.80.21.0, and Subnet mask is 255.255.255.0. Refer to Figure 367 on page 325.

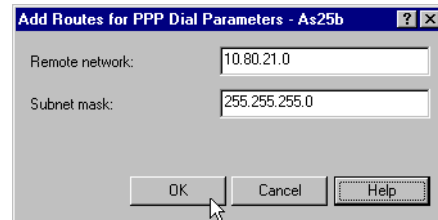


Figure 384. Add Routes for PPP Dial Parameters window

20. Click **OK**. The added route is displayed as shown in Figure 385 on page 338.

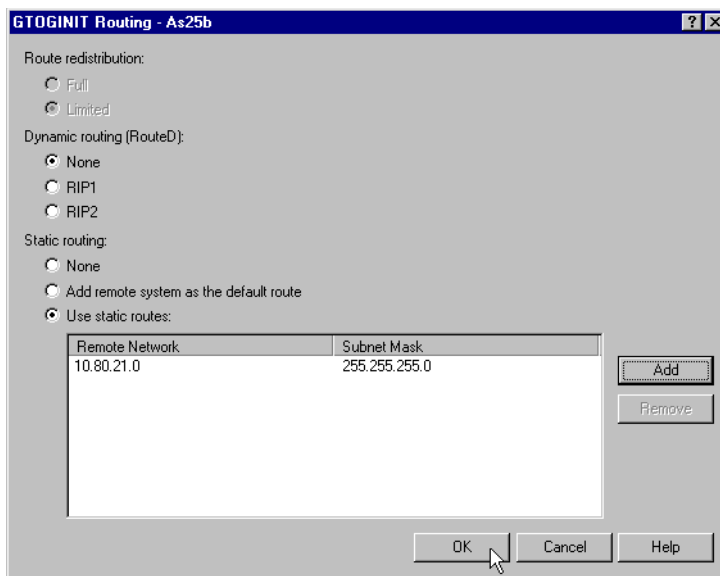


Figure 385. AS25b Static routes

21. Click **OK**.

22. Click the **Authentication** tab.

23. Select **Enable local system identification** and **CHAP only**.

24. Enter the local system User name (**AS25B**) and Password. These values must match the remote system validation list configured in step 27 on page 332. See Figure 386.

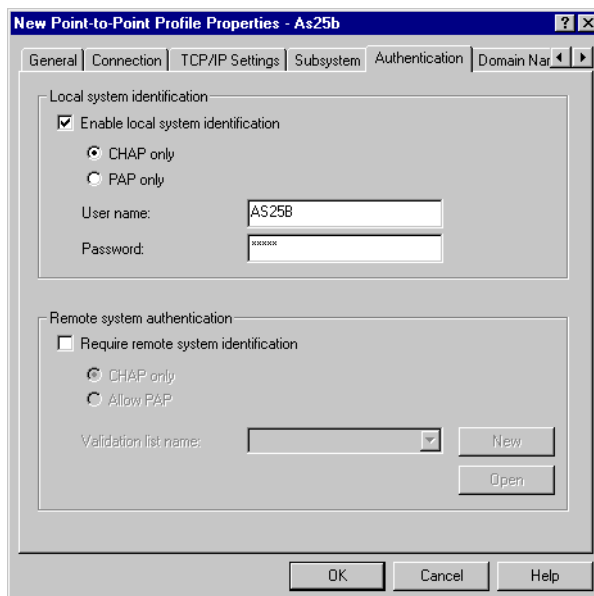


Figure 386. Authentication tab for point-to-point profile

25. Click **OK** to create the virtual PPP connection profile.

8.4 Starting the connections in an L2TP voluntary tunnel with IPsec

This section provides a summary of the tasks you need to perform to start all the required connections in an L2TP voluntary tunnel protected by IPsec.

8.4.1 Starting the LNS in an L2TP voluntary tunnel (AS05)

To start all the functions needed in the LNS (AS05), perform the following tasks:

1. Start filters.
2. Start Virtual Private Networking.
3. Start the L2TP terminator profile by following these steps:
 - a. Expand **Network**.
 - b. Expand **Point-to-Point**, and click **Connection profiles**.
 - c. Right-click on the virtual line for the L2TP terminator, **Gtogleterm**, and select Start from the pull-down menu shown in Figure 387.

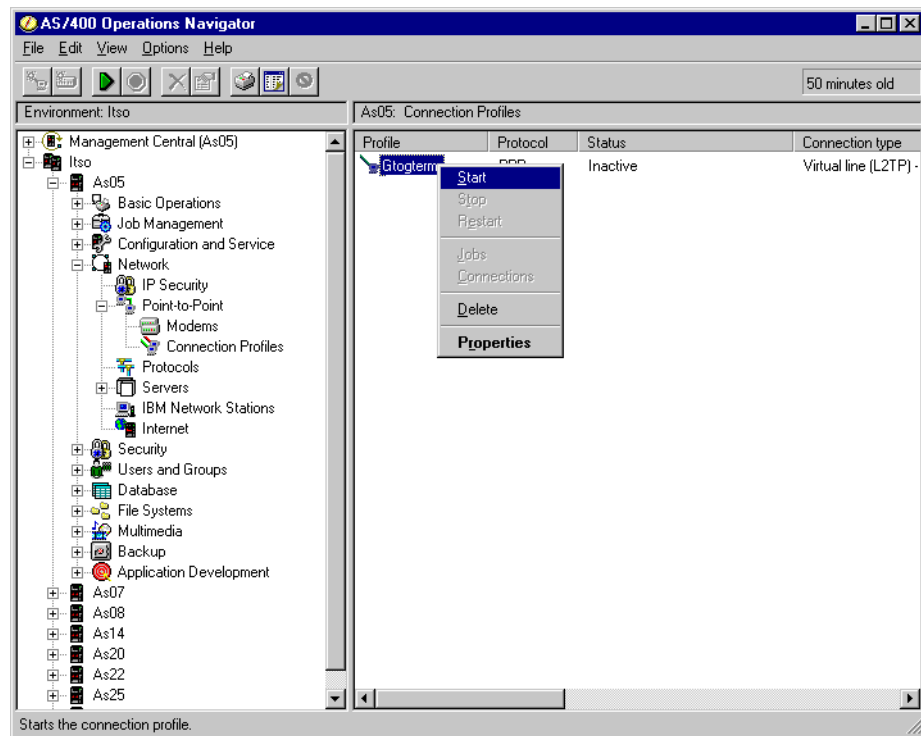


Figure 387. AS05 Starting the LNS terminator profile

After a short delay and assuming there are no errors, the profile status indicates `Waiting for connection requests` as shown in Figure 388 on page 340.

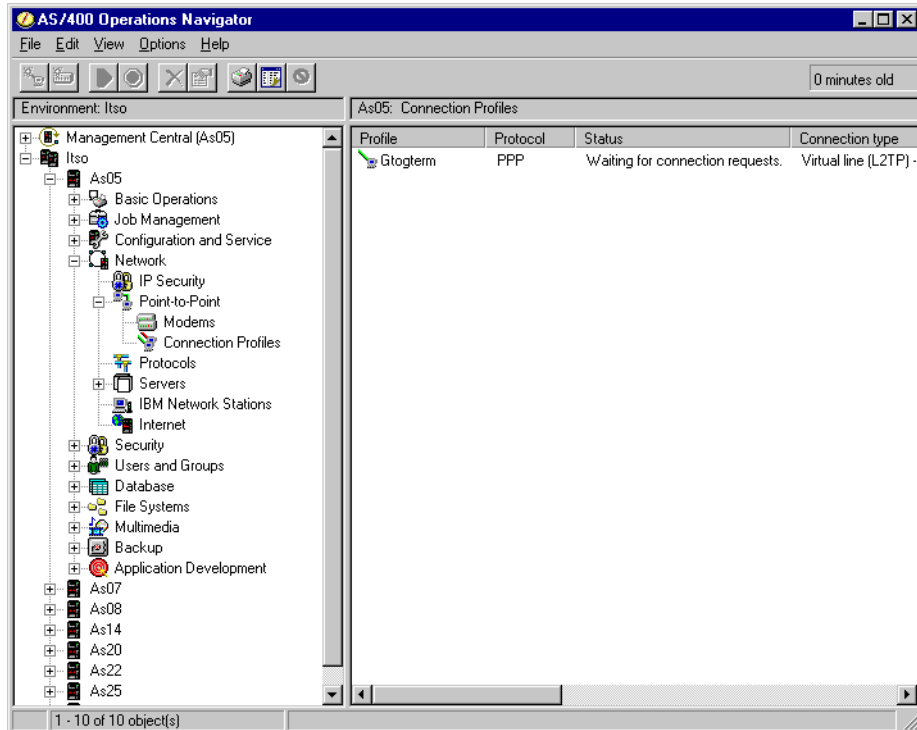


Figure 388. AS05 LNS terminator profile waiting for connection requests

8.4.2 Starting the L2TP initiator in an L2TP voluntary tunnel (AS25b)

To start all the functions needed in the L2TP client or LAC (AS25b), perform the following tasks:

1. Start filters.
2. Start Virtual Private Networking.
3. Start the physical PPP dial-up connection (PPPDIALUP) to the ISP:
 - a. From Operations Navigator, expand **Network->Point-to-Point**.
 - b. Click **Connection profiles**.
4. Right-click the physical PPP profile **PPPDIALUP**, and select **Start** from the pull-down menu as shown in Figure 389 on page 341.

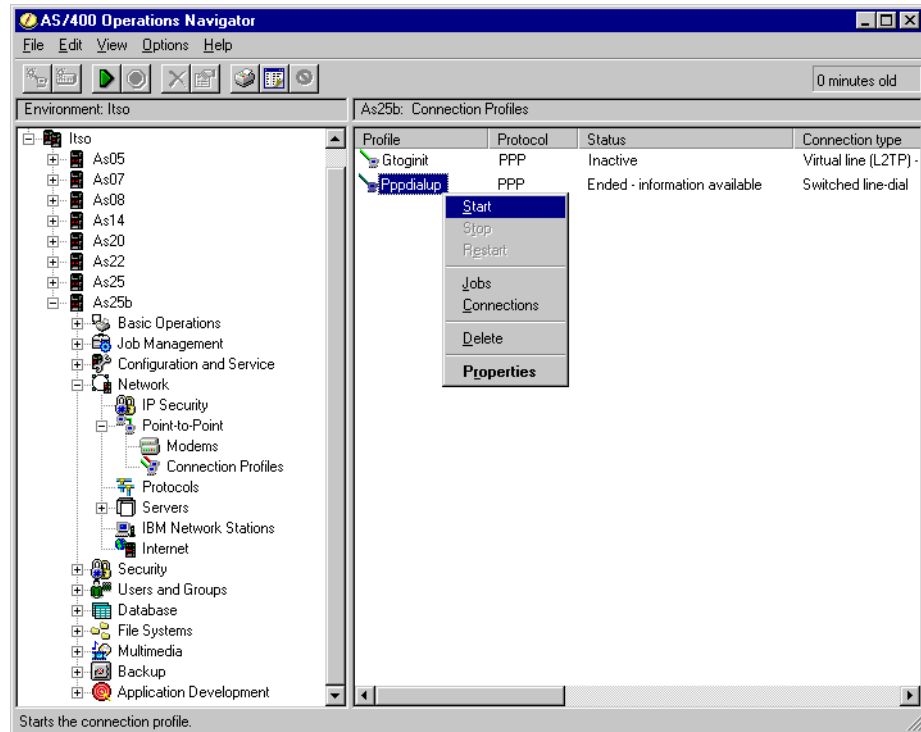


Figure 389. AS25b Starting the PPP dial-up profile to the ISP

5. Start the L2TP initiator profile by following these steps:
 - a. From Operations Navigator, expand **Network->Point-to-Point**.
 - b. Click **Connection profiles**.
 - c. Right-click the virtual PPP L2TP initiator profile **Gtugini**, and select **Start** from the pull-down menu as shown in Figure 390 on page 342.

This activates the L2TP tunnel and starts the VPN L2TP connection on the initiator automatically.

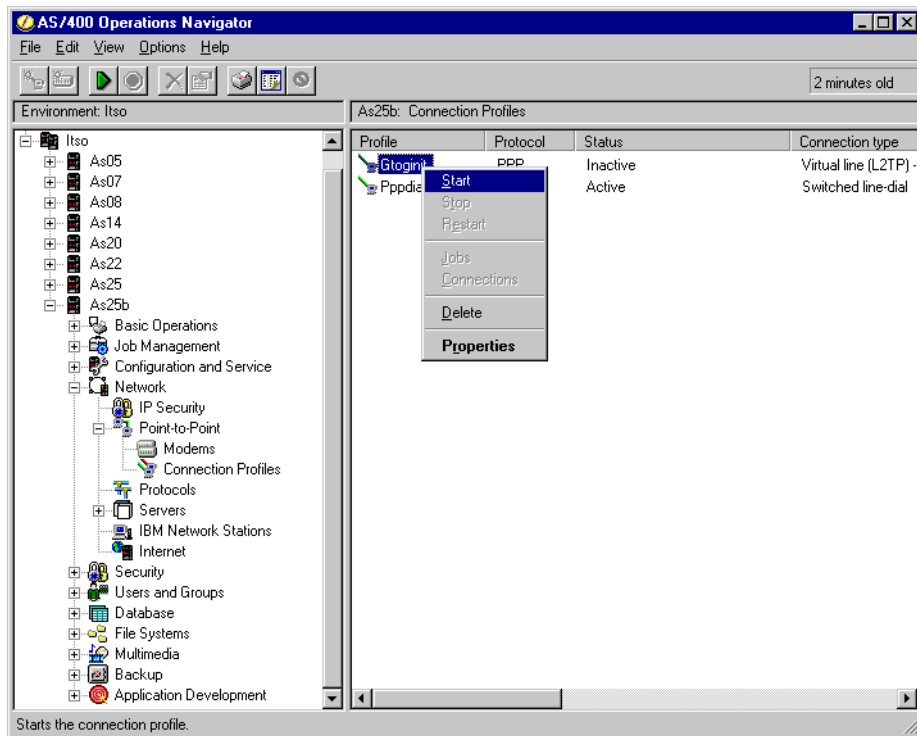


Figure 390. AS25b Starting the L2TP client initiator profile

Once the L2TP tunnel establishment is completed, the LAC initiator profile shows a status of Active Connections (Figure 391).

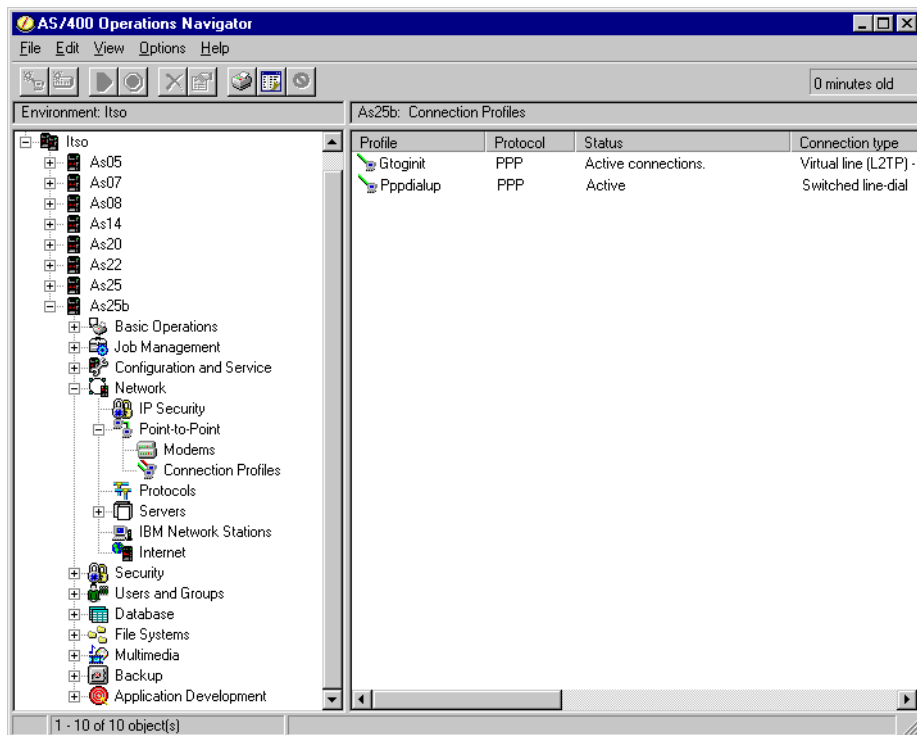


Figure 391. AS25b Active PPP and LAC initiator profiles

8.4.3 Verifying the VPN connection status

In an L2TP tunnel protected by IPsec, the VPN connection is activated when the L2TP initiator profile starts as described in step 5 on page 341.

To verify the status of the VPN connection that protects the L2TP tunnel, perform the following steps:

1. From Operations Navigator, expand **Network->IP Security**.
2. Double-click **Virtual Private Networking** to start the VPN GUI.
3. From the file menu, select **View->Active Connections** as shown in Figure 392.

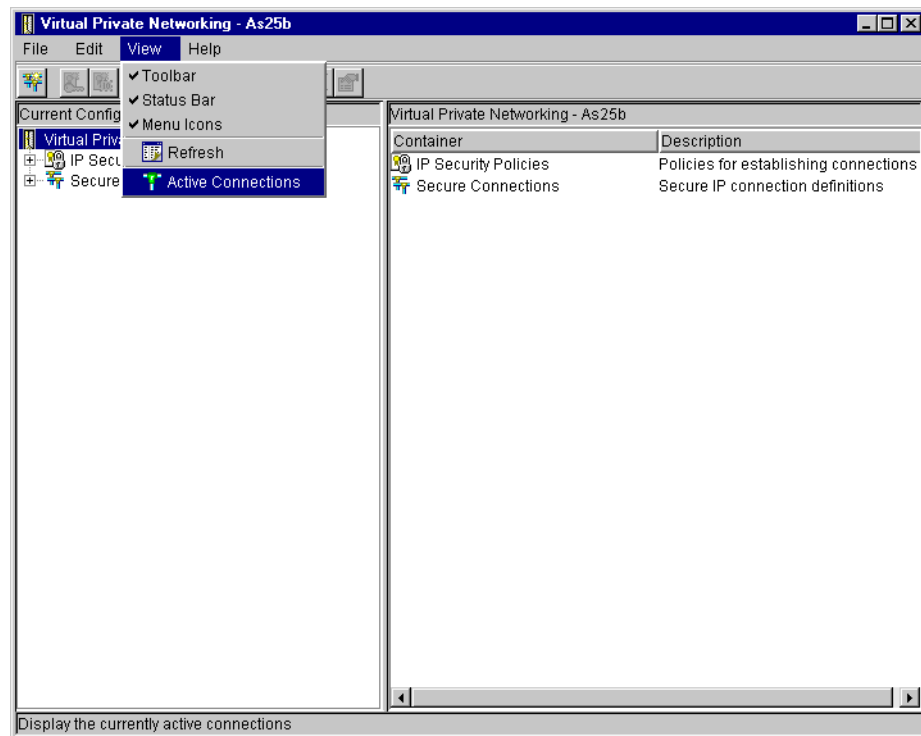


Figure 392. AS25b Verifying the status of the VPN connection

The Active Connections window displays the active IPsec connection that protects the L2TP tunnel as shown in Figure 393.

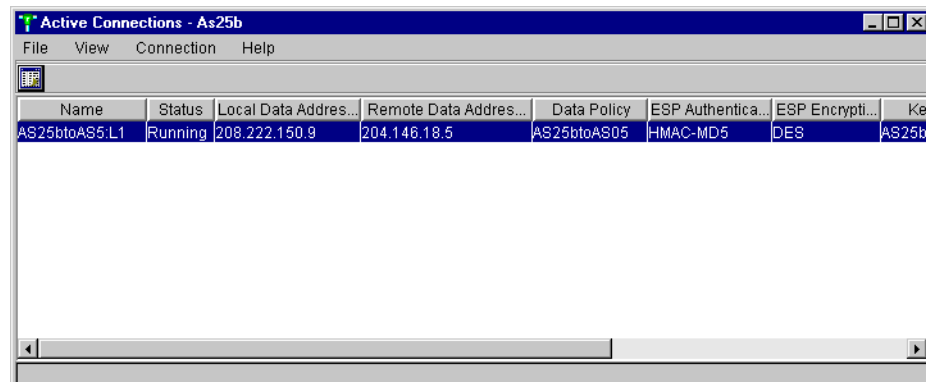


Figure 393. AS25b VPN Active Connections window

8.5 Verifying interfaces and routes

Although TCP/IP routing and transparent subnetting concepts are beyond the scope of this redbook, this section reviews the interfaces and routes in the LNS (AS05) and the L2TP client (AS25b).

8.5.1 Verifying IP interfaces in the L2TP client (AS25b)

Figure 394 shows the result of entering the command `NETSTAT OPTION(*IFC)` in AS25b.

```
Work with TCP/IP Interface Status                               System:  AS25B
Type options, press Enter.
 5=Display details      8=Display associated routes  9=Start  10=End
12=Work with configuration status  14=Display multicast groups

      Internet      Network      Line      Interface
      Address      Address      Description  Status
(A)  10.80.21.193  10.80.21.193  L22F1C0001  Active
(B)  10.80.21.254  10.80.21.192  FWCMN04     Active
(C)  127.0.0.1     127.0.0.0    *LOOPBACK   Active
(D)  208.222.150.9 208.222.150.9 PPPDIALUP    Active

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F11=Display line information  F12=Cancel
F13=Sort by column  F24=More keys
```

Figure 394. AS25b TCP/IP interfaces

The following points are worth noting (refer to Figure 394):

- Interface **A** (10.80.21.193, with subnet mask is 255.255.255.255) is dynamically assigned to the L2TP initiator (AS25b) by the LNS when the L2TP tunnel is established. This interface is added when the virtual PPP profile starts. This is the branch office gateway interface to the corporate office network. This is the local IP address of the virtual Point-to-Point connection. Hosts on the corporate office network (network B in Figure 367 on page 325) use interface **A** as the destination IP address when they need to reach AS25b. Interface **A** is bound to the virtual L2TP line description (L22F1C0001).
- Interface **B** (10.80.21.254, with subnet mask is 255.255.255.192) was manually configured using the Add TCP Interface (`ADDTCPIFC`) command. It is bound to the Token-Ring line description FWCMN04. This is the branch office gateway interface to the internal branch office network (network A).
- Interface **C** (127.0.0.1, with subnet mask 255.0.0.0) is the loopback interface. This IP address is configured on the system when the TCP/IP stack is installed. This is a virtual IP address and is not bound to any physical line. It is used for internal diagnostics and for internal communications only. A packet with a source or destination address of 127.x.x.x is never transmitted outside of the system.
- Interface **D** (208.222.150.9, with subnet mask 255.255.255.255) is dynamically assigned to AS25b when the dial-up PPP connection to the ISP is established. This is a routable IP address on the Internet. AS25b can access the Internet directly through this IP address. Conversely, other hosts on the Internet can access AS25b. The filters configured in this scenario prevent all

traffic, except for the L2TP tunnel, from using this interface. This interface is bound to the physical dial-up PPP profile PPPDIALUP. This interface is added when the physical PPP profile is started.

8.5.2 Verifying routes in the L2TP client (AS25b)

Figure 395 shows the TCP/IP route information in AS25b as a result of entering the `NETSTAT OPTION(*RTE)` command.

Display TCP/IP Route Information					System: AS25B
Type options, press Enter.					
5=Display details					
Opt	Route Destination	Subnet Mask	Next Hop	Route Available	
(E)	10.80.21.192	255.255.255.192	*DIRECT	*YES	
(F)	10.80.21.193	*HOST	*DIRECT	*YES	
(G)	10.80.21.111	*HOST	10.80.21.193	*YES	
(H)	10.80.21.0	255.255.255.0	10.80.21.193	*YES	
(J)	127.0.0.0	255.0.0.0	*DIRECT	*YES	
(K)	208.222.150.9	*HOST	*DIRECT	*YES	
(L)	208.222.150.1	*HOST	208.222.150.9	*YES	
(M)	*DEFROUTE	*NONE	208.222.150.9	*YES	
					Bottom
F3=Exit		F5=Refresh		F6=Print list	
F11=Display route type		F12=Cancel		F9=Command line	
				F13=Sort by column	
				F24=More keys	

Figure 395. AS25b Route information

The following points are worth noting (refer to Figure 395):

- Route **E** is the route to the internal branch office network (network A in Figure 367 on page 325). The branch office gateway (AS25b) routes all traffic for subnet 10.80.21.192 (with the exception of 10.80.21.193 and 10.80.21.254 that are local interfaces) through interface **B** in Figure 394 on page 344. Interface **B** is bound to the Token-Ring line FWCMN04. Next hop *DIRECT indicates that the AS/400 system has a direct connection to this network (interface **B**, 10.80.21.254).
- Route **F** is a host route to 10.80.21.193, which is a local interface. The subnet is *HOST or 255.255.255.255, making this a network of one host. This route is only used by the AS/400 system as a place holder since there are multiple interfaces into different TCP/IP networks. The next hop is set to *DIRECT since the AS/400 system has a direct connection into this network address, interface 10.80.21.193 (**A**).
- Route **G** is a host route to the host 10.80.21.111. The subnet is *HOST or 255.255.255.255, which makes this a network of one host. The next hop is set to 10.80.21.193. Route **F** and **G** represent the two endpoints of the Virtual PPP connection. The AS/400 system realizes that to reach the 10.80.21.111 host (this is really a network of one Host) it must use the local interface of 10.80.21.193 (**A**). This interface is bound to the virtual L2TP line description and will send the packets out through the dial-up connection. This route is added when the virtual PPP connection is started.
- Route **H** is a network route to the corporate office network (network B in Figure 367 on page 325, 10.80.21.0, with subnet mask 255.255.255.0). The

next hop is set to 10.80.21.193. The AS/400 system routes all traffic for network B to the local interface of 10.80.21.193 (**A**), which is bound to the virtual L2TP line description and sends the packets out the dial-up connection. This route is added when the virtual PPP connection is started. The static route was configured in step 18 on page 336 in the virtual PPP initiator profile.

- Route **J** is a network route to the loopback 127.0.0.0 network, subnet 255.0.0.0. The next hop is *DIRECT and is used for internal communications only.
- Route **K** is a host route to the 208.222.150.9 network. The subnet is *HOST or 255.255.255.255, which makes it a network of one host. The next hop is set to *DIRECT since the AS/400 system has a direct connection to this network address, the interface 208.222.150.9 (**D**).
- Route **L** is a host route to the 208.222.150.1 network. The subnet is *HOST or 255.255.255.255, which makes this a network of one host. The next hop is set to 208.222.150.9. Routes **K** and **L** represent the two endpoints of the physical dial-up PPP connection to the ISP. This routing information tells the AS/400 system to use the local interface 208.222.150.9 (**D**) to reach the ISP (208.222.150.1). Interface **D** is bound to the physical dial-up PPP connection, PPPDIALUP. This route is added when the physical dial-up PPP profile is started.
- Route **M** is the *DFTRROUTE (network 0.0.0.0, with subnet *NONE). Any address that has not been processed by an earlier route entry matches this network address. The next hop is the IP address 208.222.150.9 (interface **D**). This is the IP address assigned by the ISP. The AS/400 system forwards IP packets with a destination IP address that does not match more specific routes, to the *DFTRROUTE. This route is added when the physical PPP profile is started. This route is configured in the physical PPP dial-up profile (PPPDIALUP).

8.5.3 Verifying IP interfaces in the LNS (AS05)

Figure 396 shows the result of the NETSTAT OPTION(*IFC) command in AS05.

```

Work with TCP/IP Interface Status
System: AS05
Type options, press Enter.
 5=Display details  8=Display associated routes  9=Start  10=End
12=Work with configuration status  14=Display multicast groups

      Internet      Network      Line      Interface
Opt Address         Address      Description Status
(A)  10.80.21.111    10.80.21.0  ITSCTRNO  Active
(B)  10.80.21.193    10.80.21.192 L256FC0001 Active
(C)  127.0.0.1       127.0.0.0   *LOOPBACK Active
(D)  204.146.18.5    204.146.18.0 TRLANC    Active

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F11=Display line information  F12=Cancel
F13=Sort by column  F24=More keys

```

Figure 396. AS05 TCP/IP interfaces

The following points are worth noting (refer to Figure 396 on page 346):

- Interface **A** (10.80.21.111, with subnet mask is 255.255.255.0 and creates network address 10.80.21.0) was manually configured using the Add TCP Interface (ADDTCPIFC) command. It is bound to the Token-Ring line description ITSCTRNO. This is the corporate office gateway interface to the internal corporate office network (network B in Figure 367 on page 325).
- Interface **B** (10.80.21.193, with subnet mask of 255.255.255.192 creating a network address 10.80.21.192). This is the IP address that the LNS (AS05) assigns to AS25b when the virtual PPP connection is established. It is the interface that enables AS05 to perform proxy ARP for all hosts in the branch office network (10.80.21.192). The remote branch office gateway (AS25b represented by interface **B**) appears as a local interface in the LNS. This interface is added when the virtual PPP connection is started.

Figure 397 shows the details that are displayed by selecting option 5 (Display details), for interface **B** (10.80.21.193) in Figure 396.

```

                                Display TCP/IP Interface Status
                                System:   AS05
Interface host name . . . . . :
Internet address . . . . . : 10.80.21.193
  Subnet mask . . . . . : 255.255.255.192
  Network address . . . . . : 10.80.21.192
  Host address . . . . . : 0.0.0.1
  Directed broadcast address . . . . . : *NONE

Interface status . . . . . : Active
Change date/time . . . . . : 07/29/99 10:41:04
Line description . . . . . : L2428C0001
Line type . . . . . : *NOTFND
Associated local interface . . . . . : 10.80.21.111
Type of service . . . . . : *NORMAL
Maximum transmission unit . . . . . : 2046
Automatic start . . . . . : *NO

Press Enter to continue.

F3=Exit  F6=Print  F12=Cancel  F22=Display entire field

```

Figure 397. AS05 Associated local interface to perform proxy ARP for remote branch office network

Notice the associated local interface 10.80.21.111. When hosts in the corporate network broadcast ARP requests with destination IP address in the branch office network (10.80.21.192), AS05 recognizes that it has a direct route to the destination network since interface **B** appears to be local. AS05 responds to ARP requests on behalf of hosts in network 10.80.21.192 by sending back the MAC address corresponding to the associated local interface 10.80.21.111. Once the packet reaches AS05, it knows how to route it to the remote network through the virtual L2TP line (L2428C00001 in Figure 397).

- Interface **C** (127.0.0.1, subnet mask 255.0.0.0) is the loopback interface. This IP address is configured on the system when the TCP/IP stack is installed. This is a virtual IP address and is not bound to any physical interface. It is used for internal diagnostics and for internal communications

only. A packet with a source or destination address of 127.x.x.x is never transmitted outside of the system.

- Interface **D** (204.146.18.5, subnet mask of 255.255.255.0, which creates a network address of 204.146.18.0) is a routable IP address on the Internet. AS05 can access the Internet directly through this IP address. Conversely, other hosts on the Internet can access AS05. This is the non-secure interface of the corporate gateway. The filters configured in this scenario prevent all traffic except for the L2TP tunnel from using this interface. This interface is bound to a LAN line (TRLANC) that is connected to the ISP router.

8.5.4 Verifying routes in the LNS (AS05)

Figure 398 shows the TCP/IP route information in AS25b as a result of entering the `NETSTAT OPTION(*RTE)` command.

```

Display TCP/IP Route Information
System: AS05
Type options, press Enter.
5=Display details

Route      Subnet      Next      Route
Opt Dest      Mask       Hop       Avail
(E) 10.80.21.192 255.255.255.192 *DIRECT *YES
(F) 10.80.21.0 255.255.255.0 *DIRECT *YES
(G) 127.0.0.0 255.0.0.0 *DIRECT *YES
(H) 204.146.18.0 255.255.255.0 *DIRECT *YES
(J) *DFROUTE *NONE 204.146.18.1 *YES

Bottom
F3=Exit F5=Refresh F6=Print list F9=Commandline
F11=Display route type F12=Cancel F13=Sort by column F24=More keys

```

Figure 398. AS05 Route information

The following points are worth noting (refer to Figure 398):

- Route **E** is the route to the remote branch office associated with interface 10.80.21.193 (**B**). IP traffic to the remote network is routed to the virtual L2TP line and, in turn, to the physical LAN line (TRLANC) connected to the ISP router. This route is added when the virtual PPP profile is started.
- Route **F** is the route to the corporate network associated with the interface 10.80.21.111 (**A**). This route is added when TCP/IP is started. IP traffic for the subnet 10.80.21.0 with the exception of 10.80.21.111 and the subnet partition of 10.80.21.192 is routed out AS05 through interface **A** that is bound to the physical line description ITSCTRNO. Traffic destined for 10.80.21.111 is not routed out the system because AS05 recognizes it as a local interface. Due to transparent subnetting, route **E**, and proxy ARP, traffic for subnet partition 10.80.21.192 is routed through route **E**.
- Route **G** is a network route to the loopback 127.0.0.0 network, subnet 255.0.0.0. The next hop is *DIRECT and is used for internal communications only.
- Route **H** is associated with the interface 204.146.18.5 (**D**). Traffic for this network with the exception of 204.146.18.5 is routed out the system through interface **D**. This route is added when TCP/IP starts.

- Route **J** is the *DFTRROUTE (network 0.0.0.0, subnet *NONE). Any address that has not been processed by an earlier route entry matches this network address. The next hop is the IP address of 204.146.18.1. This is the IP address assigned of the ISP router. The AS/400 system forwards IP packets with a destination IP address that does not match more specific routes to the *DFTRROUTE. This route is added when TCP/IP starts.

Chapter 9. L2TP compulsory tunnel

In compulsory tunneling, a tunnel is created without any action from the initiator client. The dial-in client sends PPP packets to the ISP, which encapsulates them in L2TP (Layer 2 tunneling protocol) and tunnels them to the corporate office gateway. In this case, the ISP *must* be L2TP capable. In this model, the ISP is referred to as the L2TP Access Concentrator (LAC), and the corporate office gateway is referred to as L2TP Network Server (LNS). Refer to Chapter 2, “Introduction to Layer 2 Tunneling Protocol (L2TP)” on page 33, for general information on L2TP compulsory tunneling.

9.1 Branch office to main office connection using L2TP compulsory tunnel

This chapter presents a branch office AS/400 system (AS25b) connected to the corporate office network through a gateway AS/400 system (AS05) in an L2TP tunnel protected by IPsec. Figure 399 shows an overview of the network presented in this chapter.

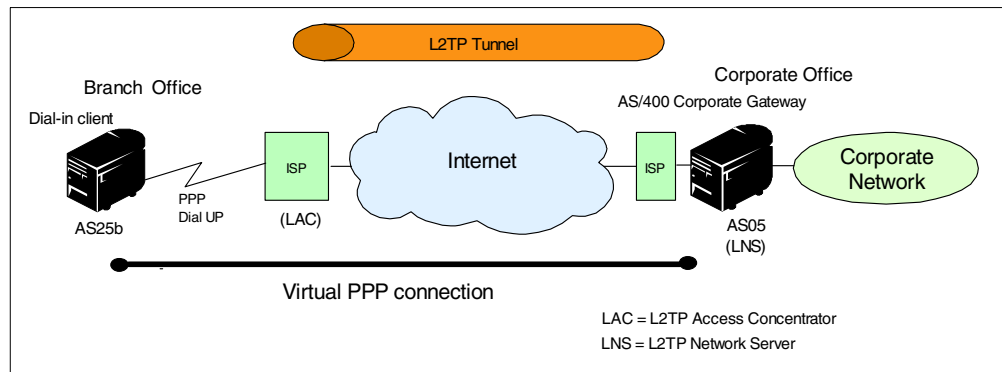


Figure 399. L2TP compulsory tunnel network overview

Important note

All the scenarios in this redbook show the AS/400 security gateway at the corporate office directly connected to the Internet. The absence of a firewall in these redbook scenarios is meant to simplify the VPN examples. It does *not* imply that the use of a firewall is unnecessary. For information about how the AS/400 security gateway interacts with a firewall, refer to Chapter 12, “Don’t forget a firewall: Protecting your VPN server” on page 515.

9.1.1 Scenario characteristics

The main characteristics of this scenario are:

- The AS/400 system at the remote branch office (AS25b) is the only system at the branch office network that needs access to the corporate network. In other words, its role is that of a host, not a gateway, for the branch office network.
- The AS/400 system at the corporate office (AS05) is the gateway into the corporate office network.

- The AS/400 system at the branch office connects to the corporate office through the Internet backbone by dialing up an ISP using a dial-up PPP connection.
- The AS/400 system at the branch office (AS25b) authenticates itself by user name and password.
- The number of remote branch offices is relatively small (30 or less).
- The ISP provides L2TP Access Concentrator (LAC) services. Therefore, there is no need to configure L2TP support on the branch office AS/400 system (AS25b).
- The routable IP addresses of the ISP routers may change without prior notification to the customer. The ISP router providing the LAC function identifies itself by key identifier.

9.1.2 Scenario objectives

The objectives of this scenario are:

- The AS/400 system at the branch office (AS25b) must be regarded as a system in the corporate office network. To achieve this objective, the LNS (AS05) assigns to AS25b an IP address in the corporate office address space. This is a fixed IP address based on the user name that AS25b sends during the authentication phase.
- The ISP LAC does *not* assign a globally routable IP address to the AS/400 system at the branch office. Because of this, two objectives are met:
 - The remote AS/400 system at the branch office cannot be accessed from the Internet. Therefore, it is protected from intrusions.
 - The remote AS/400 system can only access the Internet through the corporate gateway. Therefore, it is subjected to the same rules and limitations as other systems in the corporate network.
- The tunnel between the branch office AS/400 system (AS25b) and the LNS (AS05) must be protected with IPSec ESP encryption and authentication. To achieve this objective, and since the IP address assigned to AS25b is known because it is assigned by the LNS, configure a gateway-to-host dynamic key connection on the LNS (AS05). Configure a host-to-gateway dynamic key connection on the remote client (AS25b).
- The tunnel between the ISP LAC and the LNS must be protected with IPSec AH transforms to authenticate the tunnel endpoints. Since the IP address of the ISP router may change, configure a dynamic IP group at the LNS (AS05).

9.1.3 Scenario network configuration

Figure 400 on page 353 shows the test network used in this scenario.

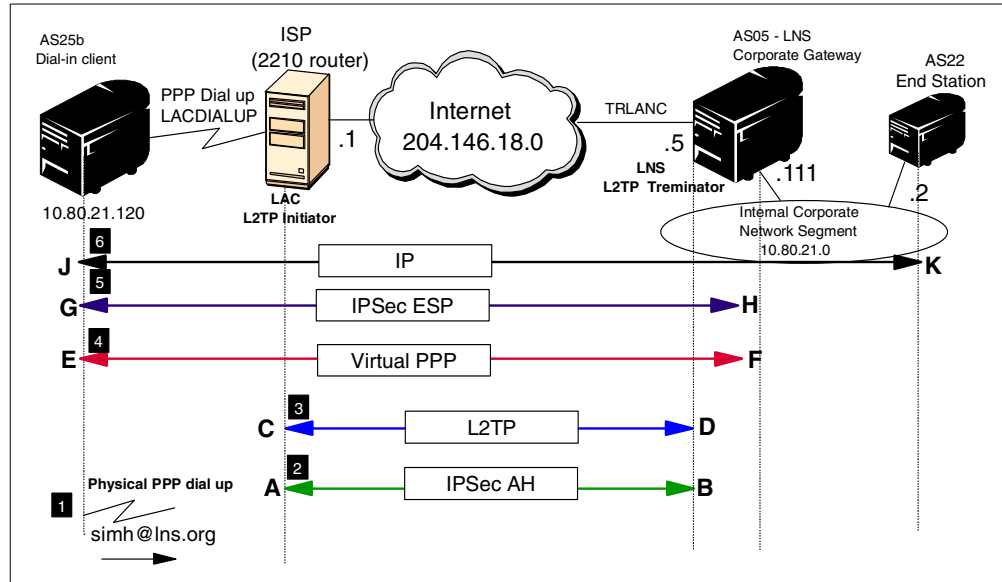


Figure 400. L2TP compulsory tunnel with IPsec test network

The time line of events that take place to establish an L2TP compulsory tunnel protected by IPsec is as follows (refer to Figure 400):

- 1** The PPP client (AS25b) dials the ISP and establishes a PPP dial-up session between the dial-in client and the ISP. The client identifies itself by sending a user name (simh@lms.org in our scenario) and password.
- 2** The LAC function in the ISP is configured to contact the LNS (AS05) based on the AS25b identifier. The IPsec AH tunnel is established between the ISP (A) router and AS05 (B).
- 3** The LAC forwards the client's user name and password to the LNS for CHAP authentication. If the user is valid, the LAC and the corporate gateway establish the tunnel and assign a session ID that identifies the user of the tunnel. The L2TP tunnel is established between the ISP LAC (C) and AS05 LNS (D). The L2TP tunnel is protected by the previously established IPsec AH tunnel.
- 4** Once the LNS authenticates the user and the L2TP tunnel is established, the client and the corporate gateway negotiate the PPP session by setting up protocols and allocating network addresses to the client. The LNS (AS05) assigns an IP address (10.80.21.120) from the corporate network address space to the client (AS25B) as configured in the LNS static routes. The virtual PPP connection is established between AS25b (E) and AS05 (F). In this model, the tunneling process is transparent to the client.
- 5** With the IP address assigned, the client can initiate the IPsec ESP tunnels that protect the connection between the branch office host (AS25b) and the corporate gateway (AS05). The IPsec ESP tunnel between AS25b (G) and AS05 (H) is established.
- 6** The client sends PPP packets to the ISP and LAC, which encapsulates them in L2TP and tunnels them to the corporate gateway. IP traffic flows between AS25b (J) and any system in the corporate network, for example AS22 (K). Since AS25b

has an IP address in the corporate office address space (10.80.21.120), AS05 interface 10.80.21.111 performs proxy ARP for packets destined for AS25b. The IP address 10.80.21.111 is the associated local interface for 10.80.21.120.

9.1.4 Implementation tasks: Summary

The following is a summary of the tasks that you need to perform to implement this L2TP compulsory tunnel protected by IPsec scenario:

1. LNS configuration (AS05)
 - a. Configure the L2TP terminator profile.
 - b. Configure the IPsec AH tunnel (Dynamic IP group - Host to Hosts) to the ISP.
 - c. Configure the IPsec ESP tunnel (Dynamic Key Group - Gateway to Hosts) to the PPP client.
 - d. Configure IP filters.
2. PPP dial-in client (AS25b)
 - a. Configure a PPP dial-up connection to the ISP.
 - b. Configure the IPsec ESP tunnel to the LNS (Dynamic Key Group - Host to Gateway).
 - c. Configure IP filters.
3. Start connections
4. Verify communications

9.2 Configuring the LNS in a compulsory tunnel protected by IPsec (AS05)

The following sections take you step-by-step through the configuration of the L2TP network server (terminator profile), VPN, and filters in AS05.

9.2.1 Configuring the L2TP terminator profile (AS05)

This section explains how to configure the LNS end of the L2TP tunnel. This is represented by **F** in Figure 400 on page 353.

Table 33 provides an overview of the most important parameters in the PPP connection profile that you must consider when configuring the L2TP terminator in a compulsory tunnel. Refer to Figure 400 on page 353 for the scenario values.

Table 33. AS05 L2TP terminator profile - Parameter summary

PPP configuration parameter	Scenario value	Comment
Name	LNSto2210	Virtual PPP terminator profile
Line connection type	Virtual line (L2TP)	Physical line is Token Ring LAN (TRLANC)
Mode type	Terminator (network server)	AS05 is LNS
Local tunnel endpoint IP address	204.146.18.5	Local L2TP tunnel endpoint is the globally known IP address.

PPP configuration parameter	Scenario value	Comment
Local IP address	10.80.21.111 (Token Ring) This value must match the <i>Local key server</i> in the VPN configuration.	Interface on the internal network. This interface performs proxy ARP on behalf of the PPP client in the compulsory tunnel. It is the associated local interface associated with the IP address assigned to the remote PPP client (AS25).
Remote IP address Defined address pool: Number of addresses	10.80.21.130 5	Pool of IP address to be assigned to remote PPP clients that are <i>not</i> in the Caller User list. This parameter is not used in this scenario.
Routing	Use static routes Caller user: simh@lsn.org IP Address: 10.80.21.120 Mask: 255.255.255.255 This value must match <i>Authentication -> User name</i> in the remote client PPP connection profile.	Fixed IP addresses (in the corporate network address space) to be assigned to PPP clients that identify themselves with User name = Caller user.
Allow IP forwarding	Allow (check box)	Allow to route traffic from/to the remote PPP client and the internal network.
Authentication (VLDL) User Name Password Protocol	simh@lms.org ppp CHAP These values must match the values in the <i>Local system identification</i> at the remote PPP client.	Authenticates the remote PPP client at the end of the compulsory tunnel. Entry must reside in validation list. Note: Case sensitive.

Perform the following steps to create the virtual PPP connection on the L2TP terminator, AS05 for a compulsory L2TP tunnel:

1. From Operations Navigator, expand the **AS05** AS/400 system.
2. Click **Network->Point-to-Point**.
3. Right-click **Connection profiles**, and select **New Profile** from the menu (Figure 401 on page 356).

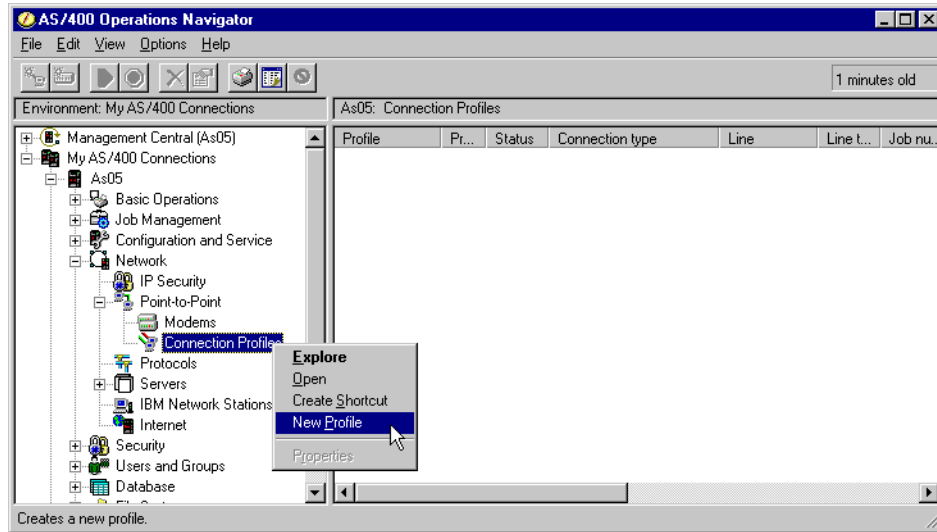


Figure 401. AS05 Creating a virtual PPP connection on the L2TP terminator

Ensure that the General tab is selected since the settings on this page affect the rest of the pages.

4. Enter LNSto2210 as the name of the virtual PPP profile.
5. Enter L2TP Compulsory Tunnel LNS - AS05 or similar for Description.
6. Select **PPP** as the type of connection.
7. Select **Virtual line (L2TP)** for the Mode parameter.
8. Select **Terminator (network server)** for the Mode - Line connection type parameter (Figure 402).

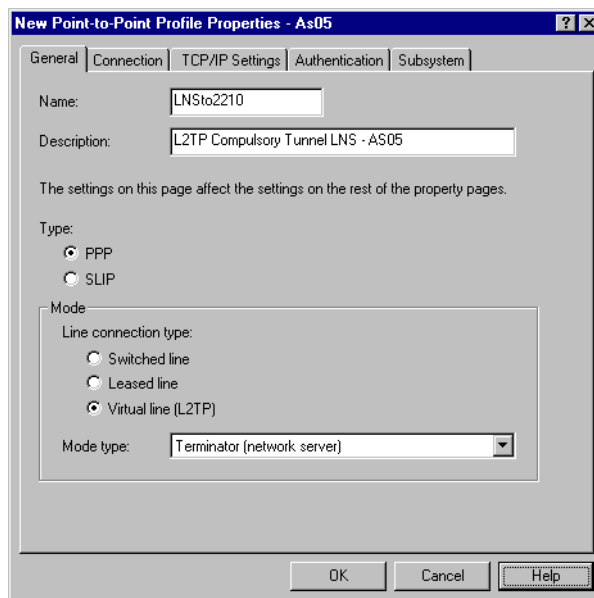


Figure 402. AS05 Creating the virtual PPP line

9. Click the **Connection** tab.

10. For the Local tunnel endpoint IP address, select **204.146.18.5** from the pull-down menu. This is the LNS globally routable IP address.
11. Enter `VLINTO2210` for the Virtual line name parameter.
12. Click **New** (Figure 403).

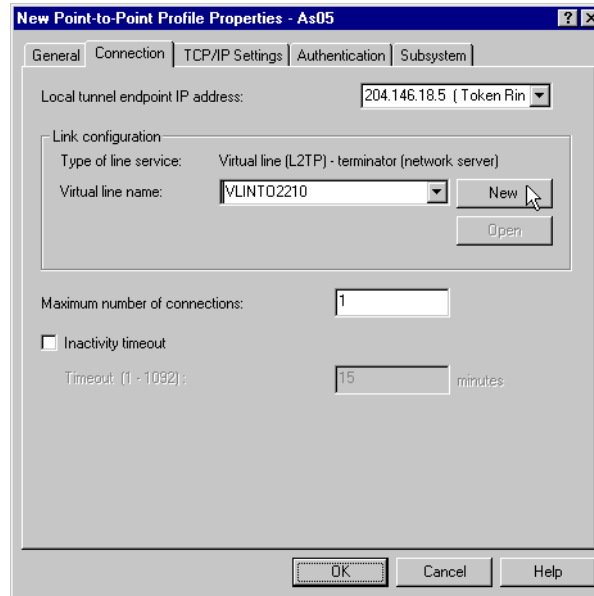


Figure 403. AS05 Defining the virtual PPP connection parameters

13. Enter `L2TP Virtual Line - AS05 LNS AS25b client` as the Description (Figure 404).

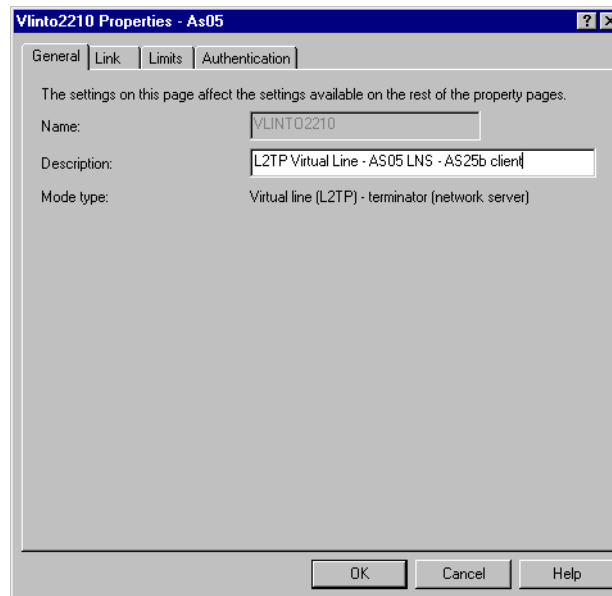


Figure 404. AS05 Entering the virtual PPP line name and description

14. Click the **Authentication** tab.
15. Enter `AS05` as the Local host name. See Figure 405 on page 358.

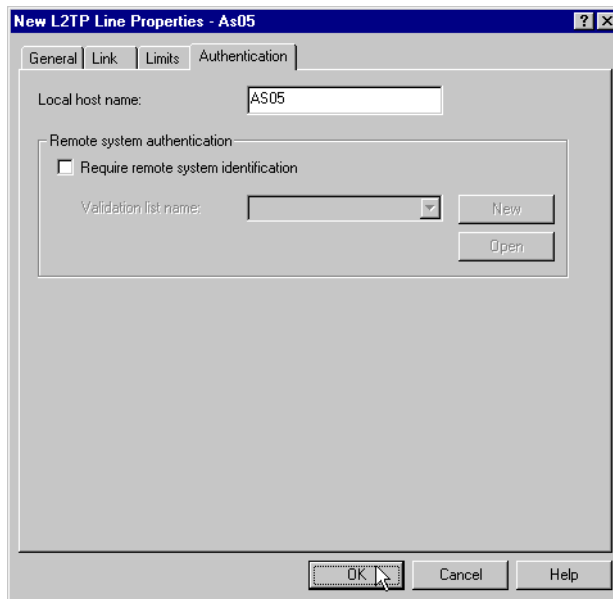


Figure 405. AS05 Virtual PPP local authentication page

16. Click **OK**.

17. Click the **TCP/IP Settings** tab.

18. For the Local IP address parameter, ensure that **IP address** is selected and select **10.80.21.111** from the pull-down menu. This is the LNS interface on the internal corporate network. This interface performs proxy ARP on behalf of the remote host. This IP address must match the local key server IP address in the IPsec tunnel between the client and the corporate gateway.

19. For the Remote IP address parameter, select **Define address pool**.

20. Enter 10.80.21.130 as the Starting IP address.

21. Enter 5 for the Number of addresses to be assigned from this pool.

Note: This pool of addresses is not used in this scenario.

22. Click **Allow IP forwarding** to select this function. IP forwarding must be enabled for the corporate gateway to forward traffic between the remote client and the corporate network. See Figure 406 on page 359.

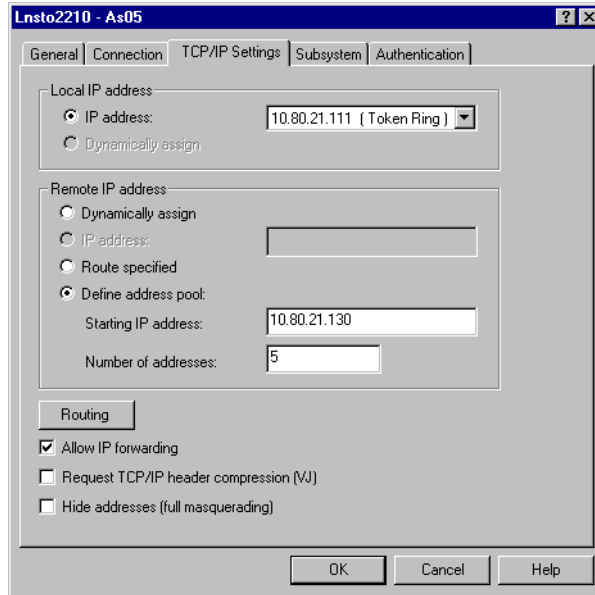


Figure 406. AS05 TCP/IP settings on the virtual PPP link

23. Click the **Routing** button (Figure 407).

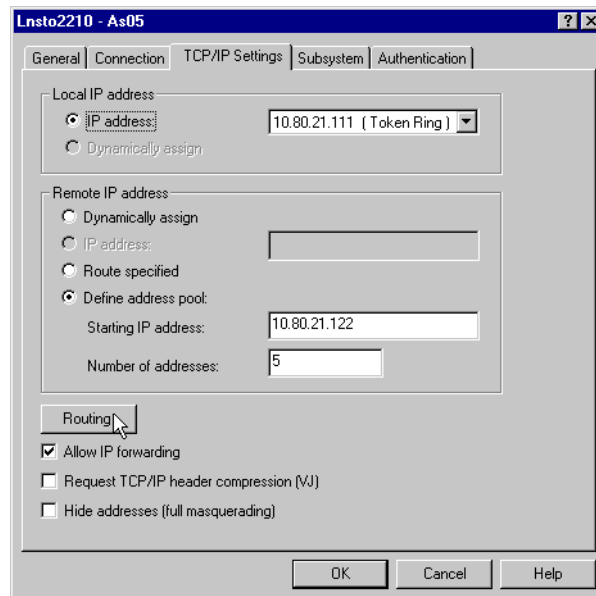


Figure 407. Defining static routes to assign a fixed IP address to the clients

24. Click **Use static routes**. Click **Add** to add the Caller User (identification that the PPP client sends at the start of the connection) and the IP address in the home address space that the LNS (AS05) assigns to the client.

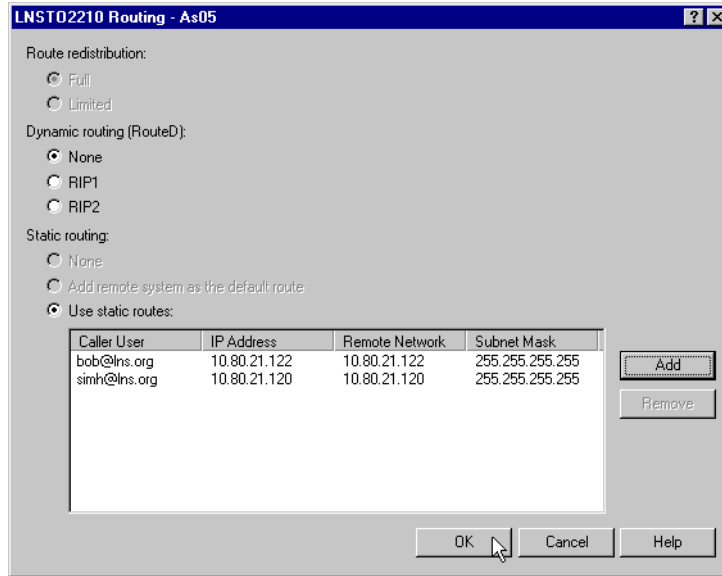


Figure 408. Assigning fixed IP address to the PPP clients based on Caller User

25. Click **OK**.

26. Click the **Authentication** tab.

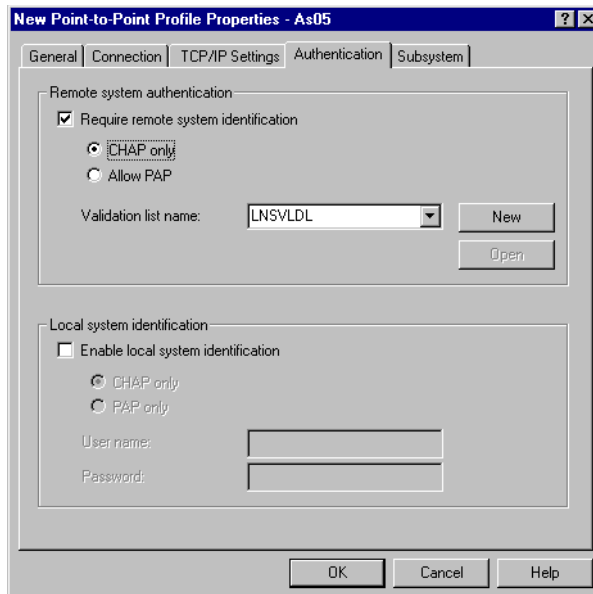


Figure 409. AS05 Configuring remote system authentication

27. Select **Require remote system authentication**, and enter a new validation list name, `LNSVLDL`.

28. Click **New** to create the validation list.

29. Click **Add**.

30. Select **CHAP only**.

31. Enter the user name and password. See Figure 410 on page 361.

32. Click **OK**.

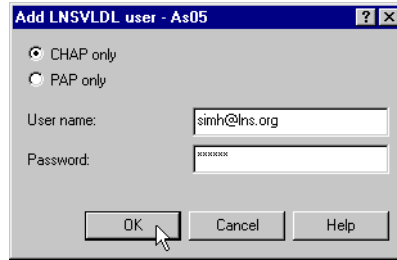


Figure 410. AS05 Enter the user ID and password for CHAP authentication

33. Confirm the password and click **OK**.

The New Validation List window is displayed (Figure 411).

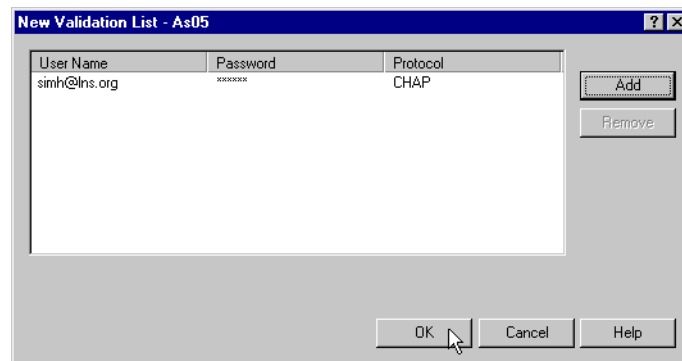


Figure 411. AS05 Validation list summary

34. Click **OK**.

35. Click **OK** to create the new PPP profile.

9.2.2 Configuring the IPSec AH tunnel to ISP: Host to Dynamic IP Users

To protect the L2TP tunnel between the LNS and the ISP, configure a VPN. This is the IPSec AH tunnel at the terminator end (AS05), shown as **B** in Figure 400 on page 353. This VPN has the following characteristics:

- It is sufficient to use only the Authentication Header (AH) protocol in this VPN. It is important to authenticate the ISP to verify that the request to establish the L2TP tunnel is genuine. However, it is not necessary to encrypt the data that flows between the ISP and the corporate gateway.
- The VPN configuration is host to dynamic IP users. ISPs may change the IP address of their routers. For that reason, we selected a Host to Dynamic IP users configuration. Keep in mind that this VPN protects the L2TP tunnel only. That is the reason why the LNS is a *host* and not a gateway from this VPN tunnel perspective.
- The filters must be applied to the physical LAN interface (TRLANC).

Table 34 summarizes the configuration values that you must enter at the VPN configuration wizard.

Table 34. AS05 New Connection Wizard planning worksheet - Host to Dynamic IP Users to ISP

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to gateway – Gateway to host – Gateway to dynamic IP user – Host to Dynamic IP User	Host to Dynamic IP Users
What will you name the connection group?	ISPAuth
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	High performance
How will you identify your local server?	IP address
What is the IP address of your local server?	204.146.18.5
How will you identify the remote server to which you are connecting?	Key identifier
What is the IP address of the remote server?	LAConISP
What is the pre-shared key?	123456789
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	High performance

9.2.2.1 Using the wizard to configure a Host to Dynamic IP Users VPN

To configure a Host to Dynamic IP Users VPN with the wizard, perform the following steps:

1. At the Virtual Private Networking window, select **File->New Connection**.
2. Select **Host to Dynamic IP Users** from the pull-down menu. This starts the New Connection Wizard as shown in Figure 412 on page 363.

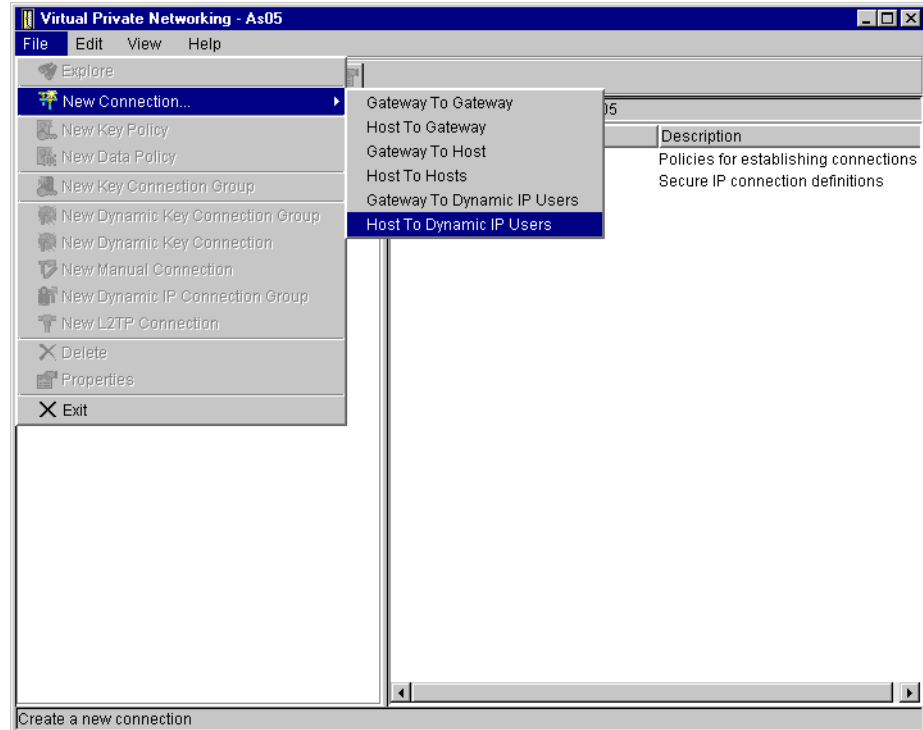


Figure 412. AS05 New Connection - Host to Dynamic IP Users

3. Click **Next** after reading the welcome window shown in Figure 413.

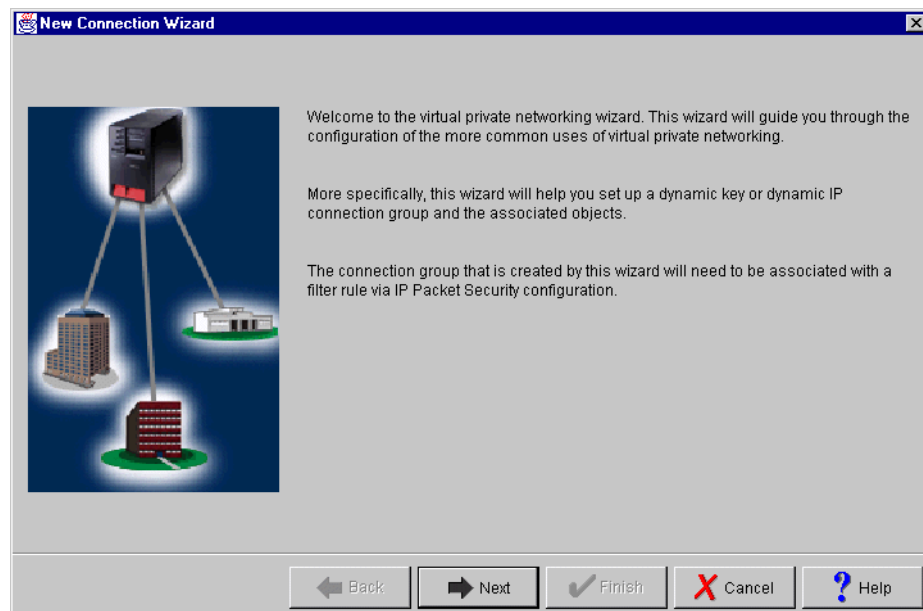


Figure 413. AS05 New Connection Wizard welcome window

4. Enter the name `ISPAuth` for the connection group, and enter a description as shown in Figure 414 on page 364.

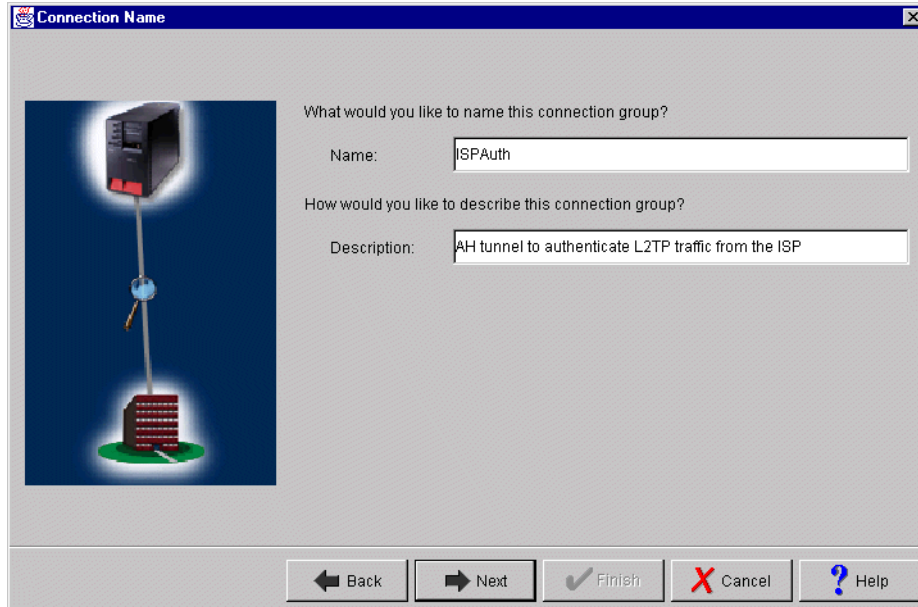


Figure 414. AS05 Connection name and description window

5. Click **Next**.
6. On the Key Policy window (Figure 415), specify the level of authentication or encryption protection that IKE uses during phase 1 negotiations. Select **Minimum security, highest performance** for this VPN. The wizard selects AH for this option.

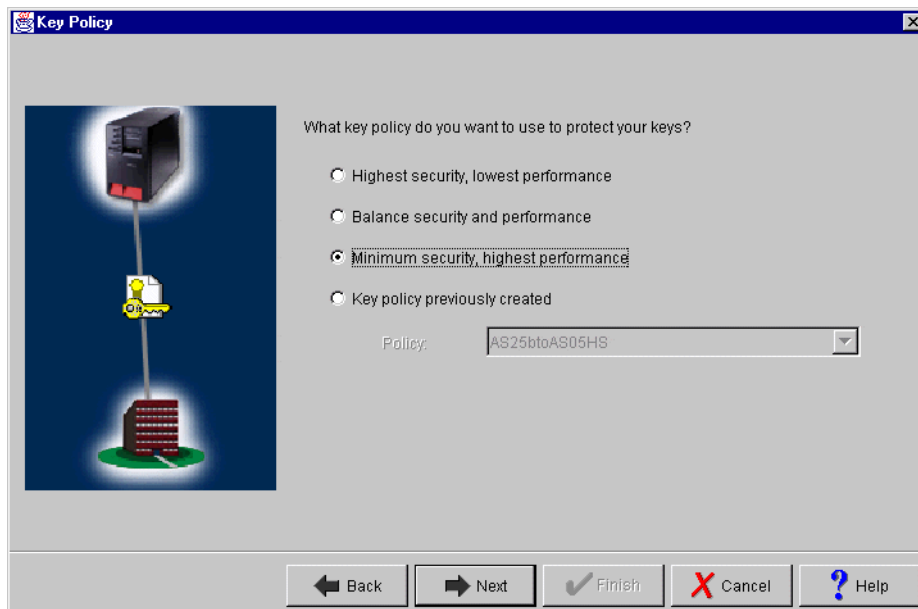


Figure 415. AS05 Key Policy window

7. Click **Next**.
8. On the Local identifier window (Figure 416 on page 365), specify the identity of the local key server. This is the globally routable IP address of the corporate gateway (AS05). Leave Identifier type as the default value, **Version 4 IP**

address. For the IP address, use the pull-down list to select the IP address for the interface **204.146.18.5**. Refer to Figure 400 on page 353 and to the planning worksheet in Table 34 on page 362.

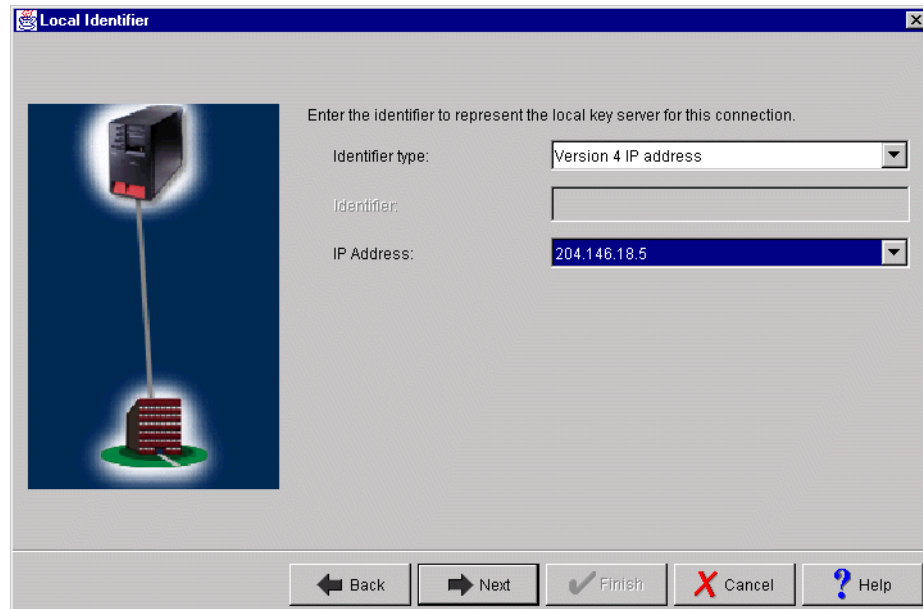


Figure 416. AS05 Local key server identifier window

9. Click **Next**.

10. Enter the identifier of the ISP in the Users window. In this scenario, we assume that the ISP identifies itself by a key identifier rather than an IP address. Leave the default value in Identifier type as **Key identifier** (Figure 417).

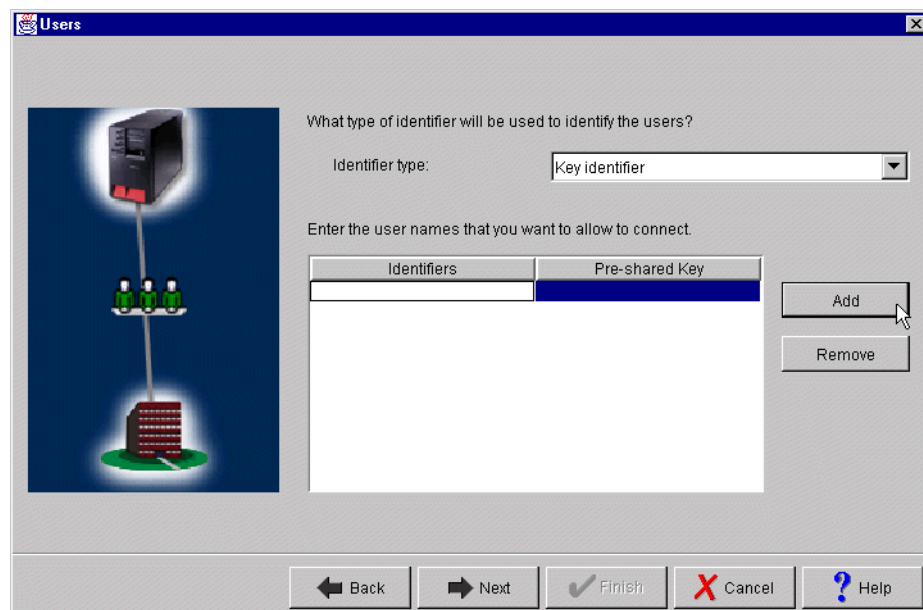


Figure 417. AS05 Remote user identification

11. Click **Add**.

12. Enter the Key identifier and Pre-shared key provided by the ISP shown in Figure 418.

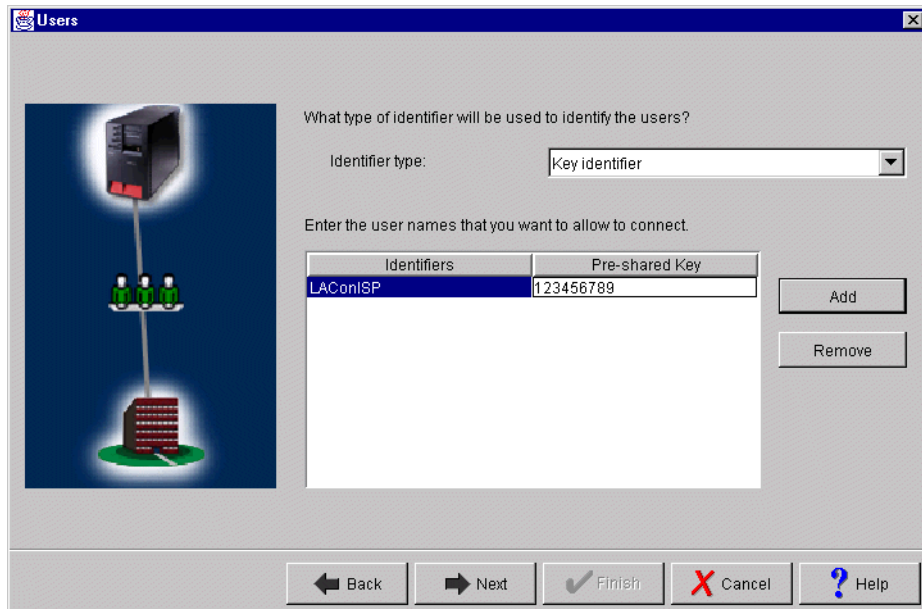


Figure 418. Specifying the key identifier and setting the pre-shared key

Important

The identifier type used in this scenario is Key Identifier and the Identifier value is LAConISP. These values depend on your ISP. Make sure that Identifier type, Identifier value, and pre-shared key are the same on both ends of the VPN connection.

13. Click **Next**.

14. On the Data Policy window (Figure 419 on page 367), specify the level of authentication or encryption protection that IKE uses during phase 2. Select **Minimum security, highest performance** for this VPN. The wizard selects AH for this option.

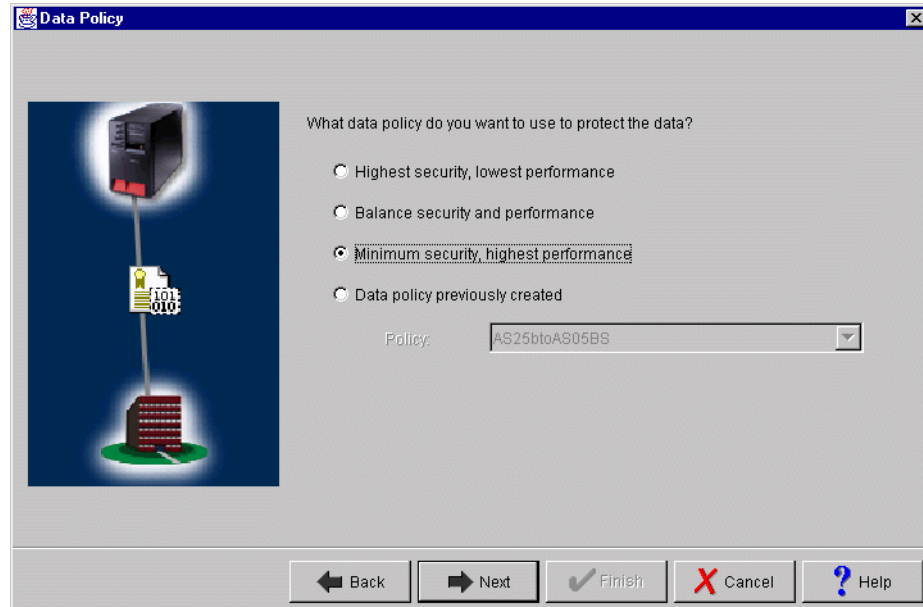


Figure 419. AS05 Data Policy window

15. Click **Next**.

16. The final window summarizes the configuration values that you entered as shown in Figure 420. If you scroll down, you can also see a list of the configuration objects that the wizard creates when you click Finish. Check the configuration values against your worksheet (Table 34 on page 362). If you need to make changes, click **Back**.

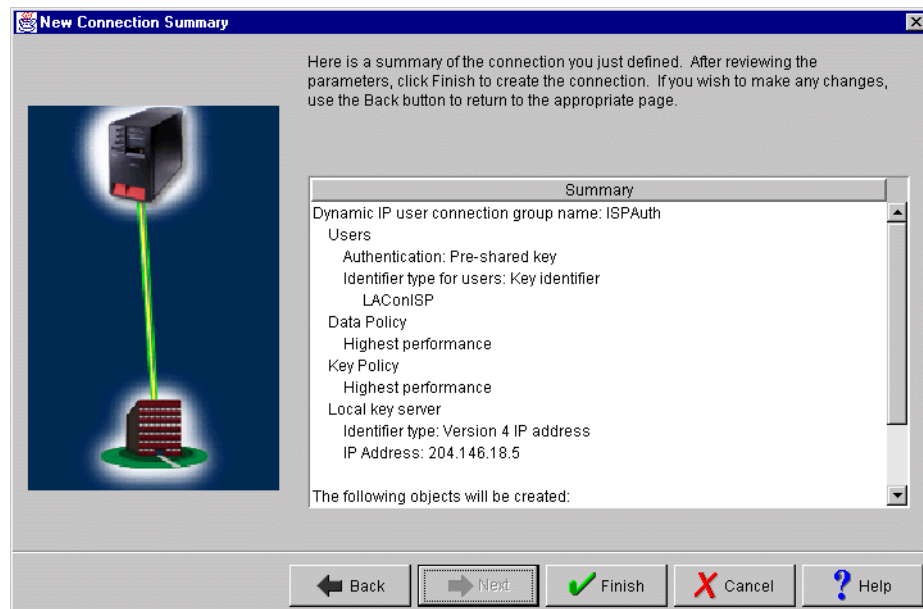


Figure 420. AS05 New Connection Summary window

17. Click **Finish**.

9.2.3 Configuring the IPSec ESP tunnel to the client: Gateway to hosts

To protect the connection between the corporate gateway and the client, configure a VPN. This is the IPSec ESP tunnel at the terminator end (AS05) shown as **H** in Figure 400 on page 353. This VPN has the following characteristics:

- Protocol must be ESP with both authentication and encryption. It is important to authenticate the client and hide the data exchanged between the client and the corporate network.
- The local key server identifier for the corporate gateway is the IP address of the interface on the corporate network side (10.80.21.111).
- The remote key server identifier (client) is the IP address that the LNS assigns to the client base on its user name and password (10.80.21.120).
- The VPN configuration is gateway to hosts.
- The filters must be applied to the virtual PPP (terminator) connection profile (LNSto2210).

Table 35 summarizes the configuration values that you must enter at the VPN configuration wizard.

Table 35. AS05 New Connection Wizard planning worksheet - Gateway to Hosts to client

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Gateway to Hosts – Gateway to Dynamic IP User	Gateway to Hosts
What will you name the connection group?	CmpDynKeyR
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	10.80.21.111
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	10.80.21.120
What is the pre-shared key?	123456789
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

9.2.3.1 Using the wizard to configure a gateway-to-hosts VPN

To configure a Gateway to Hosts VPN with the wizard, perform the following steps:

1. At the Virtual Private Networking window, select **File->New Connection**.
2. Select **Gateway to Hosts** from the pull-down menu. This starts the New Connection Wizard as shown in Figure 421.

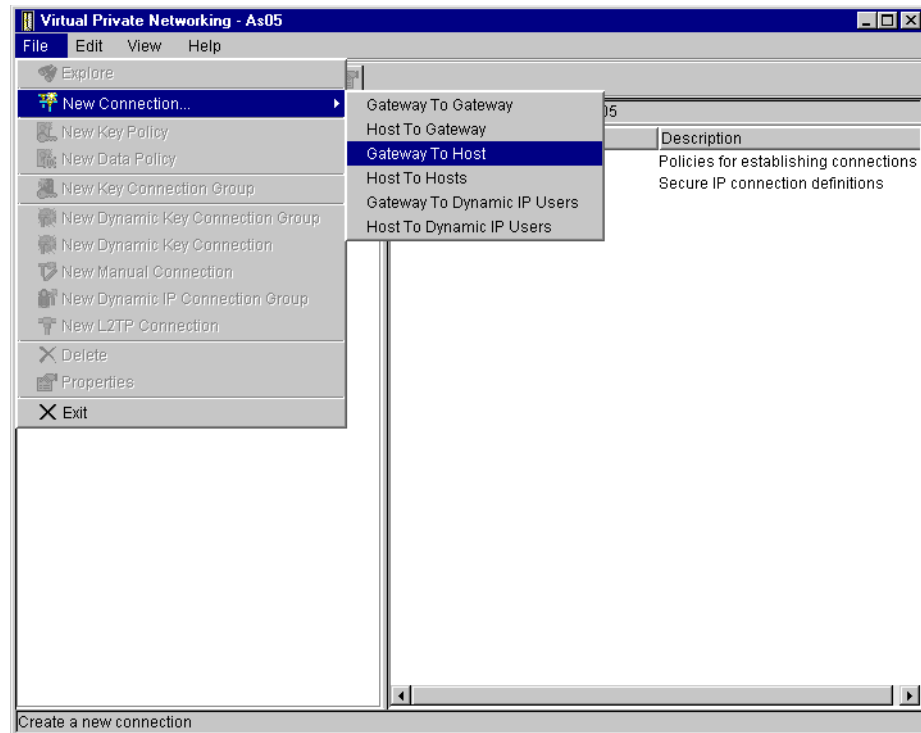


Figure 421. AS05 New Connection -> Gateway to Hosts - VPN to remote client AS25b

The New Connection Wizard starts (Figure 422 on page 370).

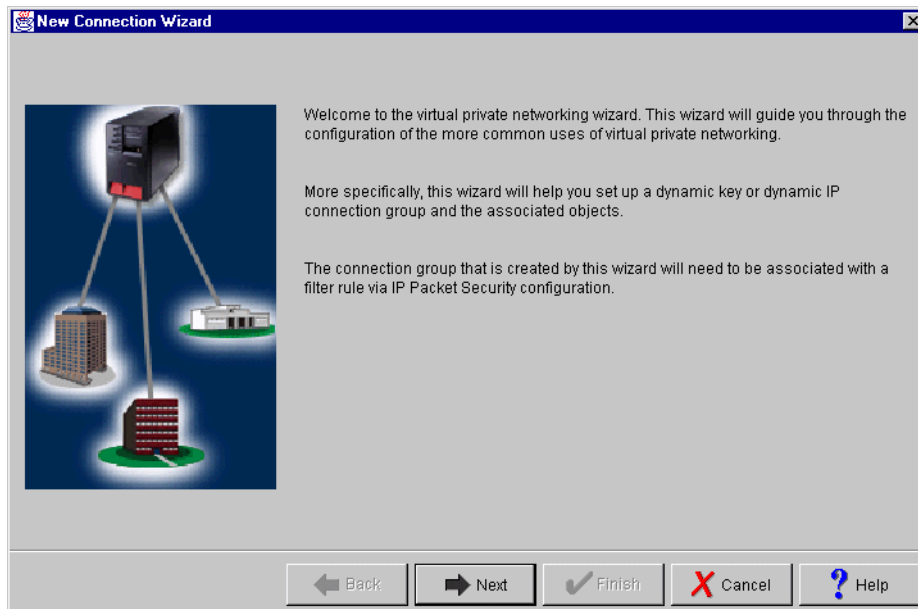


Figure 422. New Connection Wizard welcome window

3. Click **Next**.
4. Enter the name `CmpDynKeyR` for the connection group, and enter a description as shown in Figure 423.

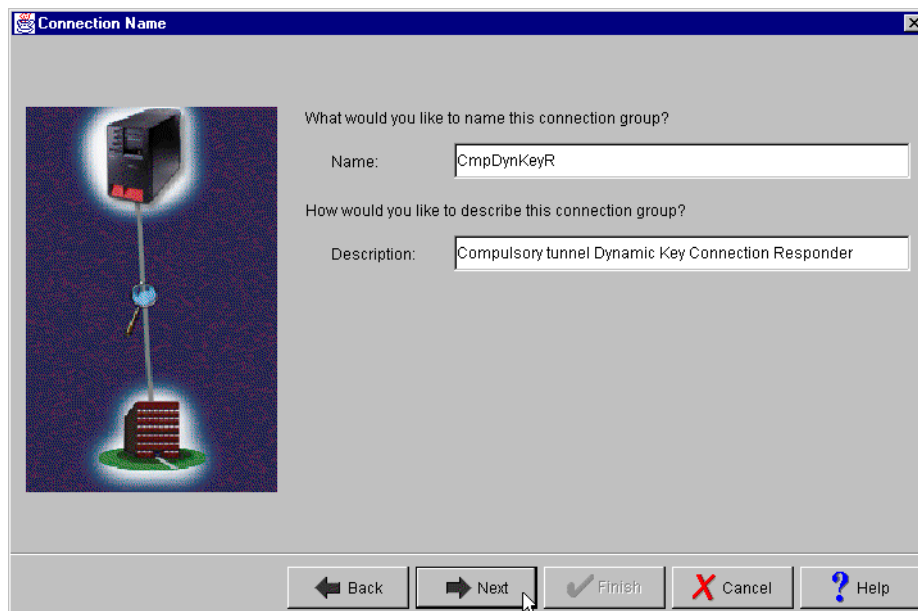


Figure 423. AS05 Connection name window

5. Click **Next**.
6. On the Key Policy window, specify the level of authentication or encryption protection that IKE uses during phase 1 negotiations. Select **Balance security and performance** as described on the planning worksheet in Table 35 on page 368. The wizard chooses MD5 for the authentication algorithm and DES for the encryption algorithm. Refer to Figure 424 on page 371.

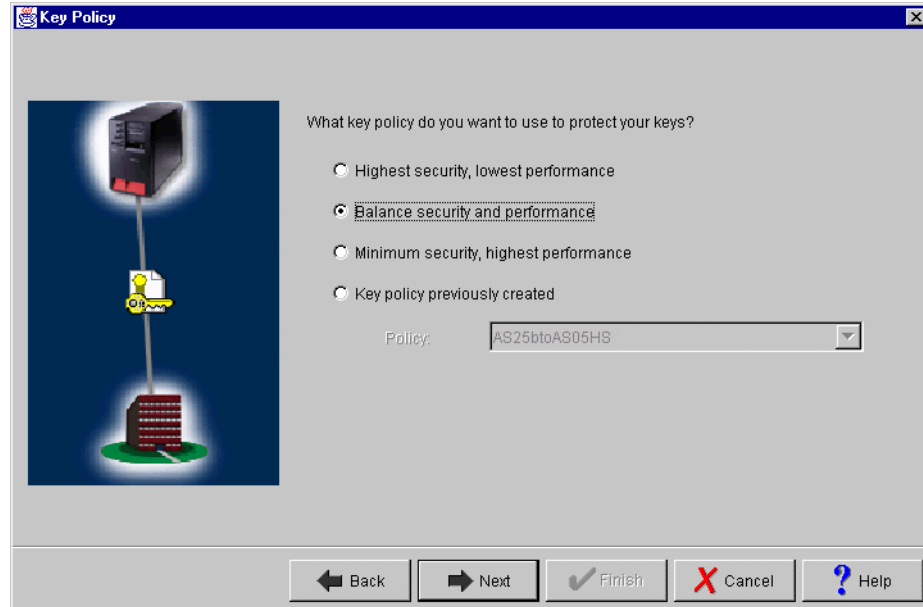


Figure 424. AS05 Key Policy window

7. Click **Next**.

8. On the Local identifier window (Figure 425), specify the identity of the local key server. This is the corporate gateway interface on the internal network. Leave Identifier type as the default value, **Version 4 IP address**. For the IP address, use the pull-down menu to select the IP address for the interface, **10.80.21.111**. Refer to Figure 399 on page 351 and to the planning worksheet in Table 35 on page 368.

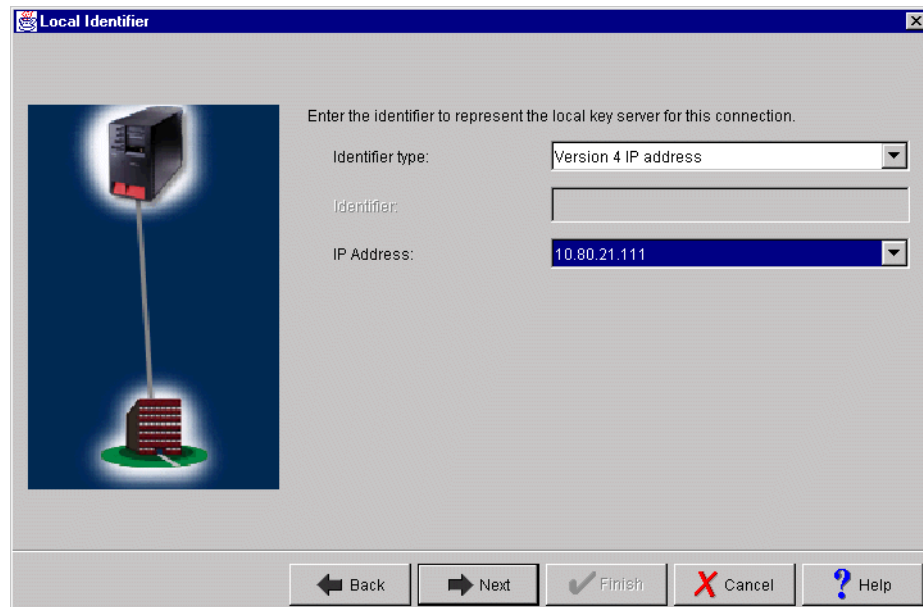


Figure 425. AS05 Local key server identifier

9. Click **Next**.

- At the Remote Network window, enter the remote key server information. Because the LNS assigns a known IP address to the client based on the client authentication information, you can use the assigned IP address as a remote key server identifier. In this scenario, it is 10.80.21.120. Specify 123456789 in the Pre-shared key field as shown in Figure 426.

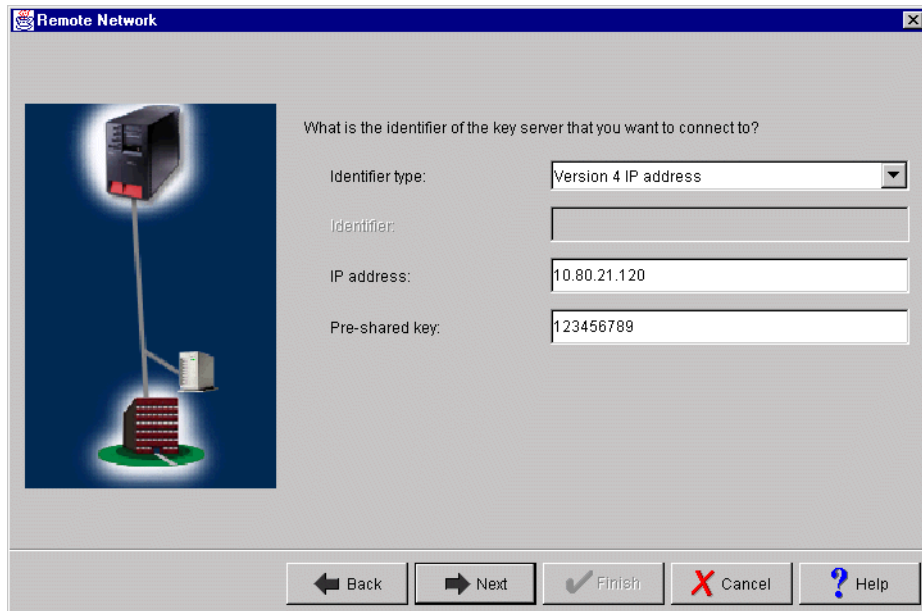


Figure 426. Remote Network window

- Click **Next**.
- On the Data Policy window (Figure 427 on page 373), specify the level of authentication or encryption protection that IKE uses during phase 2. Select **Balance security and performance** for this VPN. The wizard selects ESP with DES encryption and HMAC_MD5 authentication when you specify this option.

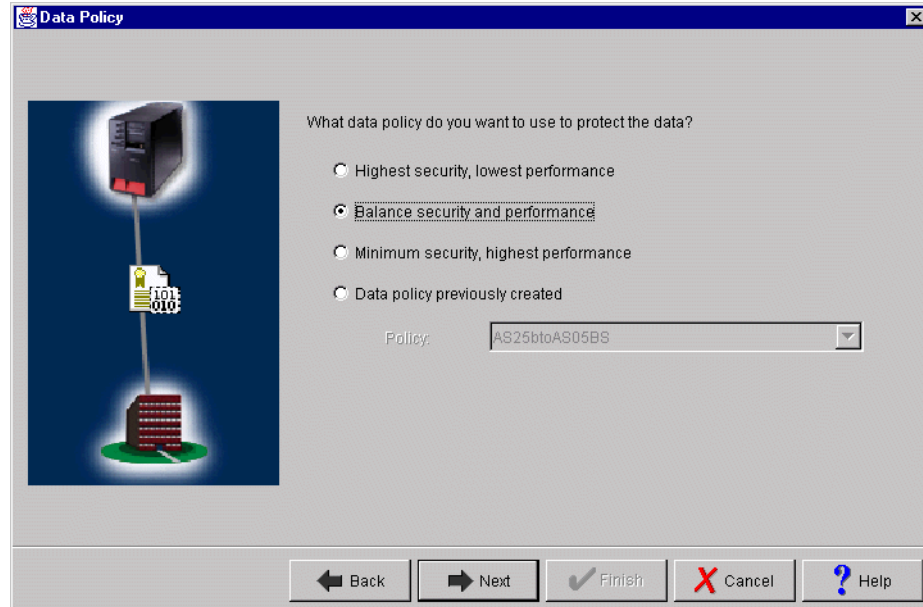


Figure 427. AS05 Data Policy window

13. Click **Next**.

14. The final window summarizes the configuration values that you entered as shown in Figure 420 on page 367. If you scroll down, you can also see a list of the configuration objects, which the wizard creates when you click Finish. Check the configuration values against your worksheet (Table 35 on page 368). If changes need to be made, click **Back**.

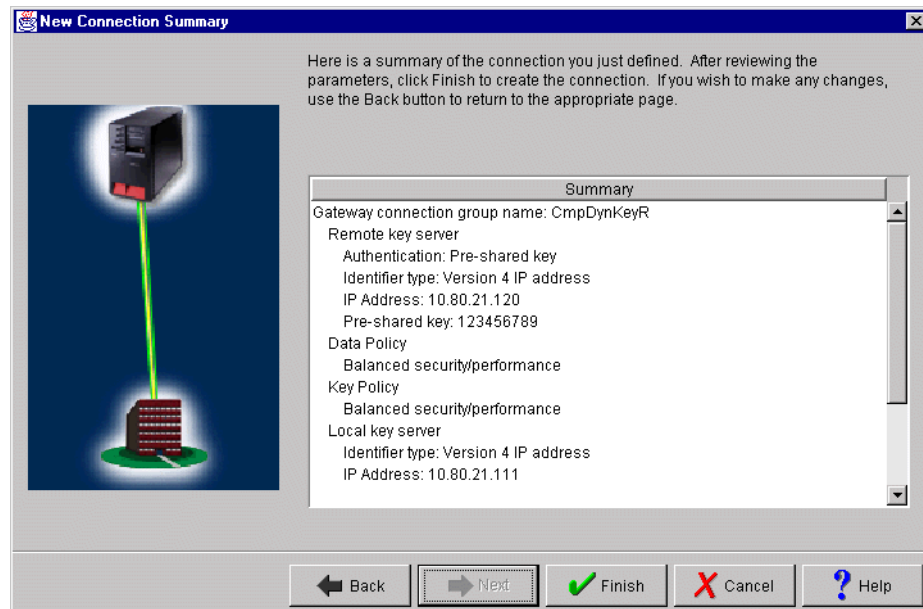


Figure 428. New Connection Summary window for AS05

15. Click **Finish**.

At this stage, you can make the changes to the base gateway-to-host configuration objects that the wizard created. Should you need to fine tune or

extend your configuration in any other way, you can view and update each of these objects by using the VPN Configuration GUI.

9.2.4 Configuring IP filters in the LNS AS/400 system (AS05)

You must configure two filter sets in this scenario:

- A filter set associated with the IPsec AH tunnel to the ISP. Apply these filter rules to the physical interface (TRLANC). The connection group associated with the IPSEC filter rule is ISPAAuth (configured in 9.2.2, “Configuring the IPsec AH tunnel to ISP: Host to Dynamic IP Users” on page 361).
- A filter set associated with the IPsec ESP tunnel to the client. Apply these filter rules to the virtual PPP terminator profile LNSto2210 (configured in 9.2.3, “Configuring the IPsec ESP tunnel to the client: Gateway to hosts” on page 368).

9.2.4.1 Configuring the filter set to the ISP (filter set ISP)

Table 36 summarizes the configuration values to create the IP filters associated with the IPsec AH tunnel to the ISP.

Table 36. AS05 Planning worksheet - IP filter rules to ISP

This is the information you need to create your IP filters to support VPN	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.	Host
Is the <i>remote</i> VPN server acting as a host or gateway ?	Host
What name do you want to use to group together the set of filters that will be created?	ISP
If <i>your</i> server is acting as a gateway ... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	
If the remote server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	*
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	204.146.8.5
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	Dynamic IP

This is the information you need to create your IP filters to support VPN	Scenario answers
What is the name of interface (for example, the Token-Ring, Ethernet, or PPP connection profile) to which these filters will be applied?	TRLANC
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

Using the values in the planning worksheet, create the following filters:

1. Configure a service alias IKE to represent the IKE negotiation (protocol UDP source and destination port 500). Referring to a service by name improves the readability of the filter. See Figure 429.

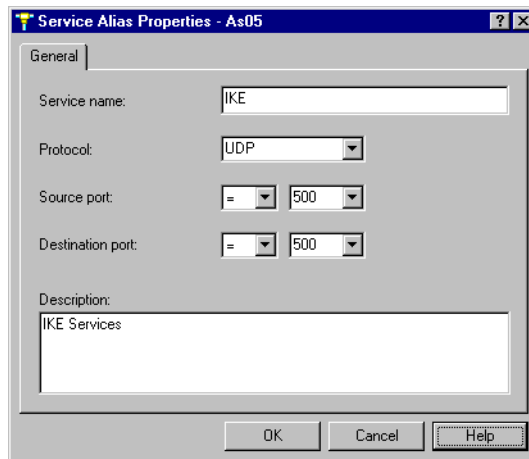


Figure 429. Configuring the IKE service alias

2. Use these outbound IKE filter rule negotiations. See Figure 430 on page 376.
 - **Source address name:** Local key server IP address (204.146.18.5)
 - **Destination address:** Wildcard (*). The remote key server IP address is dynamic.

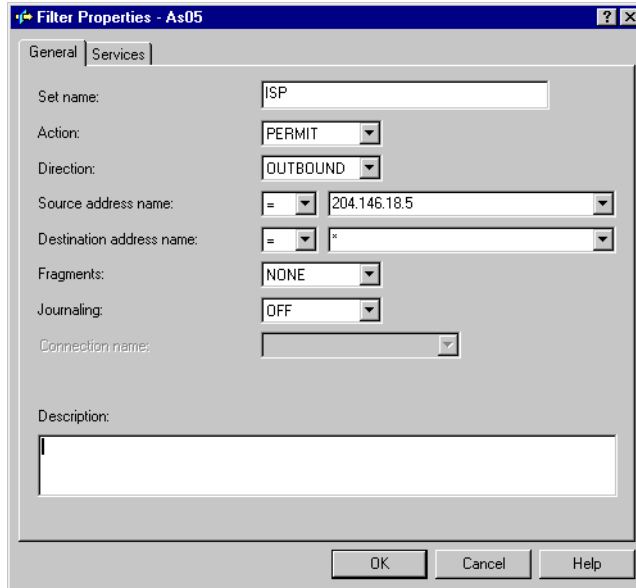


Figure 430. Outbound IKE filter rule

3. Click the **Services** tab.
4. IKE negotiations use protocol UDP, with source and destination port 500. Use the IKE service alias created in step 1. See Figure 431.

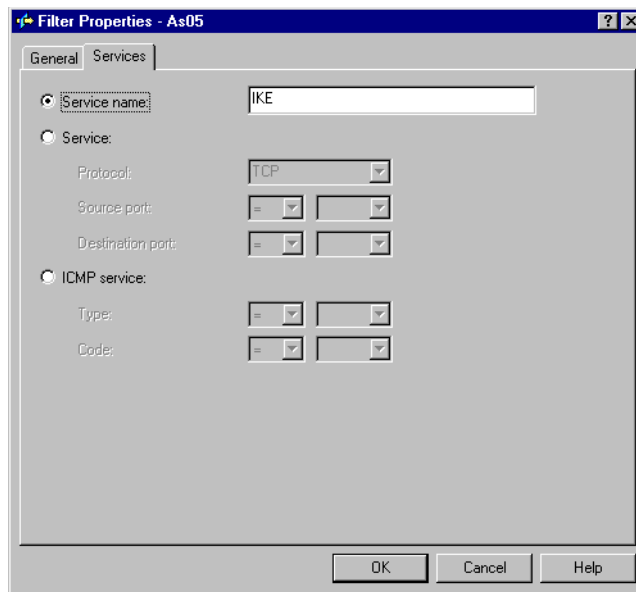


Figure 431. Outbound IKE filter rule - Services configuration

5. Click **OK**.
6. Repeat the previous four steps for the *inbound* filter rule. Remember to reverse the Source and Destination address names. Complete the Services window as you did for the outbound rule as shown in Figure 432 and Figure 433 on page 377.

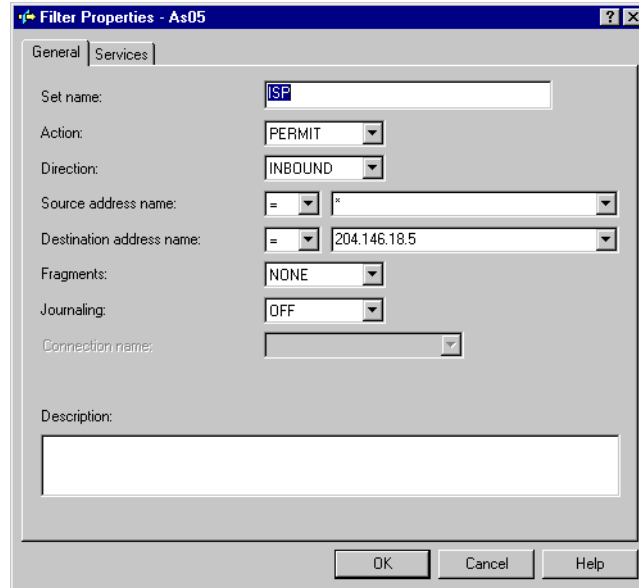


Figure 432. Inbound IKE filter rule

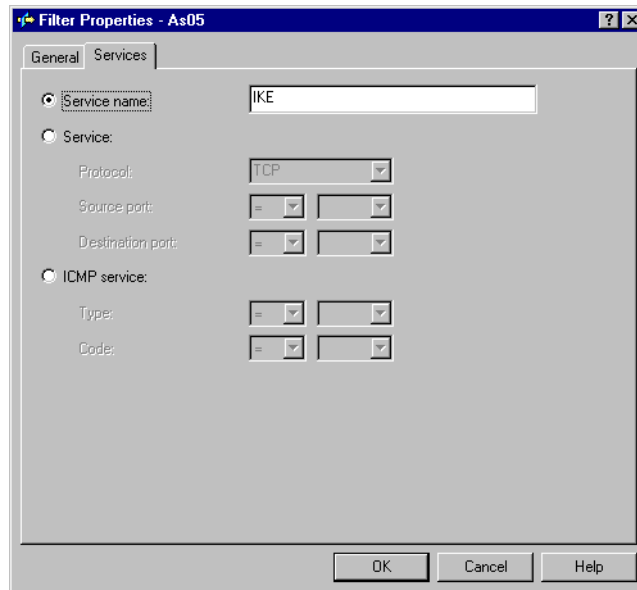


Figure 433. Inbound IKE filter rule - Services configuration

7. Click **OK**.
8. Configure the IPSEC filter rule that allows data traffic to use the VPN tunnel . Use the same filter Set name, ISP, but specify `IPSEC` in the Action field. With an IPSEC filter rule, Direction is always set to OUTBOUND and grayed out. In the Source and Destination address name fields, enter the globally routable IP address of AS05, 204.146.18.5 and a wildcard (*) for the destination address as shown in Figure 434. Since the destination is not identified by a fixed IP address, select **DYNAMICIP** for the connection name field. See Figure 434 on page 378.

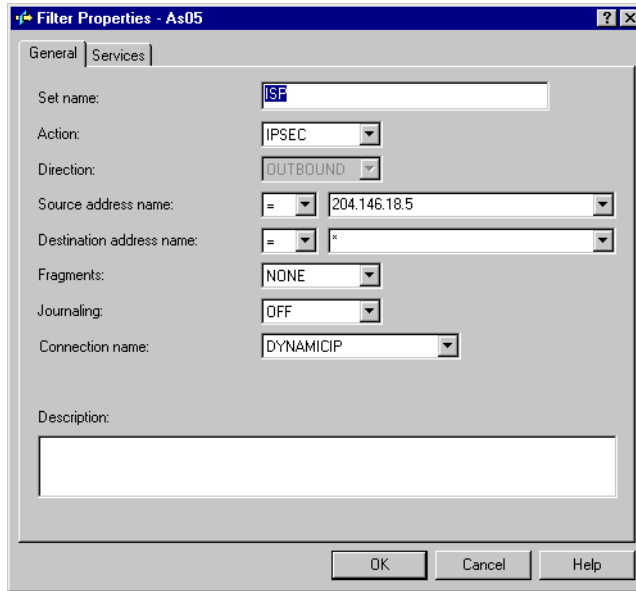


Figure 434. IPSec filter rule

9. Click the **Services** tab.

10. Enter **UDP** in the Protocol field. Enter 1701 for the Source port field. Enter wildcard (*) in the Destination port fields. This allows only L2TP traffic to use this filter rule and, therefore, the VPN tunnel. See Figure 435.

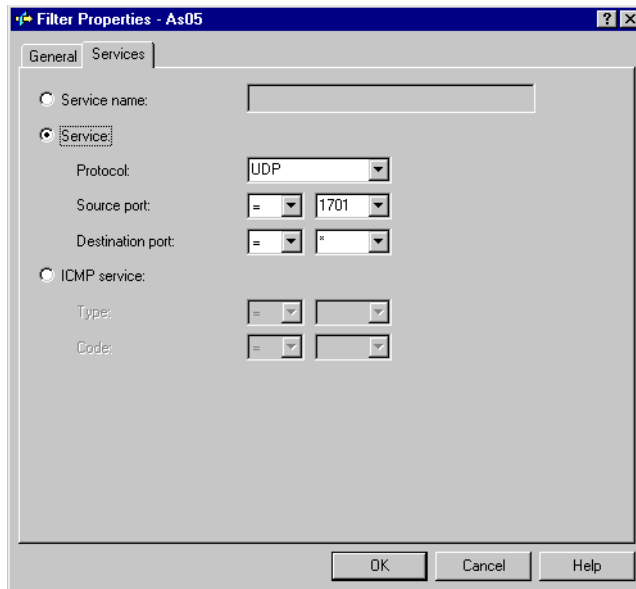


Figure 435. PSEC filter rule - Services configuration

11. Click **OK**.

12. The final rule you must create is a Filter Interface rule, which ties the filter rules you just created to the required interface. Right-click on **Filter interfaces**, and select **New Filter Interface** as shown in Figure 436 on page 379.

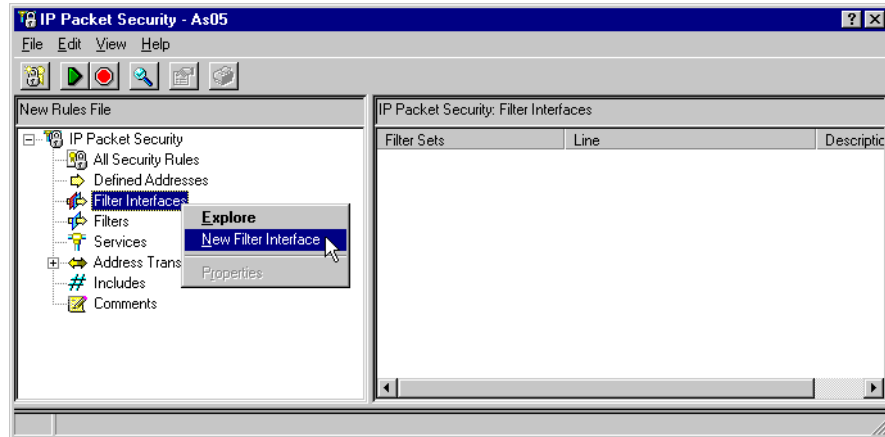


Figure 436. AS05 Defining a filter interface for the IP filter rules

13. Select **Line name** for the Line radio box, and select **TRLANC** from the pull-down menu.
14. Click on **Add** to add the filter set name of the filter rules you created previously, which is **ISP** in this scenario (Figure 437).

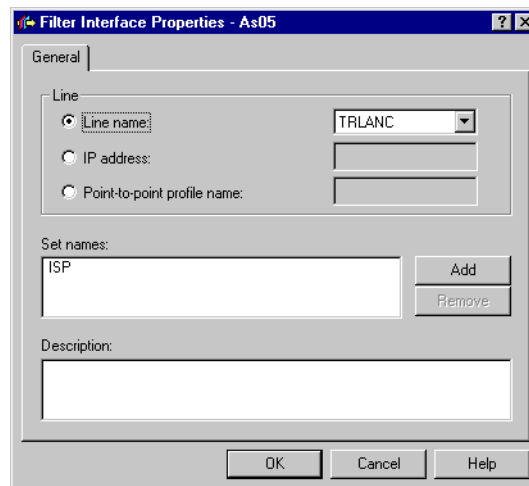


Figure 437. AS05 Filter interface to ISP

9.2.4.2 Configuring the filter set to the client (filter set COMPT)

Table 37 on page 380 summarizes the configuration values to create the IP filters associated with the IPsec ESP tunnel to the dial-in client.

The filter rules allow traffic between the dial-in client with assigned IP address 10.80.21.120 and the corporate network IP address 10.80.21.0. To configure the filter rules, you need to give a name to the subnet. In this example, we call it Corporate. You also need to choose a filter set name, COMPT, so you can group all your rules together and apply them to an interface. The interface is LNSTO2210. This is the name of the LNS virtual PPP terminator profile used to

connect the remote client and assign it an IP address out of the corporate local address space.

Table 37. AS05 Planning worksheet - IP filter rules to dial-in client

This is the information you need to create your IP filters to support your VPN	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.	Gateway
Is the <i>remote</i> VPN server acting as a host or gateway ?	Host
What name do you want to use to group together the set of filters that will be created?	COMPT
If <i>your</i> server is acting as a gateway ... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	10.80.21.0 255.255.255.0 Corporate
If the <i>remote</i> server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	10.80.21.111
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	10.80.21.120
What is the name of interface (for example, the Token-Ring, Ethernet, or PPP connection profile) to which these filters will be applied?	LNSTO2210
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> .	

Configure the following filter rules:

1. Right click on **Defined Addresses**, and select **New Defined address** from the menu (Figure 438 on page 381).

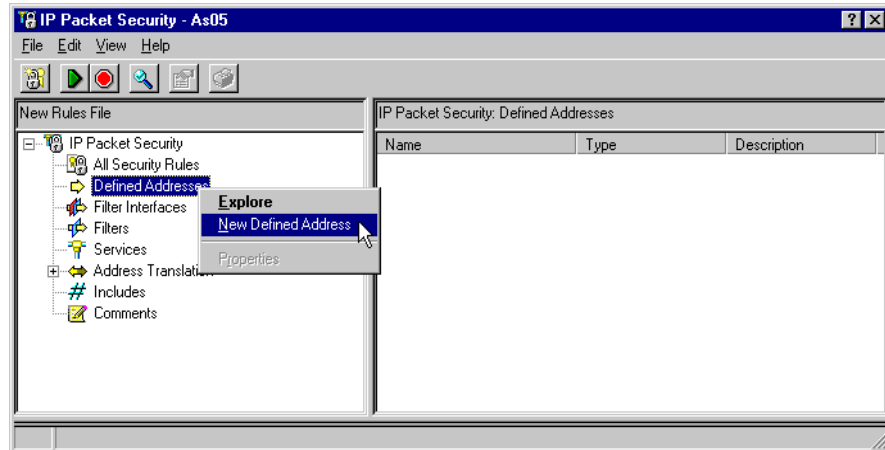


Figure 438. AS05 Creating a new defined address

2. The Address name is referenced by other rules using the defined address. In this scenario, enter `Corporate` as the address name. To configure a subnet, select **IP specification**, and enter a subnet mask. Click **Add**, and enter the **IP address** of the subnet. Add a description for the documentation purpose as shown in Figure 439.

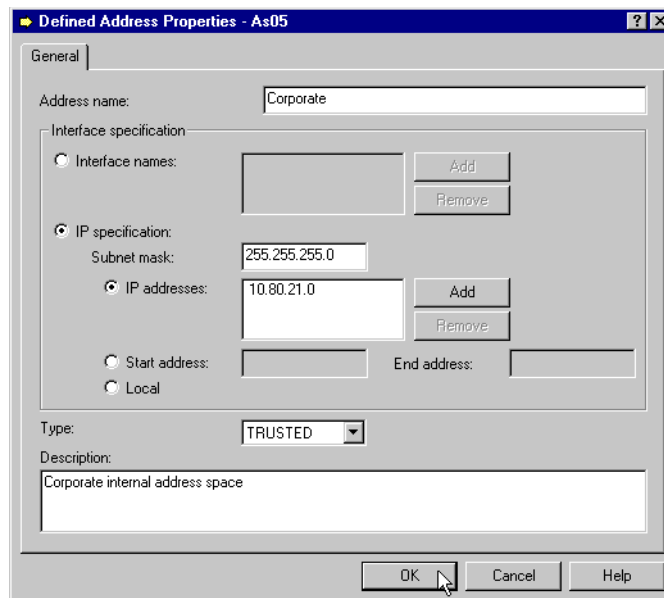


Figure 439. AS05 Defining the corporate address space

3. Click **OK**.
4. Right-click **Filters**, and select **New Filter** as shown in Figure 440 on page 382. All associated filter rules have the same *Set name*. In this example, the Set Name is **COMPT**.

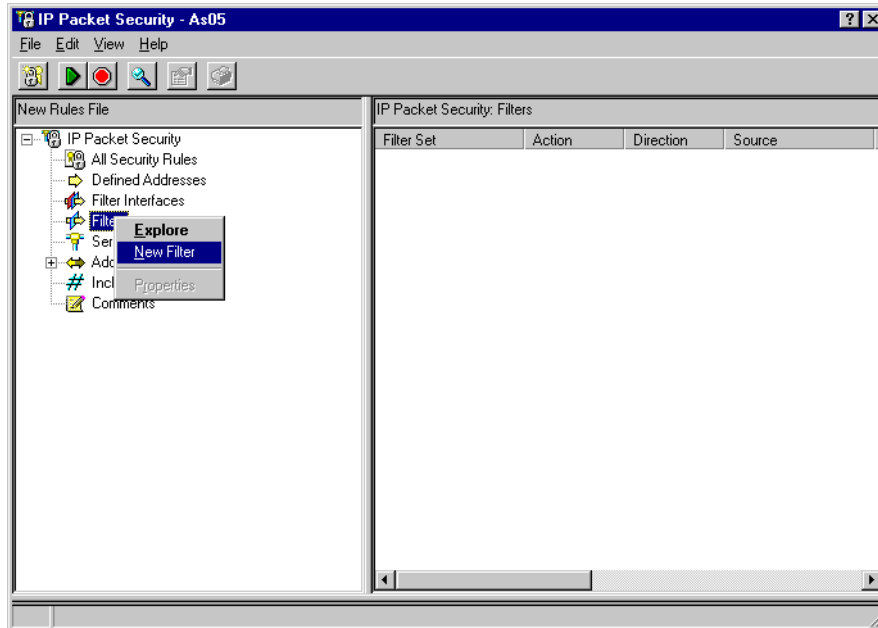


Figure 440. Creating a new filter rule

Add the filter rule to allow outbound IKE traffic. Notice the source address name. This is the local key server IP address. For the VPN to which this filter applies, this is the internal interface in the AS/400 gateway, 10.80.21.111. The Destination address name is the IP address of the remote key server. This is the IP address assigned to the client by the LNS, 10.80.21.120. See Figure 441.

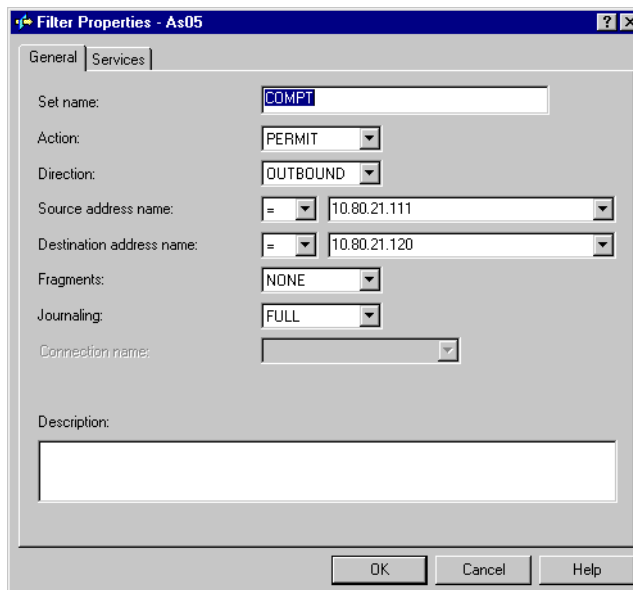


Figure 441. Outbound IKE filter rule

5. Click the **Services** tab.
6. Use the IKE service alias defined in step 1 page 375. See Figure 442 on page 383.

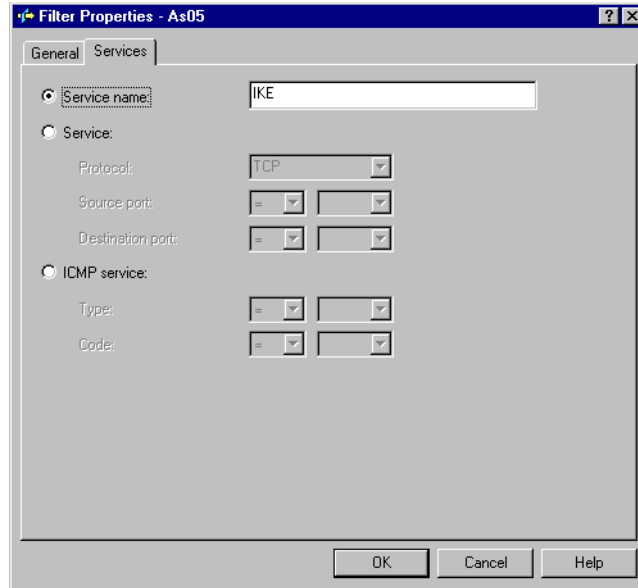


Figure 442. Outbound IKE filter rule - Services configuration

7. Click **OK**.
8. Repeat the previous four steps for the inbound filter rule. Remember to reverse the Source and Destination address names. Complete the Services window as you did for the outbound rule as shown in Figure 443 and Figure 444 on page 384.

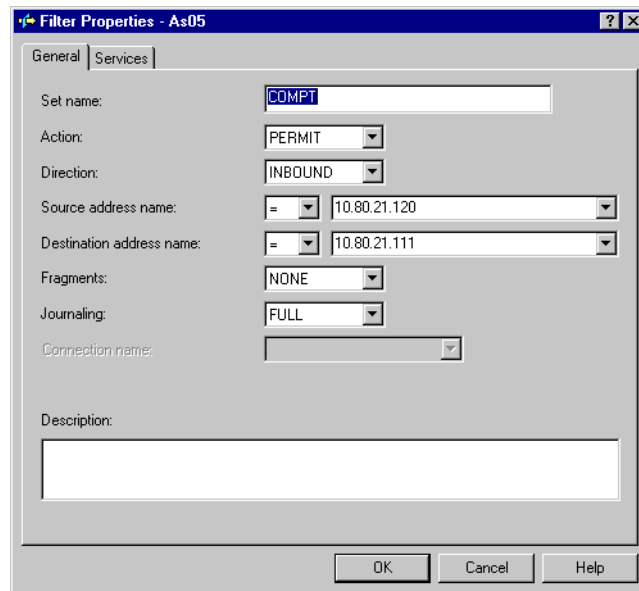


Figure 443. Inbound IKE filter rule

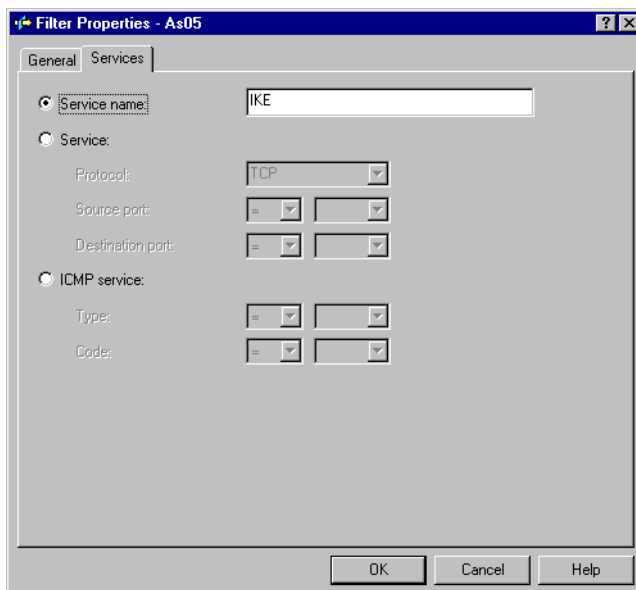


Figure 444. Services tab of inbound IKE filter rule

9. Click **OK**.

10. Configure the IPSEC filter rule that allows data traffic to use the VPN tunnel . Use the same filter Set name, **COMPT**, but specify `IPSEC` in the Action field. With an IPSEC filter rule, Direction is always set to `OUTBOUND` and grayed out. The Source address name is the corporate subnet, defined address Corporate, created above. The destination address name is the assigned IP address of the dial-in client AS25b, 10.80.21.120. See Figure 445.

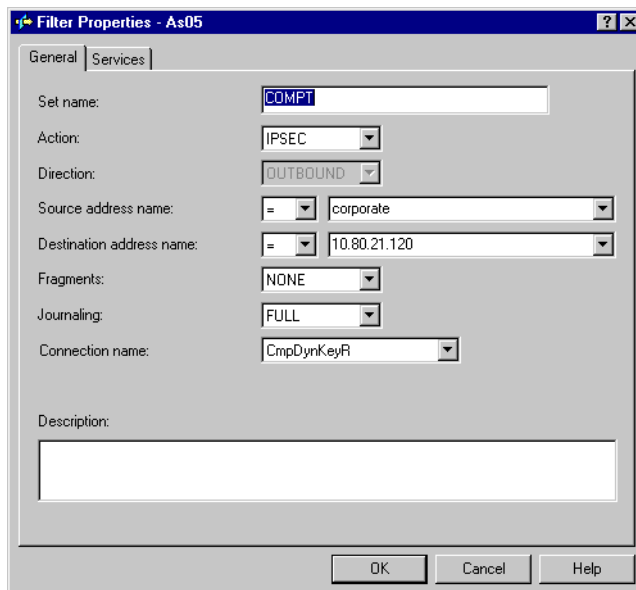


Figure 445. IPsec filter rule

In the Connection name field, select the **CmpDynKeyR** connection group from the pull-down menu.

Important

At this stage, you tie your IP filters back to the VPN configuration you built in 9.2.3, “Configuring the IPsec ESP tunnel to the client: Gateway to hosts” on page 368. The *Connection name* is, in fact, the data connection, which in this case is a dynamic key connection *group*. Use the pull-down menu to list all the data connection names that were configured on this system, and select the one required. In this example, select **CmpDynKeyR**.

Because IP filters refer to the VPN data connection name, the VPN configuration must be performed before the filters.

11. Click the **Services** tab.
12. Select **Service** and enter a wildcard (*) in the Protocol, Source port, and Destination port fields. This allows any protocol and any port to use this filter rule. The result is a VPN tunnel such as the one shown in Figure 446.

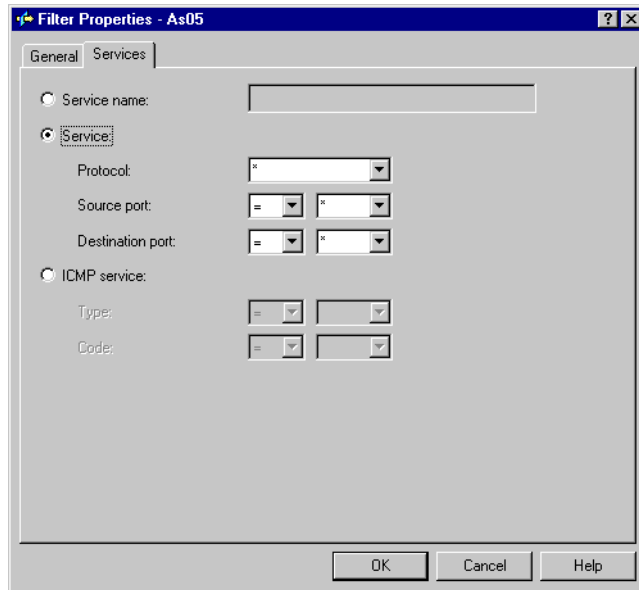


Figure 446. IPSEC filter rule - Services page

13. Click **OK**.
14. The final rule you must create is a *Filter Interface* rule, which ties the filter rules you just created to the required interface. Right-click on **Filter Interfaces**, and select **New Filter Interface** as shown in Figure 447 on page 386.

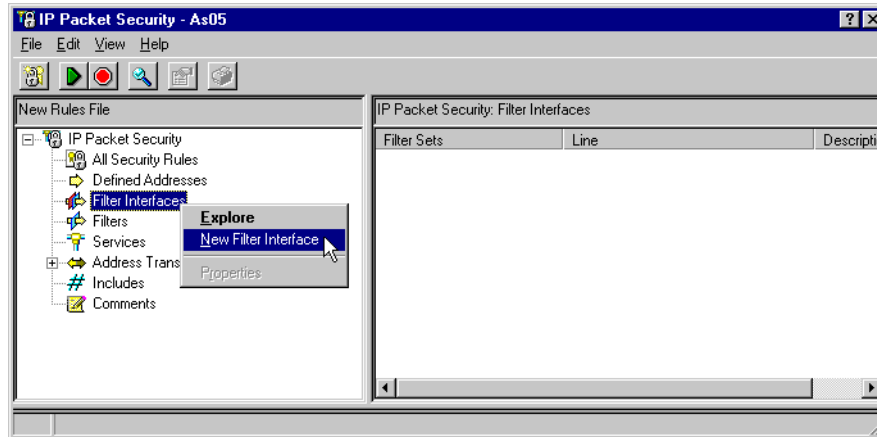


Figure 447. AS05 Defining a filter interface for the IP filter rules

15. Select **Point-to-Point profile name** for the Line, and specify the LNS terminator name created in 9.2.1, “Configuring the L2TP terminator profile (AS05)” on page 354.
16. Click **Add** to add the filter set name of the filter rules created previously, which, in this scenario, is **COMPT** (Figure 448).

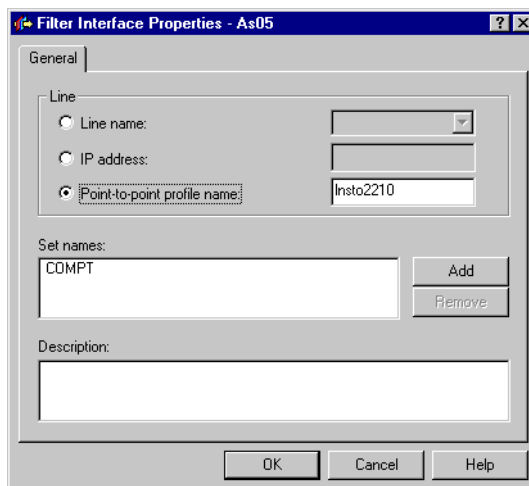


Figure 448. Filter interface rule

17. Click **OK**.

Figure 449 on page 387 shows a summary of the filters configured in the LNS (AS05).

```

IP Packet Security: Filters
#IKE Service Alias
SERVICE IKE PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
#Corporate Defined Address
ADDRESS corporate IP = 10.80.21.0 MASK = 255.255.255.0TYPE = TRUSTED
#Filter Set ISP applied to Physical line TRLANC
FILTER_INTERFACE LINE = TRLANC SET = ISP
#Filter entries in the ISP filter set
#IKE Rules - IKE negotiation for IPSec AH tunnel to ISP

FILTER SET ISP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = 204.146.18.5 SERVICE = IKE FRAGMENTS = NONE JRN = FULL
FILTER SET ISP ACTION = PERMIT DIRECTION = OUTBOUND
SRCADDR = 204.146.18.5 DSTADDR = * SERVICE = IKE
FRAGMENTS = NONE JRN = FULL
#IPSEC rule - IPSec tunnel encapsulates L2TP tunnel
FILTER SET ISP ACTION = IPSEC DIRECTION = OUTBOUND
SRCADDR = 204.146.18.5 DSTADDR = * PROTOCOL = UDP DSTPORT = *
SRCPORT = 1701 FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = DYNAMICIP

#Filter entries in the COMPT filter set
#Filter Set COMPT applied to virtual PPP terminator profile
FILTER_INTERFACE INTERFACE = lnsto2210 SET = COMPT
IKE Rules - IKE negotiation for IPSec ESP tunnel to client

FILTER SET COMPT ACTION = PERMIT DIRECTION = OUTBOUND
SRCADDR = 10.80.21.111 DSTADDR = 10.80.21.120 SERVICE = IKE
FRAGMENTS = NONE JRN = FULL
FILTER SET COMPT ACTION = PERMIT DIRECTION = INBOUND
SRCADDR = 10.80.21.120 DSTADDR = 10.80.21.111 SERVICE = IKE
FRAGMENTS = NONE JRN = FULL
#IPSEC rule - IPSec tunnel from client to corporate subnet
FILTER SET COMPT ACTION = IPSEC DIRECTION = OUTBOUND
SRCADDR = corporate DSTADDR = 10.80.21.120 PROTOCOL = *
DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = CmpDynKeyR

```

Figure 449. AS05 Filters summary at the LNS in compulsory tunnel

18. Once you complete configuring the filter rules, select **File** from the main menu. Then, select **Verify** as shown in Figure 450 on page 388. Alternatively, there is a verify icon (a magnifying glass) on the toolbar.

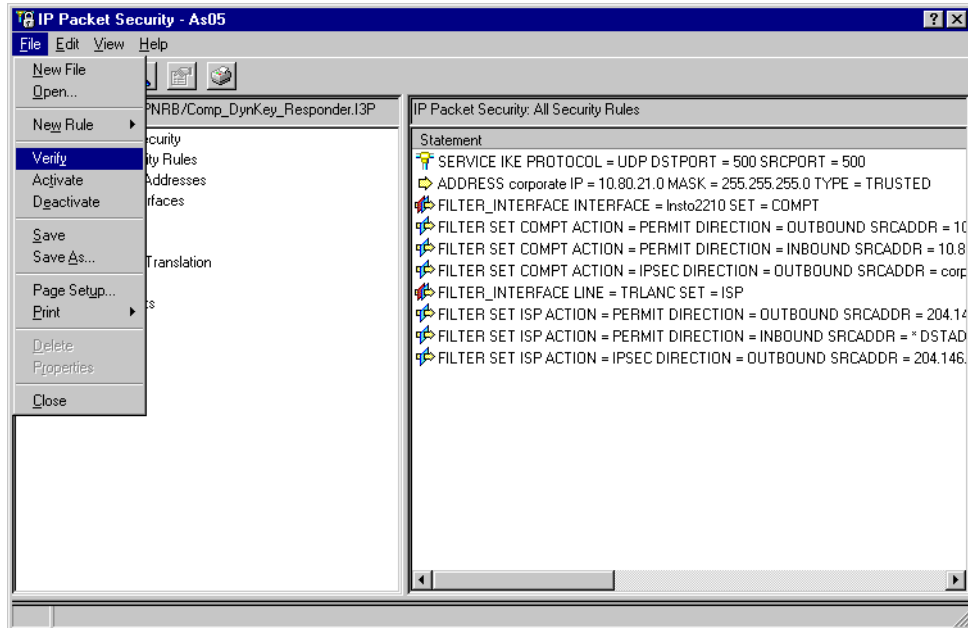


Figure 450. Verifying filter rules

19. To activate the filters, select **File->Activate** as shown in Figure 451. Alternatively, there is an activate icon (a green triangle) on the toolbar. Look for the message The rules file was successfully activated.

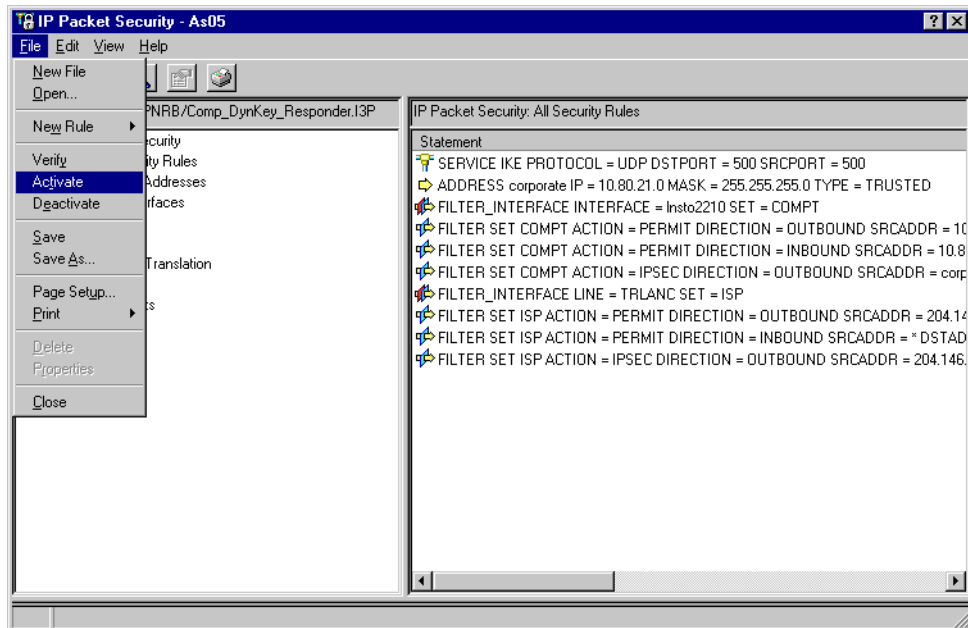


Figure 451. Activating filter rules

20. Save your filter rules file. Select **File->Save**. The file is saved into the IFS with an extension of *i3p*. In this example, we created a subdirectory, *VPNRB*, under the directory *QIBM*. Save the filter rules as *Comp_DynKey_Responder.i3p*.

9.3 Configuring the PPP dial-in client in a compulsory tunnel with IPsec

The following sections take you step-by-step through the configuration of the PPP dial-up line, VPN, and filters in AS25b.

9.3.1 Configuring the PPP dial-up connection to the ISP (AS25b)

The configuration of the PPP dial-up connection on AS25b is much like any regular PPP connection, since no special L2TP support is needed in the client (the LAC function is provided by the ISP router).

Table 38 shows the parameters that are relevant to the compulsory tunnel protected by IPsec.

Table 38. PPP dial-up connection profile (AS25b) - Parameters relevant to the compulsory tunnel

PPP configuration parameter	Scenario value	Comment
Name	LACDIALUP	Must match <i>Local Address Identifier</i> in VPN connection.
Line connection type	Switched line	Dial-up to ISP
Mode type	Dial	
Remote phone number	56109	ISP phone number
Type of line service	Analog	
Name	LACDIALUP	
Local IP address	Dynamically assigned	This is the IP address in the corporate office address space assigned by the LNS.
Remote IP address	Dynamically assigned	LNS local IP address
Routing	Add remote system as the default route	Link to the ISP must be the default route.
Local system identification	Enable local system identification	
User name	CHAP only simh@Ins.org	Must match the LNS entry in VLDL and the static route.
Password	xxxx	

1. Start Operations Navigator, and select the system **AS25b**. Sign on as required.
2. Expand **Network->Point-to-Point**.
3. Right-click on **Connection Profile**, and select **New Profile** from the menu. See Figure 452 on page 390.

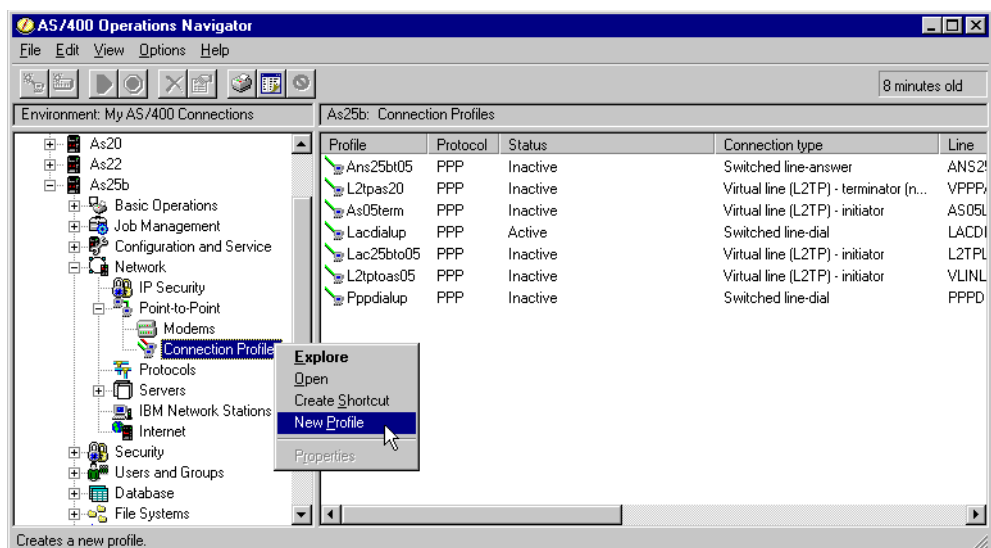


Figure 452. AS25b Defining a new PPP connection profile

4. Enter LACDIALUP as the name of the connection.
5. Enter PPP compulsory tunnel connection or similar for Description.
6. Select **PPP** in the Type parameter.
7. Select **Switched line** for Mode - Line connection type.
8. Select **Dial** from the Mode type pull-down menu (Figure 453).

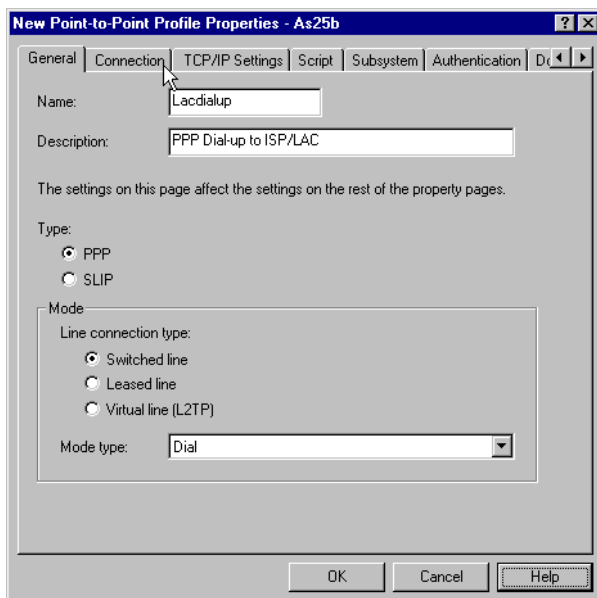


Figure 453. AS25b General PPP settings

9. Click the **Connection** tab.
10. Click **Add** to add the Remote phone numbers, and enter the number to dial your ISP. In this scenario, the number is 56109.
11. Set the Type of line service to **Analog line** by selecting it from the pull-down menu.

12. Enter `LACDIALUP` as the name of the Link configuration, and click on **New**.
13. Enter `Compulsory tunnel - Dial up to ISP or similar` for Description.
14. The valid IOP processors are displayed. Click on **CMN02** in this example.
15. Select **Asynchronous** for the Framing type parameter (Figure 454).

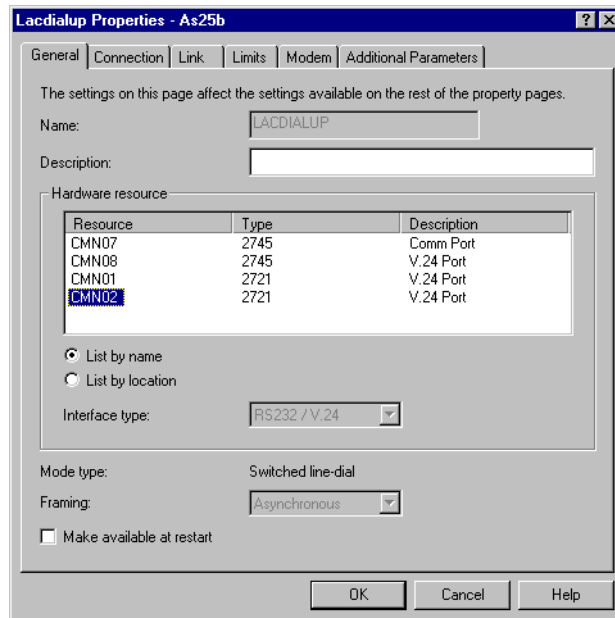


Figure 454. AS25b Selecting the network interface to use (IOP)

16. Click the **Connection** tab.
17. Select **AT command set** for the Dial command type parameter from the pull-down menu.
18. Click on **Both** for Connections allowed.
19. Click on **Use flow control (RTS/CTS)**. Refer to Figure 455 on page 392.

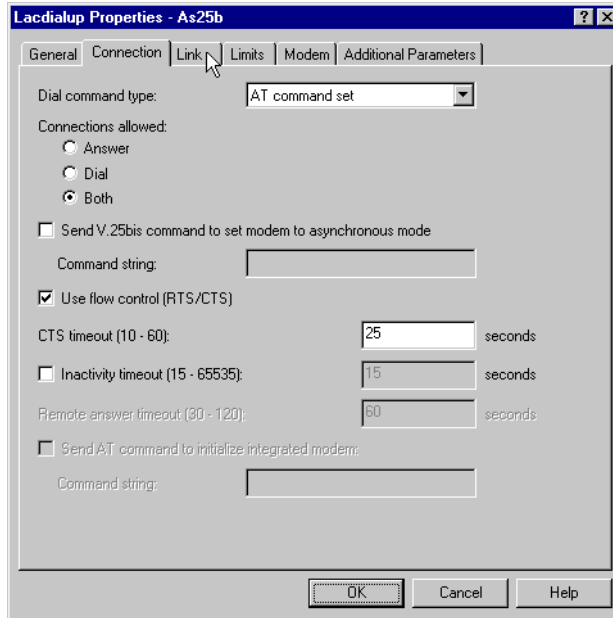


Figure 455. AS25b Dial up link connection settings

20. Click on the **Link** tab.

21. Accept the default settings on this page (Figure 456).

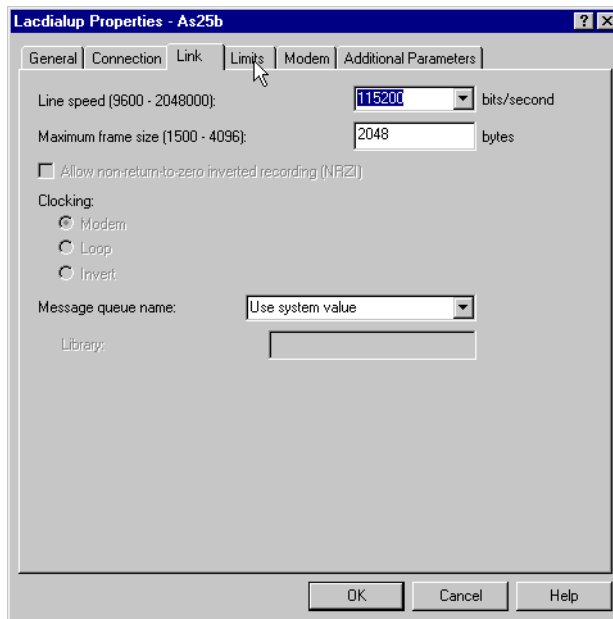


Figure 456. AS25b Defining the link settings

22. Click the **Limits** tab.

23. Accept the default settings on this page (Figure 457 on page 393).

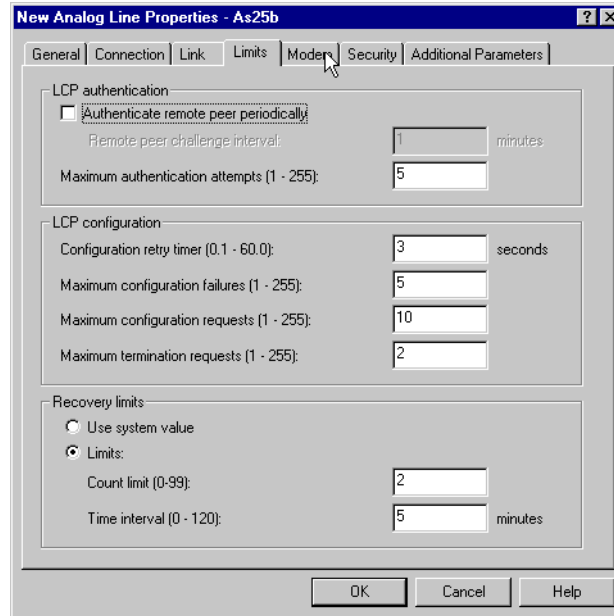


Figure 457. AS25b Setting the time out and limit values

24. Click the **Modem** tab.

25. Select your modem type from the pull-down list. In this scenario, we are using the **IBM 7852-400** modem (Figure 458).

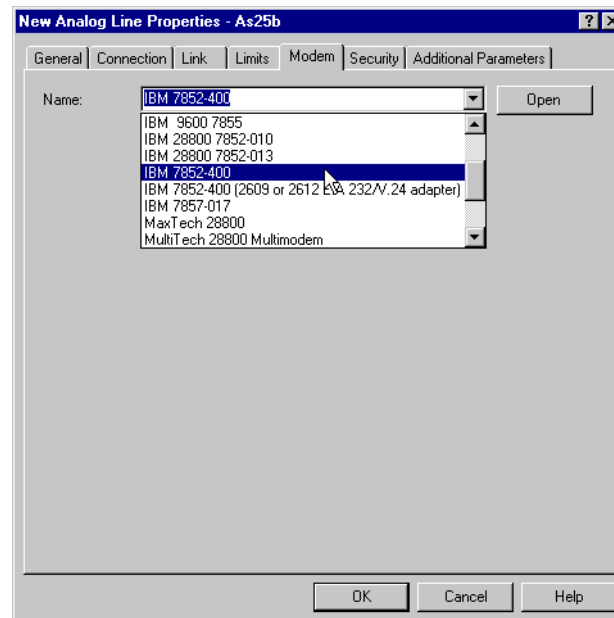


Figure 458. AS25b Selecting the modem type

26. Click **OK**.

27. Leave the Re-dial on disconnect and the Override line inactivity time out unchecked. See Figure 459 on page 394.

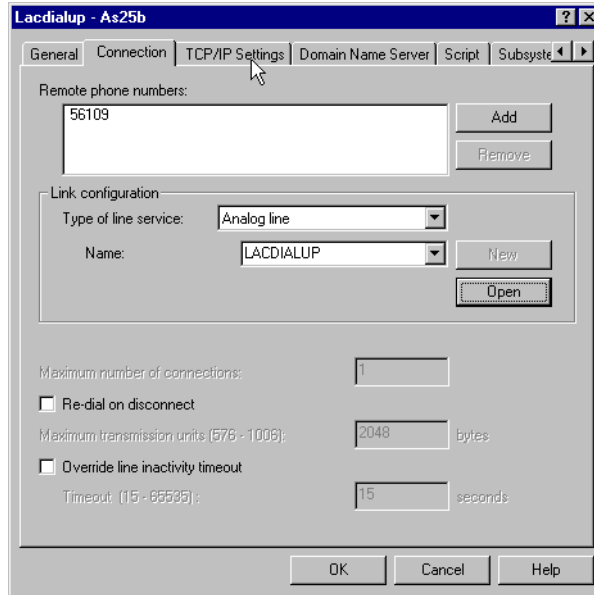


Figure 459. AS25b PPP profile connection settings

28. Click the **TCP/IP settings** tab.

29. Select **Dynamically assign** for the Local IP address parameter.

30. Select **Dynamically assign** for the Remote IP address parameter (Figure 460).

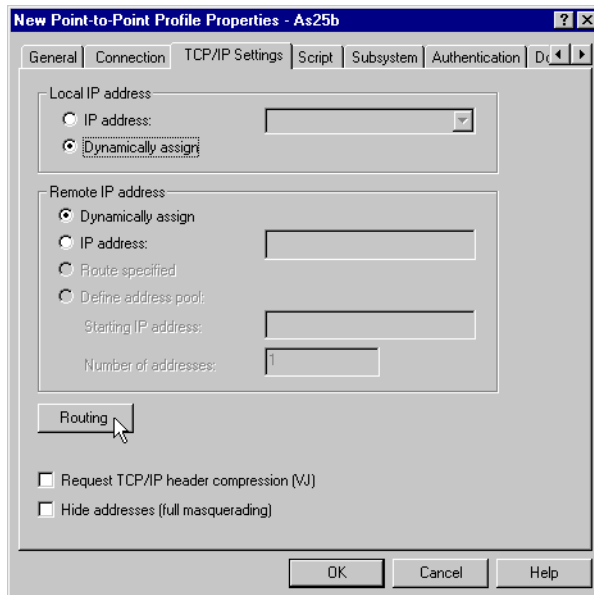


Figure 460. AS25b Defining the TCP/IP settings

31. Click the **Routing** button.

32. Select **None** for Dynamic routing (RouteD).

33. Under Static routing, select **Add remote system as the default route** (Figure 461 on page 395).

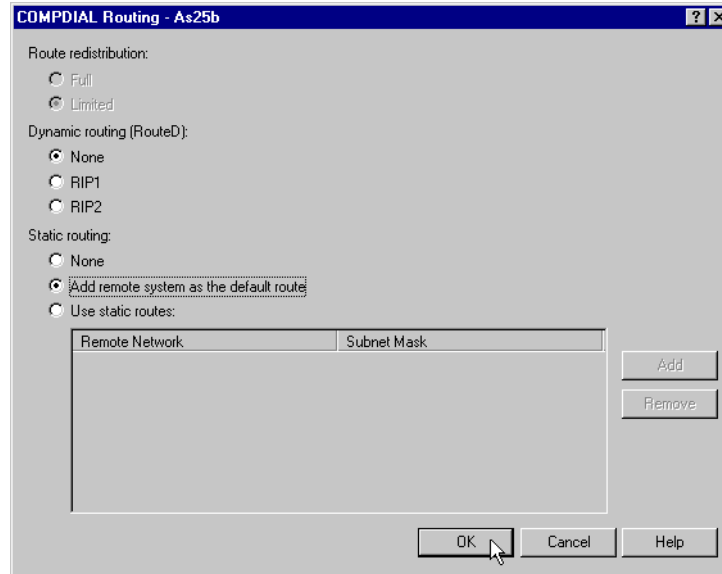


Figure 461. AS25b Defining the routing information for the PPP profile

34. Click **OK**.

35. Click the **Authentication** tab.

36. Click **Enable local system identification**.

37. Select **CHAP only**.

38. Enter `simh@lms.org` as the User name.

39. Enter the password associated with the user ID (Figure 462).

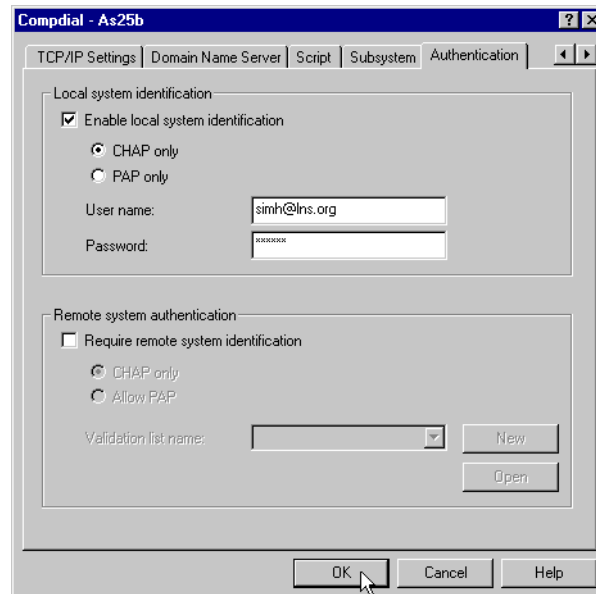


Figure 462. AS25b Setting the CHAP verification profile ID

40. Click **OK** to create the PPP profile.

9.3.2 Configuring the IPSec ESP tunnel to the LNS: Host to Gateway

Table 39 shows the planning worksheet that summarizes the values needed to configure the IPSec tunnel at the PPP dial-in client. This value is referred to as **G** in Figure 400 on page 353. The level of key and data protection must match AS05 (the wizard does *not* support multiple data protection *proposals* for negotiation with the remote VPN server). The pre-shared key must also match. The connection group is named *CmpDynKeyl*.

Table 39. AS25b New Connection Wizard planning worksheet - Host-to-gateway configuration

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Gateway
What will you name the connection group?	CmpDynKeyl
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	10.80.21.120
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	10.80.21.111
What is the pre-shared key?	123456789
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

9.3.2.1 Using the wizard to configure a host to gateway VPN on AS25b

To configure a host-to-gateway VPN with the wizard, perform the following steps:

1. Start Operations Navigator, and select system **AS25b**. Sign on as required.
2. Expand **Network->IP Security**.
3. Right click **Virtual Private Networking**, and select **Configuration** from the menu (Figure 463 on page 397).

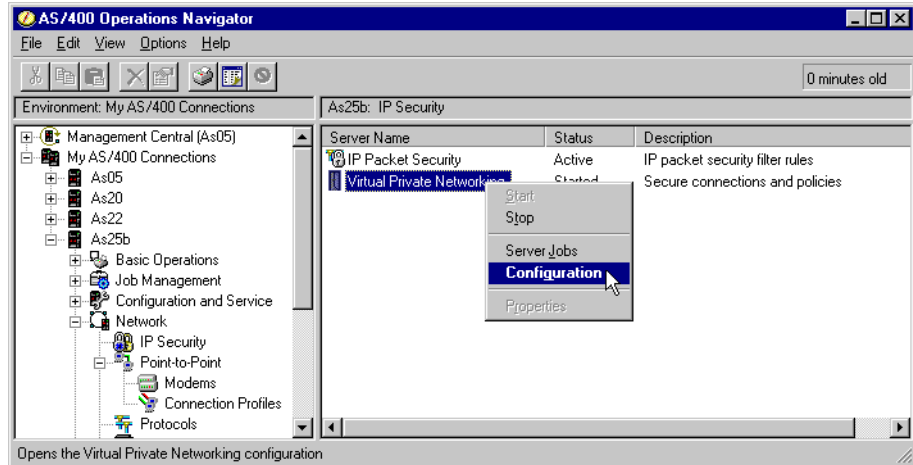


Figure 463. AS25b Starting the VPN configuration

- From the Virtual Private Networking window, select **File->New Connection... ->Host to Gateway** (Figure 464).

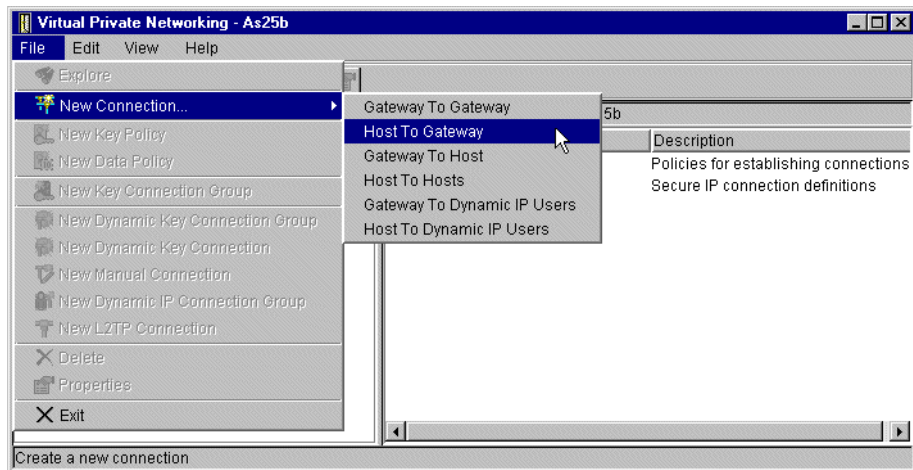


Figure 464. AS25b Starting the wizard for a Host To Gateway connection

- The New Connection Wizard starts. Click **Next**.
- Enter `CmpDynKey1` for the name of the profile.
- Enter `L2TP Compulsory tunnel with fixed IP address` or similar for the Description (Figure 465 on page 398).

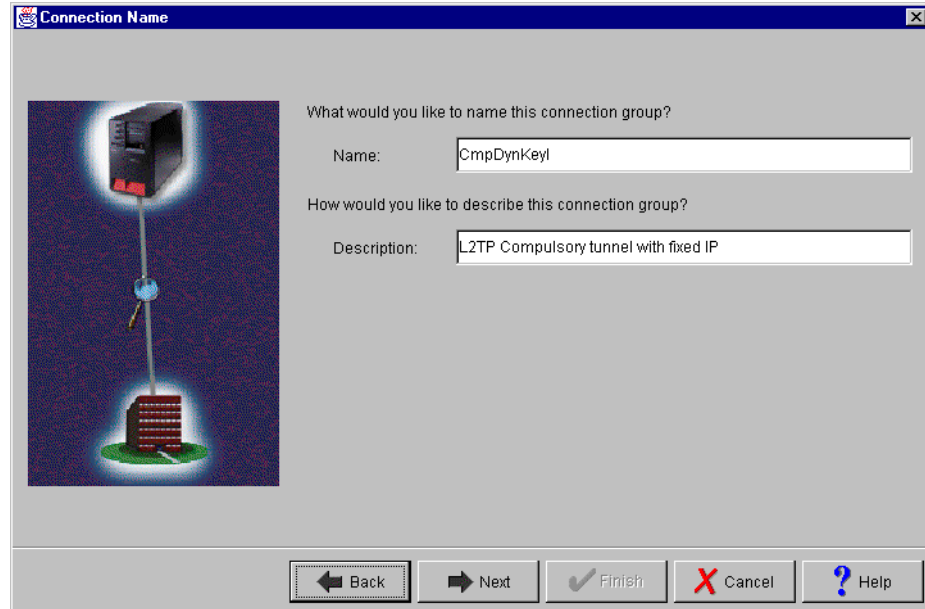


Figure 465. AS25b Configuring the connection

8. Click **Next**.
9. Click **Balance security and performance** (Figure 466).

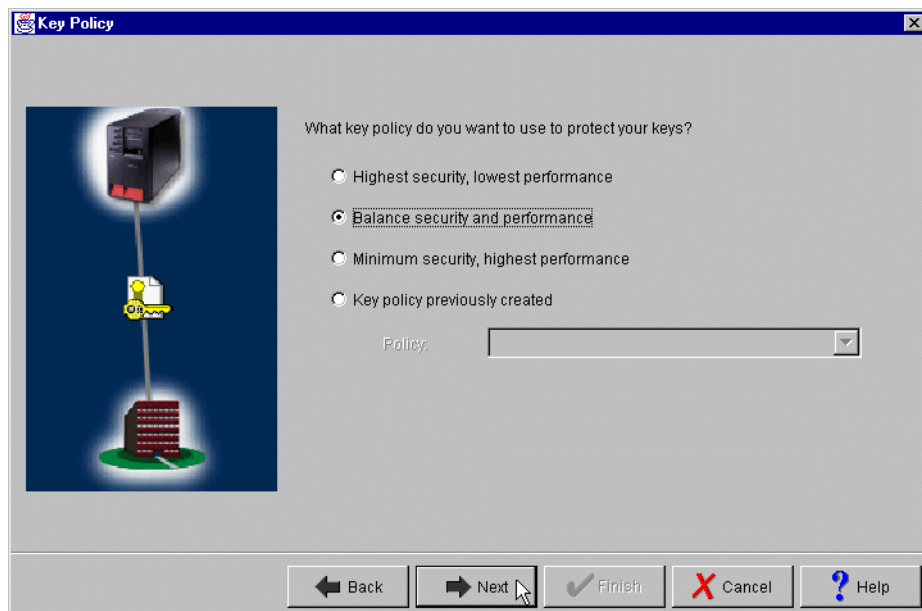


Figure 466. AS25b Key Policy - Selecting balanced security and performance

10. Click **Next**.
11. Select **Version 4 IP address** from the Identifier type pull down menu.
12. Select *any* existing interface from the IP Address pull-down menu (Figure 467 on page 399).

Tip

The Local Key Server IP address that you are configuring through the wizard in this step *must* be the IP address that the LNS assigns to the PPP dial-in client (10.80.21.120 in this scenario). Refer to planning worksheet in Table 39 on page 396 and Figure 400 on page 353. However, the wizard does not allow you to enter an IP address that is not already configured on the system. Remember, the IP address 10.80.21.120 is assigned once the L2TP tunnel is established. Therefore, you need to update this value after finishing the wizard configuration.

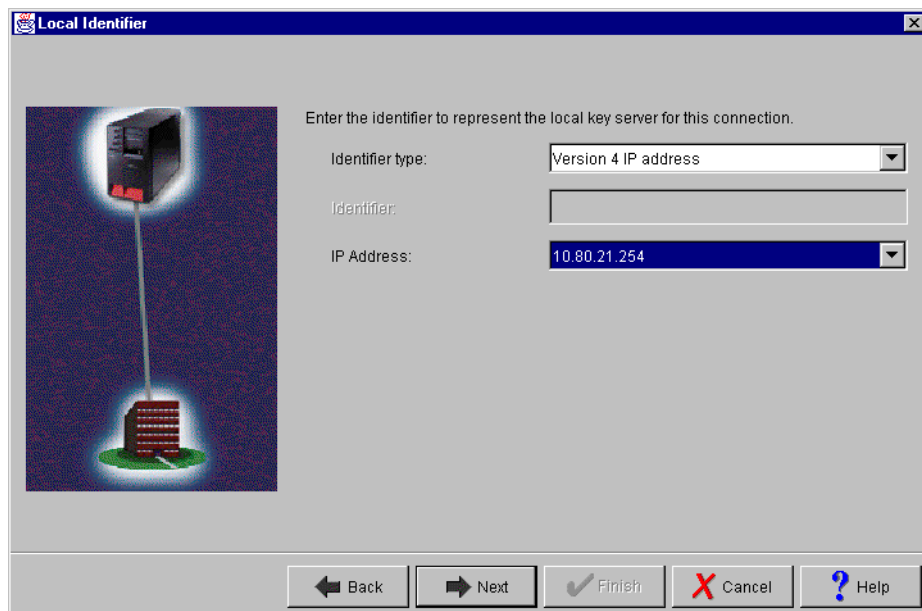


Figure 467. AS25b Local Identifier - Configuring the local key server identifier

13. Click **Next**.

14. Select **Version 4 IP address** for the Identifier type.

15. Enter 10.80.21.111 for the IP address parameter.

16. Enter 123456789 for the pre-shared key. See Figure 468 on page 400.

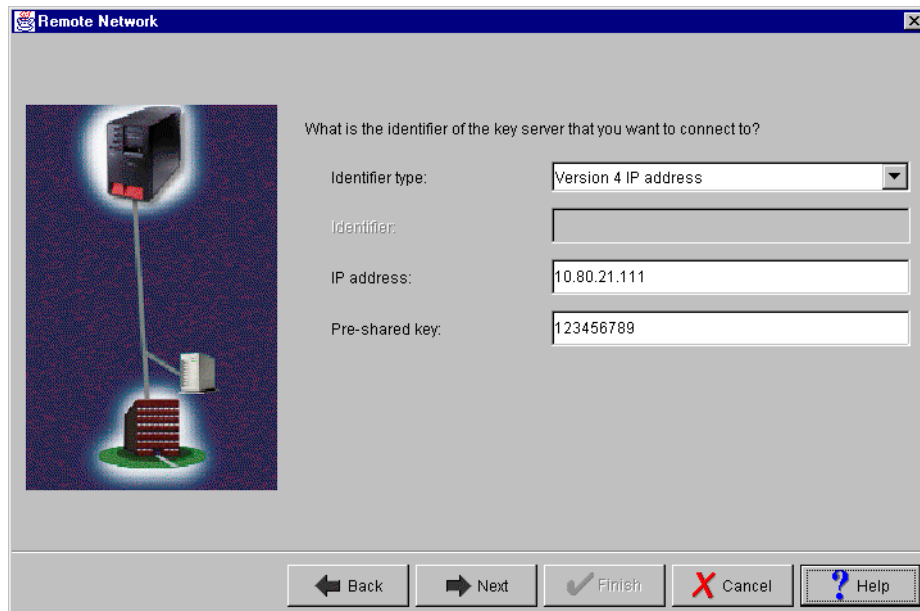


Figure 468. AS25b Setting the remote key server identifier

17. Click **Next**.

18. Select **Balance security and performance** in the Data Policy window (Figure 469).

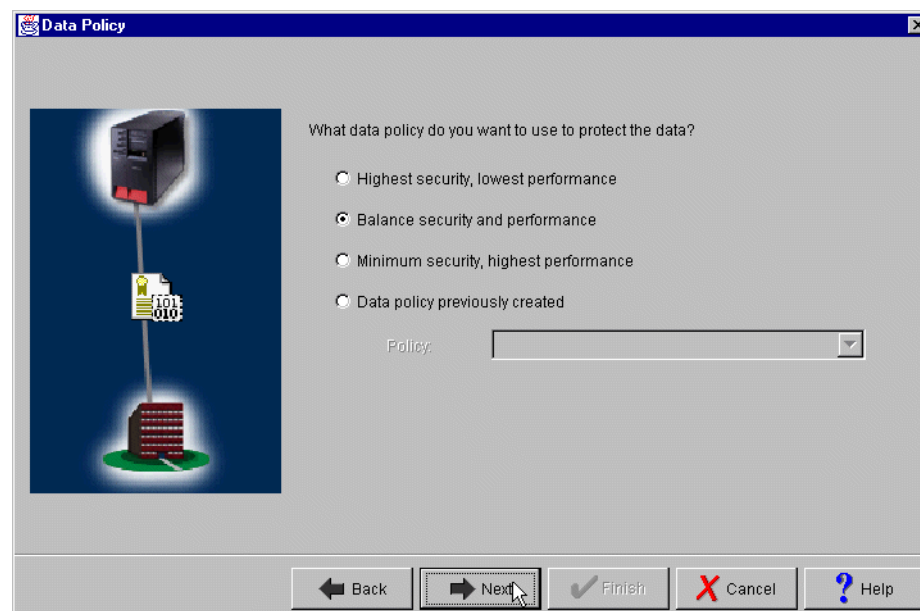


Figure 469. AS25b Defining the data security policy

19. Click **Next**.

The summary window is displayed as shown in Figure 470 on page 401.

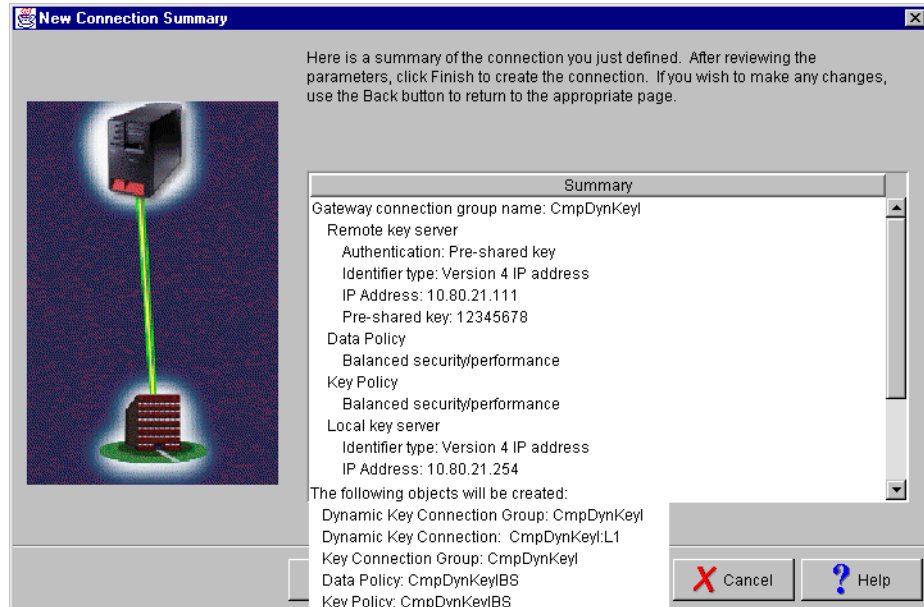


Figure 470. AS25b Wizard host-to-gateway configuration summary

20. Click **Finish**.

At this point, the wizard creates the objects listed in the summary page (Figure 470). You need to modify some of these values as required to protect the L2TP compulsory tunnel. The following sections explain how to customize the objects created by the wizard.

9.3.2.2 Modifying the local key server IP address

As explained in 9.3.2.1, “Using the wizard to configure a host to gateway VPN on AS25b” on page 396, the wizard does not allow you to enter an IP address that is not already configured on the system. The local key server IP address in the dial-in client must be the IP address that the LNS assigns to it through the virtual PPP connection (10.80.21.120 in this scenario). To modify the local key server IP address configured by the wizard, perform the following steps:

1. At the Virtual Private Networking window, click **Key Connection Groups**.
2. Select **CompDynKeyl**, and right-click on it.
3. Select **Properties** from the pull-down menu (Figure 471 on page 402).

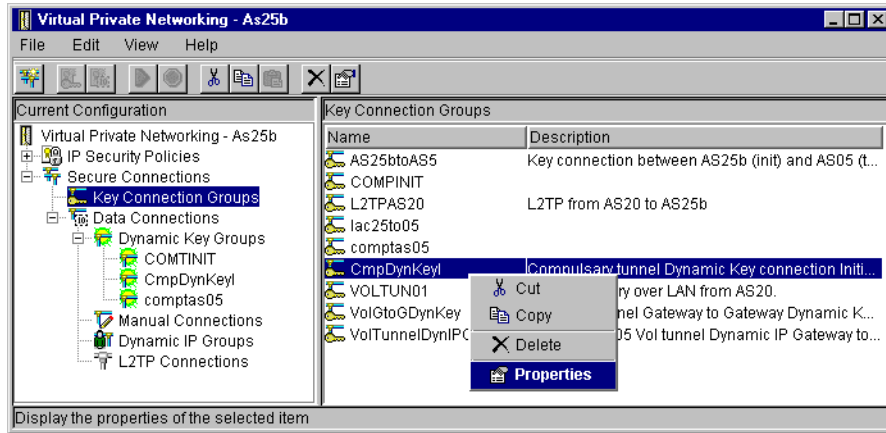


Figure 471. AS25b Modifying the key connection group - CmpDynKey1

The Properties window opens.

4. Click the **Associations** tab.
5. In the Local key server - IP address field, enter 10.80.21.120. This is the IP address that the LNS assigns to the PPP dial-in client in the compulsory tunnel.

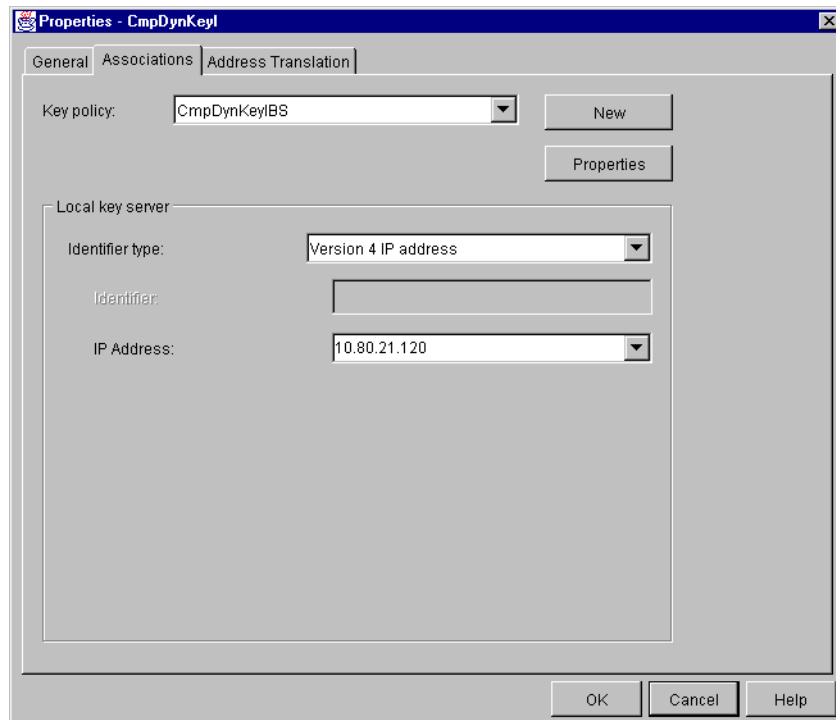


Figure 472. AS25b Modifying the local key server IP address

6. Click **OK**.

9.3.2.3 Modifying the Dynamic Key Connection

For a dial-in client in a compulsory tunnel, you must customize the connection to:

- Start when TCP/IP starts. This causes the connection to start when the PPP connection profile starts on the initiator.
- Local address must point to the PPP connection profile (initiator).

Follow these steps:

1. Expand **Data Connection->Dynamic Key Groups**.
2. Click **CmpDynKeyl**.
3. Right-click **CmpDynKeyl:L1** (connection), and select **Properties** in the pull-down menu (Figure 473).

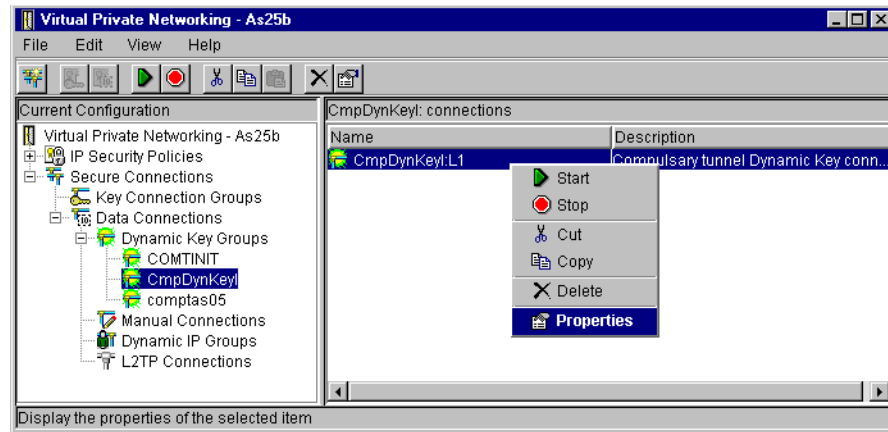


Figure 473. AS25b Modifying the dynamic key connection CmpDynKeyl

4. In the General page, select **Start when TCP/IP is started** (Figure 474).

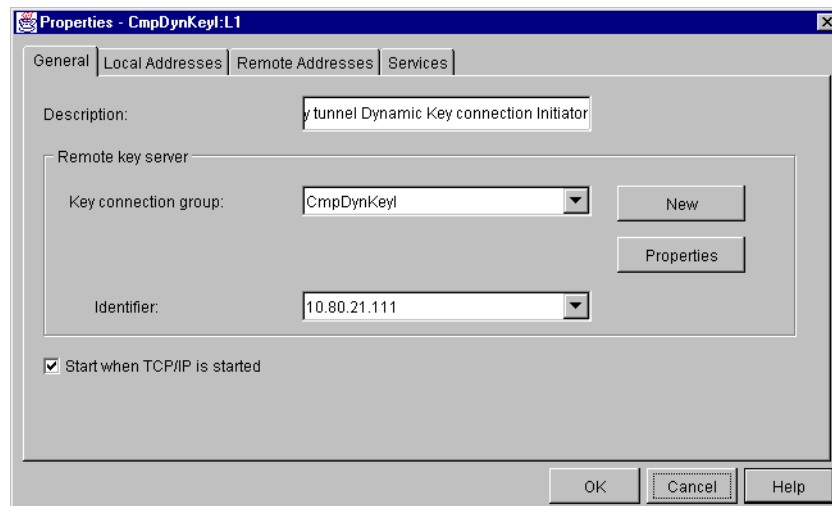


Figure 474. Starting the connection when the PPP connection profile starts

5. Click the **Local Addresses** tab.
6. In the Identifier type pull-down menu, select **Point-to-point profile**.

7. In the Identifier field, select the PPP connection profile **LACDIALUP** (Figure 475).

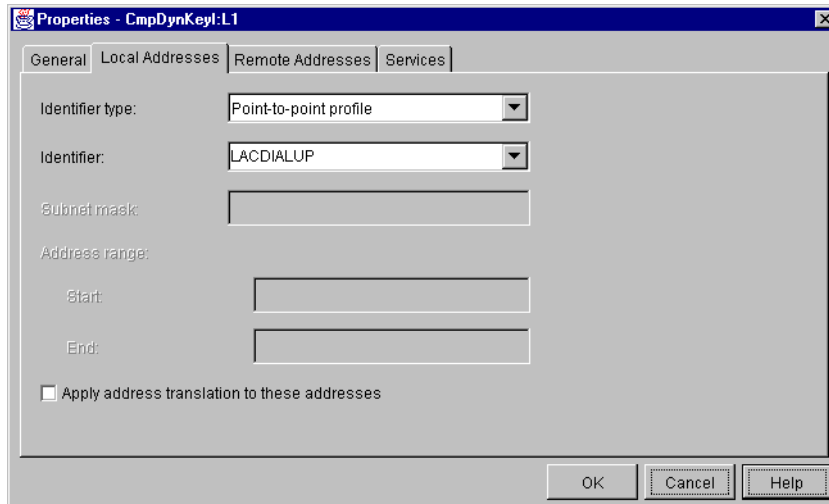


Figure 475. AS25b Local address points to virtual PPP initiator profile

8. Click **OK**.
9. Click the **Remote Addresses** tab. Enter the address of the remote data endpoint 10.80.21.0, mask 255.255.255.0. This is the corporate internal network with which the dial-in client can communicate (Figure 476).

Note: You can specify the remote address in the IPsec filter for this connection group or in the connection.

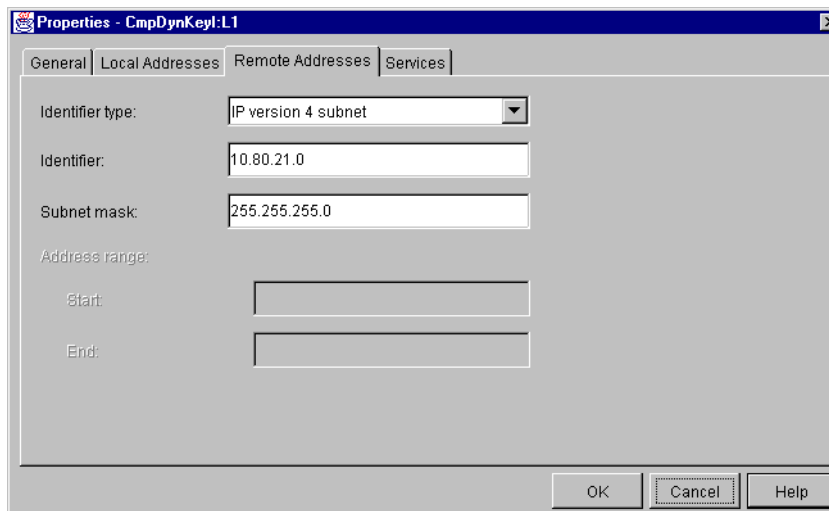


Figure 476. AS25b Defining the remote addresses for the data connection

10. Click **OK**.
11. Right-click the Dynamic Key Group **CmpDynKey1**. Select **Properties** from the pull-down menu (Figure 477 on page 405).

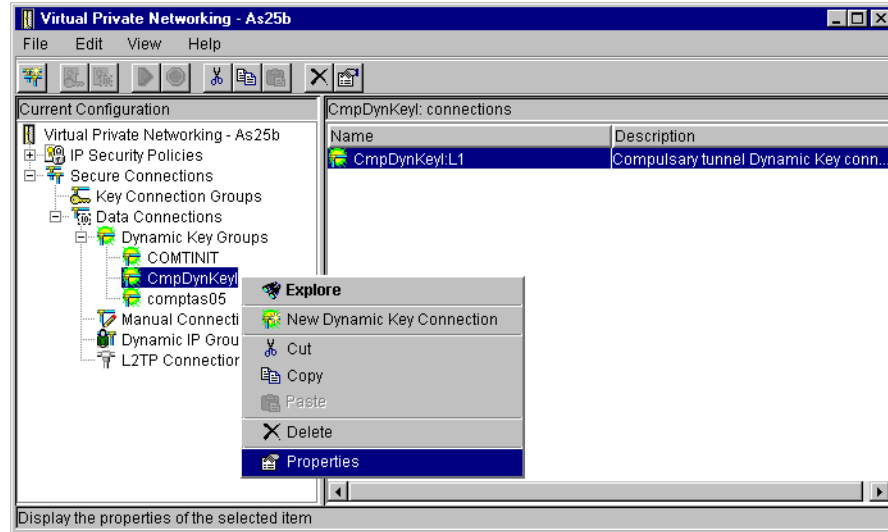


Figure 477. AS25b Dynamic key connection group CmpDynKey - Properties

12. Click the **Policy** tab. The fields in the policy window determine from where the values for active connections come. See Figure 478.

- **Local data endpoint:** Select **Connection**. The local data endpoint is the IP address assigned by the LNS over the virtual PPP initiator profile (10.80.21.120 in this scenario).
- **Remote addresses:** Select **Connection**. The remote data endpoint is the corporate subnet (10.80.21.0 subnet, mask 255.255.255.0) defined in the Connection - Remote addresses window (Figure 476). If you select Filter rules, this value comes from the IPsec filter for the connection group.
- Specify **Filter rules** for all the other fields in the Policy window.

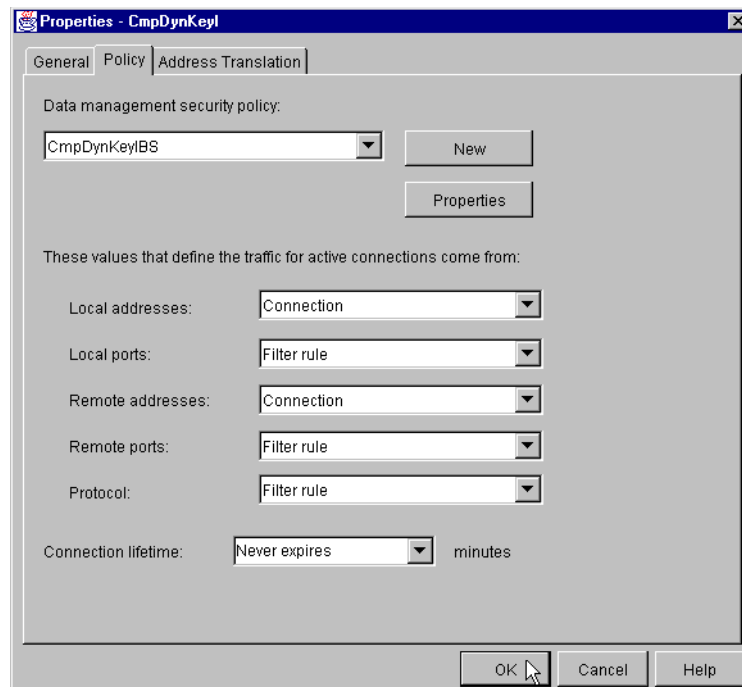


Figure 478. AS25b Policy window

9.3.3 Configuring IP filters in the initiator dial-in client (AS25b)

Table 40 shows the planning worksheet for the IP filters in the initiator AS/400 system (AS25b). It is important to notice the following points:

- Local key server is the IP address in the corporate IP address space assigned by the LNS (10.80.21.120).
- Remote key server is the IP address in the corporate IP address space of the LNS on the internal network (10.80.21.111).
- The IP address of the remote network is the corporate subnet (10.80.21.0).
- Filter interface is the PPP dial-up profile (LACDIALUP).

Table 40. Planning worksheet - IP filter rules AS25B

This is the information you need to create your IP filters to support your VPN	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.	Host
Is the <i>remote</i> VPN server acting as a host or gateway ?	Gateway
What name do you want to use to group together the set of filters that will be created?	COMPT
If <i>your</i> server is acting as a gateway ... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	
If the remote server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	10.80.21.0 255.255.255.0 Corporate
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	10.80.21.120
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	10.80.21.111
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	LACDIALUP
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

To complete the VPN configuration on AS25b, you must configure the following IP filters:

1. Defined Address. Configure the destination network subnet as shown in Figure 479.

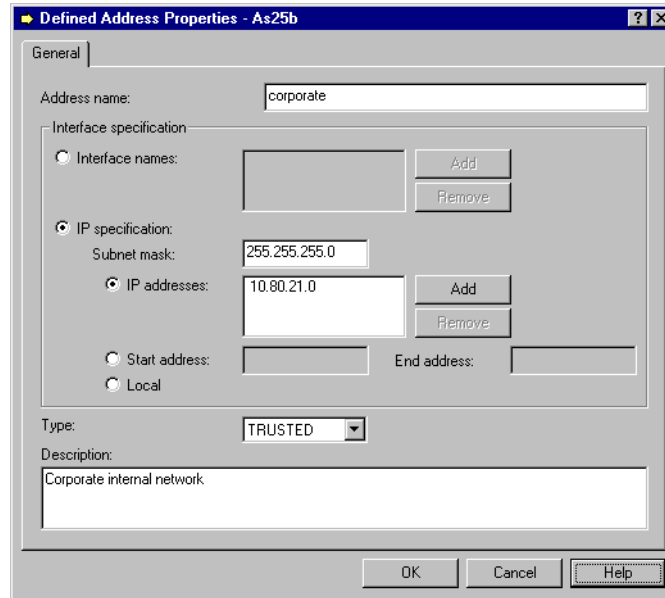


Figure 479. AS25b Defining the remote data endpoint - Corporate subnet

2. Filter interface. The filter entries must be associated to a filter interface. For the dial-in client in a compulsory tunnel, this interface is the PPP profile, which is LACDIALUP in this scenario (Figure 480).

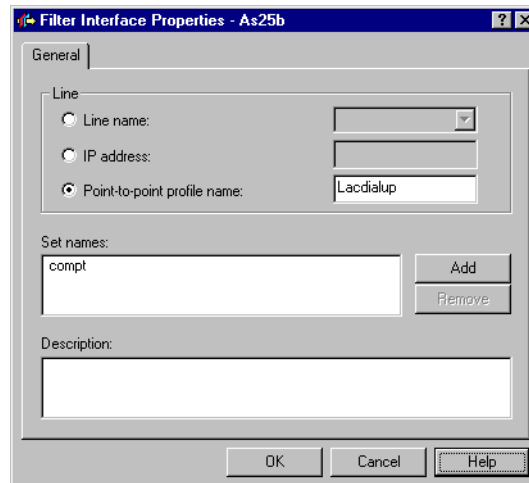


Figure 480. AS25b Filter interface PPP profile

3. IKE rules. Define the outbound filter rules to permit IKE negotiation. See Figure 481 and Figure 482 on page 408.

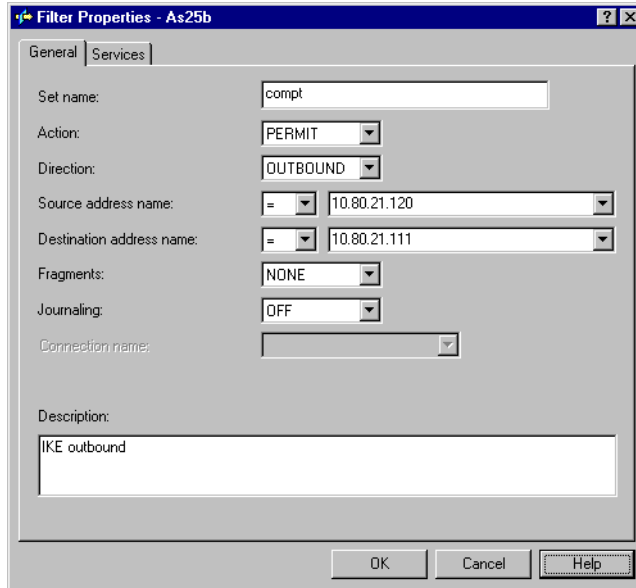


Figure 481. AS25b IKE outbound filter rule - General page

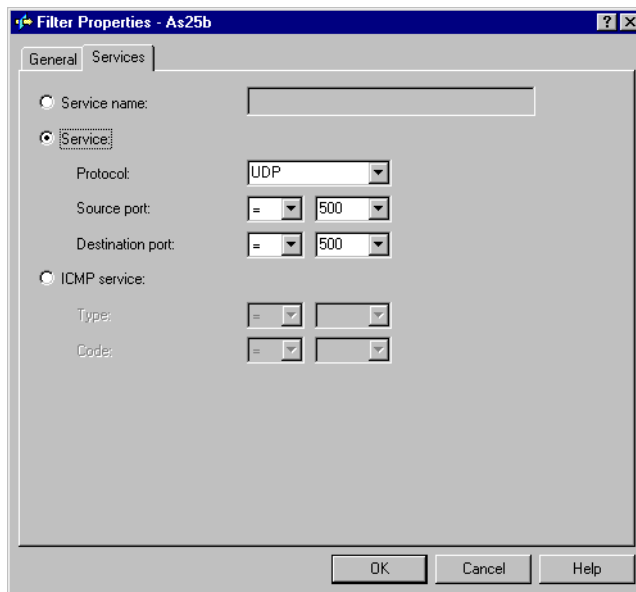


Figure 482. AS25b IKE outbound filter rule - Services page

4. IKE rules. Define the inbound filter rules to permit IKE negotiation. See Figure 483 and Figure 484 on page 409.

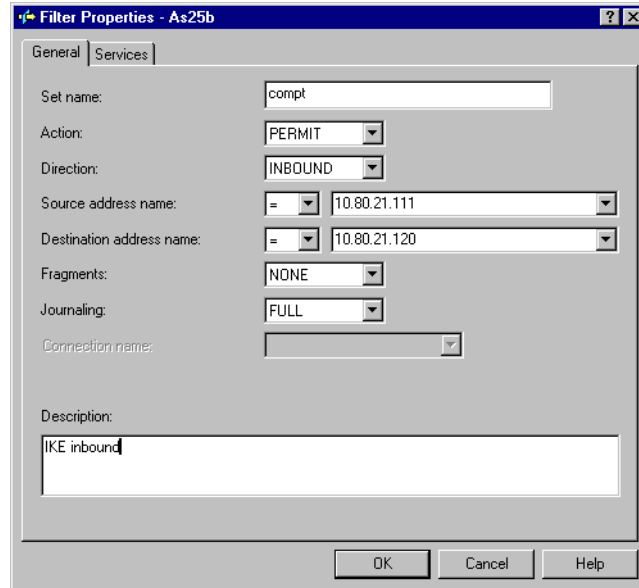


Figure 483. AS25b IKE inbound filter rule - General page

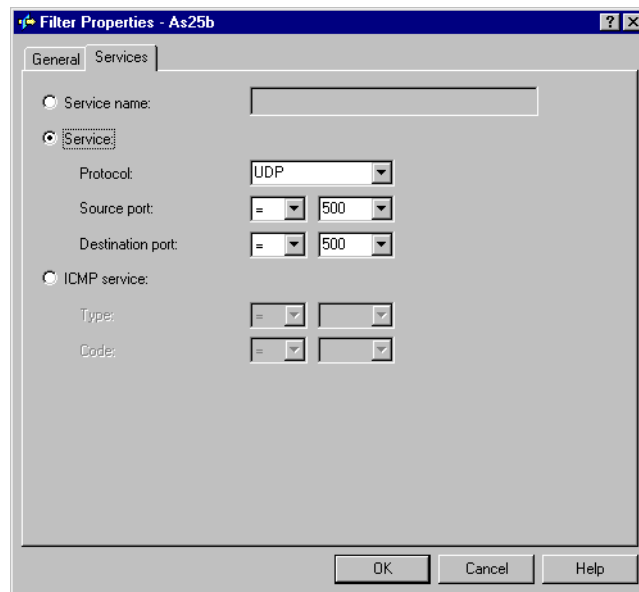


Figure 484. AS25b IKE inbound filter rule - Services page

5. IPSEC filter rule. Define the IPSEC filter rule (Figure 485 and Figure 486 on page 410). Data endpoints are local host (10.80.21.120) and corporate subnet (10.80.21.0). Connection is the dynamic key connection group configured in 9.3.2, “Configuring the IPsec ESP tunnel to the LNS: Host to Gateway” on page 396.

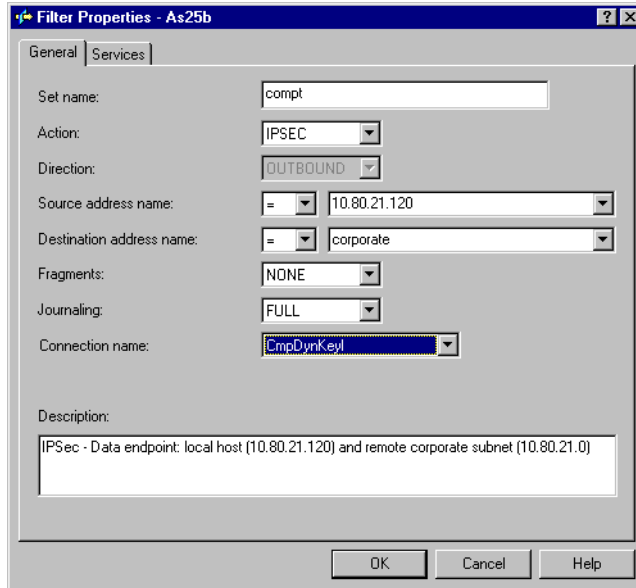


Figure 485. AS25b IPSEC filter rule - Data endpoints are the local host and corporate subnet

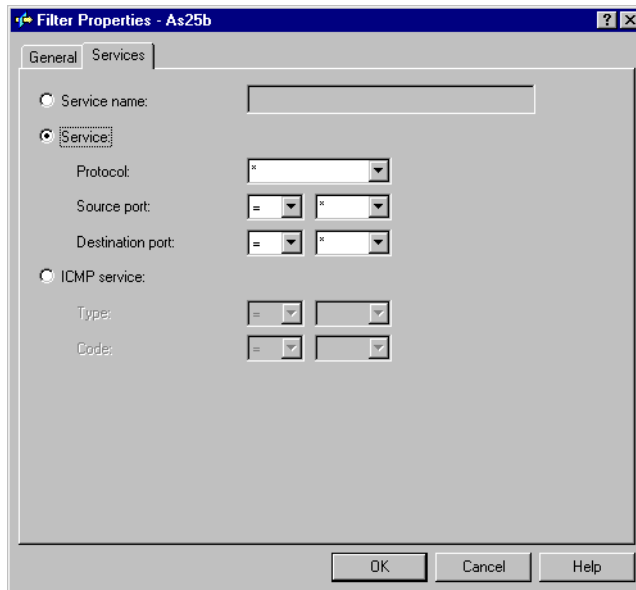


Figure 486. AS25b IPSEC filter rule - Services page

Figure 487 on page 411 shows the summary of the filters configured above.

```

IP Packet Security: All Security Rules
#Corporate Subnet
ADDRESS corporate IP = 10.80.21.0 MASK = 255.255.255.0 TYPE=TRUSTED
#Apply the filters to PPP profile LACDIALUP
FILTER_INTERFACE INTERFACE = Lacdialup SET = compt
#IKE rules
FILTER SET compt ACTION = PERMIT DIRECTION = OUTBOUND
SRCADDR = 10.80.21.120 DSTADDR = 10.80.21.111
PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = NONE
FILTER SET compt ACTION = PERMIT DIRECTION = INBOUND
SRCADDR = 10.80.21.111 DSTADDR = 10.80.21.120
PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = NONE
#IPSec Rule - Data endpoints: Local host (10.80.21.120) and corporate net
FILTER SET compt ACTION = IPSEC DIRECTION = OUTBOUND
SRCADDR = 10.80.21.120 DSTADDR = corporate PROTOCOL = * DSTPORT = * SRCPORT = *
FRAGMENTS = NONE JRN = NONE CONNECTION_DEFINITION = CmpDynKeyI

```

Figure 487. AS25b Filter rules summary at the dial-in client in an L2TP compulsory tunnel

9.4 Starting the connections in an L2TP compulsory tunnel with IPSec

This section provides a summary of the tasks you need to perform to start all the required connections in an L2TP compulsory tunnel protected by IPSec.

9.4.1 Starting the LNS in an L2TP compulsory tunnel (AS05)

To start the functions needed in the LNS (AS05), perform the following tasks:

1. Start the filters.
2. Start Virtual Private Networking.
3. Start the L2TP terminator profile by following these steps:
 - a. Expand **Network**.
 - b. Expand **Point-to-Point**, and click **Connection profiles** as shown in Figure 488 on page 412.

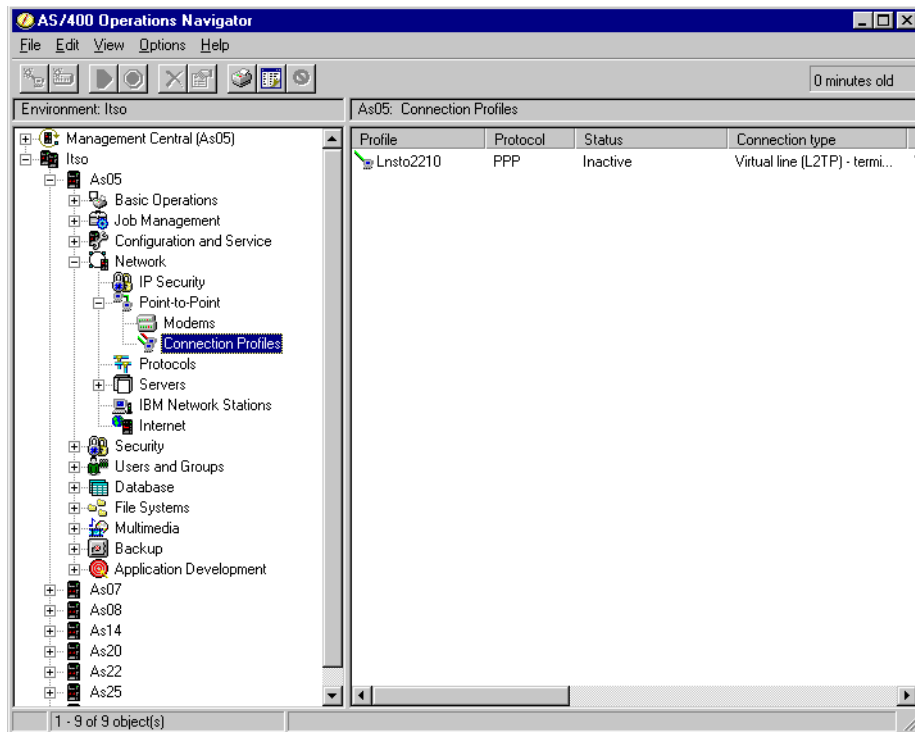


Figure 488. AS05 Starting the virtual PPP connection profile

- c. Right-click the virtual line (L2TP) terminator profile, which is **Lnsto2210** in this scenario. Select **Start** from the pull-down menu. Alternatively, there is an activate icon (a green triangle) on the toolbar. Once the profile has started, it will be in a status of *Waiting for connection requests*.

9.4.2 Starting the dial-in client in an L2TP compulsory tunnel (AS25b)

To start the functions needed in the dial-in client (AS25b), perform the following tasks:

1. Start the filters.
2. Start Virtual Private Networking.
3. Start the PPP dial-up connection profile by following these steps:
 - a. Expand **Network**.
 - b. Expand **Point-to-Point**, and click **Connection profiles** as shown in Figure 489 on page 413.

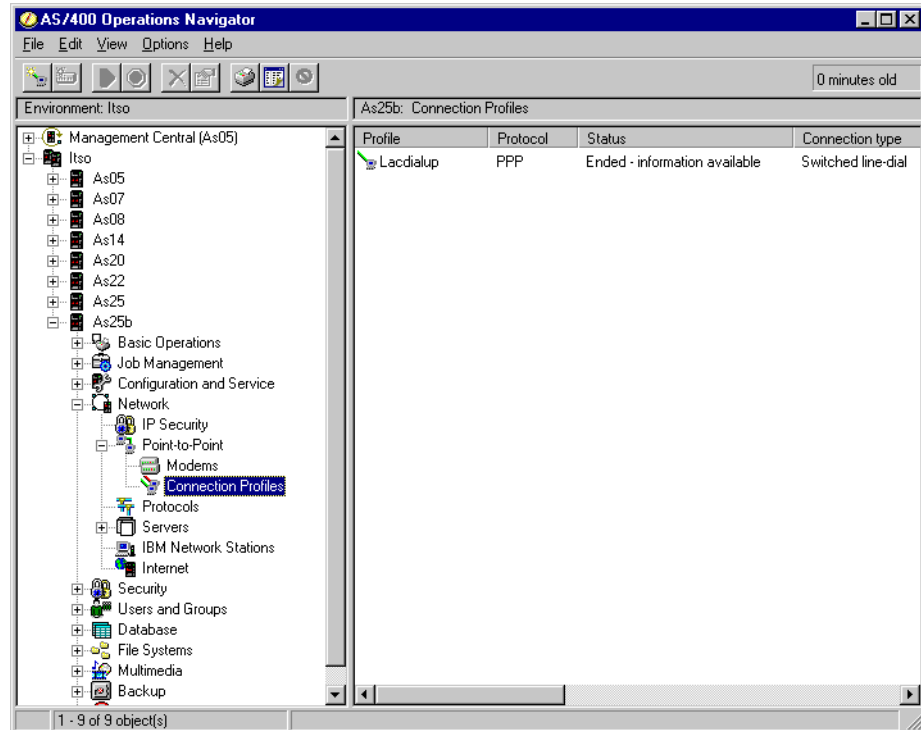


Figure 489. AS25b Point-to-Point Connection Profiles

- c. Right-click the PPP dial profile, and select **Start**. In this scenario, the profile name is **LACDIALUP** as shown in Figure 490 on page 414. Alternatively, there is an activate icon (a green triangle) on the toolbar. Once the profile has started, it dials the remote system (ISP/LAC), configures LCP, authenticates with remote systems, configures IPCP, starts TCP/IP interface, and goes to an `active` status, assuming there are no errors.

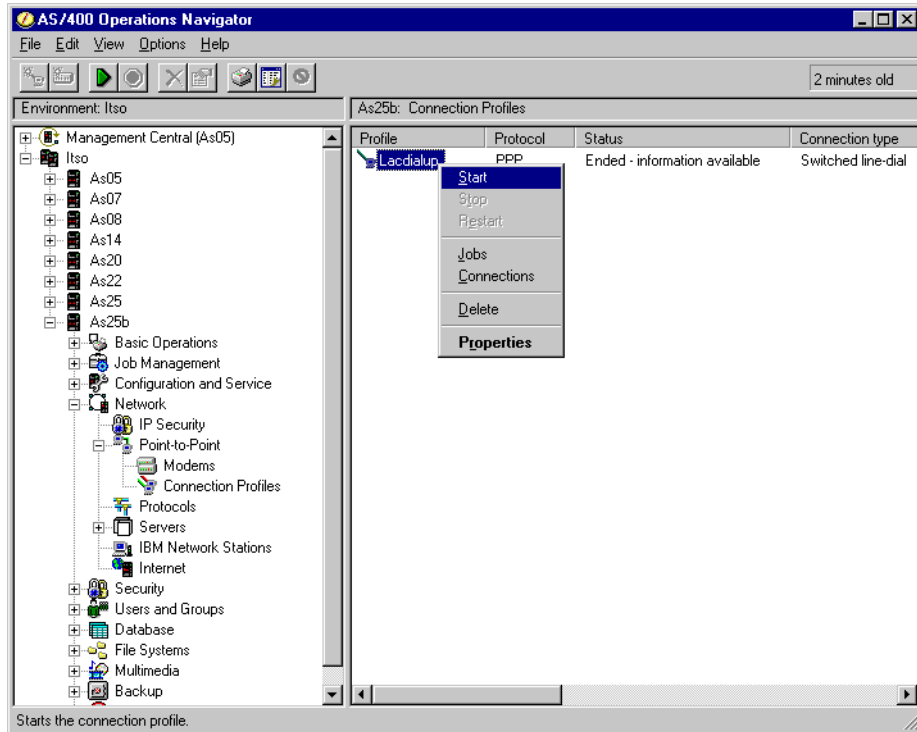


Figure 490. Starting the PPP dial profile

4. Display the connections to verify it is active. At the Virtual Private Networking window, select **View->Active Connections**. The Active Connections window is displayed as shown in Figure 491.

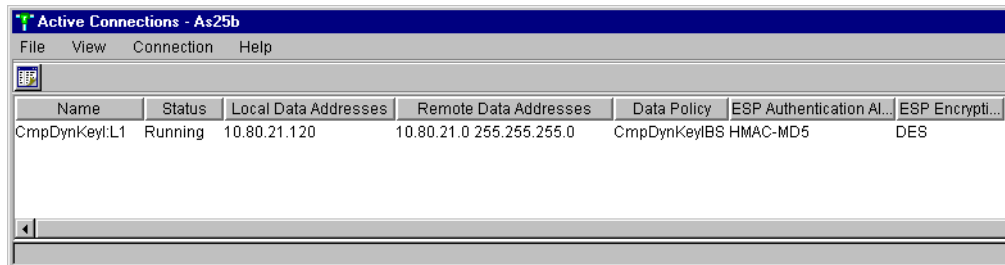


Figure 491. Active Connection window - IPsec ESP tunnel to AS25b

9.5 Verifying interfaces and routes

This section reviews the interfaces and routes in the LNS (AS05) and the dial-in client (AS25b).

9.5.1 Verifying interfaces and routes in the LNS (AS05)

Figure 492 on page 415 shows the result of the `NETSTAT OPTION(*IFC)` command in AS05. Notice that the IP address assigned to the remote dial-in client (10.80.21.120) is listed as a local interface associated with the line description L252170001.

```

Work with TCP/IP Interface Status
System: AS05

Type options, press Enter.
5=Display details 8=Display associated routes 9=Start 10=End
12=Work with configuration status 14=Display multicast groups

  Internet      Network      Line      Interface
Opt Address      Address      Description Status
-----
5  10.80.21.111  10.80.21.0   ITSCTRNO  Active
   10.80.21.120 10.80.21.120 L252170001 Active
   127.0.0.1     127.0.0.0   *LOOPBACK Active
   204.146.18.5  204.146.18.0 TRLANC    Active

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F11=Display line information  F12=Cancel
F13=Sort by column  F24=More keys

```

Figure 492. AS05 IP Interfaces

The L2TP terminator (LNS) performs proxy ARP for the remote client through the associated local interface 10.80.21.111. You can verify it by entering 5 (Display details), by the IP address assigned to the remote client 10.80.21.120 as shown in Figure 493. The client appears as a local interface in the LNS. When hosts in the internal network broadcast ARP requests with IP address 10.80.21.120, AS05 recognizes that it is a local interface. It then sends back the MAC address corresponding to the associated local interface 10.80.21.111. Once the packet reaches AS05, it knows how to route it to the dial-in client.

```

Display TCP/IP Interface Status
System: AS05

Interface host name . . . . . :
Internet address . . . . . : 10.80.21.120
Subnet mask . . . . . : 255.255.255.255
Network address . . . . . : 10.80.21.120
Host address . . . . . : *
Directed broadcast address . . . . . : *NONE

Interface status . . . . . : Active
Change date/time . . . . . : 07/27/99 16:17:45
Line description . . . . . : L252170001
Line type . . . . . : *NOTFND
Associated local interface . . . . . : 10.80.21.111
Type of service . . . . . : *NORMAL
Maximum transmission unit . . . . . : 2046
Automatic start . . . . . : *NO

Press Enter to continue.

F3=Exit  F6=Print  F12=Cancel  F22=Display entire field

```

Figure 493. AS05 - Remote client IP address and associated local interface

Figure 494 on page 416 shows the TCP/IP route information in AS05 after entering the NETSTAT OPTION(*RTE) command.

```

Display TCP/IP Route Information
System: AS05
Type options, press Enter.
5=Display details

Route      Subnet      Next      Route
Opt  Destination  Mask      Hop      Available
10.80.21.120 *HOST      *DIRECT   *YES
10.80.21.0   255.255.255.0 *DIRECT   *YES
204.146.18.0 255.255.255.0 *DIRECT   *YES

F3=Exit  F5=Refresh  F6=Print list  F9=Command line
F11=Display route type  F12=Cancel  F13=Sort by column  F24=More keys

```

Figure 494. AS05 Route information

9.5.2 Verifying interfaces and routes in the dial-in client (AS25b)

Figure 494 shows the result of the `NETSTAT OPTION(*IFC)` command in AS25b. Notice that the IP address assigned to the dial-in client (10.80.21.120) is listed as a local interface associated with the PPP connection profile LACDIALUP.

```

Work with TCP/IP Interface Status
System: AS25B
Type options, press Enter.
5=Display details  8=Display associated routes  9=Start  10=End
12=Work with configuration status  14=Display multicast groups

Internet      Network      Line      Interface
Opt  Address      Address      Description  Status
10.70.41.1    10.70.0.0    TRNLINE    Active
10.80.21.120  10.80.21.120 LACDIALUP  Active

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F11=Display line information  F12=Cancel
F13=Sort by column  F24=More keys

```

Figure 495. AS25b IP Interfaces

Figure 496 on page 417 shows the TCP/IP route information in AS05 after entering the `NETSTAT OPTION(*RTE)` command. Notice the `*HOST` route to the remote LNS, 10.80.21.111 (AS05).


```

                                Display TCP/IP Route Information
                                System:  AS25B

Type options, press Enter.
  5=Display details

   Route          Subnet          Next          Route
Opt Destination    Mask            Hop            Available
   10.80.21.120   *HOST          *DIRECT       *YES
   10.70.0.0     255.255.0.0   *DIRECT       *YES
   10.80.21.111  *HOST          10.80.21.120 *YES
  5 *DFTRROUTE    *NONE          10.80.21.120 *YES

F3=Exit  F5=Refresh  F6=Print list  F9=Command line
F11=Display route type  F12=Cancel    F13=Sort by column  F24=More keys

```

Figure 496. AS25b Route information

Figure 497 shows the *DFTRROUTE on the dial-in client, AS25b. It points to the PPP connection profile. The IP address assigned by the LNS (10.80.21.120) is the next hop.

```

                                Display Default Route Details
                                System:  AS25B

Route information:
Route destination . . . . . : *DFTRROUTE
Order used . . . . . : 1
Next hop host name . . . . . :
Next hop . . . . . : 10.80.21.120
Type of service . . . . . : *NORMAL
Route available . . . . . : *YES
Route type . . . . . : *DFTRROUTE
Route source . . . . . : *CFG
Change date/time . . . . . : 07/27/99 16:18:34
Route maximum transmission unit . . . . . : 2046
Reference count . . . . . : 0

Local interface information:
Internet address . . . . . : 10.80.21.120
Subnet mask . . . . . : 255.255.255.255
Network address . . . . . : 10.80.21.120
Interface status . . . . . : Active
Line description . . . . . : LACDIALUP
Line type . . . . . : *PPP
F3=Exit  F6=Print  F12=Cancel  F22=Display entire field

```

Figure 497. AS25b Default route

Chapter 10. Secure remote access for PC clients over the Internet

Remote users, whether at home or on the road, want to be able to communicate securely and cost-effectively with the corporate office. Remote users want to be able to use the same applications that are available to employees at the office, and with a similar level of security. For example, from home or from a hotel, they want to be able to access the latest sales report, the marketing strategy document, human resources information, and so on. Although many still use expensive long-distance calls and toll-free numbers, the general trend for companies is to take advantage of the lower rates and broad access of the Internet. Connecting the remote client to the corporate office gateway over a VPN offers a good solution to remote access over the Internet. Refer to Chapter 1, “Virtual Private Network (VPN) overview” on page 3, for a general description of the advantages of connecting remote clients using VPNs.

One way to implement this scenario is to use PC clients that support VPN protocols. Currently, there are VPN clients on the market that support IPsec protocols, such as SafeNet Soft-PK by IRE. Other clients support tunneling protocols, like PPTP and L2TP, in combination with IPsec such as WinVPN by iVasion.

IPsec VPN clients provide authentication, integrity, and encryption. L2TP-enabled clients allow the assignment of internal IP addresses (addresses in the corporate network address space) to the remote client making it appear directly connected to the internal network. Refer to Chapter 2, “Introduction to Layer 2 Tunneling Protocol (L2TP)” on page 33, for an introduction to L2TP. To satisfy security requirements, L2TP must be used in combination with IPsec. IPsec VPN clients satisfy the remote access security requirements for most AS/400 customers.

L2TP-enabled clients (always in combination with IPsec) are desirable when the security policies of the corporation rely on internal corporate IP addresses for access control. L2TP address assignment capabilities extend the intranet to the remote dial-in client over the intervening network (Internet).

Note

The VPN clients used during our tests were early beta versions of the software. Expect some differences in the final (generally available) version of the products.

10.1 Remote PC clients with IPsec-only support

This section explores the implementation of IPsec PC clients accessing the AS/400 system at the corporate office using a dial-up PPP connection to the ISP. These VPN clients do not support L2TP. The client used during the tests for this scenario was SafeNet Soft-PK by IRE. For more information about this client, including marketing information, log on to: <http://www.ire.com>

10.1.1 Scenario characteristics

The characteristics of this scenario are:

- Mobile employees access the corporate office by dialing up an ISP Point of Presence (PoP).
- ISPs *dynamically* assign globally routable IP addresses to the remote dial-in clients.
- The corporate office gateway is an AS/400 system with IPsec and L2TP support.

Note: The L2TP support at the corporate gateway is only required in the scenario described in 10.2, “Remote PC clients with IPsec and L2TP support” on page 444.

- The corporate office gateway is connected to the Internet through a leased line (LAN connection).

Figure 498 shows an overview of this scenario.

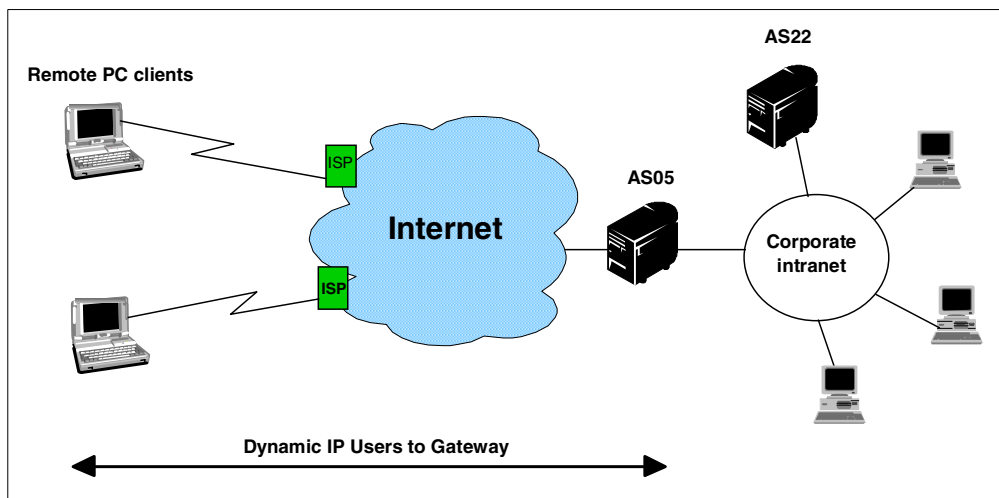


Figure 498. Remote dial-in PC clients to corporate network connection - Scenario overview

Important note

All the scenarios in this redbook show the AS/400 security gateway at the corporate office directly connected to the Internet. The absence of a firewall in these scenarios is meant to simplify the VPN examples. It does *not* imply that the use of a firewall is not necessary. For information about how the AS/400 security gateway interacts with a firewall, refer to Chapter 12, “Don’t forget a firewall: Protecting your VPN server” on page 515.

10.1.2 Scenario objectives

The objectives of this scenario are:

- All traffic between the remote PC clients and the corporate gateway AS/400 system (AS05) must be protected by IPsec.
- The company’s policies do not require the dial-in clients to be assigned internal IP addresses.

- Servers on the intranet do not need to support IPSec (except for the corporate gateway AS05).
- The corporate office gateway (AS05) must be able to handle remote clients with dynamically assigned IP addresses.

Note

If the remote dial-in clients don't support L2TP, it must be acceptable for the company to configure the default route in the internal hosts to point to the corporate gateway (AS05) as the next hop. The default route in the corporate gateway must be configured to point to the ISP router.

10.1.3 Scenario network configuration

Figure 499 shows the network configuration used for the remote dial-in VPN client scenario.

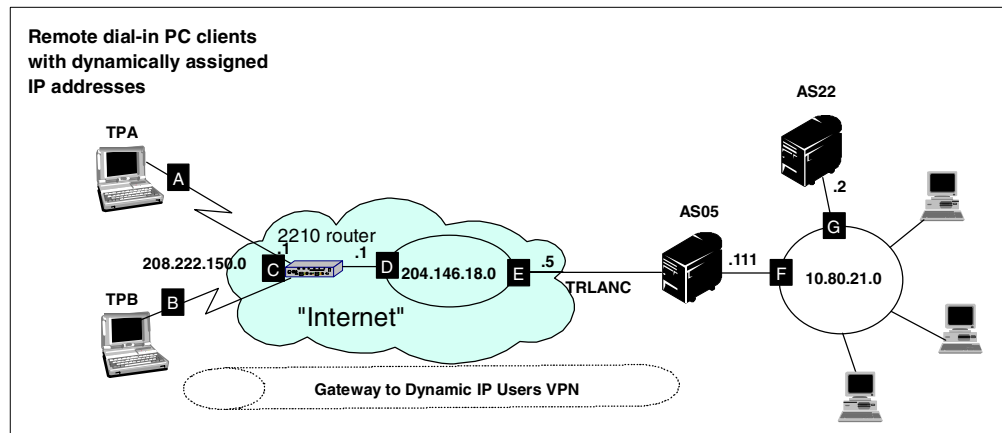


Figure 499. Remote dial-in client connection - Scenario network configuration

The "Internet" in our test network is replaced by a LAN (subnet 204.146.18.0) on the corporate side. The corporate gateway public interface (E) is connected to a router that simulates the ISP router (interface D).

The remote dial-in clients, ThinkPad A (TPA) and ThinkPad B (TPB), call the "ISP" router. The router dynamically assigns IP addresses to the clients in the subnet 208.222.150.0.

All hosts in the corporate intranet (10.80.21.0) are configured to use AS05 interface F as the default route. The corporate gateway AS05 is configured to use the ISP router interface D as the default route.

10.1.4 Implementation tasks: Summary

The following series is a summary of the tasks performed to implement this scenario:

1. Verify connectivity. Before you start configuring VPN and filters, you must ensure that the underlying TCP/IP network is properly configured and working.
2. Complete the planning worksheets for the appropriate dial-in VPN PC client.

3. Complete the planning worksheets for the corporate office gateway AS/400 system (AS05).
4. Configure a Gateway to Dynamic IP Users VPN on the AS/400 system (AS05).
5. Configure the filters in the AS/400 system (AS05).
6. Configure Windows 95 Dial-Up Networking on each client.
7. Install the VPN client on the PC.
8. Configure the VPN client (SafeNet Soft-PK) on TPA.
9. Start the VPN connections.
10. Check the VPN connection status.

10.1.5 Verifying end-to-end connectivity

Before you start configuring the VPN partners, it is important to work out any connectivity problems that may exist between the endpoints. In our scenario, we performed the following verification tests:

1. PING the AS/400 AS22 (**G**) from AS/400 AS05 (**F**). The PING command is used to check the proper IP addressing and routing setup.
2. PING the AS/400 AS05 (**F**) from AS/400 AS22 (**G**).
3. PING the router (**D**) from AS/400 AS05 (**E**).
4. From both PCs, TPA (**A**) and TPB (**B**) establish a PPP dial-up connection to the router (**C**) and PING the AS/400 AS05 (**E**).

Once the simple TCP/IP connectivity test is complete, proceed with the VPN configurations.

10.1.6 Completing the planning worksheet for the VPN PC clients

You must plan the configuration of the client end of the VPN tunnel between the remote dial-in clients and the AS/400 corporate gateway.

Since the client implementation and user interfaces are different for different vendors, we cannot provide a planning worksheet that fits all the VPN clients. However, the main objective of the planning worksheet is to show you one possible approach to plan the configuration in advance, help you to gather the necessary information, and make sure the right matching of parameters between hosts at both ends of the VPN takes place.

10.1.6.1 Planning worksheet for SafeNet Soft-PK client (TPA)

On TPA, we used the VPN client from IRE. The product name is SafeNet Soft-PK, and we tested with version 2.0.6 (Build 3). Table 41 on page 423 shows the planning worksheet with the information required to configure this client.

Table 41. IRE SafeNet planning worksheet - TPA to AS05

This is the information you need to create your VPN with IRE's SafeNet GUI	Scenario answers
What will you name the connection?	GWIntranet
How will you identify your local server? – IP address (n/a) – Domain name – E-mail address	E-mail address
What is the identifier of your local server?	tommy@itso.roch.com
How will you identify the remote server to which you are connecting?	IP subnet
What is the IP address of the remote party?	10.80.21.0
What is the subnet of the remote party?	255.255.255.0
What is the pre-shared key?	thomas12
What type of connection security is used? – Secure – Non-secure – Block	Secure
Is the client connecting to the remote host through a secure gateway tunnel? – No (checkbox remains unchecked) – Yes (checkbox is checked)	Yes
What is the identifier type of the remote gateway?	IP address
What is the IP Address of the remote gateway?	204.146.18.5
What local PC network interface is used for this connection?	Any
What are the authentication and encryption characteristics for the IKE authentication phase 1? – Authentication method – Encryption algorithm – Hash algorithm (data integrity) – SA Life – Key Group	Pre-shared key DES MD5 Seconds 7200 Diffie-Hellman Group 1
What are the key exchange characteristics for IKE phase 2? – ESP – AH	ESP
– ESP settings • Encryption algorithm • Hash algorithm • Encapsulation • SA Life	DES MD5 Tunnel Seconds 3600
– AH settings • Hash algorithm • SA Life	n/a

The ISP dynamically assigns an IP address to this PC client (TPA). Therefore, you can't use the IP address as the local identifier. The planning worksheet includes several parameters that do not appear in the AS/400 system planning

worksheet. The reason is that the AS/400 configuration is created through the VPN configuration wizard. The wizard sets many parameter values without user input.

10.1.7 Completing the planning worksheet for the AS/400 system (AS05)

In this scenario, the AS/400 system AS05 is the corporate office gateway to the remote dial-in PC clients to which IP addresses are dynamically assigned. The VPN wizard configuration option that fits this scenario is *Gateway to Dynamic IP Users*. Complete the AS/400 system planning worksheet as shown in Table 42. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 42. AS05 AS/400 New Connection Wizard planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Hosts – Gateway to Dynamic IP User – Host to Dynamic IP User	Gateway to Dynamic IP User
What will you name the connection group?	GWtoDynIP
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	204.146.18.5
How will you identify the remote server to which you are connecting?	User@fully qualified domain name
Remote user 1: What is the identifier of the remote server? – What is the pre-shared key?	tommy@itso.roch.com marion12
Remote user 2: What is the identifier of the remote server? – What is the pre-shared key?	marcela@itso.roch.com don4711a
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Balanced

10.1.8 Configuring Gateway to Dynamic IP Users VPN on AS05

Configure a Gateway to Dynamic IP Users VPN on the gateway AS/400 system at the corporate office (AS05). Since all remote clients have dynamically assigned IP addresses, a single dynamic IP group is sufficient to serve all the clients. Each remote user identifier and corresponding pre-shared key must be added to the VPN. The VPN configuration wizard creates the following configuration objects:

- Key policy

- Data policy
- Key connection group
- Dynamic IP group

On the AS/400 VPN implementation, clients with a dynamically assigned IP address are referred to as remote users. The AS/400 system supports two identifier types for remote users. These are:

- User@fully qualified domain name
- Key identifier

In this scenario, the *user@fully qualified domain name* identifier is used to identify the remote clients. It corresponds to the *e-mail address* identifier on the SafeNet Soft-PK client.

Refer to 10.1.7, “Completing the planning worksheet for the AS/400 system (AS05)” on page 424, for the configuration values.

To configure the VPN, perform the following steps:

1. Start Virtual Private Networking from the Operations Navigator.
2. Ensure that the following default values are set for Virtual Private Networking:
 - **Key Management Lifetime:** 120 minutes
 - **Key Expiration:** 60 minutes

Refer to 3.7.6, “Changing the Virtual Private Networking GUI default values” on page 76, for information on how to configure the GUI default values.

3. Select **File->New Connection->Gateway To Dynamic IP Users** to start the configuration wizard (Figure 500).

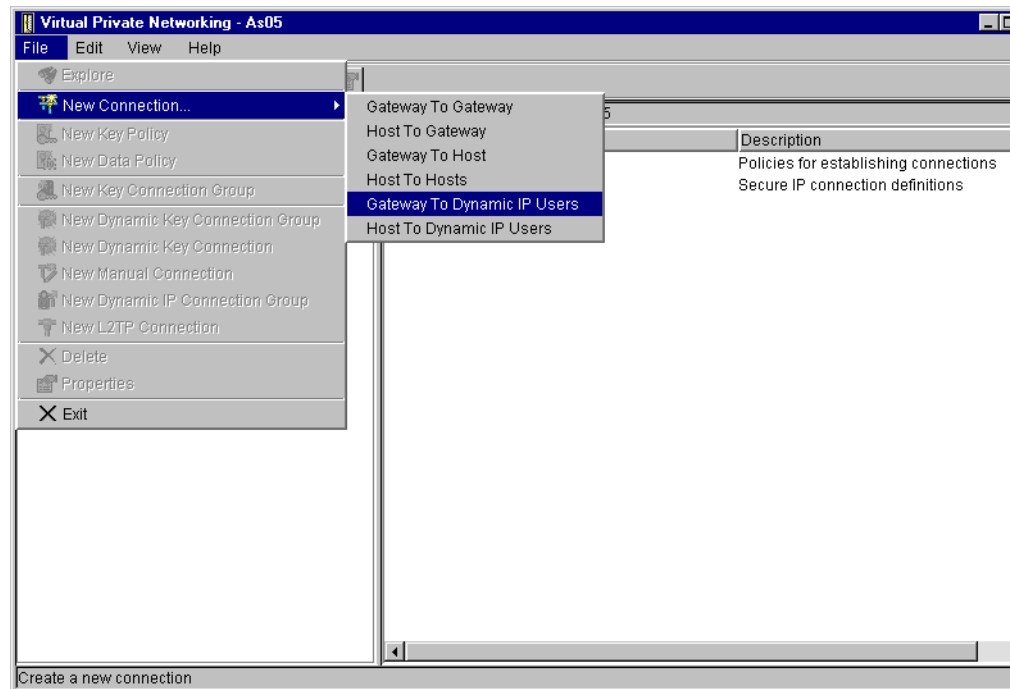


Figure 500. Virtual Private Networking - Starting the Gateway to Dynamic IP Users wizard

4. Click **Next**.

5. Enter `GWtoDynIP` in the Name field and a description in the Description field (Figure 501).

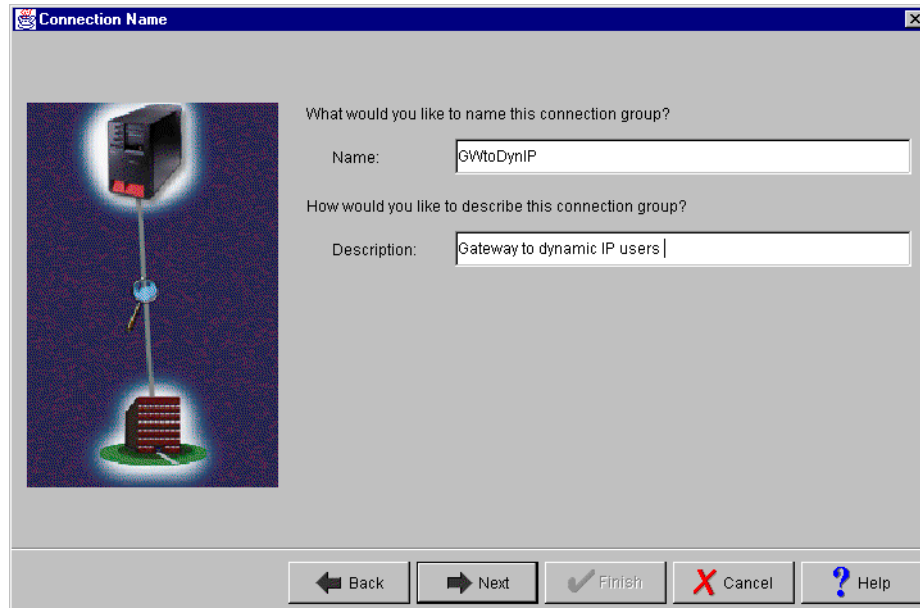


Figure 501. Gateway to Dynamic IP Users wizard - Connection Name window

6. Click **Next**.
7. Select **Balanced security and performance** for the key policy (Figure 502).

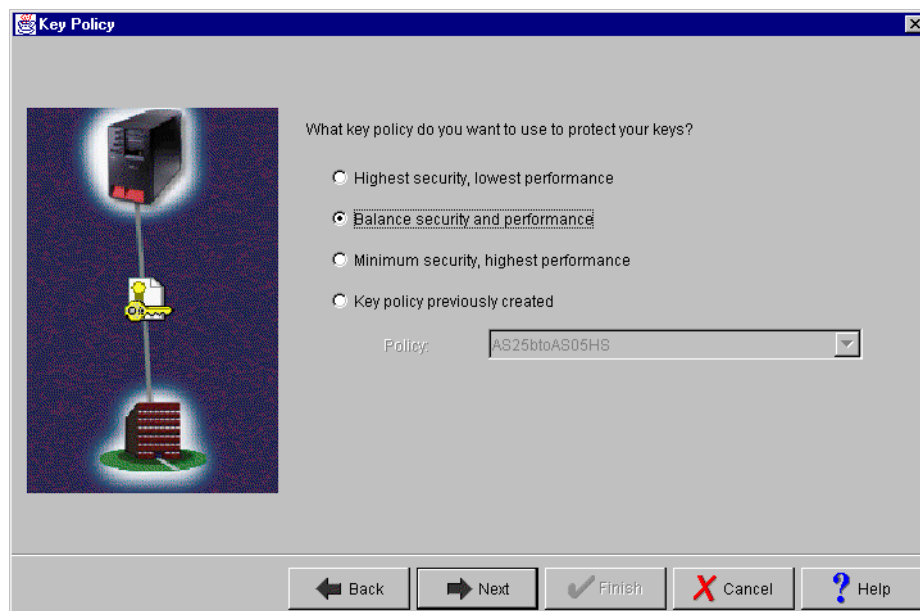


Figure 502. Gateway to Dynamic IP Users wizard - Key Policy

8. Click **Next**.
9. Select **Version 4 IP Address** for the Identifier type and **204.146.18.5** for the IP Address of the local key server (Figure 503 on page 427).

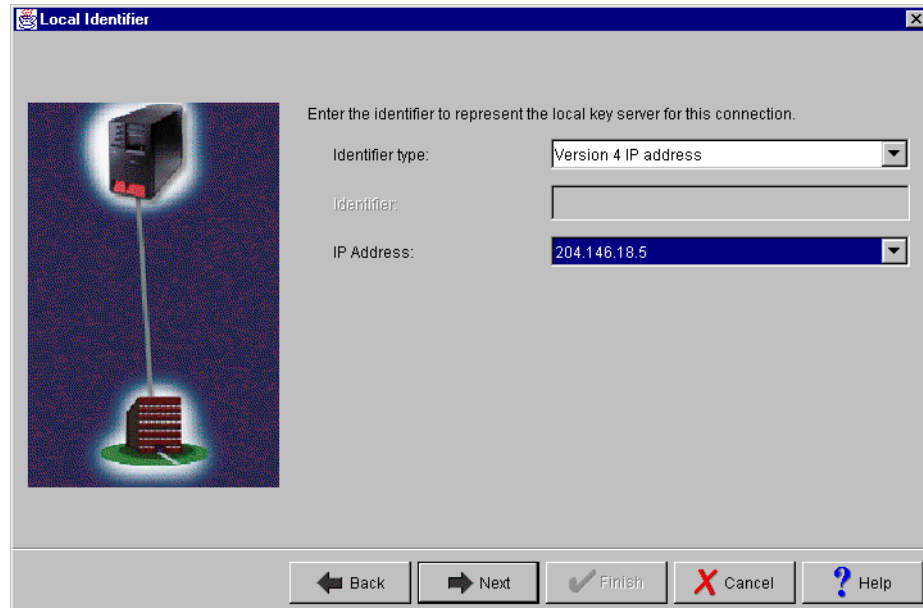


Figure 503. Gateway to Dynamic IP Users wizard - Local Identifier

10. Click **Next**.

11. Select **User@fully qualified domain name** as the Identifier type for remote users.

12. Add remote user entries to the table, using one entry for each remote client as shown in Figure 504. Refer to 10.1.7, “Completing the planning worksheet for the AS/400 system (AS05)” on page 424, for more details on the remote user entries.

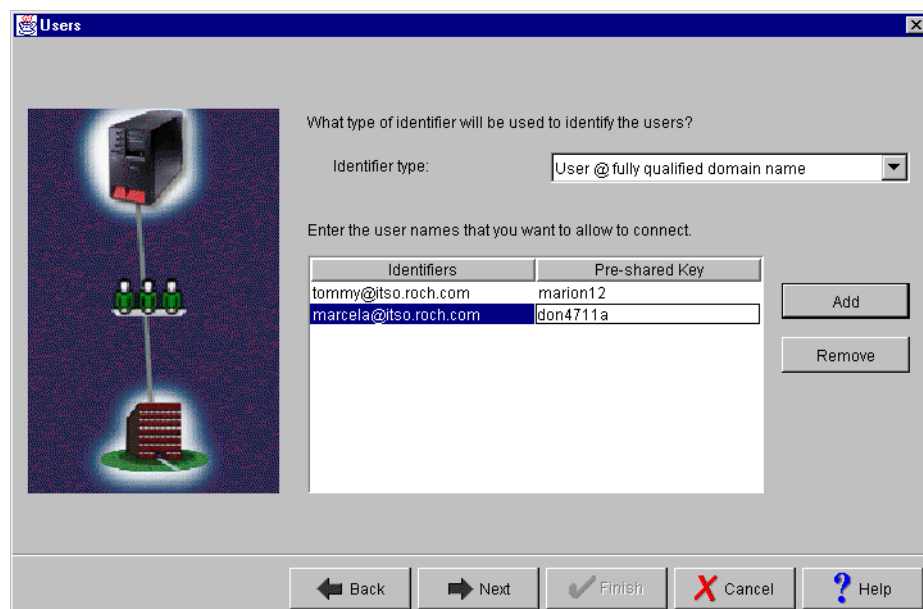


Figure 504. Gateway to Dynamic IP Users wizard - Users

13. Click **Next**.

14. Select **Balanced security and performance** for the data policy (Figure 505).

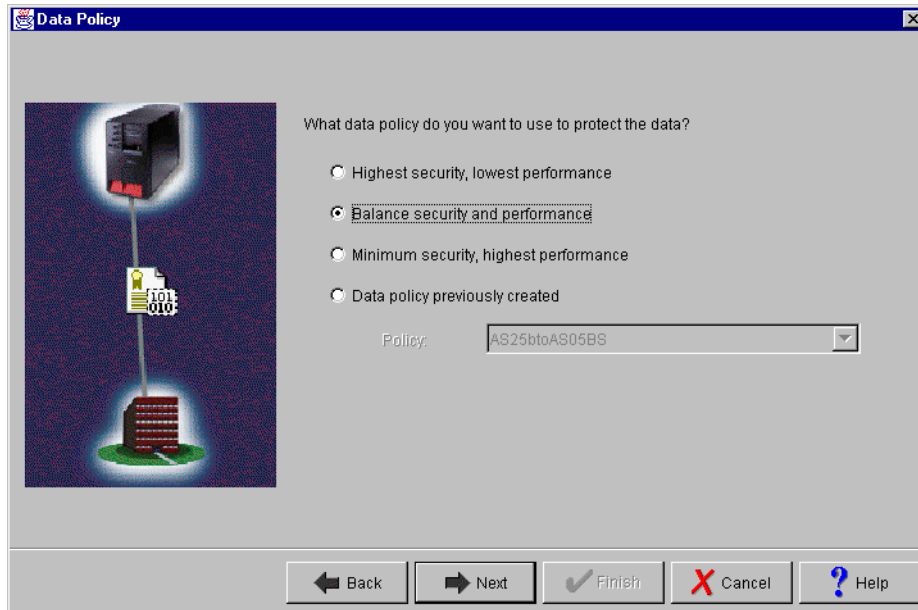


Figure 505. GWtoDyn IP Users wizard - Data Policy

15. Click **Next**.

The New Connection Summary is displayed as shown in Figure 506.

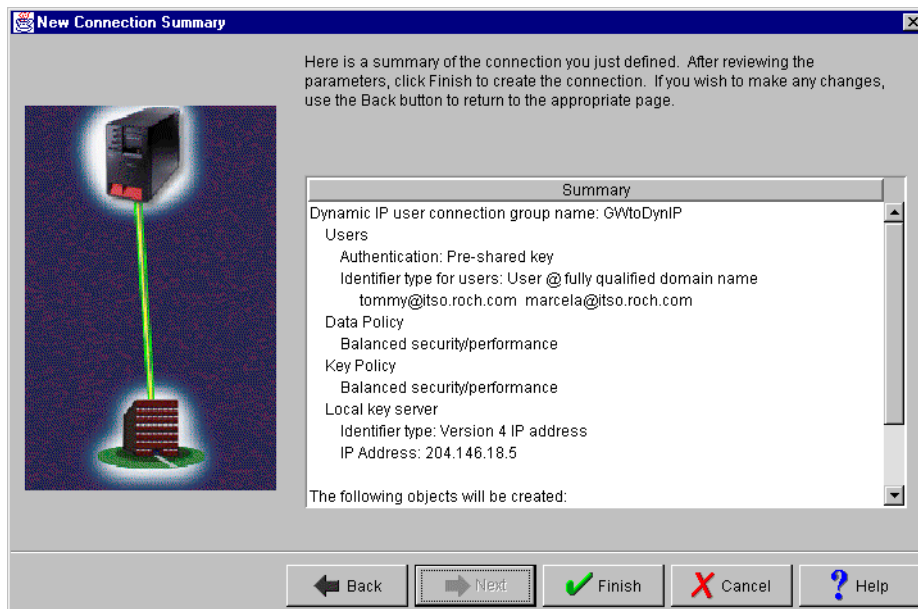


Figure 506. GWtoDyn IP Users wizard - Summary

16. Click **Finish**.

The wizard creates the new Gateway to Dynamic IP Users configuration.

17. Expand **Secure Connections->Data Connections**, and click on **Dynamic IP Groups**.

18. Right-click **GWtoDynIP**.

19. Select **Properties** (Figure 507).

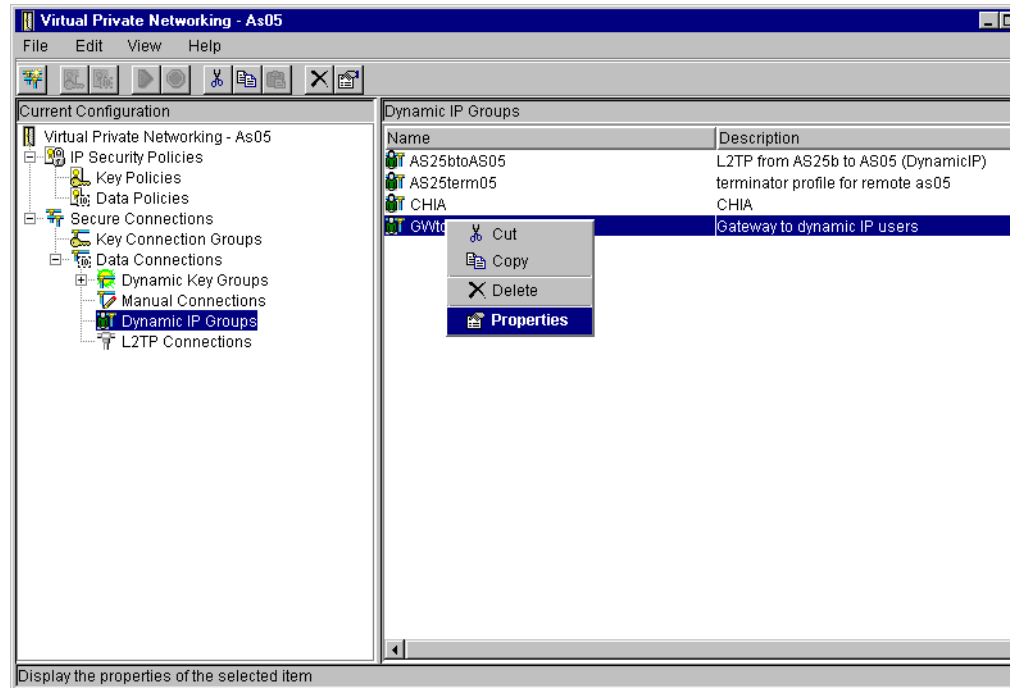


Figure 507. Virtual Private Networking - Dynamic IP Groups

20. Click **Policy**, and select **Connection** for the following parameters as shown in Figure 508 on page 430:

- Local addresses
- Local ports
- Remote addresses
- Remote ports
- Protocol

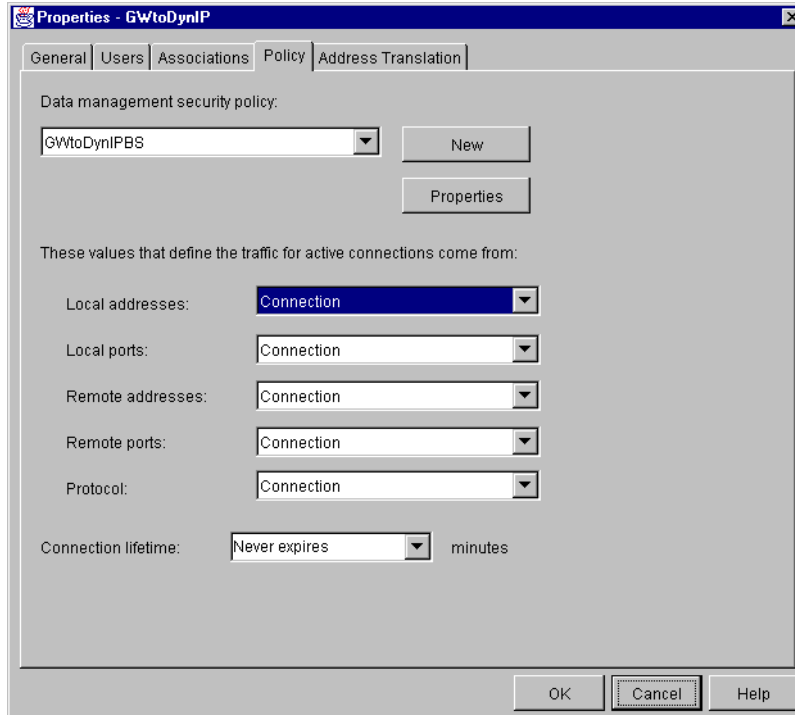


Figure 508. Dynamic IP Group - Properties

Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for an explanation of these parameters.

21. Click **OK** to save the new settings.

10.1.9 Configuring IP filters on the AS/400 system (AS05)

You must configure IP filters to complete the VPN configuration. To implement this scenario, the following filter rules are required:

- One defined address that allows you to specify the corporate subnet in the Source address name field of the IPSEC filter rule.
- Two filter rules to allow IKE negotiations.
- One IPSEC filter rule associated with the connection created in 10.1.8, “Configuring Gateway to Dynamic IP Users VPN on AS05” on page 424.
- One filter interface associated with the filter rules. This is the physical LAN line TRLANC.

Note

The filter rules presented throughout this redbook are *limited* to those required to enable the services in the proposed scenarios. If you want to enable other services beyond those in the scenarios, you need to configure additional rules. Exercise extreme caution when doing so and always take security into account.

To configure the filters, perform the following steps:

1. Start Operations Navigator.
2. Select the system **AS05**, and sign on as required.
3. Expand **Network**.
4. Click on **IP Security**.
5. In the right-hand window, right-click on **IP Packet Security**, and select **Configuration**.
6. Add a Defined Address to refer to the intranet subnet 10.80.21.0. Enter the values as shown in Figure 509.

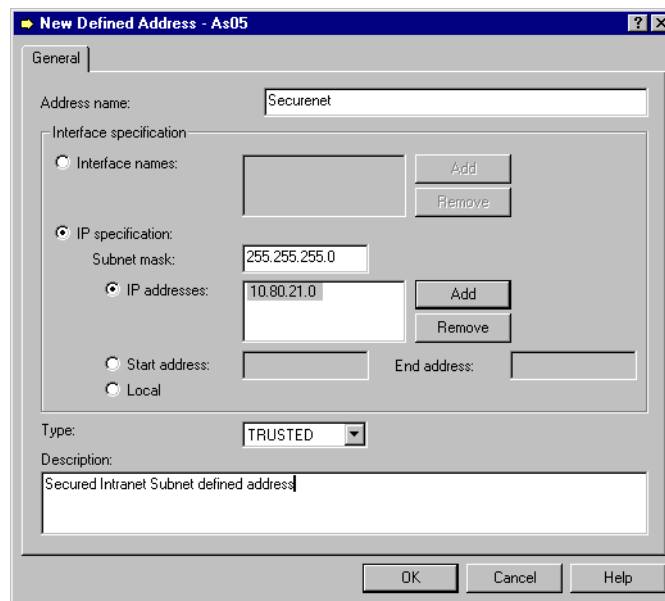


Figure 509. Filter - Defined Address for intranet subnet

7. Click **OK**.
8. Add a filter rule for the inbound IKE negotiations. See Figure 510 on page 432. This filter rule accepts any inbound IP traffic on UDP port 500 destined for IP address 204.146.18.5 (the local key server). The source address is specified as a wildcard (*) value. This allows IKE negotiations with remote clients that are assigned IP addresses dynamically by the ISPs. The set name *DynIP* binds the filter rule to the filter interface.

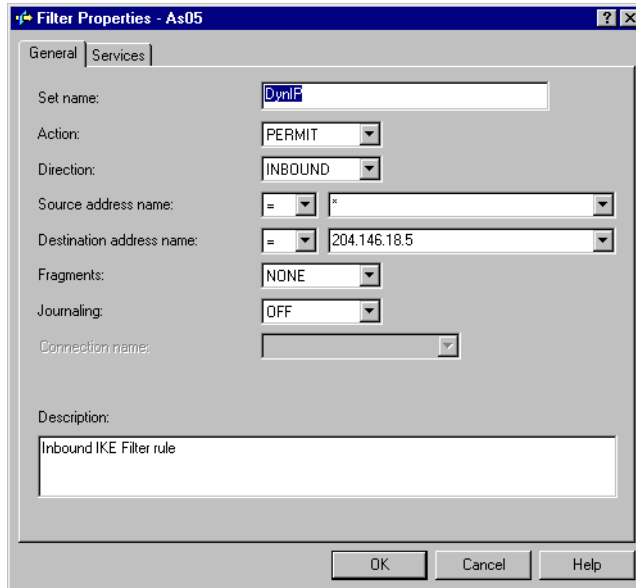


Figure 510. AS05 IKE inbound filter rule - General page

9. Click the **Services** tab.

10. IKE negotiations use protocol UDP, with source and destination port 500. Enter the values as shown in Figure 511.

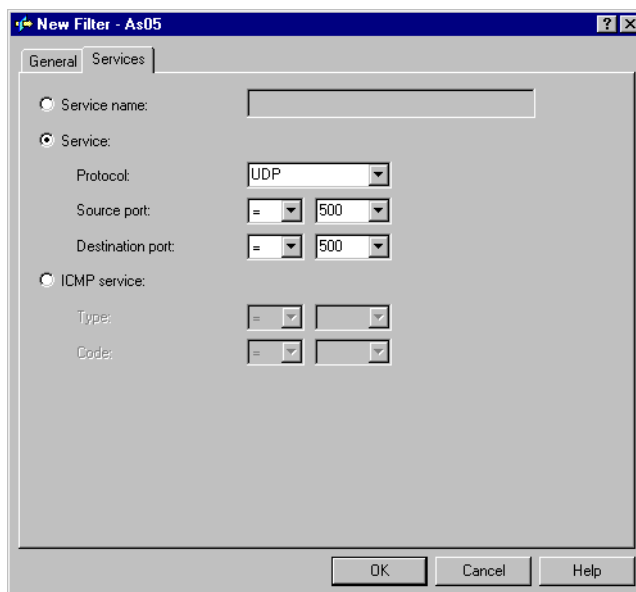


Figure 511. AS05 IKE inbound filter rule - Services page

11. Click **OK**.

12. Repeat the previous four steps for the *outbound* IKE filter rule. Remember to *reverse* the Source and Destination address names. Complete the Services window as you did for the inbound rule as shown in Figure 512 and Figure 513 on page 433.

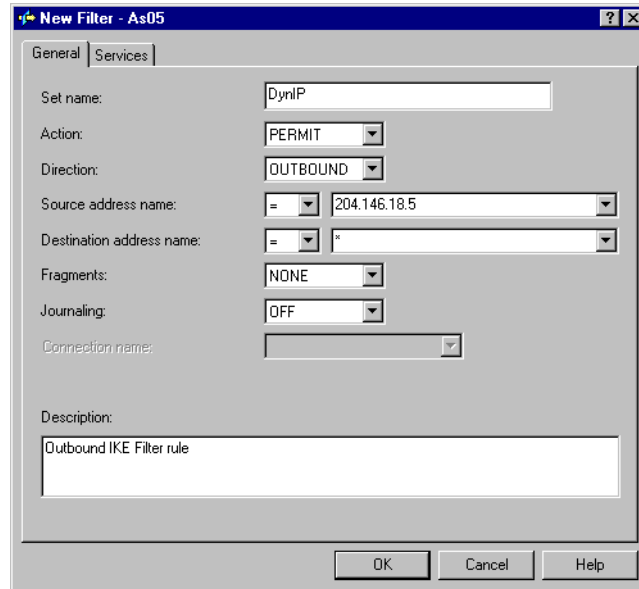


Figure 512. A05 IKE outbound filter rule - General page

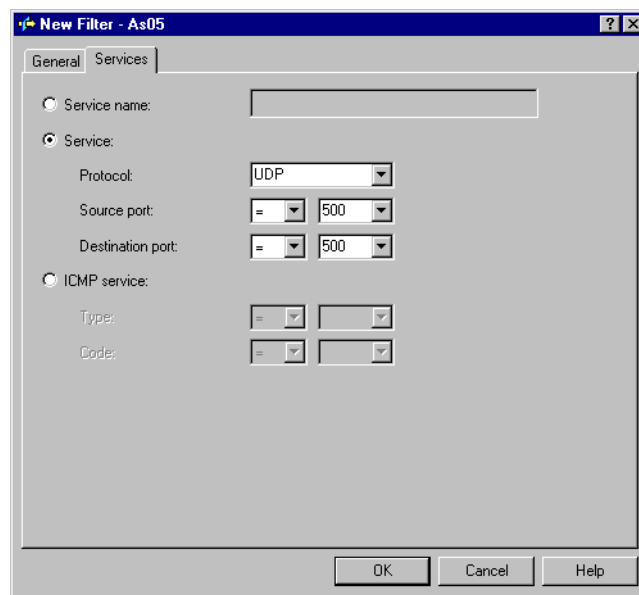


Figure 513. A05 IKE outbound filter rule - Services page

13. Click **OK**.

14. Add an IPSEC filter rule. Configure the IPSEC filter rule that allows data traffic to use the VPN tunnel. Refer to Figure 514 on page 434. Note the following fields:

- Source address name field: Securenet. This is the defined address that represents the data endpoint of the VPN, the corporate intranet.
- Destination address name: Wildcard (*). The remote clients have dynamically assigned IP addresses.
- Connection name: DYNAMICIP. A Gateway to Dynamic IP Users connection that matches the client identifier will be selected.

The IPSEC filter rule is also called an anchor filter for VPN connections. Without such a filter rule, no VPN connection is possible to or from a certain destination.

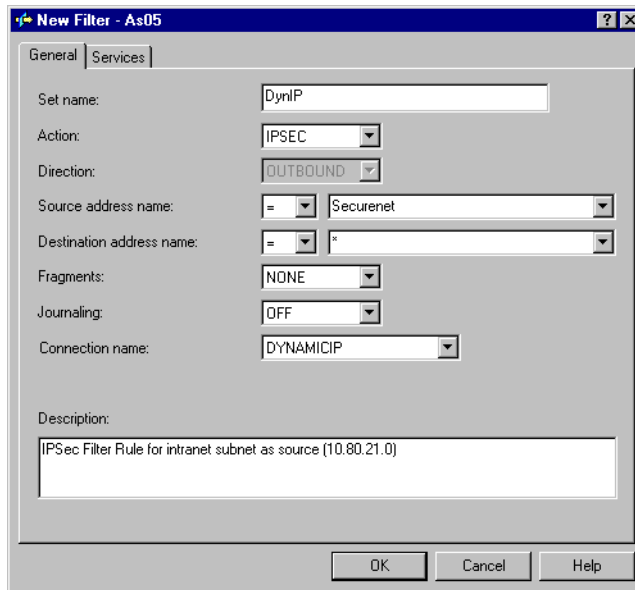


Figure 514. AS05 IPSEC filter rule

15. Click the **Services** tab.

16. Select **Service**, and specify wildcard (*) for the Protocol, Source port, and Destination port fields. See Figure 515.

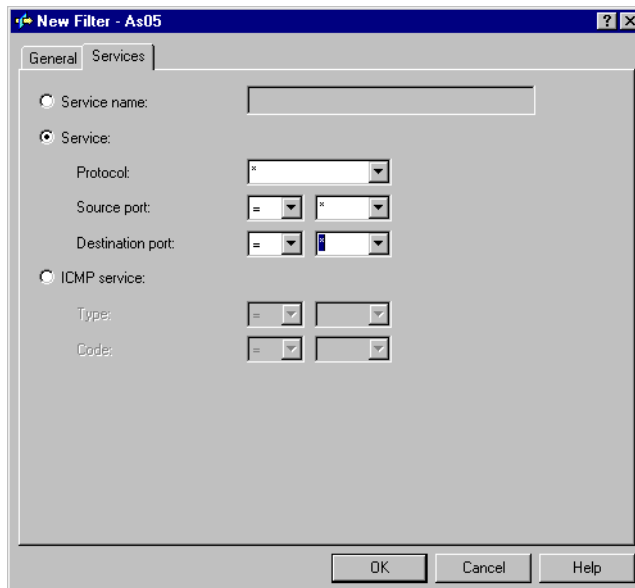


Figure 515. IPSec Filter Rule - Services page

17. Click **OK**.

Tip

Always place the non-IPSEC filter rules, such as the IKE rules, above the IPSEC filter rules.

18. Configure the Filter Interface rule which ties the filter rules to the required interface. The interface, to which the filters apply, is the physical LAN line description (TRLANC) that connects AS05 to the ISP router. Right-click **Filter Interfaces**, and select **New Filter Interface**.
19. Select **Line name**, and select the appropriate LAN line description (**TRLANC**).
20. Click **Add**, and enter DynIP in the Set name field. All filter rules in the file with the DynIP set name are associated with the interface TRLANC. See Figure 516.

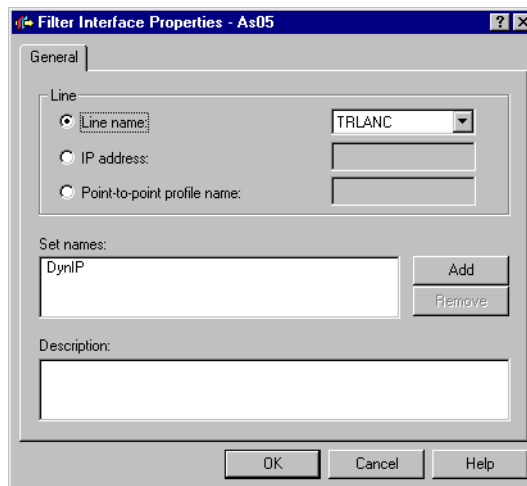


Figure 516. AS05 Filter Interface Properties

21. Click **OK**.
22. Display all the filter rules you just created. At the IP Packet Security window, click **All Security Rules**. All the filter rules as shown in Figure 517 are displayed.

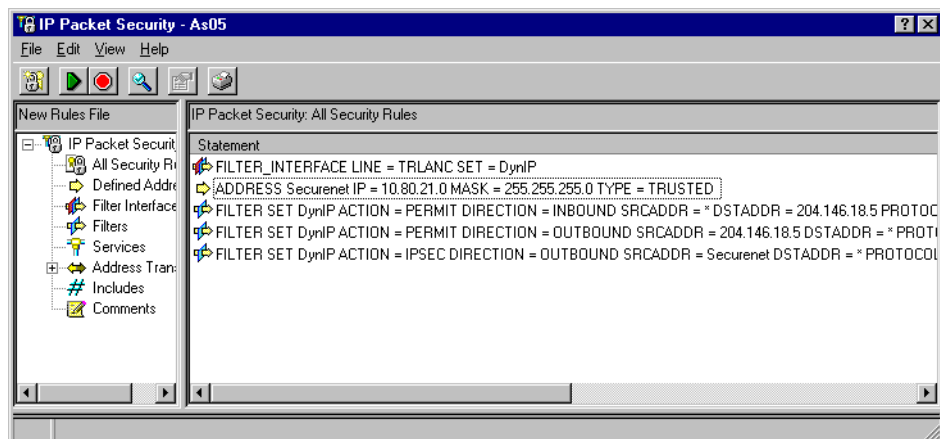


Figure 517. Filter - IP Packet Security all filter rules

23. Save and verify the new filter file.

24. Activate IP packet security.

Figure 518 shows all the filter rules used in this scenario.

```
IP Packet Security: All Security Rules
#Filters for IPSec remote clients
#Filter interface: LAN
FILTER_INTERFACE LINE = TRLANC SET = DynIP
#Intranet subnet - Securenet
ADDRESS Securenet IP = 10.80.21.0 MASK = 255.255.255.0 TYPE = TRUSTED
#IKE filter rules
FILTER SET DynIP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = 204.146.18.5 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
FRAGMENTS = NONE JRN = OFF

FILTER SET DynIP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.5
DSTADDR = * PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC Filter rule
FILTER SET DynIP ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = Securenet
DSTADDR = * PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = DYNAMICIP
```

Figure 518. AS05 IPSec remote dial-in clients - IP filters summary

This completes the configuration of the IP packet security.

10.1.10 Configuring Windows 95 Dial-Up Networking (DUN)

You must configure Dial-Up Networking on the mobile client. Refer to the client documentation for prerequisites and configuration requirements for each particular client. The general steps to configure Windows 95 Dial-Up Networking are as follows:

1. On the Windows desktop, double-click **My Computer->Dial-Up Networking**.
2. Double-click **Make New Connection**.
3. Enter a name for the connection (**PPPoISP**).
4. Select the modem you are using to connect to the Internet.
5. Click **Next**.
6. Enter the ISP telephone number, and select the country.
7. Click **Next**.
8. Click **Finish**. This creates a new PPP connection profile.

Perform the following changes after creating the connection:

1. Right-click on the newly created connection (**PPPoISP**), and select **Properties**.

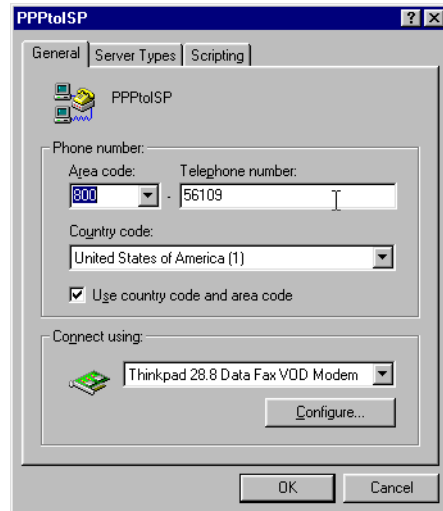


Figure 519. ThinkPad TPA PPP connection - General page

2. Click the **Server Types** tab.
3. Select the options shown in Figure 520. Checking the **Require encrypted password** check box provides another level of protection during login to the ISP. Since the AS/400 system only supports TCP/IP over PPP, select **TCP/IP**, and deselect **NetBEUI** and **IPX/SPX Compatible**.

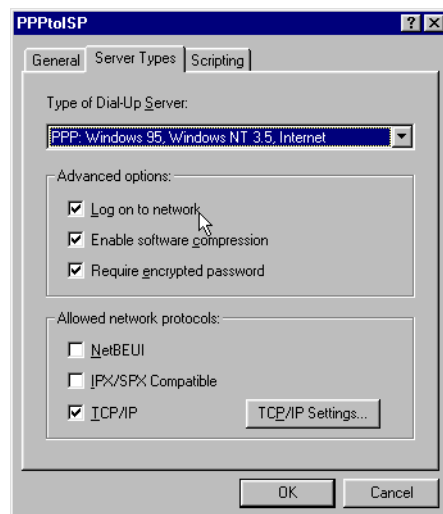


Figure 520. ThinkPad TPA PPP connection - Server Types page

4. Click the **TCP/IP Settings** tab.
5. Ensure that the settings shown in Figure 521 on page 438 are applied.

Important

It is important to select **Use default gateway on remote network**. This option ensures that the PPP interface is used as a default route.

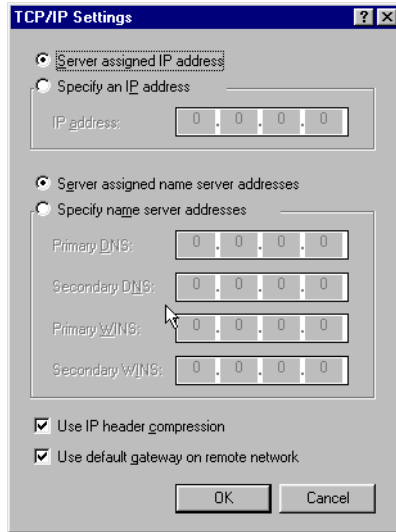


Figure 521. ThinkPad TPA PPP connection server types - TCP/IP Settings

6. Click **OK** to save the TCP/IP settings.
7. Click **OK** to save the PPP profile.

10.1.11 Installing the IRE SafeNet Soft-PK

Use the standard client documentation to install the client. There are no configuration parameters given during the installation that affect the VPN configuration.

SafeNet Soft-PK supports IPSec connections over PPP as well as over LAN (Ethernet). The configuration shown in this chapter is based on a PPP connection using the SafeNet Soft-PK Version 2.0.6 (Build 3) client software. The client has a dynamically assigned IP address. Therefore, the identification of the client can not be an IP address. This client uses the user's e-mail address as an identification.

10.1.11.1 Client characteristics

The PC client used in this scenario has the following hardware and software characteristics:

- **Hardware**
 - IBM Thinkpad 760XD
 - 80 MB memory
 - Integrated MWave modem
- **Software**
 - Microsoft Windows 95 (4.0.0 950 B) with Dial-Up Networking (DUN) 1.3
 - IRE SafeNet Soft-PK version 2.0.6 (build 3). This client supports IPSec only (no L2TP support).

SafeNet Soft-PK implementation considerations

The installation and configuration of the SafeNet Soft-PK client follows a logical flow. When adding a connection, the client automatically creates all the required configuration objects. For example, it creates one proposal for the Internet Key

Exchange (IKE) phase 1 and 2. However, the user can add more proposals manually after the initial configuration. This makes the client flexible. Another advantage of the client is the way it establishes the secured connection. Once a user starts a session (an application) with the remote host, the client starts the IKE negotiations automatically. Therefore, once the SafeNet Soft-PK client is configured, there is no manual operation required.

10.1.12 Configuring the IRE SafeNet Soft-PK client on TPA

Once you install the SafeNet Soft-PK software on the PC, a new icon comes up on the Windows task bar. To start the configuration of the SafeNet Soft-PK VPN client, you can choose one of the following two paths:

- Click the Windows 95 **Start** button, and select **Programs->SafeNet Soft-PK->Security Policy Editor**.
- Right-click the SafeNet icon on the Windows task bar.

This section documents the second method to start the configuration. Perform the following steps to configure the SafeNet Soft-PK client:

1. Right-click the **SafeNet** icon on the Windows task bar.
2. Select **Security Policy Editor** as shown in Figure 522.

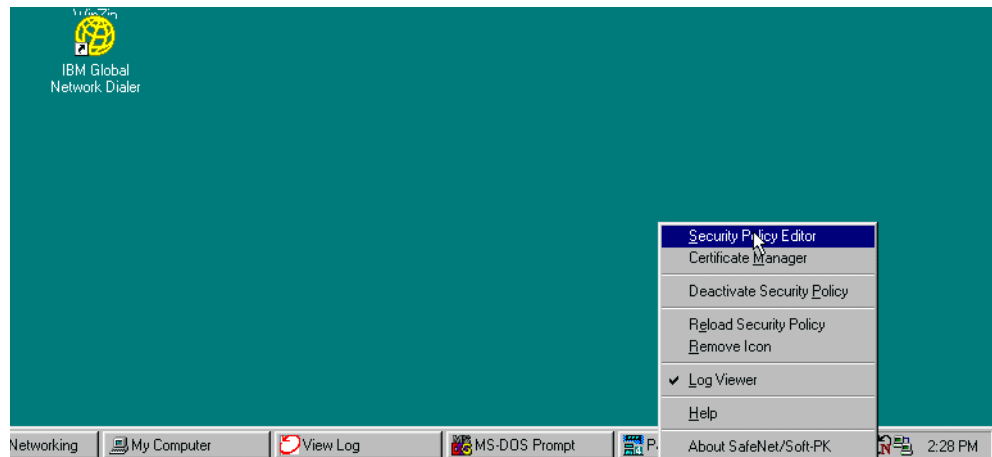


Figure 522. SafeNet Soft-PK Client - Starting Security Policy Editor

3. Click **File->New Connection** to create the first secured connection.
4. Enter **GWIntranet** as the connection name. This connection provides access to the intranet subnet 10.80.21.0 over the secured tunnel, through the VPN gateway with IP address 204.146.18.5. Refer to 10.1.6.1, “Planning worksheet for SafeNet Soft-PK client (TPA)” on page 422, to configure this connection. Input the values as shown in Figure 523 on page 440.

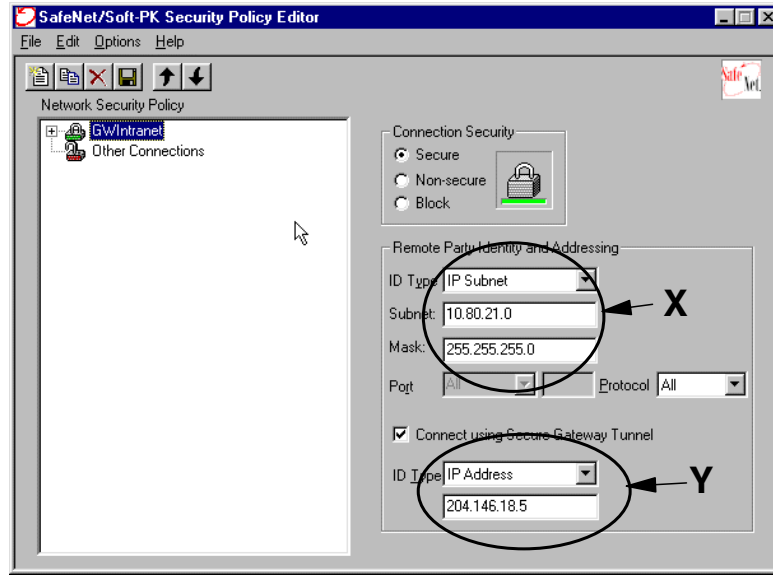


Figure 523. SafeNet Soft-PK Security Policy Editor - Configuring the connection

Note

The settings in the Remote Party Identity and Addressing fields are used to define the intranet systems that this client can access. In this scenario, the remote PC TPA is granted full access to the intranet with subnet 10.80.21.0 (see X in Figure 523). The IPSec tunnel ends at the VPN gateway. In this scenario, the VPN server is AS05 with IP address 204.146.18.5 (E) (see Y in Figure 523). In the intranet, the traffic flows in the clear.

5. Click **Security Policy**.
6. Select **Aggressive Mode**. See Figure 524.

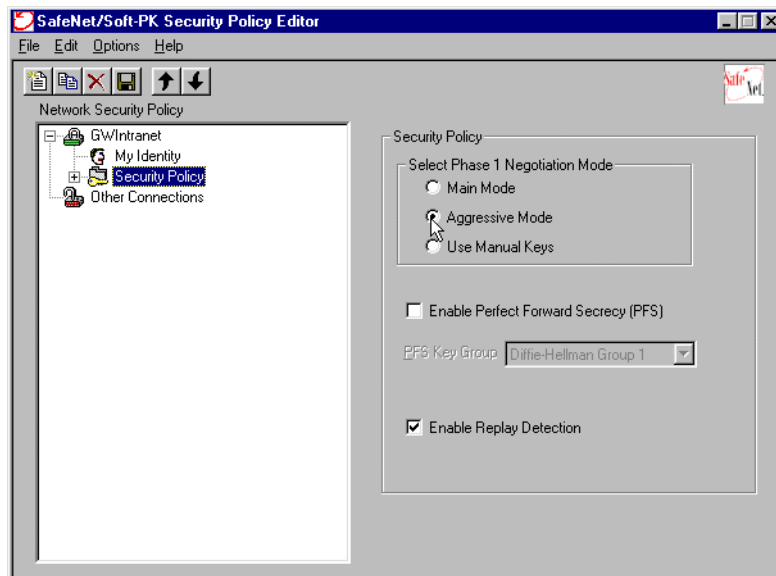


Figure 524. SafeNet Soft-PK Security Policy Editor - Security Policy window

7. Click **My Identity** under the GWIntranet connection.
8. Select **E-mail Address** for ID Type and enter `tommy@itso.ibm.com` (Figure 525).

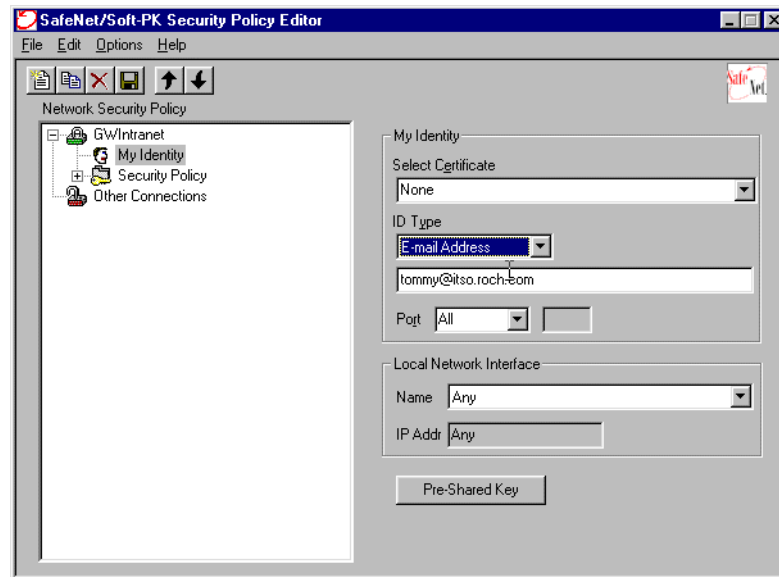


Figure 525. SafeNet Soft-PK Security Policy Editor - My Identity window

9. Click **Pre-Shared Key** (Figure 526).

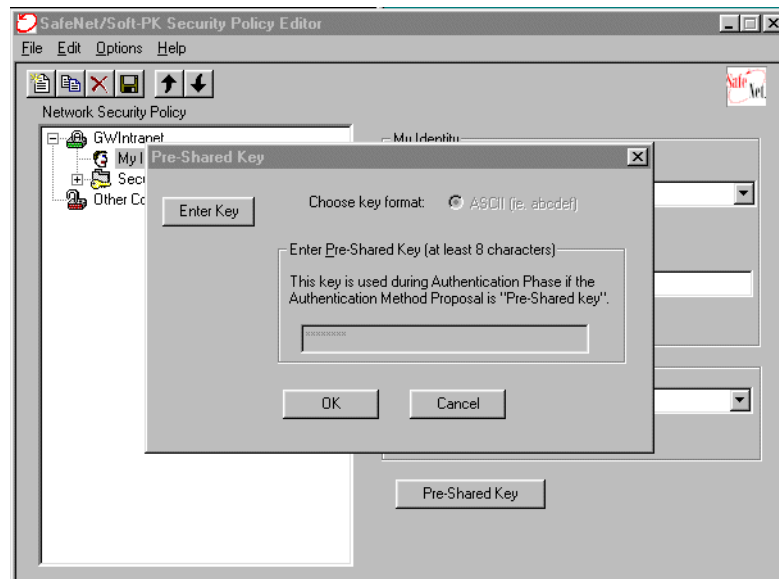


Figure 526. SafeNet Soft-PK Security Policy Editor - Entering Pre-Shared Key (Step 1)

10. Click the **Enter Key** button, and enter the key `marion12`. See Figure 527 on page 442.

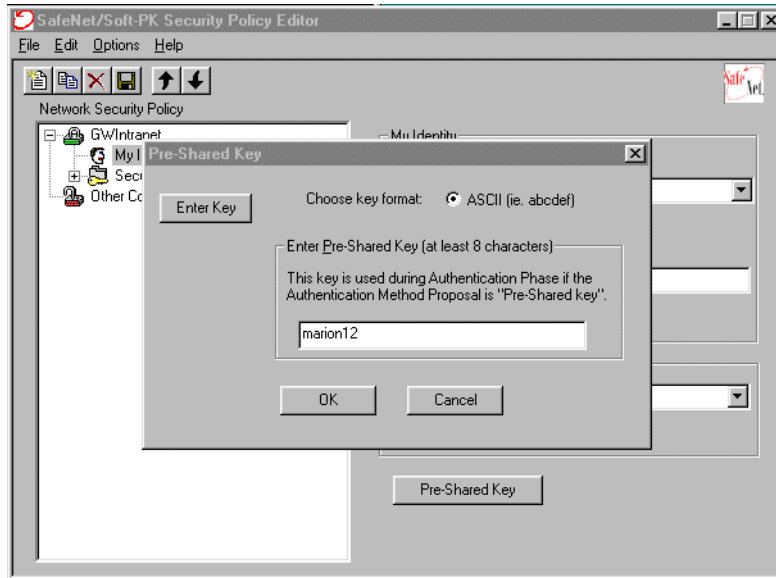


Figure 527. SafeNet Soft-PK Security Policy Editor - Entering Pre-Shared Key (Step 2)

11. Click **OK** to save the pre-shared key, and return to the My Identity window.

12. Select **Security Policy->Authentication->Proposal 1**.

13. Set the **SA Life** time to **7200 seconds**.

14. Ensure that the following settings apply (Figure 528):

- **Authentication Method:** Pre-Shared Key
- **Encrypt Alg:** DES
- **Hash Alg:** MD5
- **Key Group:** Diffie-Hellman Group 1

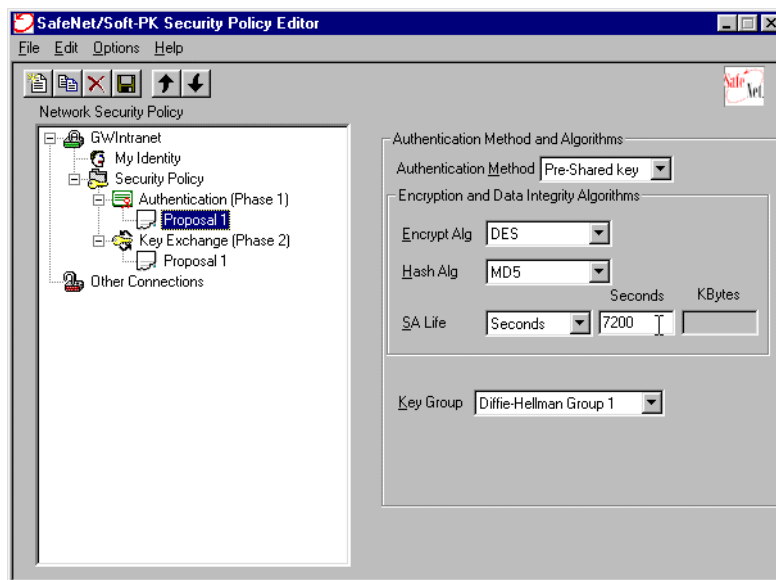


Figure 528. SafeNet Soft-PK Security Policy Editor - Phase 1 Proposal 1

15. Select **Key Exchange (Phase 2)->Proposal 1**. Set the properties for phase 2 proposal 1 as shown in Figure 529 on page 443.

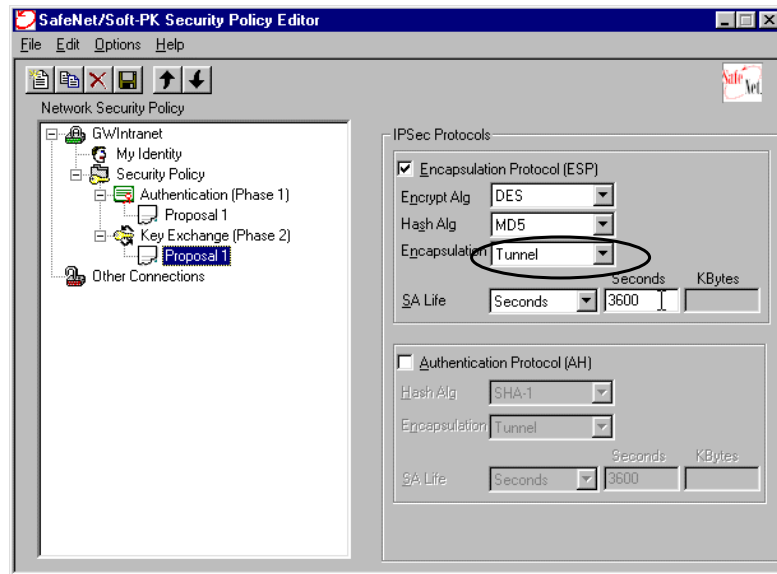


Figure 529. Security Policy Editor - Phase 2 Proposal 1

Note

The Encapsulation mode is set to Tunnel because we are implementing a host-to-gateway scenario. If the AS/400 system was the data endpoint, as well as the key server, instead of using a VPN gateway at the corporate office, specify *Transport* as the encapsulation mode.

16. Select **File->Save Changes**, or click the save icon (diskette symbol) to save the configuration.

This completes the configuration of the SafeNet Soft-PK client.

10.1.13 Starting the VPN connection

To start the VPN connection in the corporate VPN gateway, perform the following steps:

1. Start IP Packet Security (only if you have *not* done so already as indicated in step 24 on page 436).
2. Start Virtual Private Networking.
3. After the remote client calls-in, at the AS/400 system, check the connection status at the VPN Active Connections window. You should see a status similar to the one shown in Figure 530 on page 444.

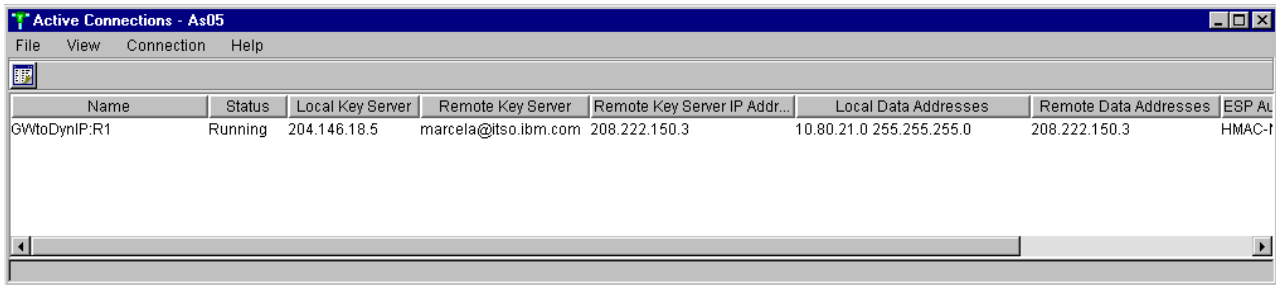


Figure 530. AS05 Active Connections window

To start the VPN connection in TPA running the IRE SafeNet Soft-PK, follow these steps:

1. Start the PPP connection to the ISP (PPPtISP).
2. Start a TCP/IP application to the corporate intranet (subnet 10.80.21.0).

The SafeNet Soft-PK log viewer logs the information about the connection as shown in Figure 531.

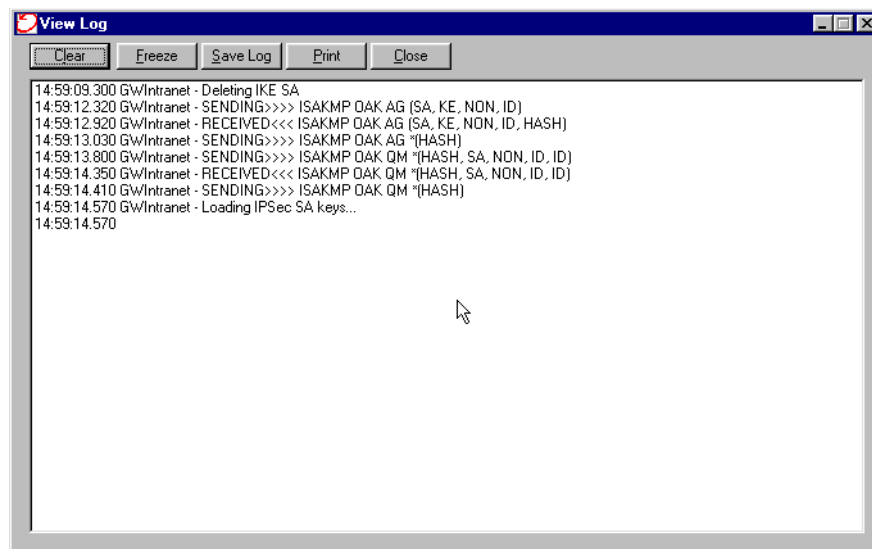


Figure 531. SafeNet Soft-PK - Log Viewer with active VPN connection

10.2 Remote PC clients with IPsec and L2TP support

Some companies control access to internal applications and servers by IP address and even by subnet address within the corporate network. The company may also want to control access to the Internet itself. For example, the employees should enter the Internet through the company's Internet gateway and not directly.

If your company security policies require that remote dial-in clients are assigned an IP address of the internal network address space, then the PC VPN client that you use must support L2TP in combination with IPsec. To test this scenario, we used the Wind River Systems WinVPN client for Windows 95. For more information on WinVPN, log on to: <http://www.wrs.com>

Refer to Chapter 2, “Introduction to Layer 2 Tunneling Protocol (L2TP)” on page 33, for an overview of L2TP.

Figure 532 shows the test network for this scenario. This is the same network used to test the IPsec PC clients. The only difference is that now an L2TP tunnel is established between the PC client (TPC) and the AS/400 corporate gateway, which is the L2TP Network Server (LNS) and the VPN server.

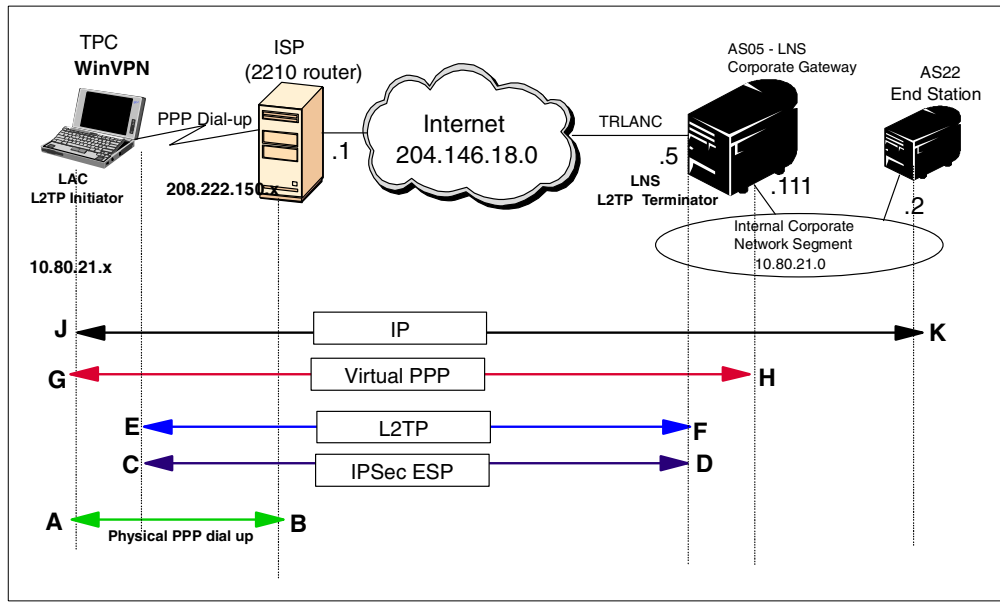


Figure 532. PC client with IPsec and L2TP support - Test network overview

This scenario is essentially the same as the one described in Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263. The only difference is that now the dial-in client is a PC instead of an AS/400 system.

10.2.1 Verifying end-to-end connectivity

Follow the process described in 10.1.5, “Verifying end-to-end connectivity” on page 422.

10.2.2 Completing the planning worksheet for the WinVPN client

On TPC, we installed the WinVPN client by Wind River Systems. Table 43 shows the planning worksheet with the configuration parameters used in this scenario.

Table 43. WinVPN L2TP with IPsec client planning worksheet

This is the information you need to configure the WinVPN client	Scenario answers
L2TP tunnel authentication	Tunnel authentication <i>not</i> used in this scenario
IKE phase 1 Transforms IPsec Authentication	DES - MD5 Pre-Shared Key
IKE phase 2 Proposal Transforms	ESP only DES - MD5

This is the information you need to configure the WinVPN client	Scenario answers
IKE peers: Peer IP address (Key server identifier) Peer pre-shared key	204.146.18.5 winvpn
IKE mode Configuration Aggressive mode Client ID type Client ID Encrypt starting from third message in the exchange Session key PFS	Checked (selected) User FQDN winvpn@itso.ibm.com Unchecked (not selected) Unchecked (not selected)
Lifetimes Phase 1 lifetime Phase 2 lifetime	120 minutes 3600 seconds
Certificates	Not configured in this scenario

10.2.3 Completing the planning worksheet for the AS/400 system (AS05)

In this scenario, the AS/400 system AS05 is the LNS and the corporate office VPN gateway. As explained in Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263, the VPN configuration is Host to Dynamic IP Users. The ISP randomly assigns global IP addresses to the client. For that reason, we selected a Host to Dynamic IP Users configuration. Keep in mind that this VPN protects the L2TP tunnel only. That is the reason why the LNS is a *host* and not a gateway from this VPN tunnel perspective.

Complete the AS/400 system planning worksheet as shown in Table 44. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 44. AS05 New Connection Wizard AS/400 planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Hosts – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Dynamic IP Users
What will you name the connection group?	L2TPPrmtclt
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	204.146.18.5
How will you identify the remote server to which you are connecting?	User@fully qualified domain name

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
Remote user 1: What is the identifier of the remote server? – What is the pre-shared key?	winvpn@itso.roch.com winvpn
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Balanced

10.2.4 Configuring a Host to Dynamic IP Users VPN on AS05

Configure a Host to Dynamic IP users VPN on the gateway AS/400 system at the corporate office (AS05). In this scenario, the *user@fully qualified domain name* identifier is used to identify the remote clients. Refer to 10.2.3, “Completing the planning worksheet for the AS/400 system (AS05)” on page 446, for the configuration values.

To configure the VPN, perform the following steps:

1. Start Virtual Private Networking from the Operations Navigator.
2. Select **File->New Connection->Host To Dynamic IP Users** to start the configuration wizard (Figure 533).

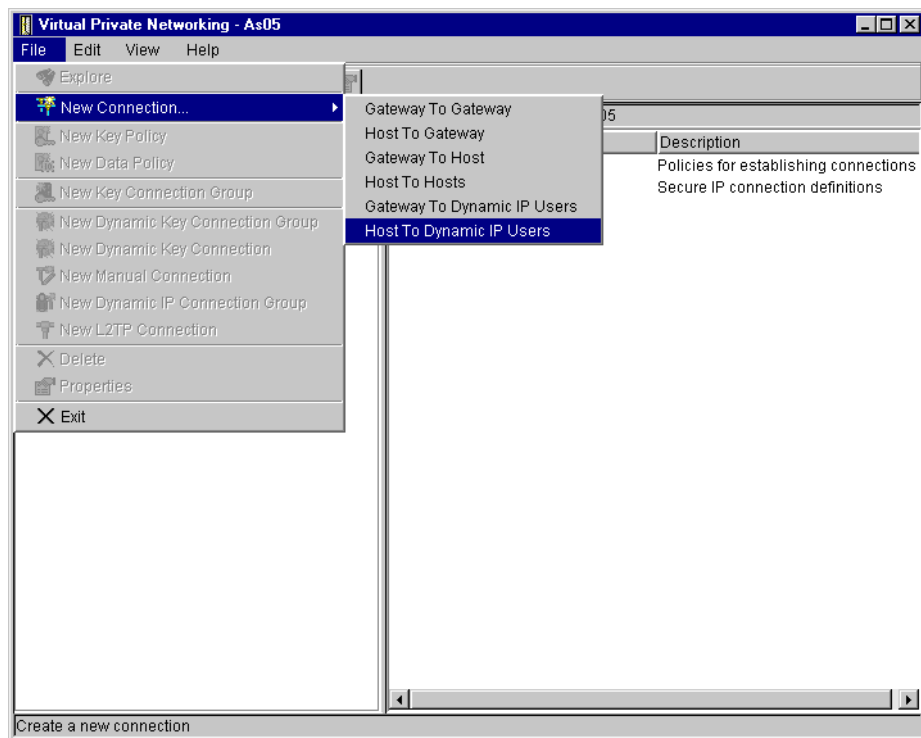


Figure 533. Virtual Private Networking - Starting Host to Dynamic IP Users wizard

3. Click **Next** at the New Connection Wizard Welcome window.
4. Enter `L2TPPrmtc1t` in the Name field and a description in the Description field (Figure 534 on page 448).

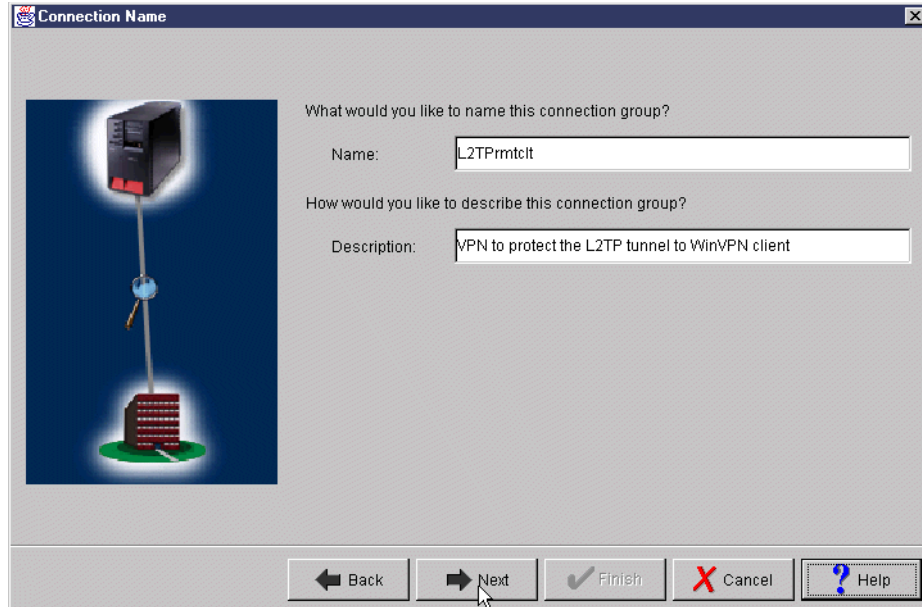


Figure 534. Host to Dynamic IP Users wizard - Connection Name window

5. Click **Next**.
6. Select **Balanced security and performance** for the key policy (Figure 535).

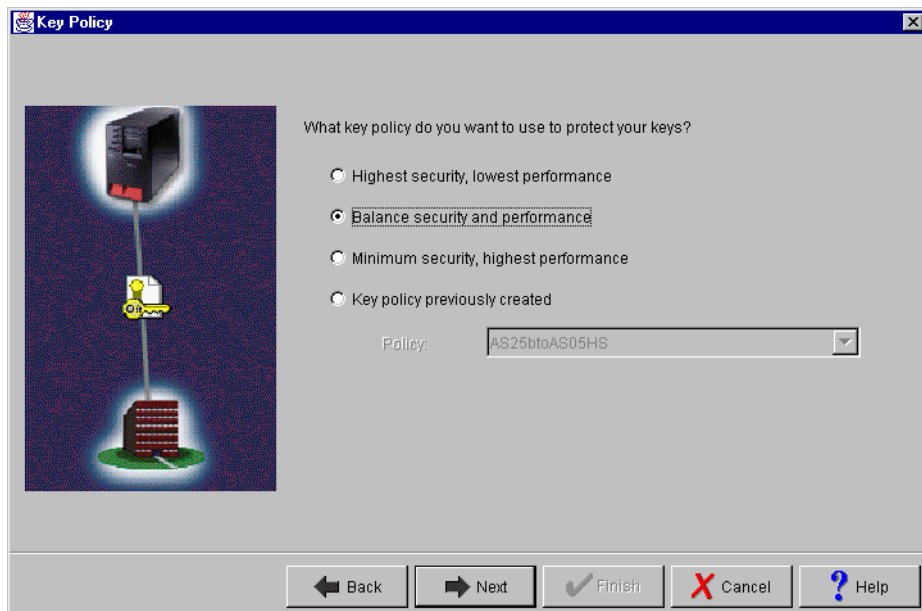


Figure 535. Host to Dynamic IP Users wizard - Key Policy

7. Click **Next**.
8. Select **Version 4 IP Address** for the Identifier type and **204.146.18.5** for the IP Address of the local key server (Figure 536 on page 449).

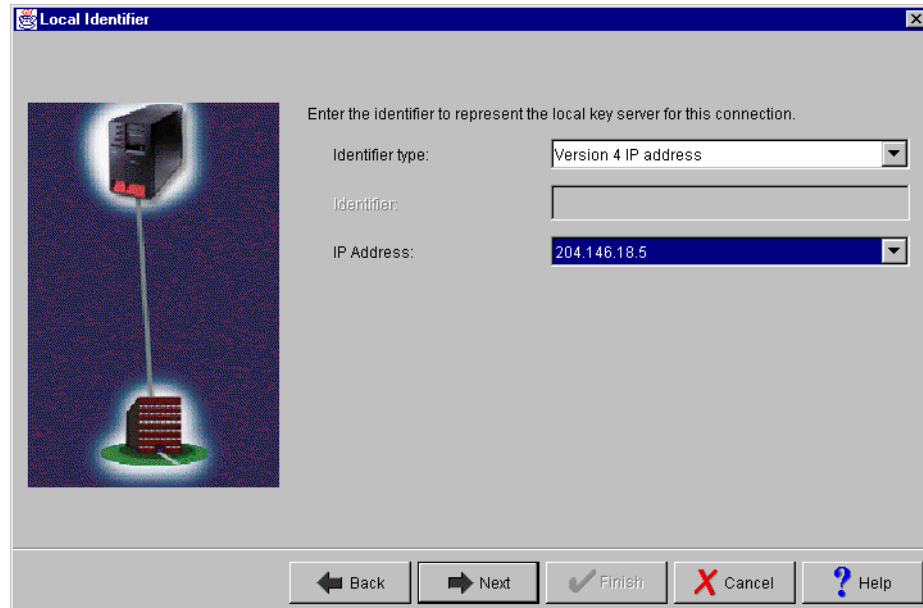


Figure 536. Host to Dynamic IP Users wizard - Local Identifier

9. Click **Next**.

10. Select **User@fully qualified domain name** as the Identifier type for remote users.

11. Add the remote user entry for TPC as shown in Figure 537.

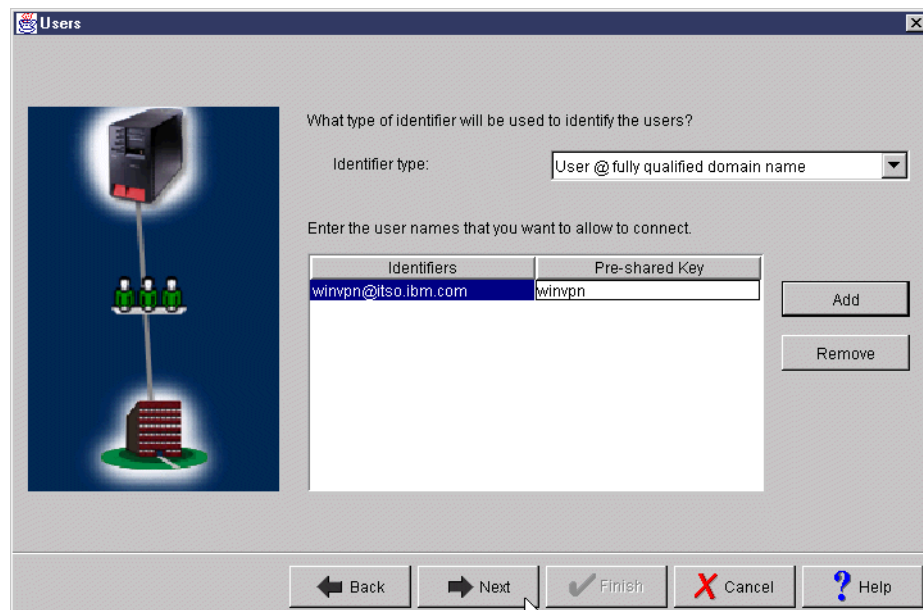


Figure 537. Host to Dynamic IP Users wizard - Users

12. Click **Next**.

13. Select **Balanced security and performance** for the data policy (Figure 538 on page 450).

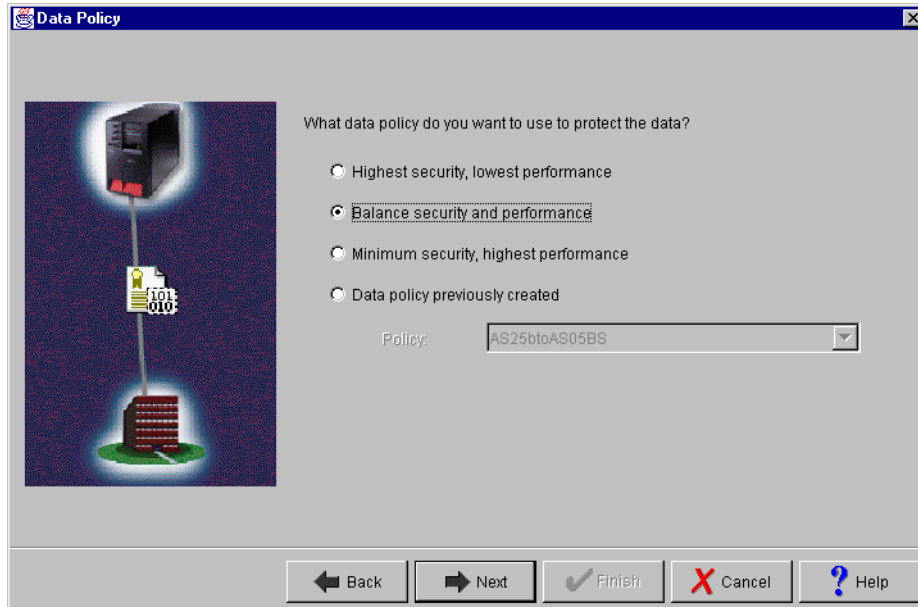


Figure 538. L2TPPrmtclt IP Users wizard - Data Policy

14. Click **Next**.

The New Connection Summary is displayed as shown in Figure 539.

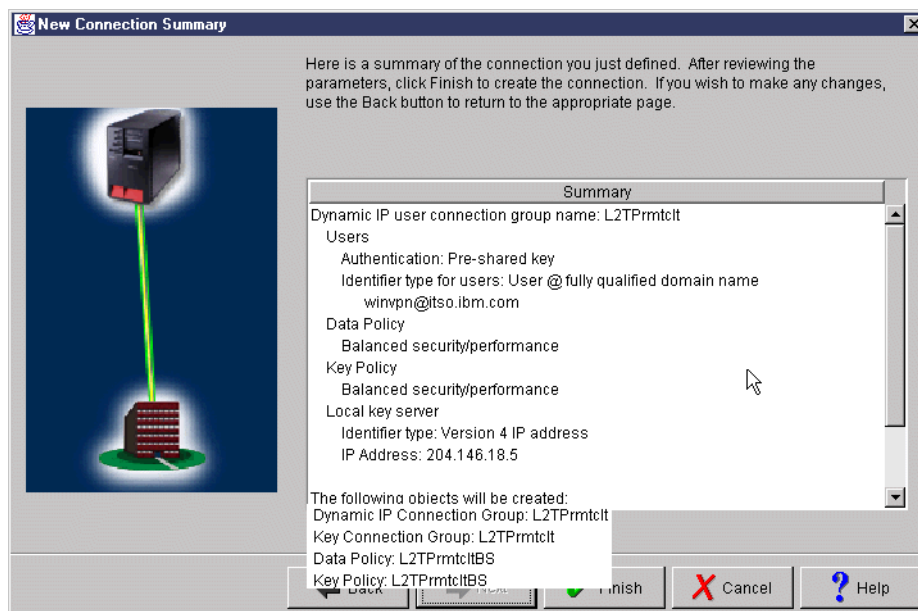


Figure 539. L2TPPrmtclt IP Users wizard - Summary

15. Click **Finish**.

The wizard creates the new Host to Dynamic IP Users configuration.

10.2.4.1 Customizing the L2TPPrmtclt VPN created by the wizard

Perform the following steps after the wizard creates the Host to Dynamic IP Users VPN:

1. Expand **Secure Connections->Data Connections**, and click on **Dynamic IP Groups**.
2. Right-click **L2TPPrmtclt**.

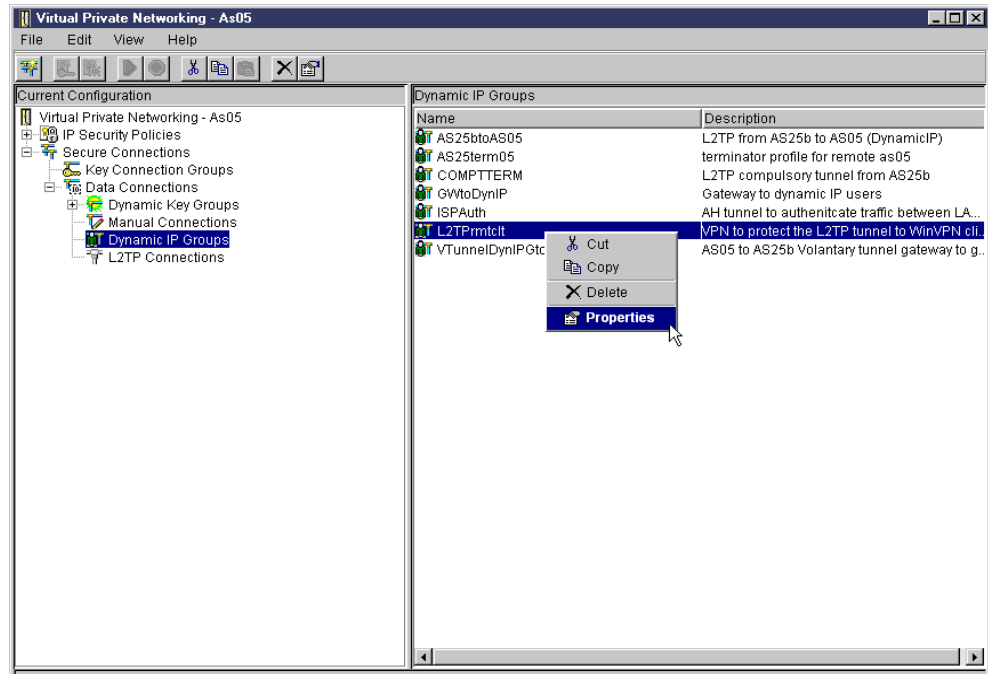


Figure 540. Virtual Private Networking - Dynamic IP Groups

3. Select **Properties**.
4. Click **Policy**, and select **Connection** for the following parameters (Figure 541 on page 452):
 - Local addresses
 - Local ports
 - Remote addresses
 - Remote ports
 - Protocol

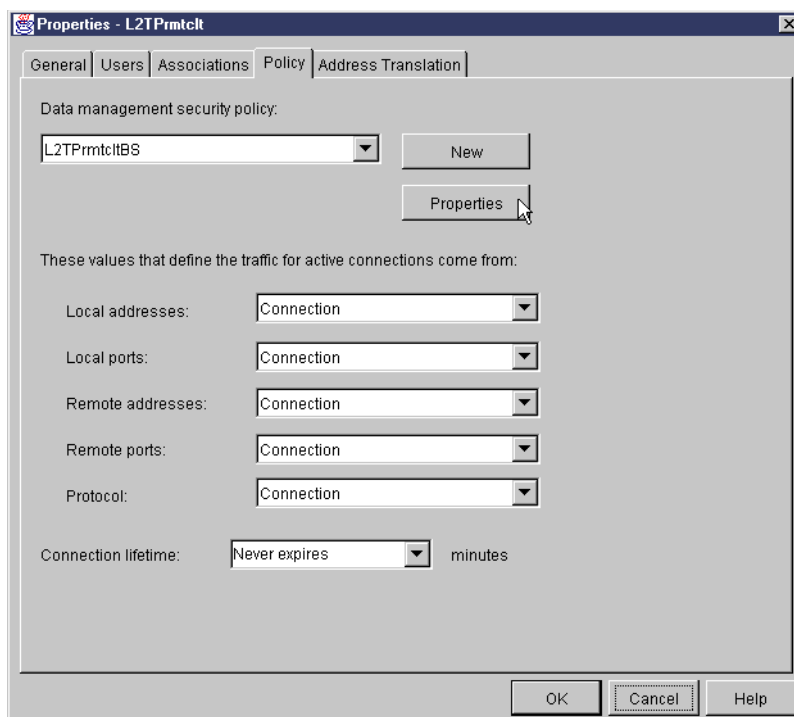


Figure 541. Dynamic IP Group - Properties

5. Click **OK** to update the VPN configuration.

10.2.5 Configuring IP filters on the AS/400 system (AS05)

You must configure IP filters to complete the VPN configuration. The filters here are the same filters configured in 7.2.3, “Configuring IP filters in the LNS AS/400 system (AS05)” on page 279.

Figure 542 shows a summary of the filters configured in the LNS (AS05).

```

IP Packet Security: Filter Interfaces
FILTER_INTERFACE LINE = TRLANC SET = L2TPSet
#IKE Rules - IKE negotiation
FILTER SET L2TPSet ACTION = PERMIT DIRECTION = OUTBOUND
SRCADDR = 204.146.18.5 DSTADDR = *
PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET L2TPSet ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = 204.146.18.5
PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC rule - IPsec tunnel encapsulates L2TP tunnel
FILTER SET L2TPSet ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 204.146.18.5
DSTADDR = * PROTOCOL = UDP DSTPORT = 1701 SRCPORT = 1701 FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = DYNAMICIP

```

Figure 542. AS05 Filters summary

10.2.6 Configuring the L2TP terminator profile (AS05)

In this scenario, we use the L2TP terminator profile AS25bterm configured in 7.2.2, “Configuring the L2TP terminator profile (AS05)” on page 273. Refer to that section for details.

10.2.7 Configuring Windows 95 Dial-Up Networking for WinVPN

WinVPN requires Windows 95/98 Dial-Up Networking (DUN) 1.2 or later. Refer to the *WinVPN Client Installation and Troubleshooting Guide* that came with your product for information on how to install and configure DUN.

In our test environment, after upgrading the Dial-Up Networking support in the client (TPC) to DUN 1.3, we configure the dial-up PPP connection to the ISP (*PPPoISP*) as described in 10.1.10, “Configuring Windows 95 Dial-Up Networking (DUN)” on page 436.

10.2.8 Installing the WinVPN client

For client installation information, refer to *WinVPN Client Installation and Troubleshooting Guide* that came with your product. WinVPN requires:

- Windows 95, Windows 98, or Windows NT 4.0 operating systems
- Microsoft Dial-Up Networking (DUN) version 1.2 or higher

Note: DUN 1.3 is standard with Windows 98.

- One Ethernet or a WAN adapter with Microsoft TCP/IP protocol bound to it
- Internet Explorer 5.0 or higher

After verifying the pre-requisites in the PC client, perform the WinVPN client installation by following the prompts and the standard documentation provided with the client.

In the WinVPN Setup - Adapter Selection window, select **Connect through Wide Area Network Adapter** as shown in Figure 543.

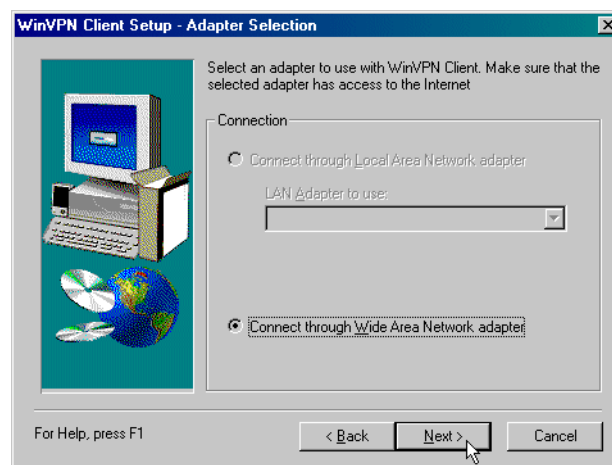


Figure 543. WinVPN client installation - Selecting the adapter

10.2.9 Configuring iVasion WinVPN client

Once WinVPN is installed on the PC, the WinVPN icon appears on the Windows task bar as shown in Figure 544.



Figure 544. WinVPN client icon on the Windows task bar

To configure the WinVPN client, perform the following steps:

1. Right-click the WinVPN icon on the Windows task bar. The WinVPN configuration menu pops up as shown in Figure 545.

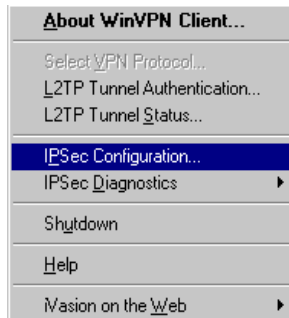


Figure 545. WinVPN configuration menu

Note: Do not use L2TP tunnel authentication because the client is already authenticated through IKE. Use this option if L2TP authentication is enabled at the LNS.

2. Select **IPSec Configuration**. The IKE Configuration window shown in Figure 546 is displayed.

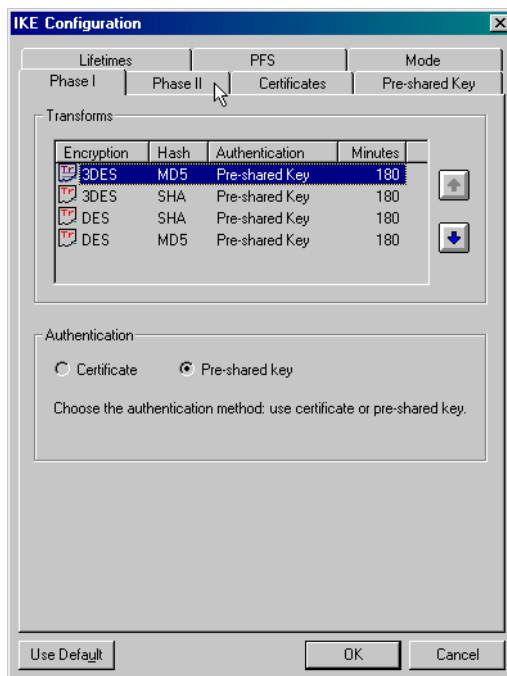


Figure 546. WinVPN client IKE Configuration - Phase I

3. For Authentication, select **Pre-shared key**. The AS/400 system only supports the pre-shared key as an authentication method in V4R4.
4. Accept the phase I transforms already configured in the client. You can move up the one that matches the AS/400 configuration for a faster match, but it is not necessary to do that at this time. See Figure 546 on page 454.

- Click the **Phase II** tab. The IKE phase II proposals and transforms configuration window is displayed as shown in Figure 547.

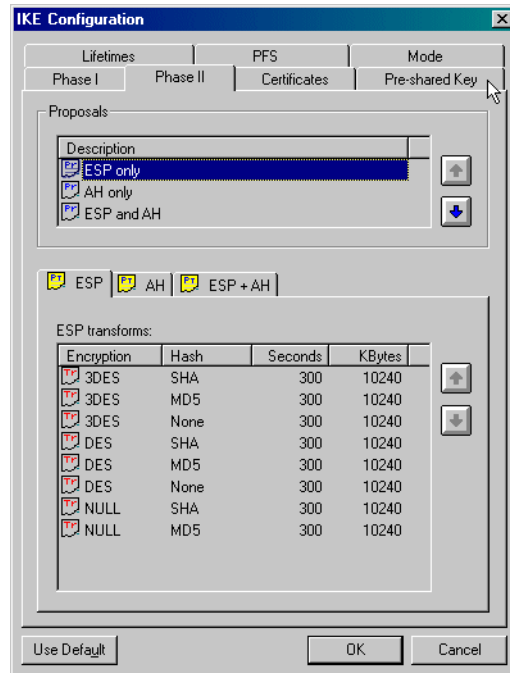


Figure 547. WinVPN client - IKE Configuration - Phase II

- Select **ESP Only** for Proposals Description.
- Accept the pre-configured ESP transforms. One of them (Encryption DES, Hash MD5) matches the AS/400 system configuration. See Figure 547.
- Click the **Pre-shared Key** tab. The window to configure the remote VPN server is displayed as shown in Figure 548 on page 456.

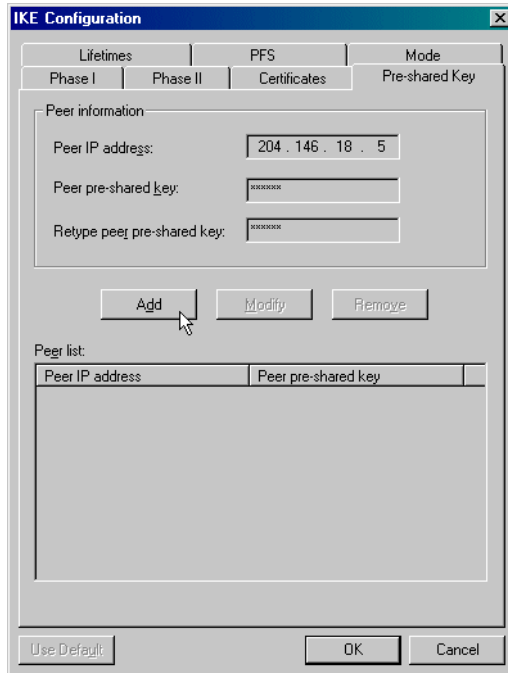


Figure 548. WinVPN - Remote VPN server configuration

9. Enter the IP address of the AS/400 VPN server at the corporate office (AS05).
In this scenario, enter 204.146.18.5.
10. Enter the pre-shared key configured for this client at the VPN server. In this scenario, the pre-shared key value is winvpn, which must match the pre-shared key configured on the AS/400 system in step 11 on page 449.
11. Click **Add** to add the peer VPN host you just configured. The IP address and the pre-shared key of the remote VPN server (AS05) are added to the Peer list as shown in Figure 549 on page 457.

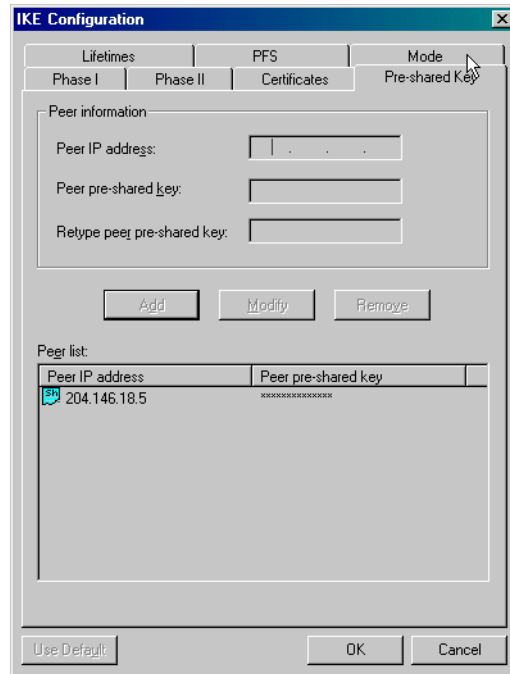


Figure 549. WinVPN - VPN Peer list

12. Click the **Mode** tab. The window to configure the IKE mode is displayed as shown in Figure 550.
13. Select **Aggressive mode**.
14. Select **User FQDN** for the client ID type, and enter `winvpn@itso.ibm.com` as client ID. Refer to Figure 550. These values must match the AS/400 system configuration specified in step 11 on page 449.

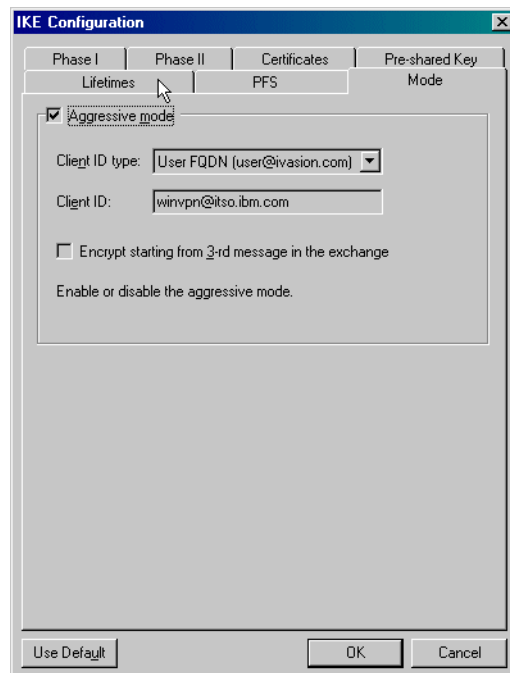


Figure 550. WinVPN client - IKE mode configuration

15. Click the **Lifetimes** tab to configure the session key lifetimes. The window shown in Figure 551 is displayed.

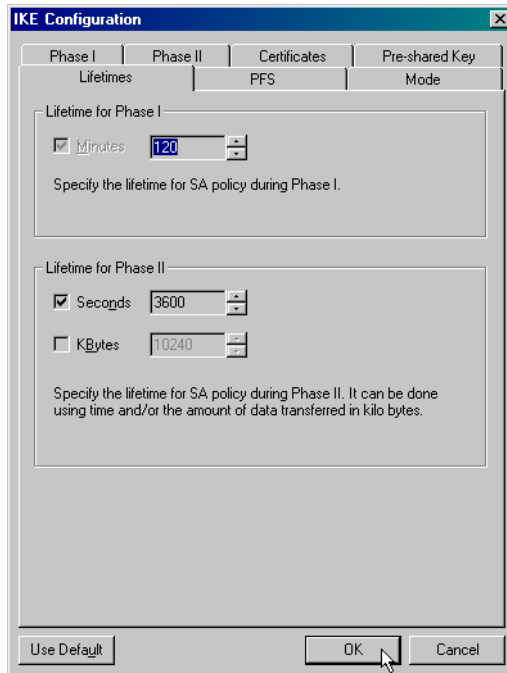


Figure 551. IKE key lifetime configuration

16. Enter the key expiration values that match your AS/400 system configuration. In this scenario, select **120** minutes for Lifetime for Phase I and **3600** seconds for Lifetime for Phase II.

17. Click **OK** to complete the WinVPN client configuration.

10.2.10 Configuring the L2TP initiator for the WinVPN client

After installing the WinVPN client, you must create and configure a new Dial-Up Networking (DUN) connection that represents the L2TP tunnel to the corporate LNS. This is done the same way you configured the DUN connection to the ISP as described in 10.1.10, "Configuring Windows 95 Dial-Up Networking (DUN)" on page 436. The main difference is that, instead of selecting *Thinkpad 28.8 Data Fax Modem* in the Connect using field (see Figure 519 on page 437), you must select the VPN (#1 or #2) adapter.

To configure the L2TP initiator in the WinVPN client, perform the following steps:

1. On the Windows desktop, double-click **My Computer->Dial-Up Networking**.
2. Double-click **Make New Connection**.
3. Enter a name for the connection (**L2TPtoLNS**).
4. Select VPN Adapter #1 (Figure 552 on page 459).

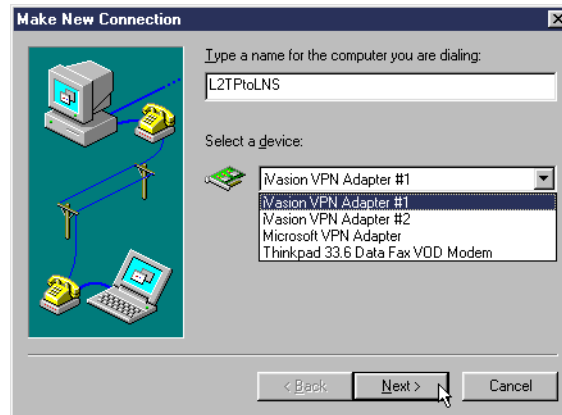


Figure 552. Configuring the L2TP initiator in the WinVPN client - Selecting VPN adapter

5. Click **Next**.

Note

Microsoft Dial-Up Networking (DUN) 1.3 adds the device Microsoft VPN Adapter as shown in Figure 552. This includes *only* PPTP support, which is *not* supported by the AS/400 system.

6. In the Host Name or IP Address field, enter the IP address of the LNS terminator as 204.146.18.5. See Figure 553.

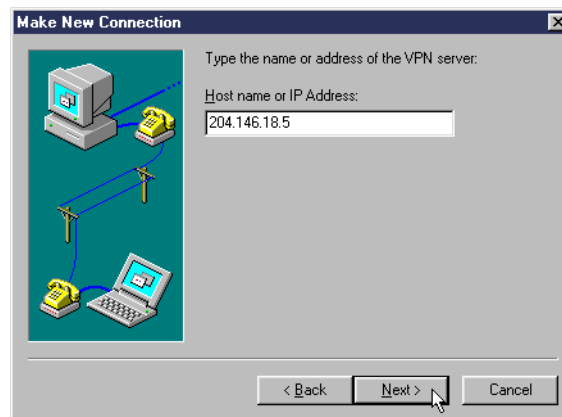


Figure 553. L2TP initiator in the WinVPN client - Configuring the L2TP terminator IP address

7. Click **Next**.

8. Click **Finish** to create the new connection.

There are two new connections in the Dial-Up Networking window as shown in Figure 554 on page 460.

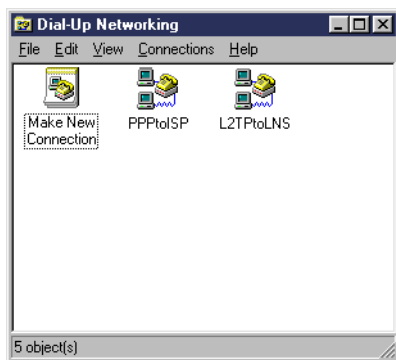


Figure 554. Dial-Up connections window - PPPtoISP and L2TPtoLNS

To complete the setup of the new dial-up connection that represents the client end of the L2TP tunnel, perform the following steps:

1. Right-click the dial-up connection entry that you just created (**L2TPtoLNS**), and then click **Properties**.
2. Click the **Server Types** tab to bring that page to the front.
3. Under Advanced Options, ensure that only the **Log On To Network** check box is selected. All other check boxes under Advanced Options must be cleared.
4. Under Allowed Network Protocols, select only **TCP/IP**.
5. Click **TCP/IP Settings**.
6. On the TCP/IP Settings dialog box, ensure that the **Server Assigned IP Address** and **Server Assigned Name Server Addresses** options are selected.
7. Clear the **Use IP Header Compression** check box.
8. Click **OK** to close the TCP/IP Settings dialog box.
9. Click **OK** to complete the dial-up connection configuration.

For more information about WinVPN installation, configuration, and problem determination, refer to the *WinVPN Client Installation and Troubleshooting Guide*.

10.2.11 Starting the LNS AS05

To start all the functions needed in the LNS (AS05), follow this process:

1. Start IP filters.
The status of IP packet security should be *Started*.
2. Start Virtual Private Networking.
The status of Virtual Private Networking should be *Active*.
3. Start the L2TP terminator profile (AS25bterm in this scenario).
The status of the virtual line L2TP terminator should be *Waiting for connection requests*.

Refer to 7.4.1, “Starting the LNS in an L2TP voluntary tunnel (AS05)” on page 315, for more information on the tasks listed in this section.

10.2.12 Starting the L2TP with IPsec PC client (WinVPN)

To start the WinVPN client, perform the following tasks:

1. Start the PPP dial-up connection to the ISP. Complete these steps:
 - a. On the Windows desktop, double-click **My Computer->Dial-Up Networking**.
 - b. Double-click the connection to the ISP, **PPPToISP**.
 - c. Enter the sign-on information, and click **Connect**.
2. Start the PPP dial-up connection to the corporate LNS. In this task you establish the L2TP tunnel to the corporate gateway. Follow these steps:
 - a. On the Windows desktop, double-click **My Computer->Dial-Up Networking**.
 - b. Double-click the connection to the LNS **L2TPtoLNS**.
 - c. Enter the sign-on information as shown in Figure 555, and click **Connect**. In our tests, we did not use L2TP authentication, so we enter any User name and Password.

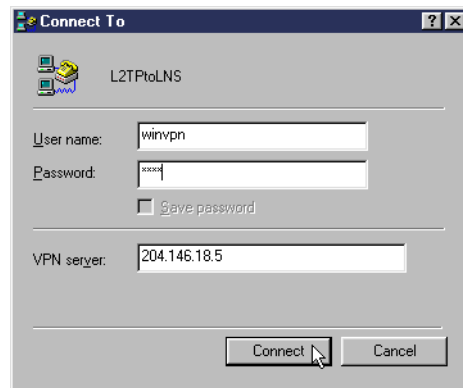


Figure 555. WinVPN client - Connecting to corporate LNS (AS05)

10.2.13 Verifying the status of the connection

Once the L2TP tunnel protected by IPsec is established, the status of the objects at the LNS are as follows:

- The PPP connection profile L2TP terminator (AS25term in our scenario) is Active.
- The VPN Active Connections window shows the status of the IPsec tunnel to the client (Figure 556 on page 462).

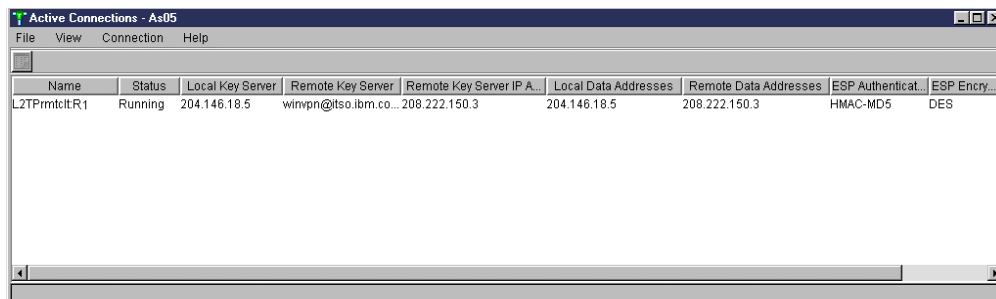


Figure 556. VPN Active Connections window - IPsec tunnel to WinVPN client

Note

For information about TCP/IP interfaces and routes on the LNS, refer to 7.5, “Verifying interfaces and routes” on page 317.

At the PC client, there are two Dial-Up Networking connections that are active: the connection to the ISP (PPPToISP, see Figure 557) and the connection to the corporate LNS (L2TPtoLNS, see Figure 558).

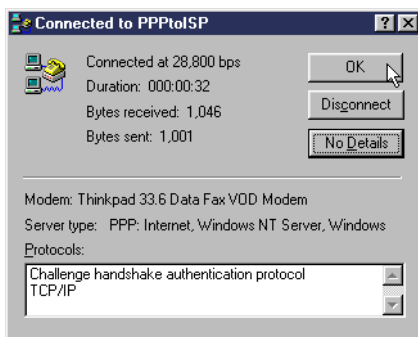


Figure 557. WinVPN PPPToISP dial-up networking connection status

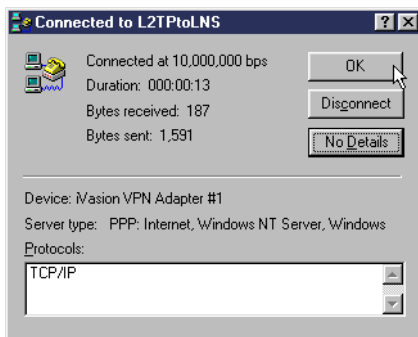


Figure 558. WinVPN L2TPtoLNS Dial-up Networking Connection status

There are two icons on the Windows task bar that represent the two DUN connections (Figure 559 on page 463). As you pause the mouse pointer over the WinVPN icon on the windows task bar, a small pop-up indicates that the PC client is currently connected (WinVPN Client - Tunnel Up).



Figure 559. Windows task bar after starting both dial-up connections

You can use the WinVPN menu options L2TP tunnel Status... and IPsec Diagnostics to monitor the status of the tunnel.

Figure 560 shows the WinVPN client log. Notice the messages reporting phase I and phase II negotiations. You can display this log by selecting **IPsec Diagnostics->View log** from the WinVPN icon menu.

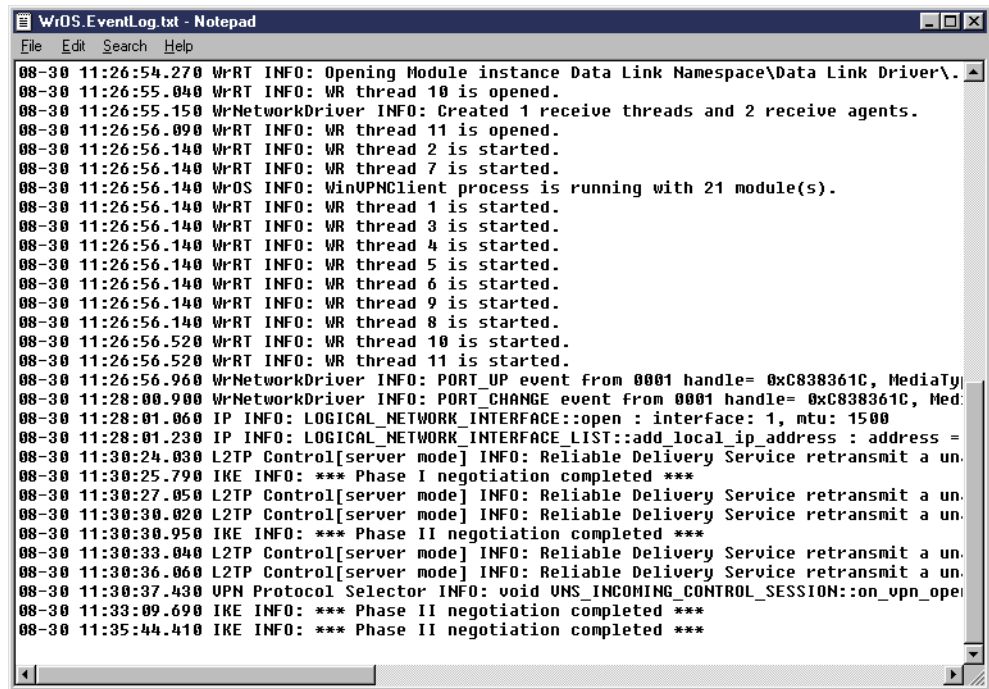


Figure 560. WinVPN view log

Figure 561 shows the network status displayed when you select **IPsec Diagnostics->Network Status** from the WinVPN menu.

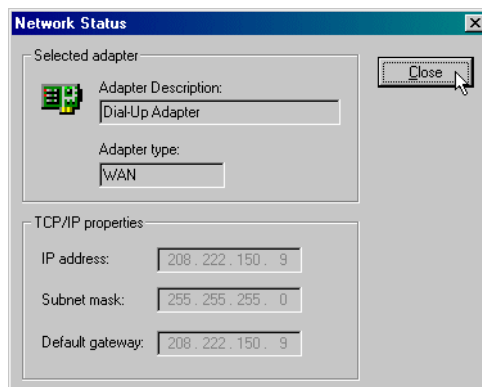


Figure 561. WinVPN client - Network Status

Figure 562 shows the WinVPN client status with information about the L2TP tunnel.

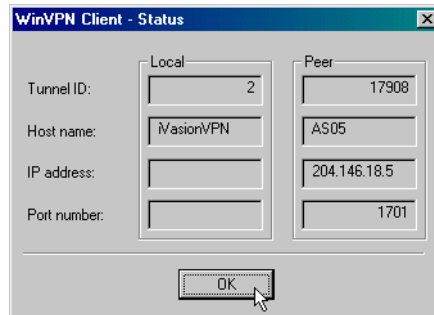


Figure 562. WinVPN client - L2TP tunnel information

10.3 Supporting a mixed client environment

The previous sections of this chapter covered two distinctive types of VPN clients: IPsec-only clients (IRE SafeNet Soft-PK) and L2TP with IPsec clients (WinVPN). The implementations presented in 10.1, “Remote PC clients with IPsec-only support” on page 419, and 10.2, “Remote PC clients with IPsec and L2TP support” on page 444, are independent of each other.

To support both environments, the IP filters used must be a super set of those used in the previous sections. This section shows you how to configure IP packet security to support both types of clients.

10.3.1 Modifying IP filters for IPsec-only and L2TP with IPsec clients

The IPSEC filter rule configured in 10.1.9, “Configuring IP filters on the AS/400 system (AS05)” on page 430, has the secured intranet subnet as a data endpoint. The Services window opens all protocols, the source port, and the destination port with a wildcard (*) configuration. See Figure 514 on page 434 and Figure 515 on page 434.

The IPSEC filter rule configured in 10.2.5, “Configuring IP filters on the AS/400 system (AS05)” on page 452, has the L2TP tunnel endpoint IP address as a data endpoint. See the SRCADDR field in Figure 542 on page 452. Notice also in the same figure that the services in the IPSEC filter rule are restricted to protocol UDP, with source and destination port 1701.

To support both environments simultaneously, configure the IP filter rules as shown in Figure 563 on page 465.


```

IP Packet Security: All Security Rules
#Filter interface
FILTER INTERFACE LINE = TRLANC SET = DynIP
#IKE filter rules
FILTER SET DynIP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = 204.146.18.5 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
FRAGMENTS = NONE JRN = OFF

FILTER SET DynIP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.5
DSTADDR = * PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
FRAGMENTS = NONE JRN = OFF
#IPSEC filter rule
FILTER SET DynIP ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = * DSTADDR = *
PROTOCOL = * DSTPORT = * SRCPORT = *
FRAGMENTS = NONE JRN = OFF CONNECTION_DEFINITION = DYNAMICIP

```

Figure 563. IP packet security configuration to support a mixed VPN client environment

This filter configuration enables the AS/400 system VPN server and LNS at the corporate office to support connections from IPSec-only clients as well as L2TP with IPSec clients as shown in Figure 564.

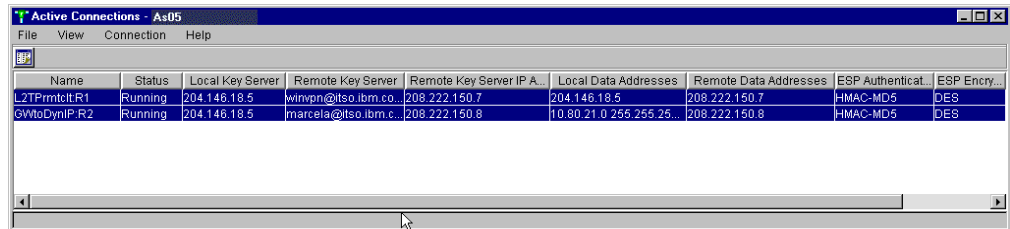


Figure 564. AS05 Active Connections - IPSec-only and L2TP with IPSec client sessions

10.3.2 Verification tests

Table 45 presents a summary of the TCP/IP applications that ran through the VPNs configured in the scenarios presented in this chapter.

Table 45. Verification test - Secure PC clients to AS/400 servers

	CA400/Ops Nav	TELNET	FTP	PING
From SafeNet Soft-PK to AS05	Yes	Yes	Yes	Yes
From WinVPN client to AS05	Yes	Yes	Yes	Yes
From SafeNet Soft-PK to AS22	Yes	Yes	Yes	Yes
From WinVPN client to AS22	Yes	Yes	Yes	Yes

Chapter 11. Secure LAN access for PC clients in the intranet

Chapter 10, "Secure remote access for PC clients over the Internet" on page 419, explores the options for securely connecting traveling or work-at-home employees to the corporate office through a dial-up connection to an Internet Service Provider (ISP).

Data traveling the Internet is not the only data that needs to be protected. Companies are becoming increasingly concerned about the confidentiality of sensitive information traversing company LANs. It may be important to encrypt and authenticate all traffic to and from the human resources server. In some cases, only authentication may be required. There are some scenarios where remote clients look like LAN attached to the corporate security gateway, for example, employees accessing the corporate office using a cable modem to the ISP.

This chapter explores a scenario where PC clients are LAN-connected to AS/400 systems in an intranet environment. Two PC clients with IPsec clients are presented in this chapter:

- IRE SafeNet Soft-PK. For more information about this client, visit:
<http://www.ire.com>
- Any Windows client that supports IPsec. This is a generic client and is only presented as an example to show the corresponding VPN configuration on the AS/400 system.

Note

The VPN clients used during our tests were early beta versions of the software. You can expect some differences in the final (generally available) version of the products.

11.1 VPN connections between PC clients and AS/400s in an intranet

There are some differences in the characteristics of secure access for PC clients on an intranet and Internet environments. They are:

- IP address assignment
Clients in the intranet are either assigned fixed IP addresses or dynamically assigned IP addresses by a DHCP server. In both cases, the IP addresses are in the company's private address space.
Clients on the Internet are dynamically assigned a globally routable IP address that is not in the company's private address space, unless L2TP is used.
- Access control
On the intranet, clients usually need access to multiple servers with different security requirements. Some connections need to be protected by IPsec encryption and authentication and some only by authentication. Others don't need to be protected at all.

In the Internet, all traffic between the remote client and the corporate gateway must be protected by IPSec. Beyond the corporate gateway, in the intranet, the traffic may flow in the clear or be protected until it reaches the target host.

This chapter covers host-to-host VPN connections between LAN-attached PC clients and AS/400 systems in an intranet.

11.1.1 Scenario characteristics

The characteristics of this scenario are:

- Clients and servers are connected to the same LAN in the company's intranet.
- All systems are in the same subnet in the company's intranet.
- Some clients, represented by ThinkPad C in Figure 565, are dynamically assigned IP addresses in the company's address space by a DHCP server.
- Some clients, represented by PC D in Figure 565, are permanently assigned fixed IP addresses.

11.1.2 Scenario objectives

The objectives of this scenario are:

- All traffic to AS/400 RALYAS4A (**A**) must be protected using encryption and authentication.
- All the traffic to AS/400 RALYAS4C (**B**) must be authenticated.
- Traffic to all other systems in the intranet flows in the clear.
- The company's security policy requires that the keys for IKE phase 1 are changed every 120 minutes. For IKE phase 2 (data), the keys are changed every 60 minutes.

Figure 565 shows the test network used for this scenario.

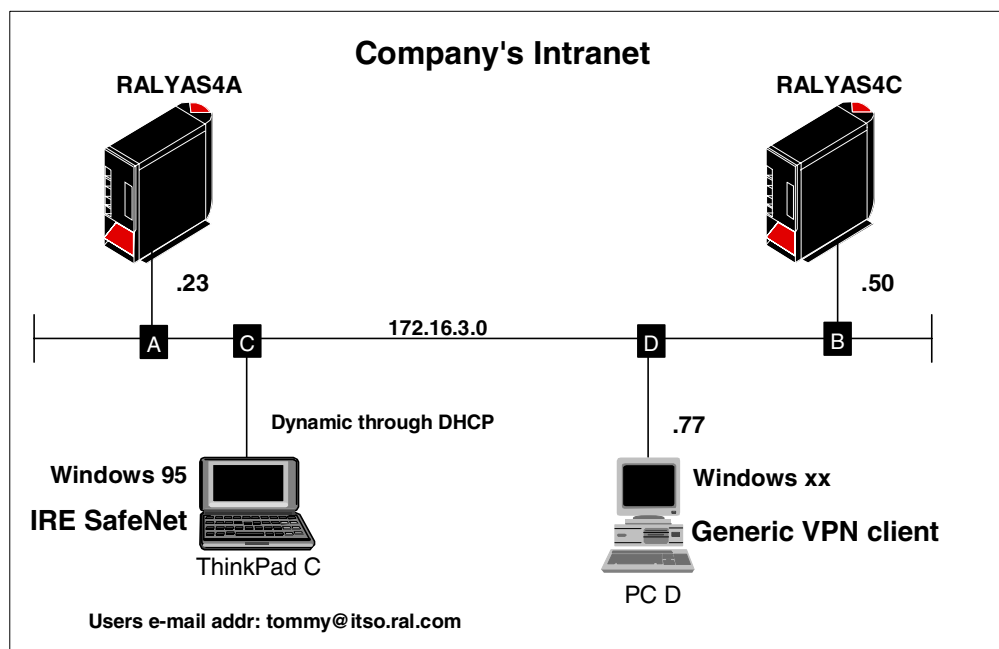


Figure 565. Intranet host-to-host connections - Scenario network configuration

11.1.3 Implementation tasks: Summary

The following is a summary of the tasks used to implement this VPN host-to-host environment:

1. Verify connectivity. Before you start configuring VPN and the filters, you must ensure that the underlying TCP/IP network is properly configured and working.
2. Complete the planning worksheet for the appropriate VPN client.
3. Complete the planning worksheet for the AS/400 system.
4. Configure a Host to Dynamic IP Users VPN on the AS/400 system.
5. Configure a host-to-hosts VPN on the AS/400 system.
6. Configure filters in the AS/400 system.
7. Configure the VPN client on ThinkPad C.
8. Configure the VPN client on PC D.
9. Start the VPN connections.
10. Check the VPN connection status.

11.1.4 Verifying end-to-end connectivity

Before you start configuring the VPN partners, it is important to work out any connectivity problems that may exist between the endpoints. In our scenario, we performed the following verification tests:

1. PING RALYAS4A (**A**) from ThinkPad C and PC D. The PING command is used to check the proper IP addressing and routing setup.
2. PING RALYAS4C (**B**) from ThinkPad C and PC D.
3. PING ThinkPad C and PC D from RALYAS4A (**A**).
4. PING ThinkPad C and PC D from RALYAS4C (**B**).
5. FTP a file from both PCs to either AS/400 system.

If you experience problems with mismatching MTU sizes, adjust the MTU sizes and FTP in both directions to verify the settings.

Once the simple TCP/IP connectivity test is complete, proceed with the VPN configurations.

11.1.5 Completing the planning worksheet for IRE SafeNet Soft-PK

On ThinkPad C, we used the VPN client from IRE. The product name is SafeNet Soft-PK, and we tested with version 2.0.4 (Build 6). Table 46 on page 470 shows the planning worksheet with the information required to configure the VPN in this client to RALYAS4A and RALYAS4C.

Notice that, according to the 11.1.2, “Scenario objectives” on page 468, the VPN connection to RALYAS4A must support ESP with encryption and authentication.

The VPN to RALYAS4C only requires authentication. Therefore, AH is sufficient in this case.

Table 46. IRE SafeNet planning worksheet - ThinkPad C

This is the information you need to create your VPN with IRE SafeNet GUI	Scenario answers for RALYAS4A	Scenario answers for RALYAS4C
What will you name the connection?	RALYAS4A	RALYAS4C
How will you identify your local server? – IP address (n/a) – Domain name – E-mail address	E-mail address	E-mail address
What is the identifier of your local server?	tommy@itso.ral.com	tommy@itso.ral.com
How will you identify the remote server to which you are connecting?	IP address	IP address
What is the IP address of the remote server?	172.16.3.23	172.16.3.50
What is the pre-shared key?	thomaswashere	unbelievable
What type of connection security is used? – Secure – Non-secure – Block	Secure	Secure
Is the client connecting to the remote host through a secure gateway tunnel? – No (checkbox remains unchecked) – Yes (checkbox is checked)	No	No
What local PC network interface is used for this connection?	Any	Any
What are the authentication and encryption characteristics for the IKE authentication phase I?		
– Authentication method – Encryption algorithm – Hash algorithm (data integrity) – SA life – Key group	Pre-shared key DES MD5 Seconds 7200 Diffie-Hellman Group 1	Pre-shared key DES MD5 Seconds 7200 Diffie-Hellman Group 1
What are the key exchange characteristics for IKE phase II? – ESP – AH	ESP	AH
– ESP settings • Encryption algorithm • Hash algorithm • Encapsulation • SA Life	DES MD5 Transport Seconds 3600	n/a

This is the information you need to create your VPN with IRE SafeNet GUI	Scenario answers for RALYAS4A	Scenario answers for RALYAS4C
- AH settings <ul style="list-style-type: none"> • Hash algorithm • SA Life 	n/a	MD5 Seconds 3600

The company's DHCP server dynamically assigns an IP address to this PC client (ThinkPad C). Therefore, you cannot use the IP address as the local identifier. The planning worksheet also includes several parameters that do not appear in the AS/400 system planning worksheet. The reason is that the AS/400 configuration is created through the VPN configuration wizard. The wizard sets many parameter values without user input.

11.1.6 Completing the planning worksheet for generic VPN client (PC D)

Table 47 shows the configuration information for PC D. PC D is assigned a fixed IP address. Main mode is used in IKE phase 1. Note that in main mode, the identifier is the IP address. This connection encrypts and authenticates the traffic to the remote system.

Note

The generic VPN client in our scenario represents any client available on the market which supports IPsec. The PC client can be a Windows 2000 Professional edition that provides native IPsec support as part of the operating system. Notice that Windows 2000 does not support the IKE aggressive mode when pre-shared keys are used for authentication. Windows 2000 only supports the main mode. In V4R4, the AS/400 system requires a pre-shared key for authentication. If the main mode is used in IKE phase 1, then the identifier must be an IP address. Therefore, Windows 2000 cannot be used in an environment where the IP addresses are dynamically assigned. However, PC D in this scenario could be running Windows 2000 since it is assigned a fixed IP address.

Note that the pre-shared keys are unique for each VPN configuration.

Table 47. Generic VPN client planning worksheet - PC D

This is the information you need to create the VPN configuration	Scenario answers for RALYAS4A	Scenario answers for RALYAS4C
What will you name the connection?	RALYAS4A	RALYAS4C
What type of connection you are creating? – Host to Host – Host to Gateway	Host to hosts	Host to hosts
What IKE negotiation mode is used? – Aggressive mode – Main mode	Main mode	Main mode
How will you identify your local server?	IP address	IP address
What is the identifier of your local server?	172.16.3.77	172.16.3.77

This is the information you need to create the VPN configuration	Scenario answers for RALYAS4A	Scenario answers for RALYAS4C
How will you identify the remote server to which you are connecting?	IP address	IP address
What is the IP address of the remote server?	172.16.3.23	172.16.3.50
If this is a host-to-gateway connection, what is the IP subnet mask? A host-to-host connection uses always 255.255.255.255.	n/a	n/a
What is your pre-shared key?	12345678	wolfsheim
What are the IKE phase 1 characteristics?		
<ul style="list-style-type: none"> – Authentication method – Encryption algorithm – Hash algorithm – Life duration (key lifetime) 	Pre-shared keys DES MD5 Seconds 7200	Pre-shared keys DES MD5 Seconds 7200
What are the data security characteristics? (Security Consideration)	Require data confidentiality	Require data integrity and authentication
<ul style="list-style-type: none"> – Encryption algorithm – Hash algorithm – SA life duration – Encapsulation mode 	DES MD5 Seconds 3600 Transport mode	n/a MD5 Seconds 3600 Transport mode

11.1.7 Completing the planning worksheet for RALYAS4A

This scenario covers two different types of VPN connections:

- Connections from PC D to the AS/400 systems are *host to host* because PC D is assigned a fixed IP address.
- Connections from ThinkPad C to the AS/400 systems are *host to dynamic IP users* because the DHCP server dynamically assigns IP addresses to ThinkPad C.

Complete the AS/400 system planning worksheet as shown in Table 48. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 48. RALYAS4A New Connection Wizard AS/400 planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers for ThinkPad C	Scenario answers for PC D
What type of connection are you creating? <ul style="list-style-type: none"> – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Hosts – Gateway to dynamic IP User – Host to Dynamic IP User 	Host to Dynamic IP Users	Host to Hosts
What will you name the connection group?	HtoDynIPC	HtoHD

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers for ThinkPad C	Scenario answers for PC D
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Balanced	Balanced
How will you identify your local server?	IP address	IP address
What is the IP address of your local server?	172.16.3.23	172.16.3.23
How will you identify the remote server to which you are connecting?	User@fully qualified domain name	IP address
What is the identifier of the remote server?	tommy@itso.ral.com	172.16.3.77
What is the pre-shared key?	thomaswashere	12345678
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Balanced	Balanced

11.1.8 Completing the planning worksheets for RALYAS4C

This scenario covers two different types of VPN connections:

- Connections from PC D to the AS/400 systems are *host to host* because PC D is assigned a fixed IP address.
- Connections from ThinkPad C to the AS/400 systems are *Host to Dynamic IP Users* because the DHCP server dynamically assigns IP addresses to ThinkPad C.

Complete the AS/400 system planning worksheet as shown in Table 49. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 49. RALYAS4C New Connection Wizard AS/400 planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers for ThinkPad C	Scenario answers for PC D
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Hosts – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Dynamic IP Users	Host to Hosts
What will you name the connection group?	HtoDynIPC	HtoHD

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers for ThinkPad C	Scenario answers for PC D
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Minimum security	Minimum security
How will you identify your local server?	IP address	IP address
What is the IP address of your local server?	172.16.3.50	172.16.3.50
How will you identify the remote server to which you are connecting?	User@fully qualified domain name	IP address
What is the identifier of the remote server?	tommy@itso.ral.com	172.16.3.77
What is the pre-shared key?	unbelievable	wolfsheim
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Minimum security	Minimum security

Tip

When configuring a Dynamic IP group or a dynamic key group, as is the case in this scenario, you must provide the pre-shared key in ASCII format to the AS/400 GUI. Notice that some clients require the key in hexadecimal format.

11.1.9 Configuring the AS/400 system RALYAS4A

You must configure two VPNs on the AS/400 systems:

- *Host to Dynamic IP Users* to support clients with dynamically assigned IP addresses (ThinkPad C)
- *Host to Hosts* to support clients with fixed IP addresses (PC D)

RALYAS4A runs highly confidential applications and stores sensitive data. All traffic to this AS/400 system must be protected with ESP encryption and authentication.

11.1.9.1 A Host to Dynamic IP Users connection for ThinkPad C

Use the VPN configuration wizard to configure the *Host To Dynamic IP Users* connection. The wizard creates the following configuration objects:

- Key policy
- Data policy
- Key connection group
- Dynamic IP group

On the AS/400 system, clients with a dynamically assigned IP address are referred to as *remote users*. This does not mean that the client has to be remotely

attached to the network. Clients in a LAN environment, as is the case in this scenario, are considered remote users. The AS/400 system supports two identifier types for remote users. These are:

- User@fully qualified domain name
- Key identifier

In this scenario, use *user@fully qualified domain name* as the identifier for ThinkPad C. It corresponds to the *e-mail address* identifier on the SafeNet Soft-PK client.

Refer to Table 48 on page 472 for configuration details. Perform the following steps:

1. Start Virtual Private Networking from the Operations Navigator.
2. Select **File->New Connection->Host To Dynamic IP Users** to start the VPN configuration wizard.
3. Click **Next**. The Connection Name window as shown in Figure 566 on page 475 is displayed.
4. Enter the connection Name as `HtoDynIPC` and a Description as shown in Figure 566.

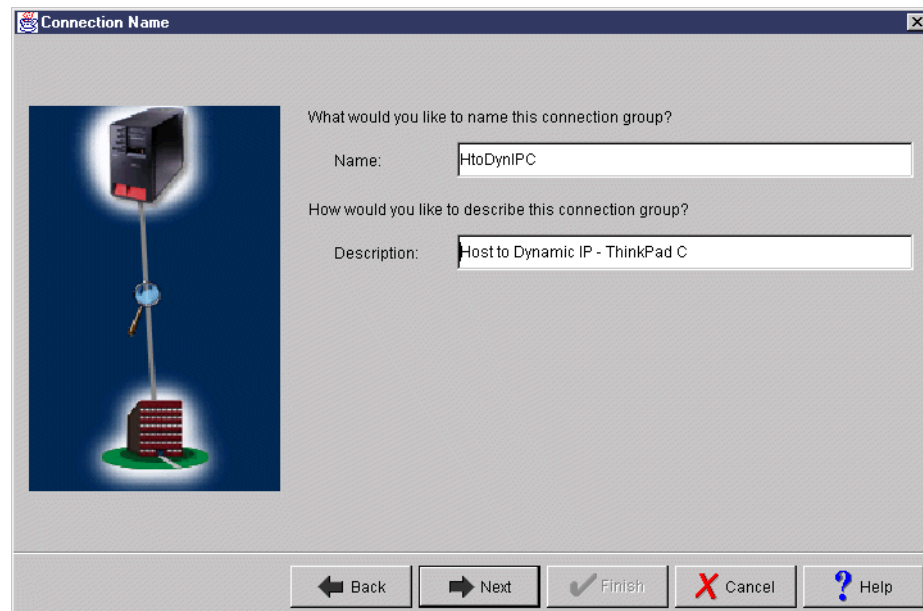


Figure 566. RALYAS4A Host to Dynamic IP Users configuration wizard - Connection Name

All objects created by the wizard for this particular connection are named after the name specified in the Connection Name window. The key and data policy objects get a suffix according to the security policy chosen in the wizard.

5. Click **Next**. The Key Policy window is displayed, as shown in Figure 567 on page 476.
6. Select **Balanced security and performance**. Based on the selection you make on this window, the wizard creates the appropriate key policy with its proposal and transform. For more information about the relationship between the wizard and the created objects, refer to 3.6.6, “New Connection Wizard planning” on page 63.

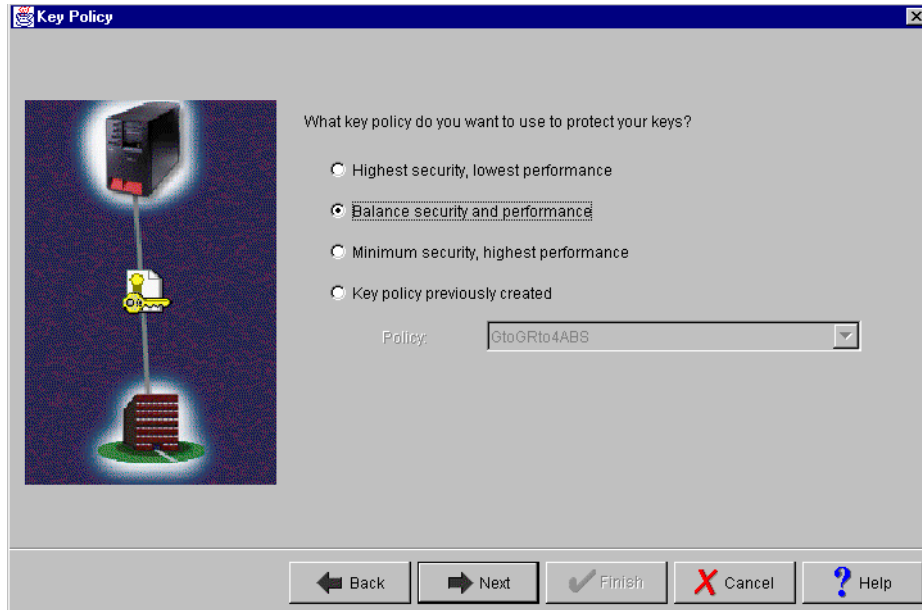


Figure 567. RALYAS4A Host to Dynamic IP Users configuration wizard - Key Policy

7. Click **Next**. The Local Identifier window is displayed, as shown in Figure 568.
8. Select **Version 4 IP address** as the Identifier type.
9. Select **172.16.3.23** for the local key server IP Address, as defined in Table 48 on page 472.

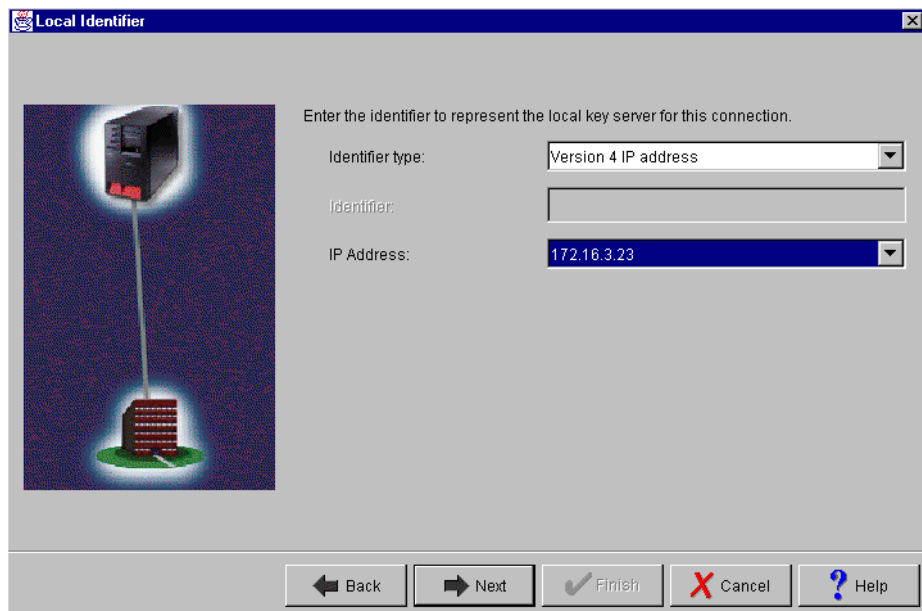


Figure 568. RALYAS4A Host to Dynamic IP Users configuration wizard - Local Identifier

10. Click **Next**. The Users window is displayed, as shown in Figure 569 on page 477.
11. Select **User@fully qualified domain name** as the Identifier type. The identifier type must match the client configuration.

12. Click **Add** to add a new identifier. In this scenario, enter `tommy@itso.ral.com` as the Identifier type and `thomaswashere` as the Pre-shared key. The identifier is used to select the appropriate dynamic IP group within the security policy database. Since the PC has a dynamically assigned IP address, the AS/400 system RALYAS4A can only be the responder and never the initiator of the connection.

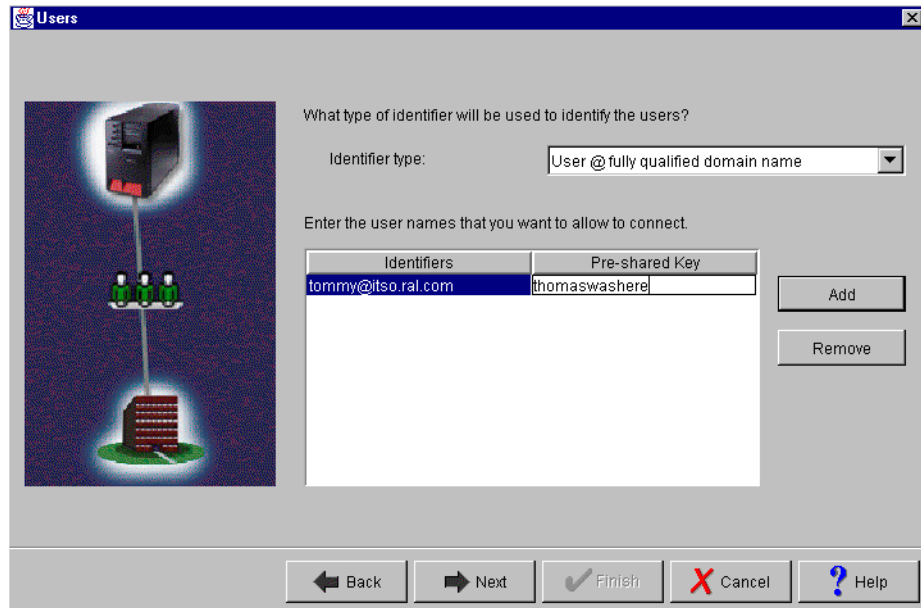


Figure 569. RALYAS4A Host to Dynamic IP Users configuration wizard - Users

13. Click **Next**. The Data Policy window is displayed, as shown in Figure 570.

14. Select **Balanced security and performance** for the data policy. Based on this selection, the wizard creates the data policy with the appropriate data encryption options.

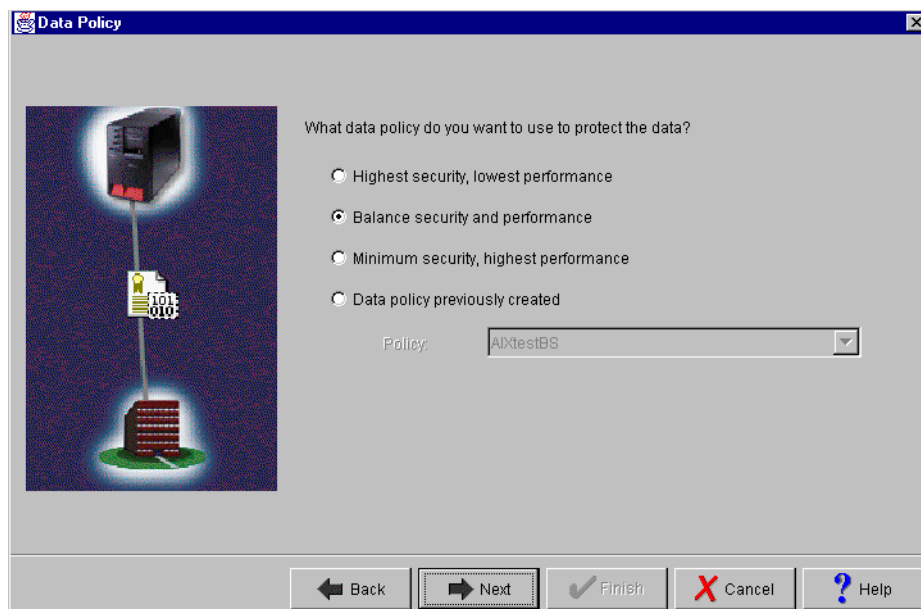


Figure 570. RALYAS4A Host to Dynamic IP Users configuration wizard - Data Policy

15. Click **Next**. The New Connection Summary window is displayed, as shown in Figure 571.

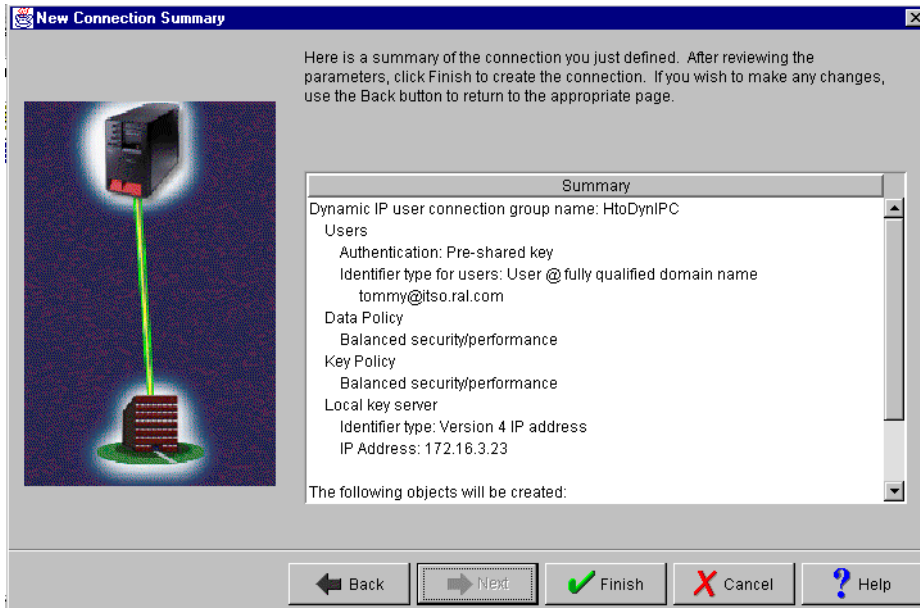


Figure 571. RALYAS4A Host to Dynamic IP Users - New Connection Summary

16. Click **Finish** to create the new connection.

17. Expand IP Security Policies, and click **Key Policies**.

18. Double-click **HtoDynIPCBS** to open the properties of the key policy. The Properties window is displayed (Figure 572). Note that the suffix BS is automatically appended by the wizard. The suffix is based on the policy selection made during the wizard configuration.

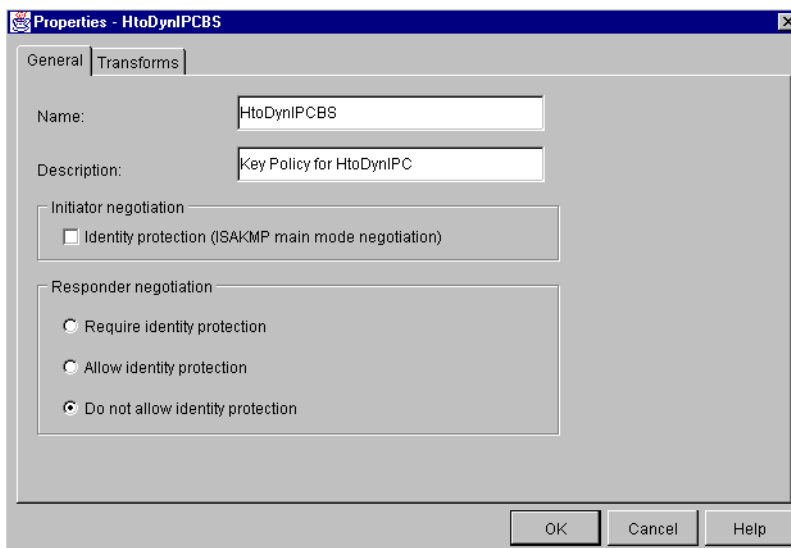


Figure 572. RALYAS4A to ThinkPad C key policy - General page

19. Click the **Transforms** tab (Figure 573 on page 479).

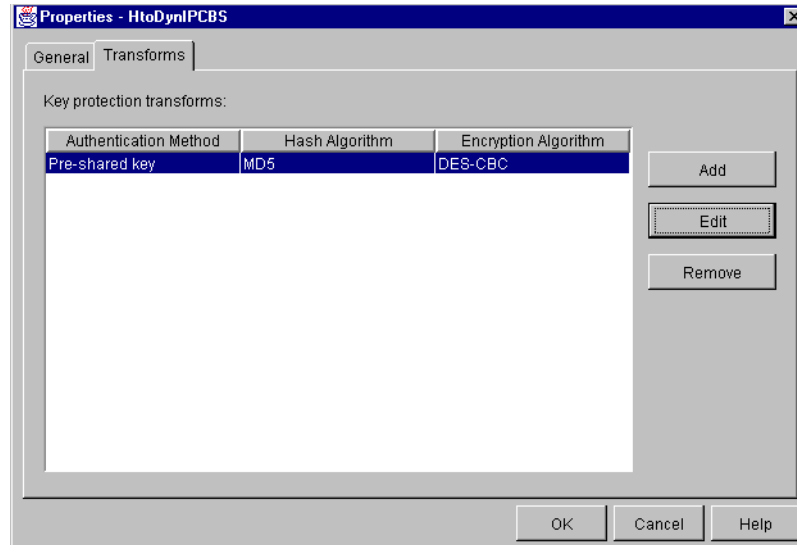


Figure 573. RALYAS4A to ThinkPad C key policy - Transforms page

20. Select the listed transform, and click **Edit** to update the transforms properties.
21. Change the Maximum key lifetime to 120 minutes (Figure 574).

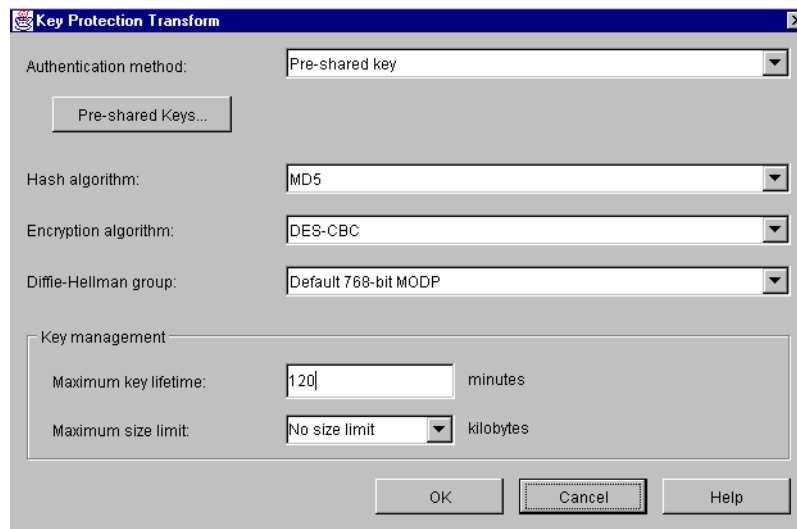


Figure 574. RALYAS4A to ThinkPad C key policy - Edit transform

Note

You can also change the lifetime values prior to using the configuration wizard. To do this, change the default settings for Virtual Private Networking. Detailed information is provided in 3.7.6, “Changing the Virtual Private Networking GUI default values” on page 76.

22. Click **OK** to save the transform.
23. Click **OK** to save the changed key policy.
24. Click **Data Policies**.

25. Double-click **HtoDynIPCBS** to open the data policy properties (Figure 575).

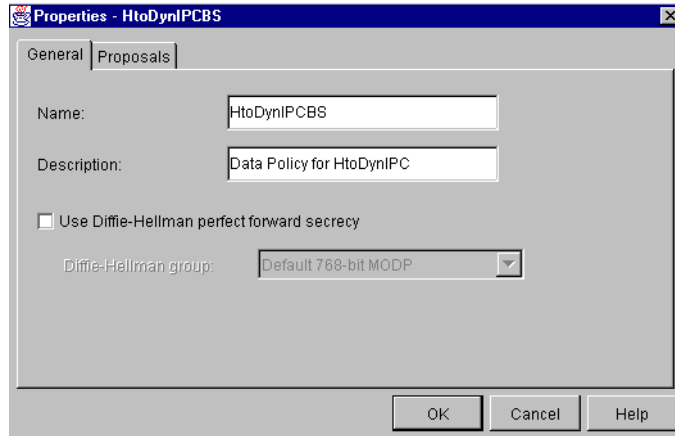


Figure 575. RALYAS4A to ThinkPad C data policy - General page

26. Click the **Proposals** tab (Figure 576).

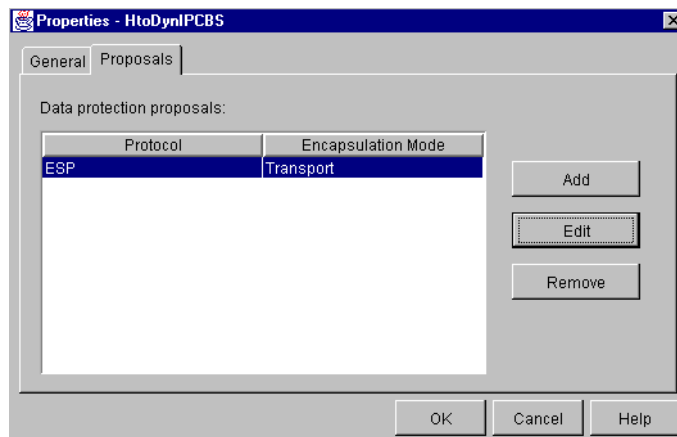


Figure 576. RALYAS4A to ThinkPad C data policy - Proposals page

27. Select the listed proposal, and click **Edit** to open the Data Protection Proposal properties (Figure 577 on page 481). Ensure that the encapsulation mode is set to **Transport**. Based on the scenario characteristics, the systems are not connected through a VPN gateway. Therefore, the encapsulation mode is Transport.

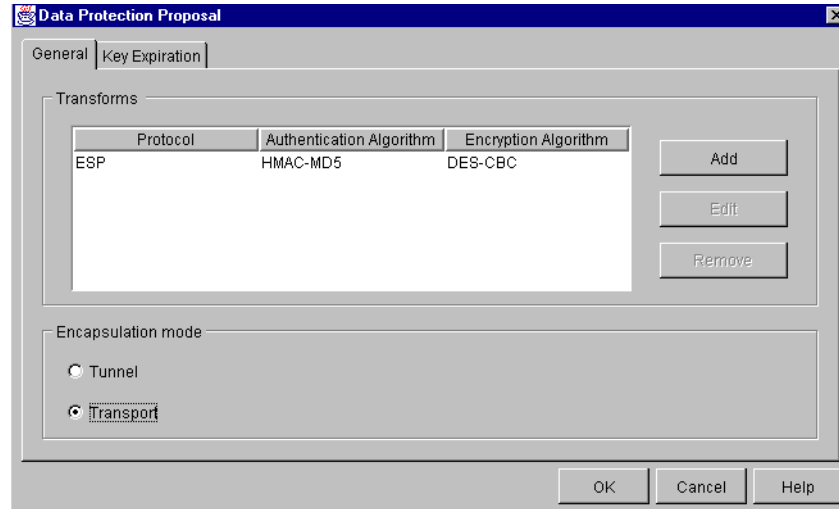


Figure 577. RALYAS4A to ThinkPad C data policy - Edit proposal

28. Click the **Key Expiration** tab, and change the **Expire after** field to 60 minutes as shown in Figure 578.

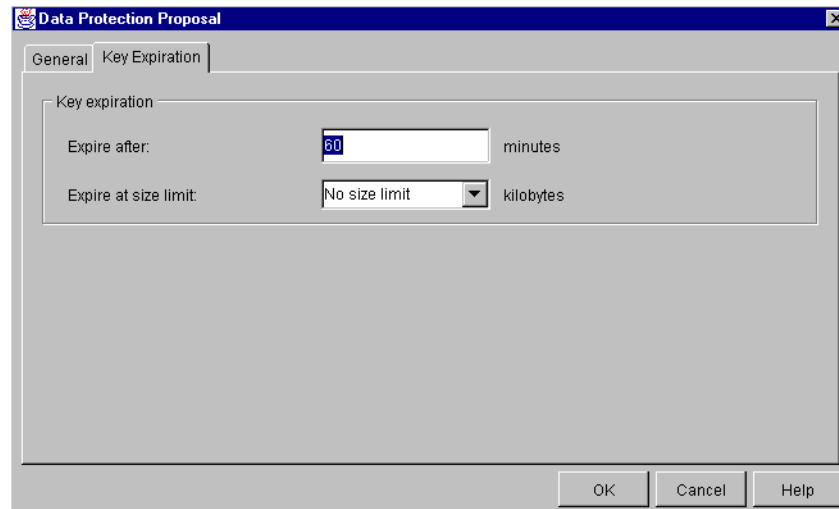


Figure 578. RALYAS4A to ThinkPad C data policy edit proposal - Key Expiration page

29. Click **OK** to save the proposal.

30. Click **OK** to save the data policy.

31. Expand **Secure Connections->Data Connections**, and click **Dynamic IP Groups**.

32. Right-click **HtoDynIPC** connection, and select **Properties** (Figure 579 on page 482).

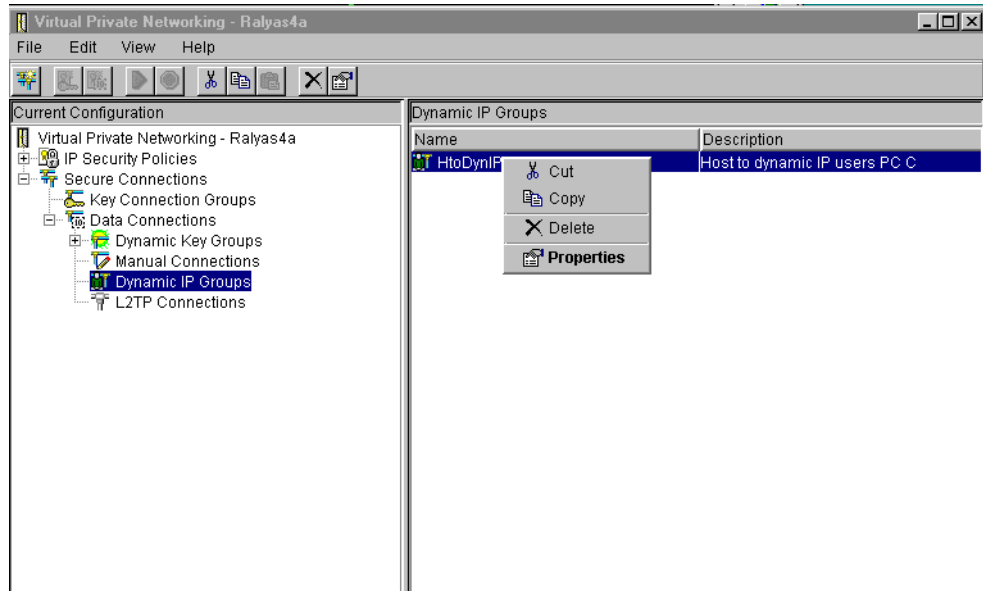


Figure 579. RALYAS4A to ThinkPad C - Dynamic IP Groups

33. Click **Policy**.

34. Change the following parameters from *Filter rule* to **Connection** as shown in Figure 580 on page 483:

- Local ports
- Remote addresses
- Remote ports
- Protocol

Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for more information.

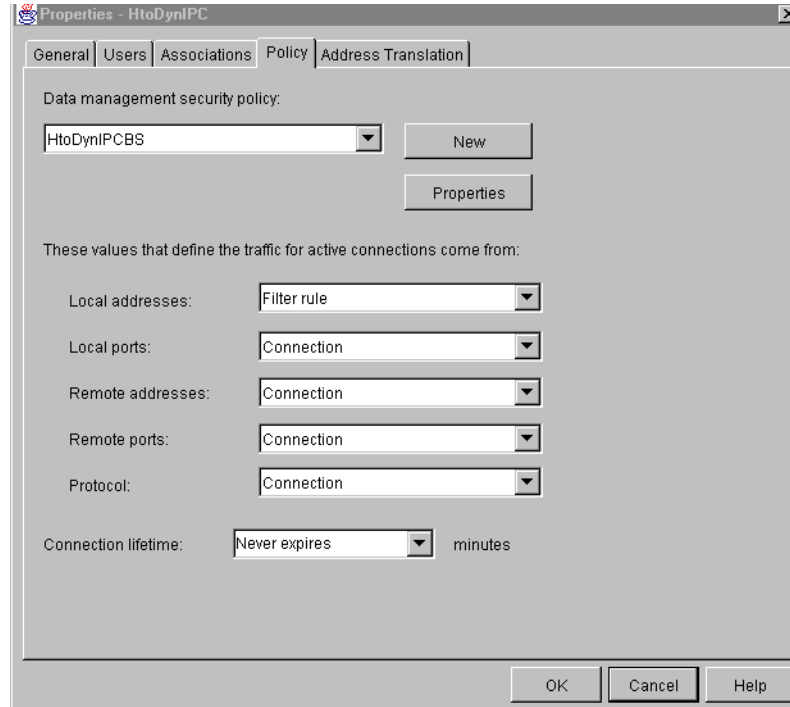


Figure 580. RALYAS4A to ThinkPad C Dynamic IP Group - Policy Page

35. Click **OK** to save the dynamic IP group.

This completes the VPN configuration on RALYAS4A for ThinkPad C.

11.1.9.2 A Host to Hosts connection for PC D

Use the VPN configuration wizard to configure the *Host To Hosts* connection. Both the AS/400 system and the PC have fixed IP addresses. The VPN configuration wizard creates the following objects:

- Key policy
- Data policy
- Key connection group
- Dynamic key group
- Dynamic key connection

Some changes are also required after the wizard creates the objects. Since some changes are the same as for the ThinkPad C configuration, not all screen captures are shown in the following process. Complete these steps for the Host to Hosts VPN configuration.

1. From Virtual Private Networking, select **File->New Connection...->Host To Hosts**.
2. Click **Next** at the New Connection Wizard welcome window.
3. Enter the connection name `HtoHD` and description as shown in Figure 581 on page 484.

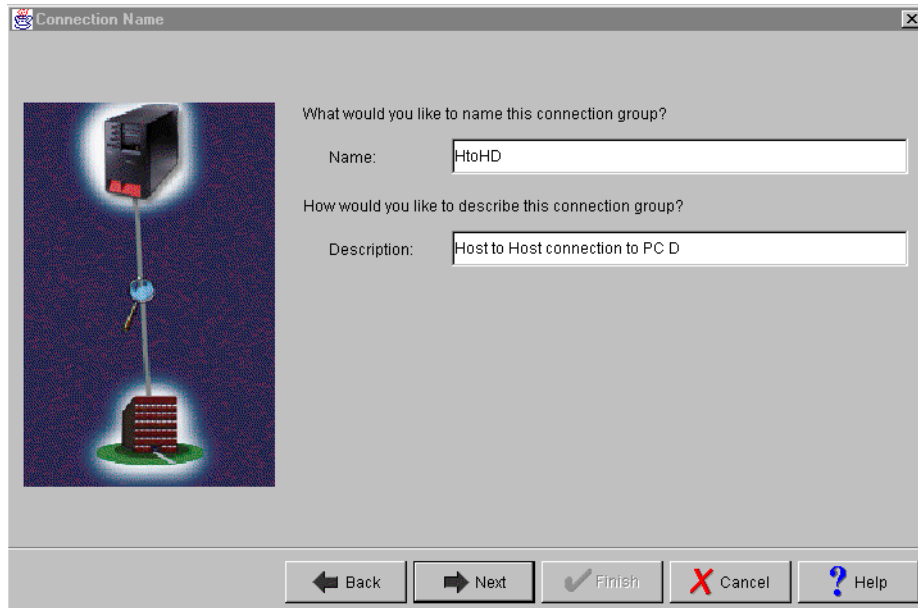


Figure 581. RALYAS4A to PC D - Connection Name

4. Click **Next**.
5. Select **Balanced security and performance** on the wizard Key Policy window (Figure 582).

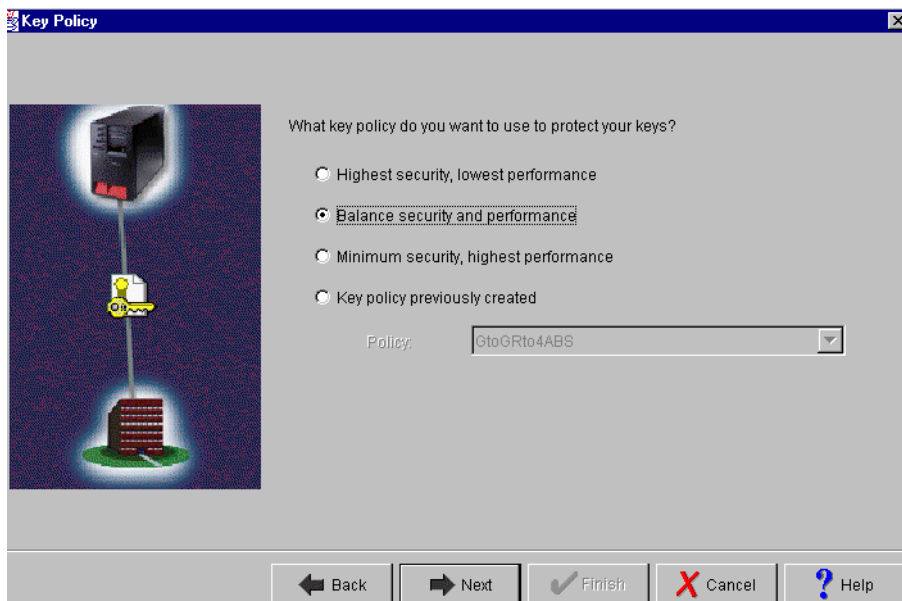


Figure 582. RALYAS4A to PC D - Key Policy

6. Click **Next**.
7. At the Local Identifier window, select **Version 4 IP address** for Identifier type and **172.16.3.23** as the local key server IP address, for this scenario. Note that the local IP address has to be already configured on the system. See Figure 583 on page 485.

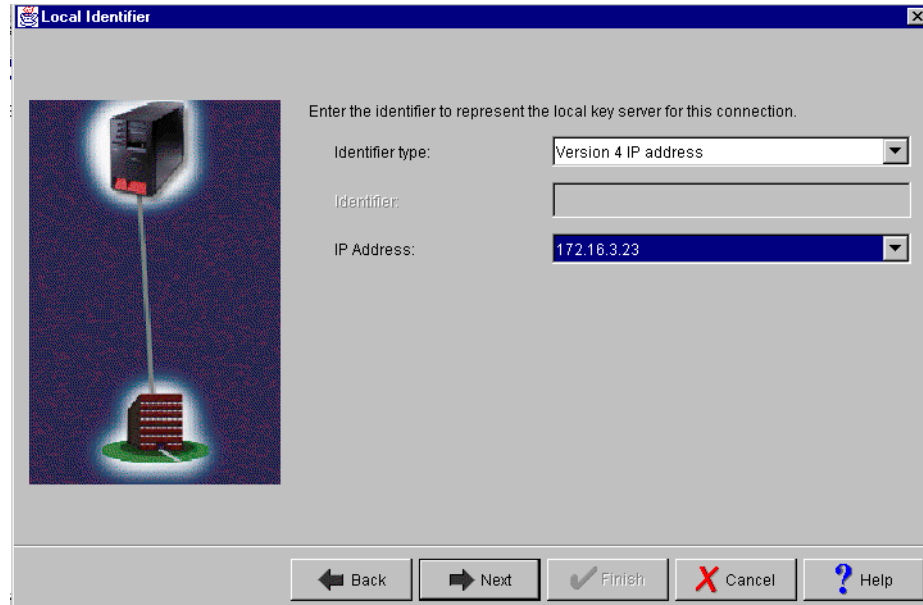


Figure 583. RALYAS4A to PC D - Local Identifier

8. Click **Next**. The Remote Hosts window is displayed.
9. Click **Add** to add the remote identifier for PC D.
10. Select **Version 4 IP address** as the identifier type. Enter the IP address of PC D as 172.16.3.77 and the Pre-Shared Key 12345678, as shown in Figure 584.

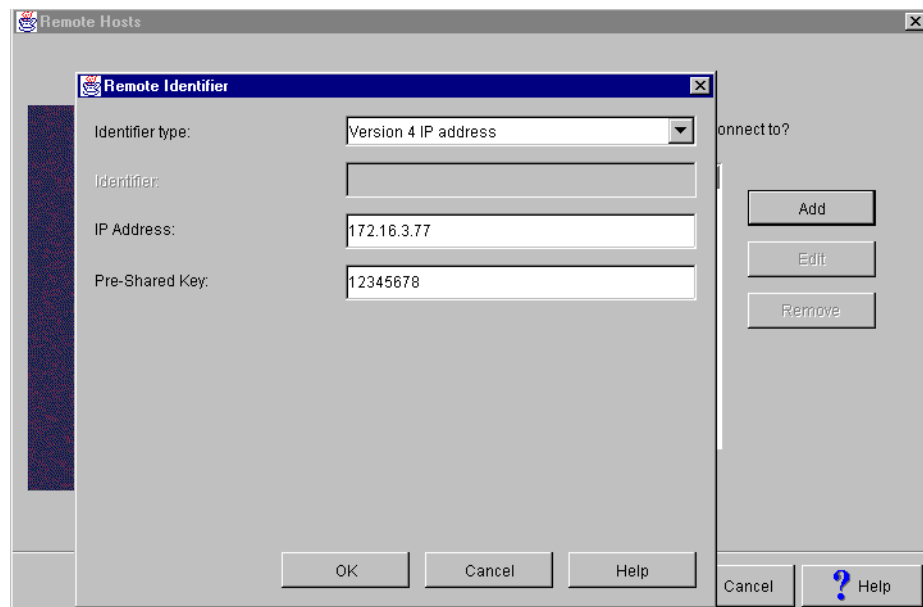


Figure 584. RALYAS4A to PC D - Remote Hosts

11. Click **OK**.
12. Click **Next**. The Data Policy window is displayed.

13. Select **Balanced security and performance** on the Data Policy window (Figure 585).

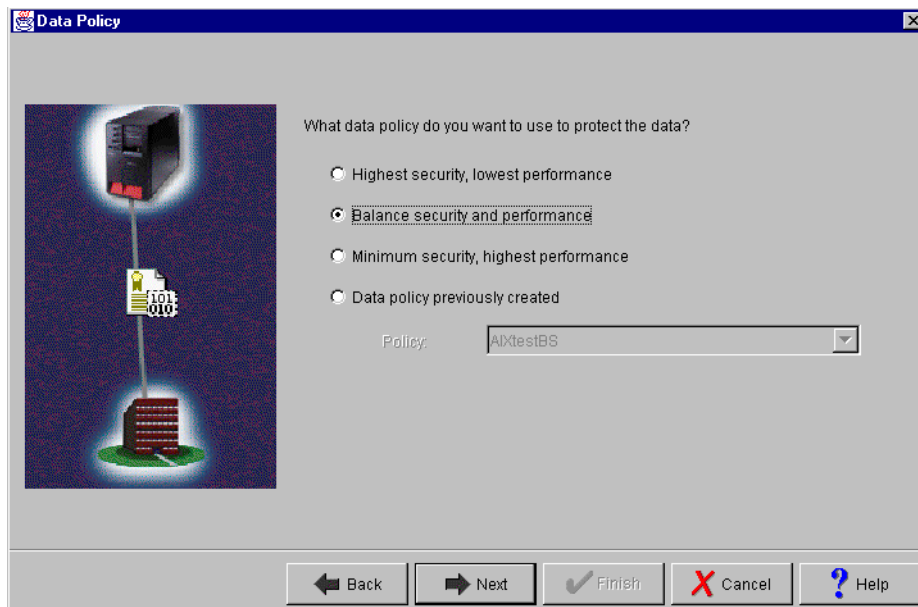


Figure 585. RALYAS4A to PC D - Data Policy

14. Click **Next**.

The summary page shows the configuration input and gives information about the objects created by the wizard (Figure 586).

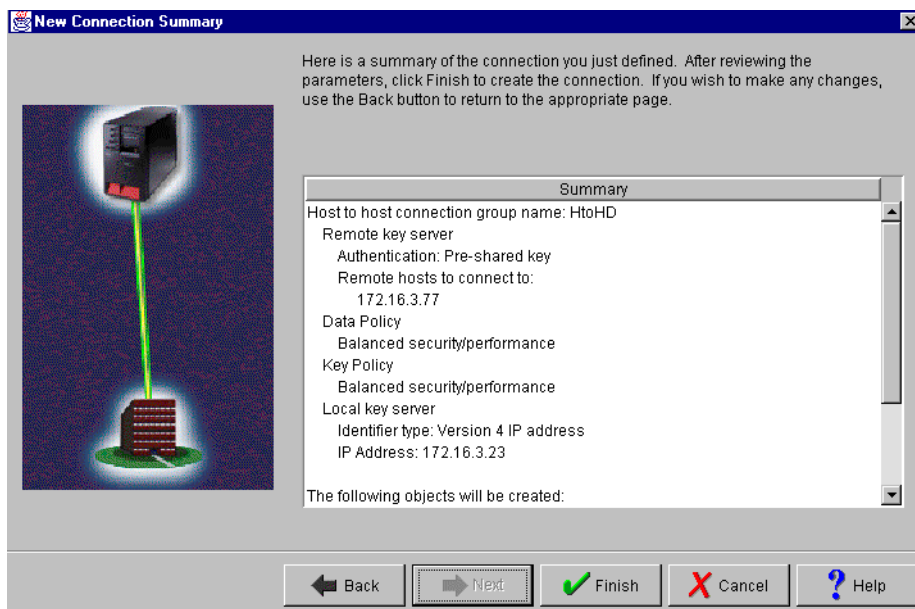


Figure 586. RALYAS4A to PC D - New Connection Summary

15. Click **Finish**. The wizard creates the new host-to-hosts connection.

16. From Virtual Private Networking, expand **IP Security Policies->Key Policies**.

17. Double-click the **HtoHDBS** key policy to open its properties.

18. Select Responder negotiation, **Allow identity protection**, to allow main mode negotiation (Figure 587).

Note

The IKE protocol allows you to choose between two modes for phase 1 authentication:

- The aggressive mode does not encrypt the identity of the client during phase 1 negotiations. For example, the IP address or e-mail address used as the identifier flows in the clear when you configure the aggressive mode.
- The main mode encrypts (protects) the identity of the client during phase 1 negotiations. This mode can only be used when the identifier type is an IP address.

The wizard allows you to configure a main or aggressive mode. In this step, you are using the VPN configuration GUI to allow identity protection. This option allows both aggressive mode and main mode negotiations.

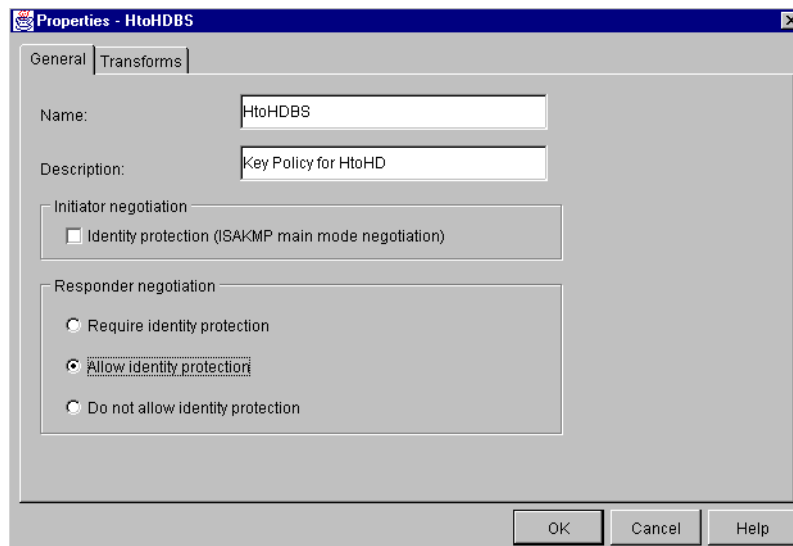


Figure 587. RALYAS4A to PC (D) key policy - General page

19. Click the **Transforms** tab.

20. Change Maximum Key Lifetime to 120 minutes, and save the key policy.

21. Open the properties of the data policy **HtoHDBS**.

22. Change the proposals key expiration time to 60 minutes. Save the data policy.

This completes the Host to Hosts VPN configuration for PC D on the AS/400 system RALYAS4A.

11.1.10 Configuring IP packet security on RALYAS4A

You must configure IP filters to complete the VPN configuration. To implement this scenario, the following filter rules are required:

- One filter interface associated with the filter rules. This is the physical LAN line ETHERNET.
- Two filter rules to allow IKE negotiations.
- Two IPSEC filter rules. One IPSEC filter rule is associated with the connection created in 11.1.9.1, “A Host to Dynamic IP Users connection for ThinkPad C” on page 474. The other IPSEC filter rule is associated with the connection created in 11.1.9.2, “A Host to Hosts connection for PC D” on page 483.

Note

The filter rules presented throughout this redbook are *limited* to those required to enable the services in the proposed scenario. If you want to enable other services beyond those in the scenario, you need to configure additional rules. Exercise extreme caution when doing so and always take security into account.

To configure the filters, perform the following steps:

1. Open IP Packet Security from the Operations Navigator.
2. Configure the Filter Interface rule which ties the filter rules to the required interface. The interface to which the filters apply is the physical LAN line description (ETHERNET). Right-click **Filter Interfaces**, and select **New Filter Interface**.
3. Select **Line name**, and select the appropriate LAN line description (**ETHERNET**).
4. Click **Add**, and enter `VPN` in the Set name field. All filter rules in the file with `VPN` as set name are associated with the interface ETHERNET. See Figure 588.

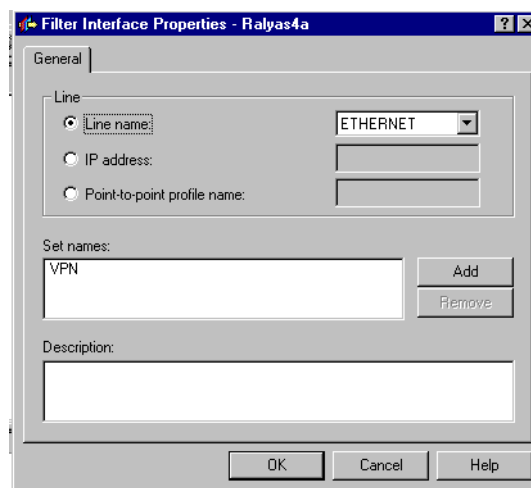


Figure 588. RALYAS4A IP packet security - Filter Interface Properties

5. Click **OK** to save the interface definition.
6. Add a filter rule for the inbound IKE negotiations. See Figure 589 on page 489. This filter rule accepts any inbound IP traffic on UDP port 500, destined for IP address 172.16.3.23 (the local key server). The source address is specified as a wildcard (*) value. This allows IKE negotiations with remote clients that are

assigned IP addresses dynamically by the DHCP server, as well as clients that have fixed IP addresses. The set name VPN binds the filter rule to the filter interface created above.

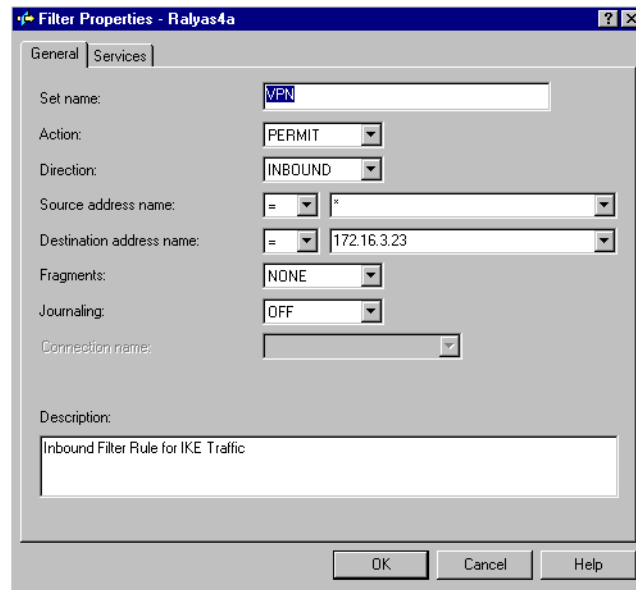


Figure 589. RALYAS4A IP packet security Inbound IKE filter rule - General page

7. Click the **Services** tab.
8. IKE negotiations use protocol UDP, with source and destination port 500. Enter the values as shown in Figure 590.

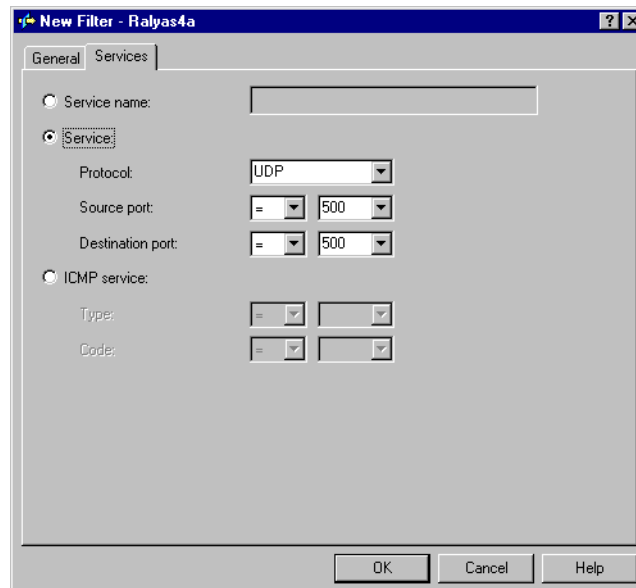


Figure 590. RALYAS4A IP packet security inbound IKE filter rule - Services page

9. Click **OK** to save the filter rule.
10. Repeat the previous four steps for the *outbound* IKE filter rule. Remember to reverse the Source and Destination address names. Complete the Services

window as you did for the inbound rule as shown in Figure 591 and Figure 592.

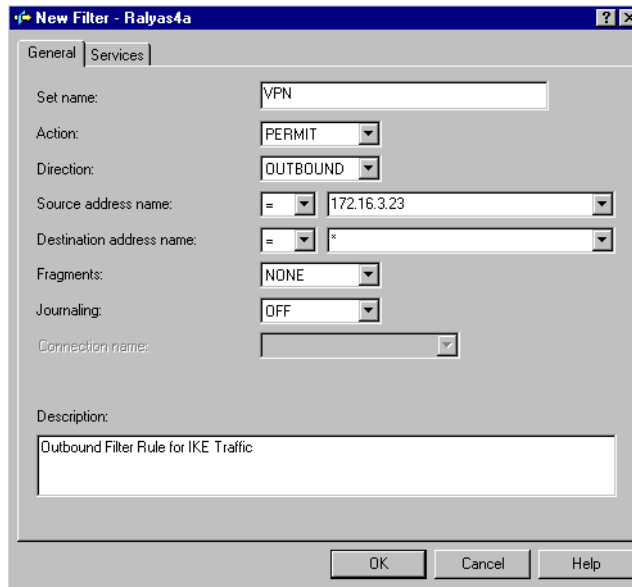


Figure 591. RALYAS4A IP packet security outbound IKE filter rule - General page

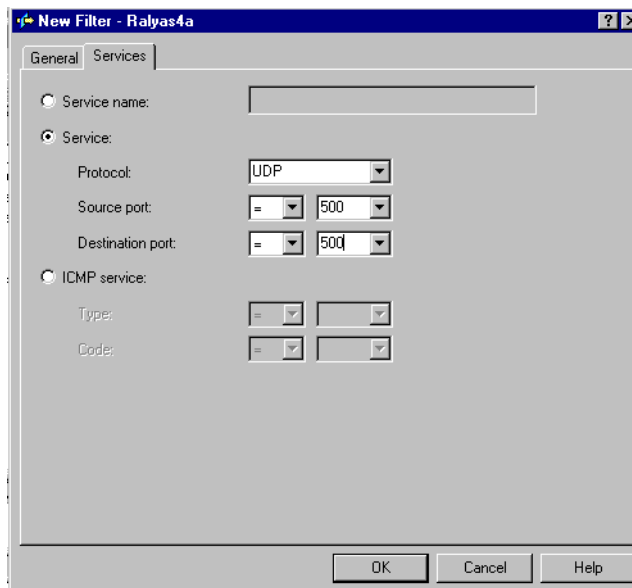


Figure 592. RALYAS4A IP packet security outbound IKE filter rule - Services page

11. Click **OK** to save the filter rule.

12. Add an IPSEC filter rule associated with the connection HtoHD created in 11.1.9.2, "A Host to Hosts connection for PC D" on page 483. Configure the IPSEC filter rule that allows data traffic to use the VPN tunnel. Refer to Figure 593 on page 491. Notice the following fields:

- Direction is always set to OUTBOUND for IPSEC filter rules.
- Source address name field is 172.16.3.23. This is the local IP address that represents the data endpoint of the VPN.

- Destination address name is 172.16.3.77. The remote client (PC D) has a fixed IP address.
- Connection name is HtoHD. This is the host-to-hosts connection previously configured.

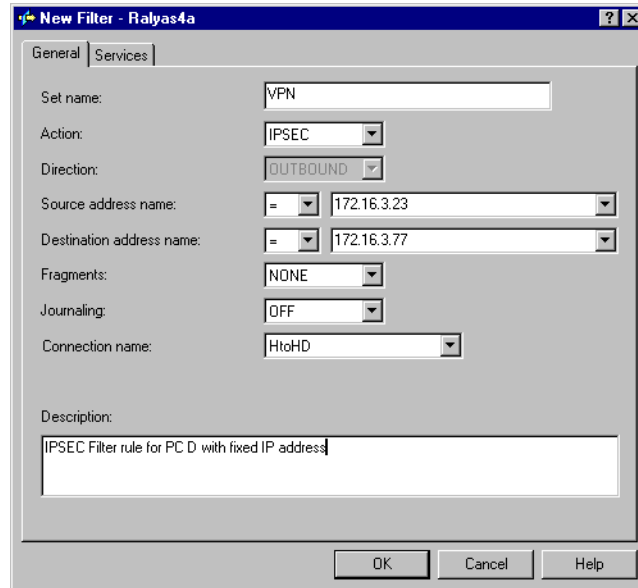


Figure 593. RALYAS4A IP packet security IPSEC filter for PC D - General page

13. Click the **Services** tab.

14. Select **Service**, and specify wildcard (*) for the Protocol, Source port, and Destination port fields (Figure 594).

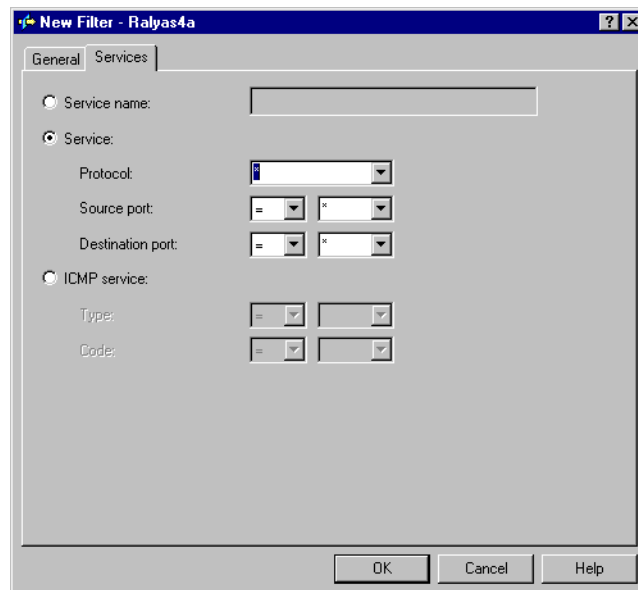


Figure 594. RALYAS4A IP packet security IPSEC filter for PC D - Services page

15. Click **OK** to save the filter rule.

16. Add an IPSEC filter rule associated with the connection created in 11.1.9.1, “A Host to Dynamic IP Users connection for ThinkPad C” on page 474. Configure the IPSEC filter rule that allows data traffic to use the VPN tunnel. Refer to Figure 595. Notice the following fields:

- Direction is always set to **OUTBOUND** for IPSEC filter rules.
- Source address name field is `172.16.3.23`. This is the local IP address that represents the data endpoint of the VPN.
- Destination address name is a wildcard (*). The remote clients have dynamically assigned IP addresses.
- Connection name is `DYNAMICIP`. A Host to Dynamic IP Users connection that matches the client identifier will be selected.

Tip

There can only be one IPSEC filter rule associated with a `DYNAMICIP` connection in the filter file.

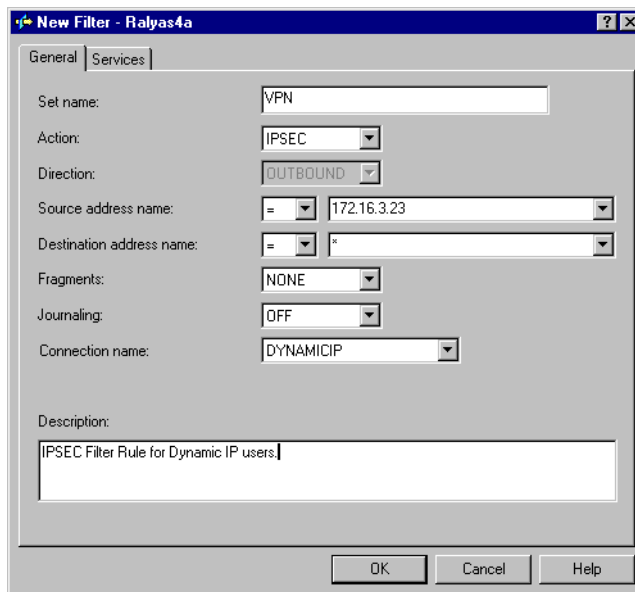


Figure 595. RALYAS4A IP packet security IPSEC filter for dynamic IP - General page

17. Click the **Services** tab.

18. Select **Service** fields, and specify wildcard (*) for the Protocol, Source port, and Destination port. See Figure 596 on page 493.

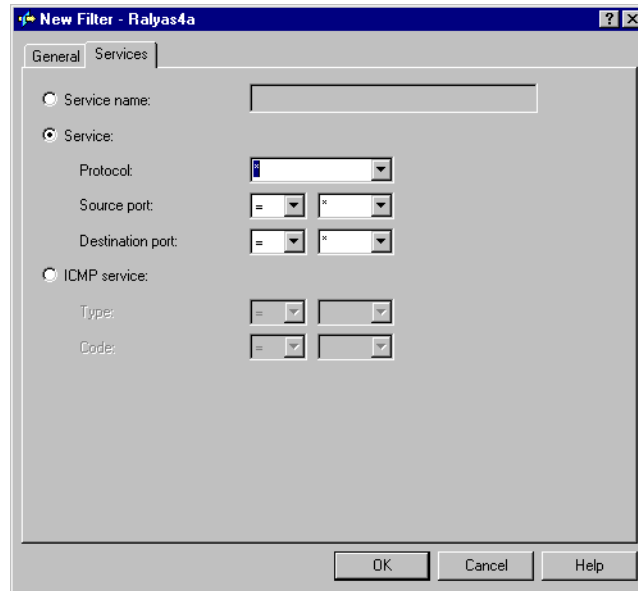


Figure 596. RALYAS4A IP packet security IPSEC filter for dynamic IP - Services page

19. Click **OK** to save the filter rule.

20. Display all the filter rules you just created. At the IP Packet Security window, click **All Security Rules**. All the filter rules as shown in Figure 597 are displayed.

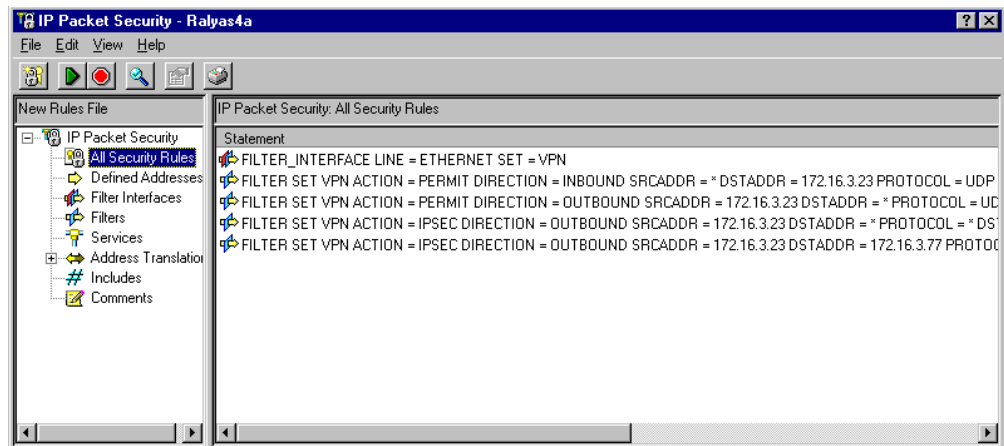


Figure 597. RALYAS4A IP Packet Security - All Security Rules

21. Save and verify the new filter file.

22. Activate IP packet security.

Figure 598 on page 494 shows all the filter rules used in this scenario.

```

IP Packet Security: All Security Rules
#Filters for RALYAS4A remote clients
#Filter interface: LAN
FILTER_INTERFACE LINE = EHERNET SET = VPN
#IKE filter rules
FILTER SET VPN ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = 172.16.3.23 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
FRAGMENTS = NONE JRN = OFF

FILTER SET VPN ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 172.16.3.23
DSTADDR = * PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC Filter rule
FILTER SET VPN ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 172.16.3.23
DSTADDR = 172.16.3.77 PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE
JRN = OFF CONNECTION_DEFINITION = HtoHD

FILTER SET VPN ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 172.16.3.23
DSTADDR = * PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = DYNAMICIP

```

Figure 598. RALYAS4A IP filters summary

This completes the configuration of the IP packet security in RALYAS4A.

11.1.11 Configuring the AS/400 system RALYAS4C

The VPN configurations on the AS/400 system RALYAS4C are almost the same as on system RALYAS4A. The major difference is the data-protection level. The data traffic to and from RALYAS4C is authenticated only. No encryption is used for user data. This section highlights only the configuration differences and, therefore, does not include every single step.

11.1.11.1 A Host to Dynamic IP Users connection for ThinkPad C

The VPN configuration for ThinkPad C is also a dynamic IP configuration on the AS/400 system RALYAS4C. Perform the following steps to configure the Host to Dynamic IP Users connection for ThinkPad C:

1. Start Virtual Private Networking from the Operations Navigator.
2. Select **File->New Connection->Host To Dynamic IP Users** to start the configuration wizard.
3. Follow the wizard windows, and enter the parameter values specified in Table 49 on page 473, column *Scenario answers for ThinkPad C*.

Based on the *Minimum security, highest performance* option specified for the data policy, the wizard selects AH as the IPSec protocol. Note that from a certain point in the IKE negotiation, the messages are *always* encrypted, even if you select *Minimum security, highest performance*.

When all configuration parameters are entered, the New Connection Summary window is displayed, as shown in Figure 599 on page 495.

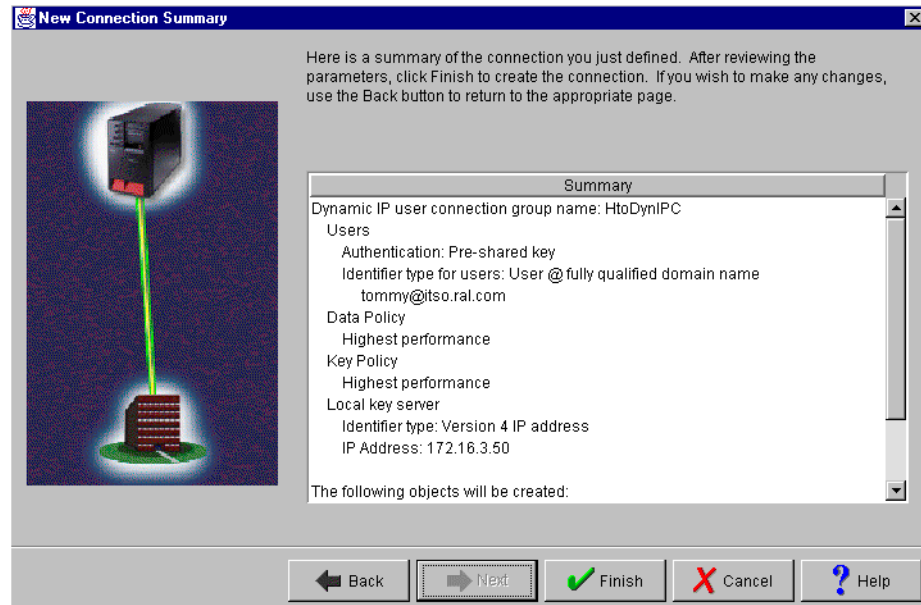


Figure 599. RALYAS4C Configuration wizard - Host to Dynamic IP Users configuration summary

4. Click **Finish** to create the connection configuration.
5. Change the key lifetime in the HtoDynIPCHP key policy to 120 minutes.
6. Change the key expiration time to 60 minutes in the data policy HtoDynIPCHP. Ensure that the encapsulation mode in the proposal is set to **Transport**.
7. On the Policy page of the dynamic IP group HtoDynIPC, set the parameter for local port, remote address, remote port, and protocol to **Connection**. The parameter for local address remains **Filter rule**.

This completes the Host to Dynamic IP Users VPN configuration in RALYAS4C for ThinkPad C.

11.1.11.2 A Host to Hosts connection for PC D

The VPN configuration for PC D is also a Host to Hosts configuration on the AS/400 system RALYAS4C. Perform the following steps to configure the Host to Hosts connection for PC D:

1. Start Virtual Private Networking from the Operations Navigator.
2. Select **File->New Connection->Host To Hosts** to start the configuration wizard.
3. Follow the wizard windows and enter the parameter values specified in Table 49 on page 473, column *Scenario answers for PC D*.

Based on the *Minimum security, highest performance* option specified for the data policy, the wizard selects AH as the IPSec protocol. Note that from a certain point in the IKE negotiation, the messages are *always* encrypted, even if you select *Minimum security, highest performance*.

When all configuration parameters are entered, the New Connection Summary window is displayed, as shown in Figure 600 on page 496.

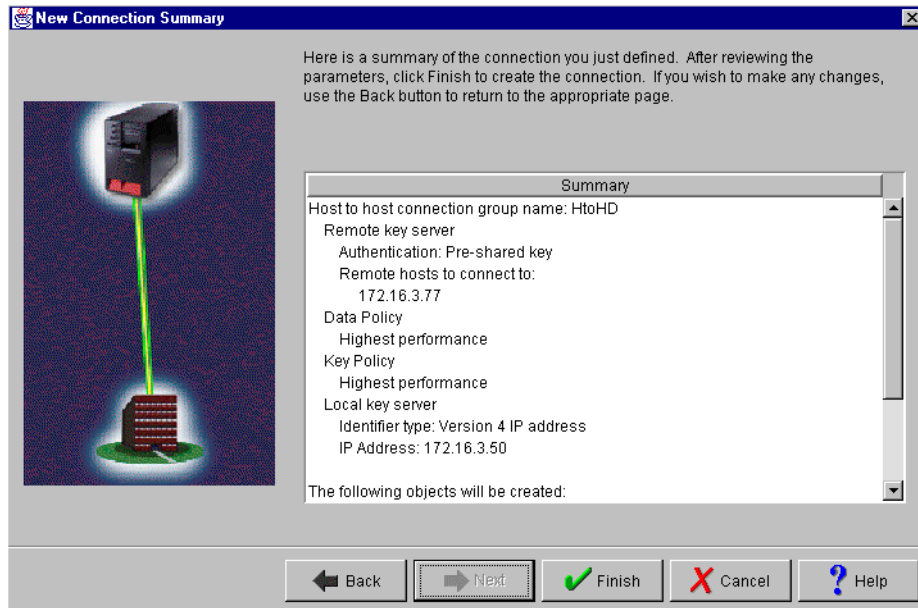


Figure 600. RALYAS4C Configuration wizard - Host to Hosts configuration summary

4. Click **Finish** to create the connection configuration.
5. Allow identity protection in the key policy HtoHDHP.
6. Change the key lifetime to 120 minutes.
7. Change the key expiration time to 60 minutes in the data policy HtoHDHP.
8. Ensure that the encapsulation mode in the proposal is set to **Transport**.

This completes the VPN configuration for PC D.

11.1.12 Configuring IP packet security on RALYAS4C

You must configure IP filters to complete the VPN configuration. To implement this scenario, the following filter rules are required:

- One filter interface associated with the filter rules. This is the physical LAN line ETHERNET.
- Two filter rules to allow IKE negotiations.
- Two IPSEC filter rules. One IPSEC filter rule is associated with the connection created in 11.1.11.1, “A Host to Dynamic IP Users connection for ThinkPad C” on page 494. The other IPSEC filter rule is associated with the connection created in 11.1.11.2, “A Host to Hosts connection for PC D” on page 495.

Note

IP packet filtering is essential to VPN connections. You should configure the filter rules to only allow IP addresses and services that you want to explicitly permit.

The filter rules included in this chapter only support the connections for this scenario. In a typical customer environment, you may need to add more filter rules or defined addresses to permit connections to a group of clients.

To configure IP packet security in RALYAS4C, follow the steps described in 11.1.10, “Configuring IP packet security on RALYAS4A” on page 487. Use the parameters in Table 50.

Table 50. RALYAS4C - IP packet security configuration summary

Rule	Parameter description	Parameter value
Interface rule	Line name	ETHERNET
	Set name	VPN
IKE Inbound	Set name	VPN
	Action	PERMIT
	Direction	INBOUND
	Source address name	*
	Destination address name	172.16.3.50
	Description	Inbound IKE filter rule
	Service	
	– Protocol	UDP
	– Source port	500
	– Destination port	500
IKE Outbound	Set name	VPN
	Action	PERMIT
	Direction	OUTBOUND
	Source address name	172.16.3.50
	Destination address name	*
	Description	Outbound IKE filter rule
	Service	
	– Protocol	UDP
	– Source port	500
	– Destination port	500
IPSEC PC D	Set name	VPN

Rule	Parameter description	Parameter value
	Action	IPSEC
	Direction	OUTBOUND
	Source address name	172.16.3.50
	Destination address name	172.16.3.77
	Connection name	HtoHD
	Description	IPSEC filter rule for PC D
	Service	
	– Protocol	*
	– Source port	*
	– Destination port	*
IPSEC ThinkPad	Set name	VPN
	Action	IPSEC
	Direction	OUTBOUND
	Source address name	172.16.3.50
	Destination address name	*
	Connection name	DYNAMICIP
	Description	IPSEC filter rule for dynamic IP users
	Service	
	– Protocol	*
	– Source port	*
	– Destination port	*

Figure 601 on page 499 shows all the filter rules used in this scenario.

```

IP Packet Security: All Security Rules
#Filters for RALYAS4A remote clients
#Filter interface: LAN
FILTER_INTERFACE LINE = EHERNET SET = VPN
#IKE filter rules
FILTER SET VPN ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = 172.16.3.50 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
FRAGMENTS = NONE JRN = OFF

FILTER SET VPN ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 172.16.3.50
DSTADDR = * PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC Filter rule
FILTER SET VPN ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 172.16.3.50
DSTADDR = 172.16.3.77 PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE
JRN = OFF CONNECTION_DEFINITION = HtoHD

FILTER SET VPN ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 172.16.3.50
DSTADDR = * PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = DYNAMICIP

```

Figure 601. RALYAS4C IP filters summary

This completes the IP packet filter configuration on RALYAS4C.

11.1.13 Installing IRE SafeNet Soft-PK client: ThinkPad C

In Chapter 10, “Secure remote access for PC clients over the Internet” on page 419, we used the IRE SafeNet Soft-PK client on a dial-up PPP connection. Refer to 10.1.11, “Installing the IRE SafeNet Soft-PK” on page 438, for more information about SafeNet Soft-PK. This client supports IPsec connections over PPP as well as LAN, both Ethernet and Token Ring. The configuration shown in this chapter is based on an Ethernet LAN connection using the SafeNet Soft-PK Version 2.0.4 (Build 6) client software. The DHCP server dynamically assigns an IP address to this client.

11.1.13.1 Client characteristics

The PC client used in this scenario has the following hardware and software characteristics:

- **Hardware**
 - IBM Thinkpad 760XD
 - 80 MB memory
 - Ethernet 10/100 Mbps PCMCIA adapter
- **Software**
 - Microsoft Windows 95 (4.0.0 950 B)
 - IRE SafeNet Soft-PK version 2.0.4 (build 6). This client supports IPsec only.

11.1.14 Configuring the IRE SafeNet Soft-PK client on ThinkPad C

In this section, you configure two VPN connections on ThinkPad C using IRE SafeNet Soft-PK client. The first connection is to the AS/400 system RALYAS4A. The second connection is to the AS/400 system RALYAS4C.

11.1.14.1 Configuring the VPN connection to RALYAS4A

Once you install the SafeNet Soft-PK software on the PC, a new icon comes up on the Windows task bar.

To start the configuration of the SafeNet Soft-PK VPN client, you can choose one of the following two paths:

- Click the Windows 95 **Start** button, and select **Programs->SafeNet Soft-PK->Security Policy Editor**.
- Right-click the **SafeNet** icon on the Windows task bar.

This chapter documents the second method to start the configuration. Perform the following steps to configure the SafeNet Soft-PK client:

1. Right-click the **SafeNet** icon on the Windows task bar. The SafeNet menu appears as shown in Figure 602.

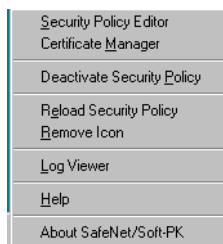


Figure 602. SafeNet Soft-PK menu on the Windows task bar

2. Select **Security Policy Editor**.

This menu option opens the Security Policy Editor as shown in Figure 603. All VPN connections are configured through this editor. By default, all configurations are enabled. If the security policy is deactivated, the configurations are disabled. To activate them again, select **Activate Security Policy** from the SafeNet Soft-PK client task menu.

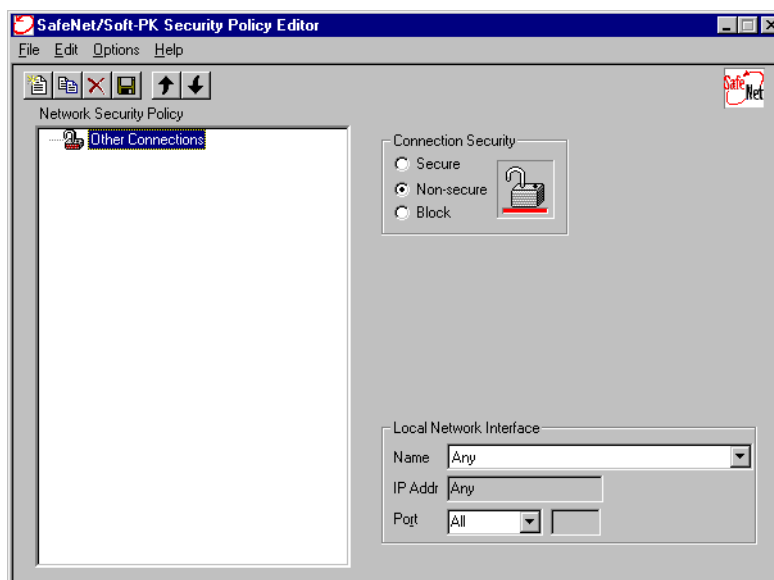


Figure 603. RALYAS4A SafeNet Soft-PK Security Policy Editor

3. Click **File->New Connection** to create the first secured connection (Figure 604). This is the client end of the VPN. The corresponding AS/400 VPN configuration was created in 11.1.9.1, “A Host to Dynamic IP Users connection for ThinkPad C” on page 474. Refer to Table 46 on page 470 for the client’s configuration parameters.

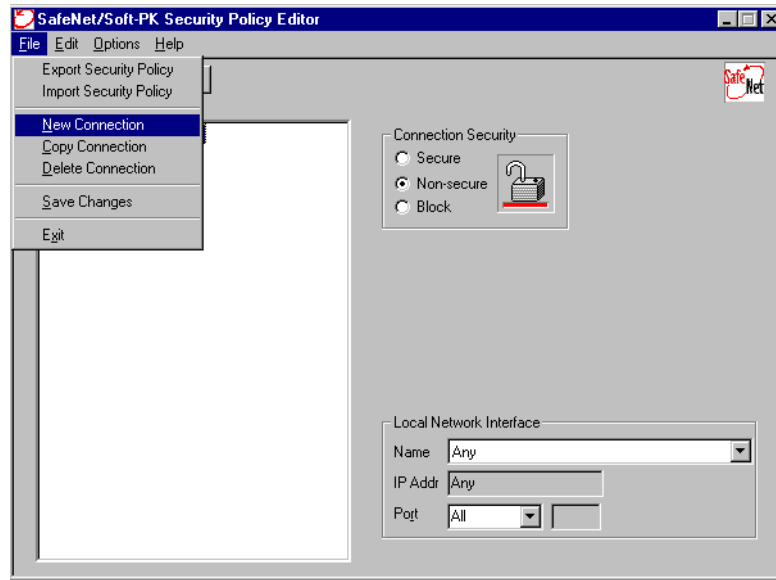


Figure 604. SafeNet Soft-PK to RALYAS4A Security Policy Editor - New Connection

The Local Network Interface defines the physical interfaces to which this connection is bound. We specified `Any` in this scenario because the PC has only the Ethernet interface installed.

4. Enter the connection name `RALYAS4A`, and press **Enter**. The window shown in Figure 605 is displayed.

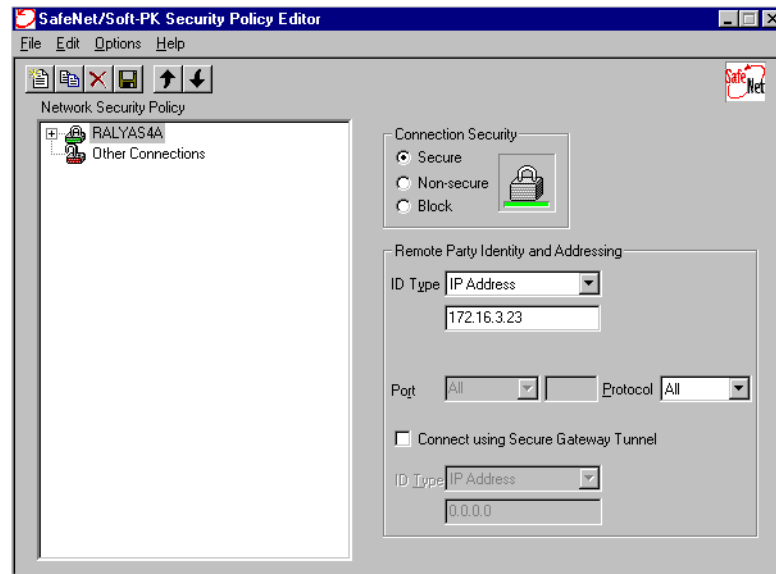


Figure 605. SafeNet Soft-PK to RALYAS4A Security Policy Editor - Connection information

The initial configuration window defines the following connection properties:

- **Connection Security:** This parameter defines the security options for the traffic between the local client and the remote party. The following three options are available:
 - **Secure:** The traffic is secured by the IPSec protocol. Unless the client is connected through a gateway, each destination requires a separate connection definition. Select **Secure** for this scenario.
 - **Non-secure:** The traffic flows in the clear, with no encryption protection.
 - **Block:** The traffic to the remote party is blocked.

If you configure multiple connections, the order is important. For example, assume you want to secure the traffic to one specific host while allowing non-secure traffic to other hosts in the network. Configure the secure connection to the specific host IP address before the non-secure connection to an IP address range that also includes the single host IP address.

- **Remote party identity and addressing:** Specifies the remote destination. In this scenario, it is the IP address of the AS/400 system RALYAS4A (172.16.3.23). This is a host-to-host connection. Therefore, you cannot specify an IP subnet or an address range.
5. Click the + symbol next to the RALYAS4A connection to expand the connection definition.
 6. Click **Security Policy**, and select **Aggressive Mode** (Figure 606).

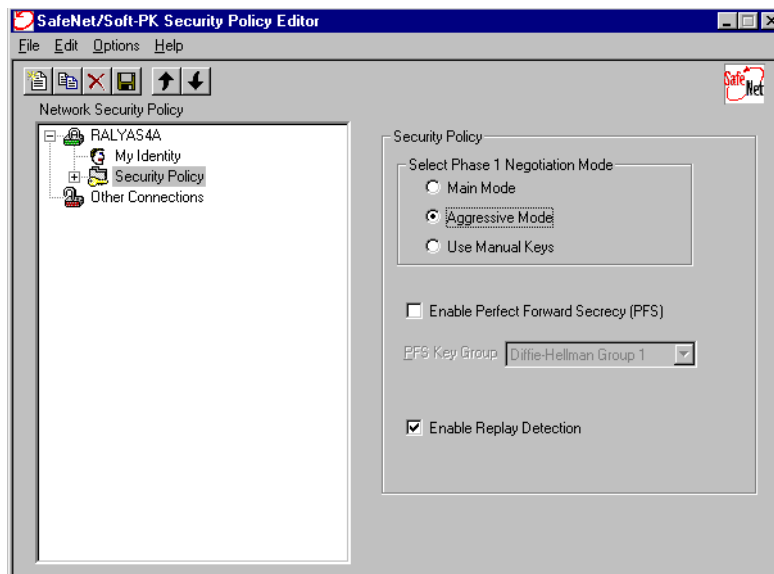


Figure 606. SafeNet Soft-PK to RALYAS4A Security Policy Editor - Security Policy window

Note

By default, the SafeNet Soft-PK client sets IKE main mode for a new connection. Since ThinkPad C is dynamically assigned an IP address, the identifier type used is e-mail address. You must change to aggressive mode.

7. Click **My Identity** under the RALYAS4A connection (Figure 607).

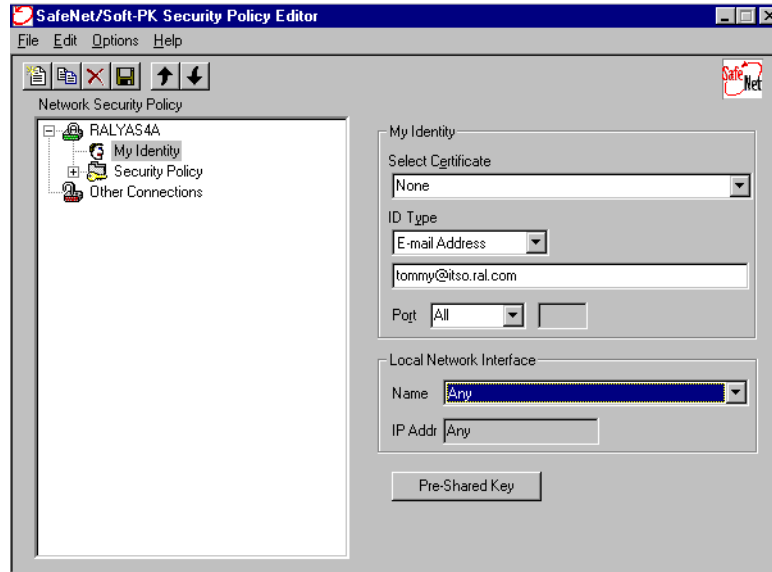


Figure 607. SafeNet Soft-PK to RALYAS4A Security Policy Editor - My Identity window

8. My Identity page provides information to identify the client. Refer to Table 46 on page 470 for information about configuration values for this scenario.

- **Select Certificate:** The AS/400 system currently does not support certificates for IKE authentication. Therefore, the Select Certificate parameter is set to **None**.
- **ID Type:** Select **E-mail Address** as the identifier type for the PC. Enter the e-mail address `tommy@itso.ral.com`
- **Local Network Interface:** Accept the default value **Any**.

9. Click **Pre-Shared Key**. The Pre-Shared Key pop-up window is displayed as shown in Figure 608.

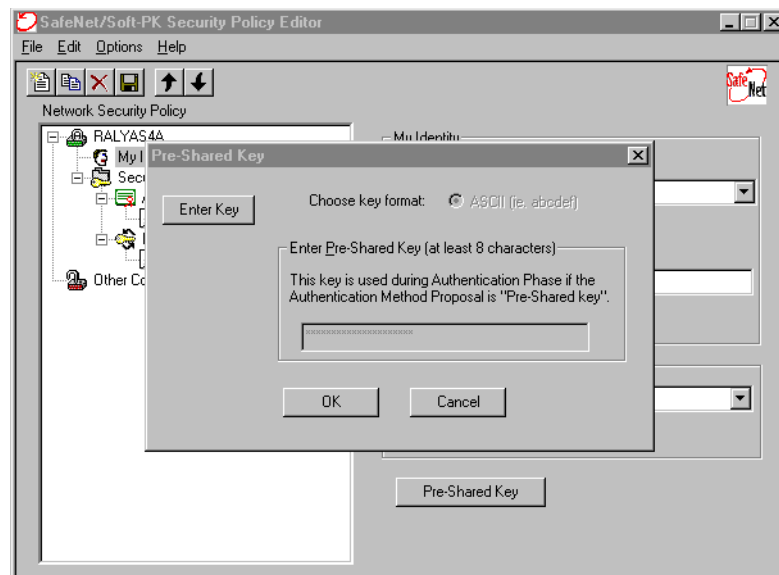


Figure 608. Security Policy Editor RALYAS4A - My Identity page clicked on Pre-Shared Key

10. Click **Enter Key**, and enter the pre-shared key `thomaswashere` as shown in Figure 609.

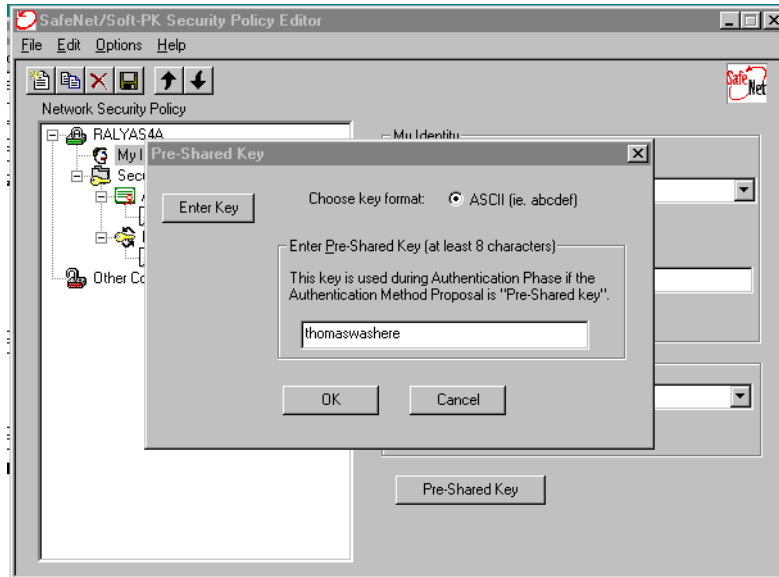


Figure 609. SafeNet Soft-PK to RALYAS4A Security Policy Editor - Pre-Shared Key

The pre-shared key is entered in ASCII format. Note that some products require the key to be entered in hex format. The SafeNet Soft-PK client requires a key length of at least eight characters. The pre-shared key is always associated with the local identifier, which, in this case, is the e-mail address. It must match the pre-shared key entered in the AS/400 VPN configuration.

11. Click **OK** to save the pre-shared key, and return to the My Identity page.
12. Expand **Security Policy->Authentication**, and click on **Proposal 1** (Figure 610).

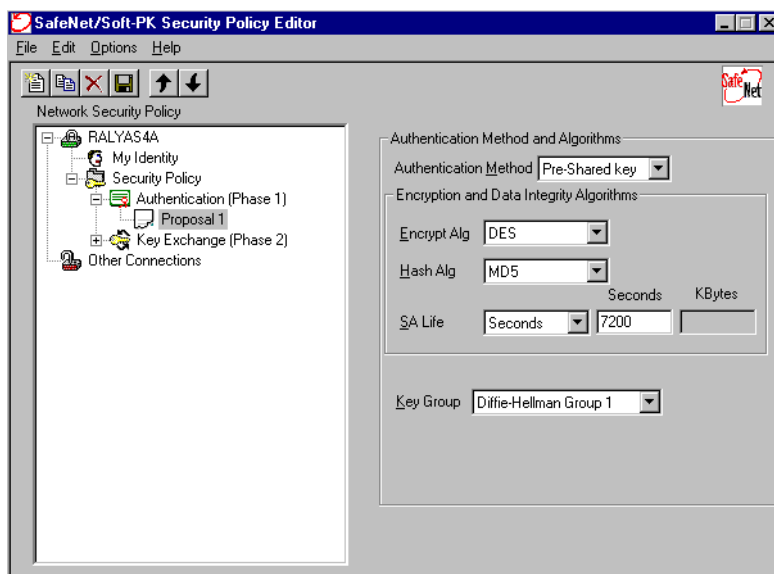


Figure 610. SafeNet Soft-PK to RALYAS4A Security Policy Editor - Phase 1 proposal

The proposal for IKE phase 1 is automatically created when adding a secure connection. In this scenario, you have to define the security association lifetime (SA Life). To do this, select **Seconds** from the pull-down menu. Specify 7200 for Seconds. Verify that the default parameters match the AS/400 system VPN configuration created in 11.1.9.1, “A Host to Dynamic IP Users connection for ThinkPad C” on page 474.

13. Expand **Key Exchange (Phase 2)**, and click on **Proposal 1** (Figure 611).

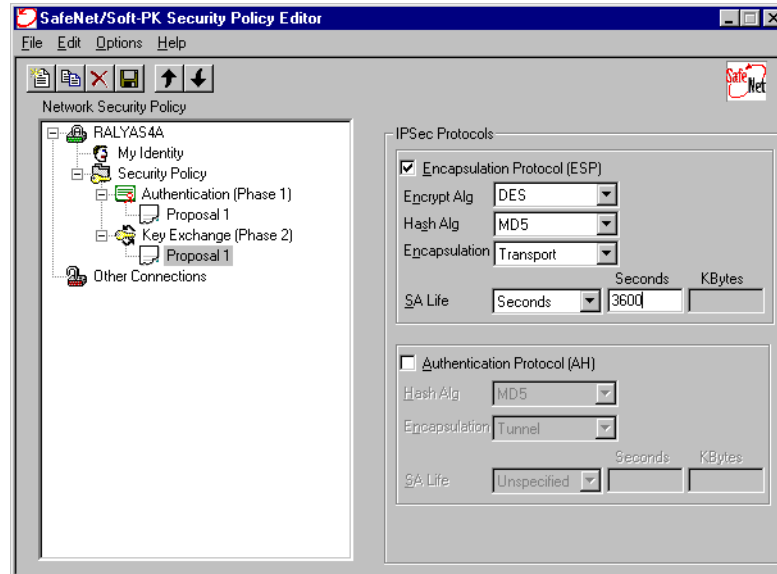


Figure 611. SafeNet Soft-PK to RALYAS4A Security Policy Editor - Phase 2 proposal

The phase 2 proposal has to match a proposal in the AS/400 system data policy. For this scenario, select **ESP** for the IPSec protocol. Configure the parameter as shown in Figure 611.

This completes the VPN connection configuration on ThinkPad C for the AS/400 system RALYAS4A.

11.1.14.2 Configuring the VPN connection to RALYAS4C

To continue with the configuration of the connection to the AS/400 system RALYAS4C, perform the following steps:

1. Click **File->New Connection**. The Security Policy Editor window, as shown in Figure 612 on page 506, is displayed. This is the client end of the VPN configured in 11.1.11.1, “A Host to Dynamic IP Users connection for ThinkPad C” on page 494.

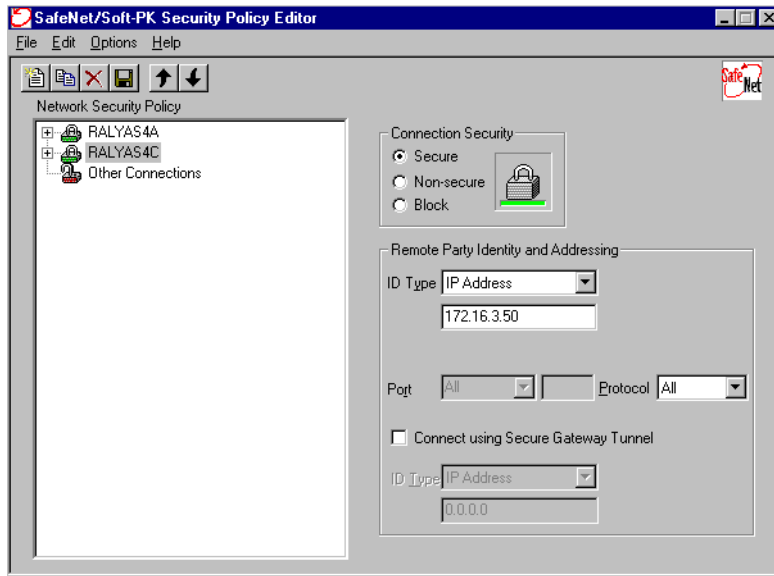


Figure 612. SafeNet Soft-PK to RALYAS4C Security Policy Editor - Connection

The connection RALYAS4C authenticates data traffic to the AS/400 system RALYAS4C. Enter the IP address of the remote key server as 172.16.3.50.

2. Click the + symbol next to the RALYAS4C connection to expand the connection definition.
3. Click **Security Policy**, and select **Aggressive Mode** (Figure 613).

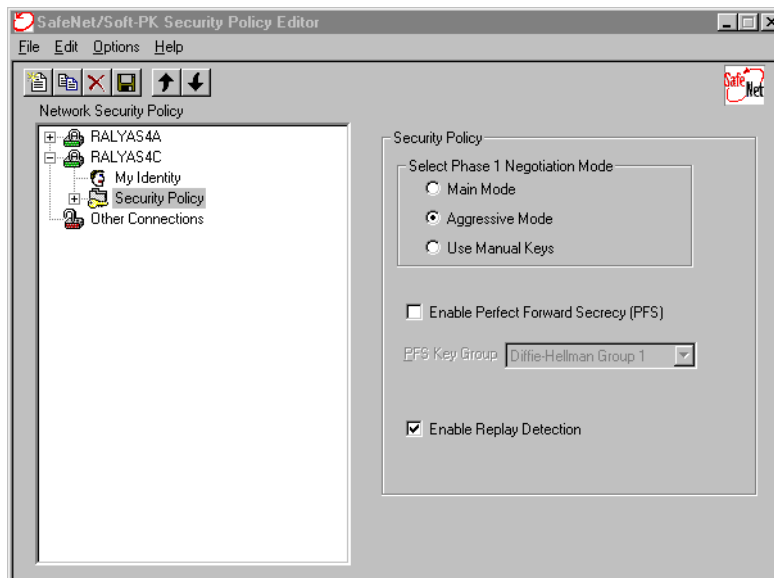


Figure 613. SafeNet Soft-PK to RALYAS4C Security Policy Editor - Security Policy page

4. Click **My Identity** in the RALYAS4C connection, and configure the parameter values as shown in Figure 614 on page 507.

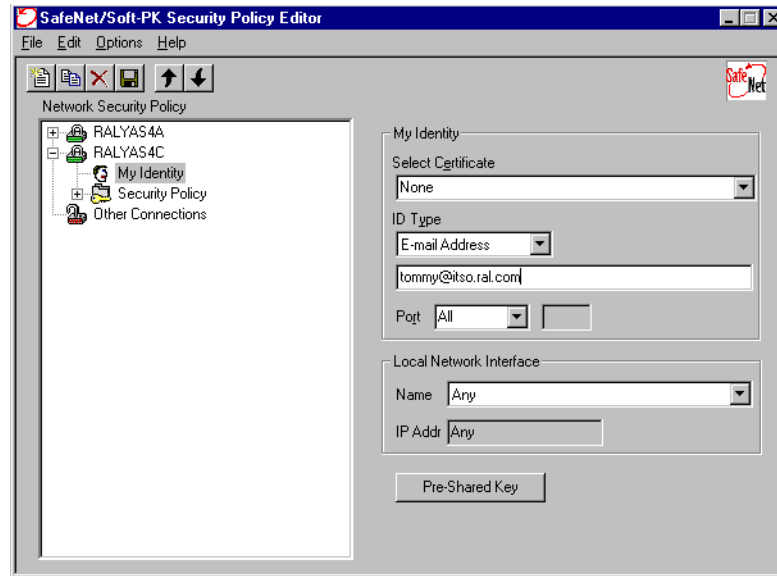


Figure 614. SafeNet Soft-PK to RALYAS4C Security Policy Editor - My Identity page

5. Click **Pre-Shared Key**.
6. Enter the pre-shared key `unbelievable` as shown in Figure 615.

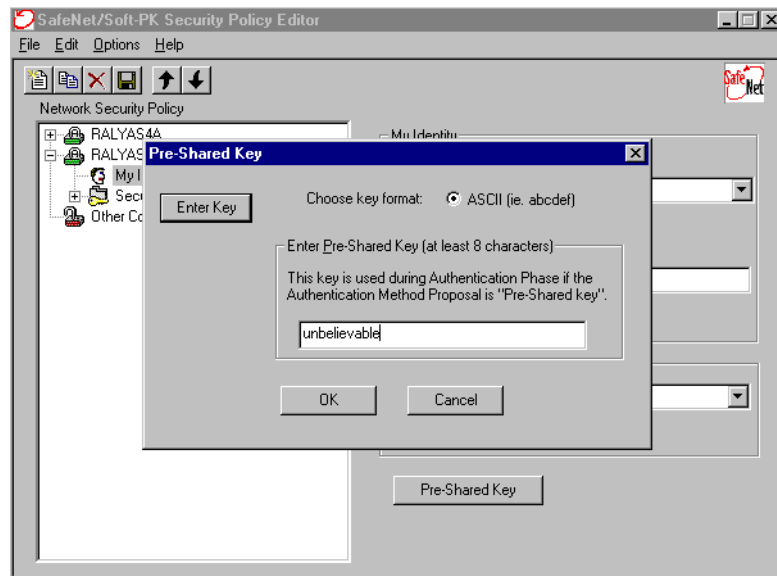


Figure 615. SafeNet Soft-PK to RALYAS4C Security Policy Editor - Pre-Shared Key

Each connection key configured in the client may have different local identifiers associated with a unique pre-shared key.

7. Click **OK**.
8. Select **Proposal 1** for phase 1, and configure the parameters as shown in Figure 616 on page 508.

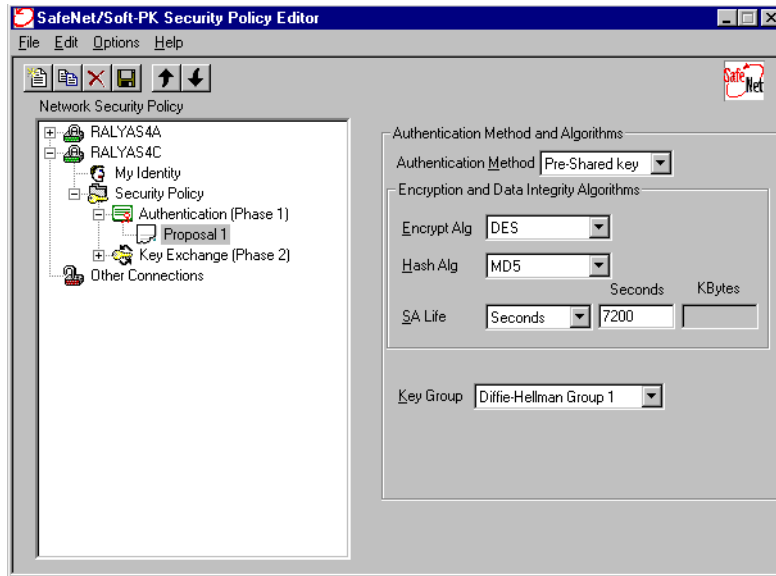


Figure 616. SafeNet Soft-PK to RALYAS4C Policy - Phase 1 proposal

9. Expand **Key exchange (Phase 2)**, and select **Proposal 1**.

10. Configure the IPSec Protocols parameters as shown in Figure 617.

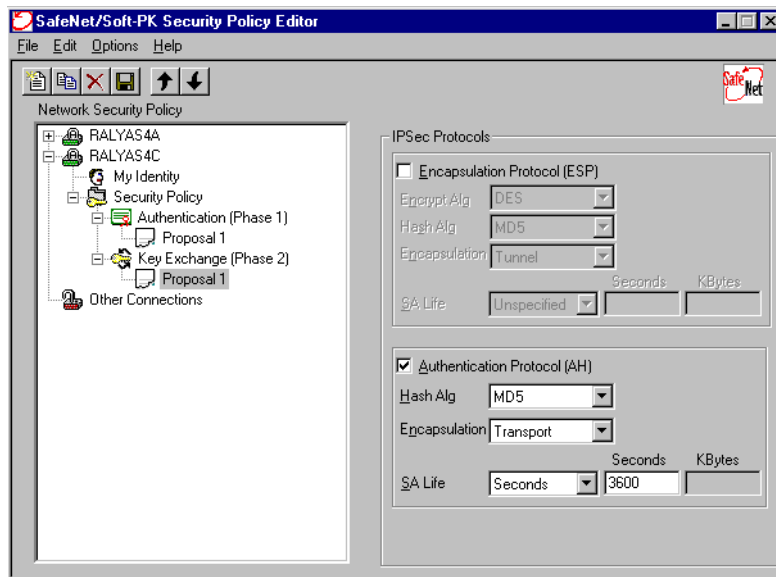


Figure 617. SafeNet Soft-PK to RALYAS4C Security Policy Editor - Phase 2 proposal

For the connection to RALYAS4C, select **Authentication Header (AH)** for the IPSec protocol. The traffic between ThinkPad C and the AS/400 system RALYAS4C is then authenticated but not encrypted. Since it is a host-to-host connection, the encapsulation is **Transport**.

11. Select **File->Save Changes**, or click the save icon (diskette symbol) to save the configuration.

This completes the configuration of the SafeNet Soft-PK client on ThinkPad C to the AS/400 system RALYAS4C.

11.1.15 AS/400 and SafeNet Soft-PK VPN configuration cross-reference

Table 51 provides a cross reference between the AS/400 system RALYAS4A VPN configuration and ThinkPad C with SafeNet Soft-PK VPN configuration parameters.

Table 51. RALYAS4A to ThinkPad C SafeNet Soft-PK VPN configuration cross-reference table

<u>AS/400</u>	<u>SafeNet Soft-PK Client</u>
Key Policy	Connection properties
Name = HtoDynIPCBS (20)	Connection Security= Secure
Initiator Negotiation = Aggressive Mode (Main mode not selected) (1)	Remote Part Identity and Addressing
Responder Negotiation = Do not allow identity protection (2)	ID Type= IP Address (18)
Key Protection Transforms	172.16.3.23 (19)
Authentication Method = Pre-shared key (3)	My Identity
Pre-shared key value = thomaswashere (4)	My Identity
Hash Algorithm = MD5 (5)	Select Certificate= None
Encryption Algorithm = DES-CBC (6)	ID Type= E-mail Address (16)
Diffie-Hellman Group = Default 768-bit MODP (7)	tommy@itso.ral.com (17)
Key Management	Local Network Interface
Maximum key lifetime (minutes) = 120 (8)	Name=Any
Maximum size limit (kilobytes) =	Pre-Shared Key= thomaswashere (4)
Data Policy	Security Policy
Name = HtoDynIPCBS (22)	Phase 1 negotiation mode= Aggressive Mode (1) (2)
Use Diffie-Hellman Perfect Forward Secrecy = No (9)	Perfect Forward Secrecy= Disabled (9)
Diffie-Hellman Group = Not Applicable	Replay Protection = Enabled
Data Protection Proposals	Authentication (Phase 1) - Proposal 1
Encapsulation mode = Transport (10)	Authentication Method= Pre-Shared key
Protocol = ESP (11)	Encryption and Data Integrity Algorithms (3)
Algorithms	Encrypt Alg.= DES (6)
Authentication Algorithm = HMAC-MD5 (12)	Hash Alg.= MD5 (5)
Encryption Algorithm = DES-CBC (13)	SA Life= Seconds 7200 (8)
Key Expiration	Key Group= Diffie-Hellman Group 1 (7)
Expire after (minutes) = 60 (14)	
Expire at size limit (kilobytes) = (15)	Key Exchange (Phase 2) - Proposal 1
Key Connection Group	ESP (11)
Name = HtoDynIPCB	Encrypt Alg.= DES (13)
Remote Server Identifier	Hash Alg.= MD5 (12)
Identifier Type = User@fully qualified domain name (16)	Encapsulation= Transport (10)
Identifier = tommy@itso.ral.com (17)	SA Life= Seconds 3600 (14)(15)
Local Key Server	AH
Identifier Type = Version 4 IP address (18)	Hash Alg.=
IP address = 172.16.3.23 (19)	Encapsulation=
Key Policy = HtoDynIPCBS (20)	
Dynamic IP Group	
Name = HtoDynIPCB	
System Role = Both systems are hosts	
Policy	
Data Management Security Policy = HtoDynIPCBS (21)	
Local addresses = Filter rule	
Local ports = Connection	
Remote addresses = Connection	
Remote ports = Connection	
Protocol = Connection	
IP Filters	
IKE Inbound rule	
Direction= INBOUND	
Source address name = *	
Destination address name= 172.16.3.23 (19)	
Protocol = UDP	
Source port =500	
Destination port =500	
IKE Outbound rule	
Direction= OUTBOUND	
Source address name = 172.16.3.23 (19)	
Destination address name= *	
Protocol = UDP	
Source port =500	
Destination port = 500	
IPSEC rule	
Source address name = 172.16.3.23 (19)	
Destination address name = *	
Connection Name = DYNAMICIP	
Protocol = *	
Source port = *	
Destination port = *	

Table 52 provides a cross reference between the AS/400 system RALYAS4A VPN configuration and ThinkPad C with SafeNet Soft-PK VPN configuration parameters.

Table 52. RALYAS4C to ThinkPad C SafeNet Soft-PK VPN configuration cross-reference table

<u>AS/400</u>	<u>SafeNet Soft-PK Client</u>
Key Policy	Connection properties
Name = HtoDnIPCHP (20)	Connection Security=Secure
Initiator Negotiation = Aggressive Mode (Main mode not selected) (1)	Remote Part Identity and Addressing (18)
Responder Negotiation = Do not allow identity protection (2)	ID Type= IP Address (19)
Key Protection Transforms	172.16.3.50
Authentication Method = Pre-shared key (3)	My Identity
Pre-shared key value = unbelievable (4)	My Identity
Hash Algorithm = MD5 (5)	Select Certificate= None (16)
Encryption Algorithm = DES-CBC (6)	ID Type= E-mail Address (17)
Diffie-Hellman Group = Default 768-bit MODP (7)	tommy@itso.rai.com
Key Management	Local Network Interface
Maximum key lifetime (minutes) = 120 (8)	Name= Any
Maximum size limit (kilobytes) =	Pre-Shared Key=unbelievable (4)
Data Policy	Security Policy
Name = HtoDnIPCHP (22)	Phase 1 negotiation mode=Aggressive Mode (1) (2)
Use Diffie-Hellman Perfect Forward Secrecy = No (9)	Perfect Forward Secrecy= Disabled (9)
Diffie-Hellman Group = Not Applicable	Replay Protection = Enabled
Data Protection Proposals	Authentication (Phase 1) - Proposal 1
Encapsulation mode = Transport (10)	Authentication Method= Pre-Shared key (3)
Protocol = AH (11)	Encryption and Data Integrity Algorithms
Algorithms	Encrypt Alg.= DES (6)
Authentication Algorithm = HMAC-MD5 (12)	Hash Alg.= MD5 (5)
Key Expiration	SA Life= Seconds 7200 (8)
Expire after (minutes) =60 (14)	Key Group= Diffie-Hellman Group 1 (7)
Expire at size limit (kilobytes) = (15)	Key Exchange (Phase 2) - Proposal 1
Key Connection Group	ESP
Name = HtoDnIPCHP	Encrypt Alg.=
Remote Server Identifier	Hash Alg.=
Identifier Type = User@fully qualified domain name (16)	Encapsulation=
Identifier = tommy@itso.rai.com (17)	SA Life=
Local Key Server	(11) AH
Identifier Type = Version 4 IP address (18)	(12) Hash Alg.= MD5
IP address = 172.16.3.50 (19)	(10) Encapsulation= Transport
Key Policy = HtoDnIPCHP (20)	(14)(15) SA Life= Seconds 3600
Dynamic IP Group	
Name = HtoDnIPCHP	
System Role = Both systems are hosts	
Policy	
Data Management Security Policy = HtoDnIPCHP (21)	
Local addresses = Filter rule	
Local ports = Connection	
Remote addresses = Connection	
Remote ports = Connection	
Protocol = Connection	
IP Filters	
IKE Inbound rule	
Direction= INBOUND	
Source address name = *	
Destination address name= 172.16.3.50	
Protocol = UDP	
Source port =500 (19)	
Destination port =500	
IKE Outbound rule	
Direction= OUTBOUND	
Source address name = 172.16.3.50	
Destination address name= *	
Protocol = UDP	
Source port =500 (19)	
Destination port =500	
IPSEC rule	
Source address name = 172.16.3.50	
Destination address name = *	
Connection Name = DYNAMICIP	
Protocol = *	
Source port = * (19)	
Destination port = *	

11.1.16 Starting the VPN connections

Once the VPN configurations are completed, you must start the connections. Start the responder end of the VPN first. The following sections describe how to start VPN on the AS/400 systems and the VPN clients.

11.1.16.1 Starting VPN on the AS/400 systems

To start the VPN connections in RALYAS4A and RALYAS4C, perform the following steps:

1. Activate IP Packet Security.
2. Start Virtual Private Networking.

Since the AS/400 systems are responders in this chapter's scenarios, only the VPN server jobs need to be started. You do not need to start an individual connection. Refer to 3.8.2, "VPN server operations" on page 87, for information on how to activate IP filters and start VPN server jobs.

11.1.16.2 Starting the IRE SafeNet Soft-PK client

You do not need any special operator intervention to start the SafeNet Soft-PK client. After configuring the client, the VPN client software is updated and started automatically. Once an application requests a session destined for a secured IP address, the SafeNet Soft-PK client starts the IKE negotiation and completes the Security Association (SA) setup. IP traffic for IP addresses not configured for a secured connection is processed, as usual, outside of the VPN.

11.1.17 Checking the VPN connection status

This section shows how to verify the status of the VPN connections on the AS/400 systems and VPN clients.

11.1.17.1 VPN connection status on the AS/400 systems

To check the status of the VPN connection on the AS/400 systems, perform the following steps:

1. From Operations Navigator, double-click **Virtual Private Networking**.
2. Select **View->Active Connections**.

The VPN Active Connections window shown in Figure 618 is displayed.

Name	Status	Encapsulation Mode	Local Key Server	Remote Key Server	Local Data Addr...	Remote Data #
HtoDynIPC:R2	Running	Transport	172.16.3.23	tommy@itso.ral.com	172.16.3.23	172.16.3.122
HtoHD:L1	Running	Transport	172.16.3.23	172.16.3.77	172.16.3.23	172.16.3.77

Figure 618. Active Connections on RALYAS4A

The Active Connections window shown in Figure 618 provides information about two active VPN connections.

- HtoDynIPC is the VPN connection between the RALYAS4A and ThinkPad C. Since ThinkPad C has a dynamically assigned IP address, the Remote Key Server is not an IP address. Instead, it shows the user identifier (e-mail address) of the PC client. R2 indicates that the AS/400 system is the responder in this connection.
- HtoHD identifies the VPN connection between RALYAS4A and PC D, which has a fixed IP address. Even when the AS/400 system is the responder in this connection, L1 is appended to the connection name. This is because the VPN configuration wizard created a Dynamic Key Connection with the name

HtoHD:L1 that matches the responder's characteristics, and the existing name is used.

Figure 619 shows the corresponding Active Connections window on RALYAS4C.

Name	Status	Local Key Serve...	Remote Key Server	Remote Key Se...	Remaining k
HtoDynlPC:R3	Running	172.16.3.50	tommy@itso.ral.com	172.16.3.122	19
HtoHD:L1	Running	172.16.3.50	172.16.3.77	172.16.3.77	56

Figure 619. Active Connections on RALYAS4C

11.1.17.2 VPN connection status on the IRE SafeNet Soft-PK client

SafeNet Soft-PK includes a Log View, which allows you to monitor the status of the VPN such as the various steps during IKE negotiation.

Note

The Log Viewer starts logging only *after* you open it. The log does not include any messages issued prior to starting the Log Viewer. For example, to monitor IKE negotiations with the log viewer, open the Log Viewer first and then start a connection to the remote VPN partner system.

To open the Log Viewer, perform the following steps:

1. Right-click the **SafeNet Soft-PK** icon on the Windows task bar, and select **Log Viewer**.
2. Start a connection, for example, to system RALYAS4A.
3. Monitor the Log Viewer for upcoming messages.

Figure 620 on page 513 shows a log after ThinkPad C establishes a connection to the AS/400 system RALYAS4A.

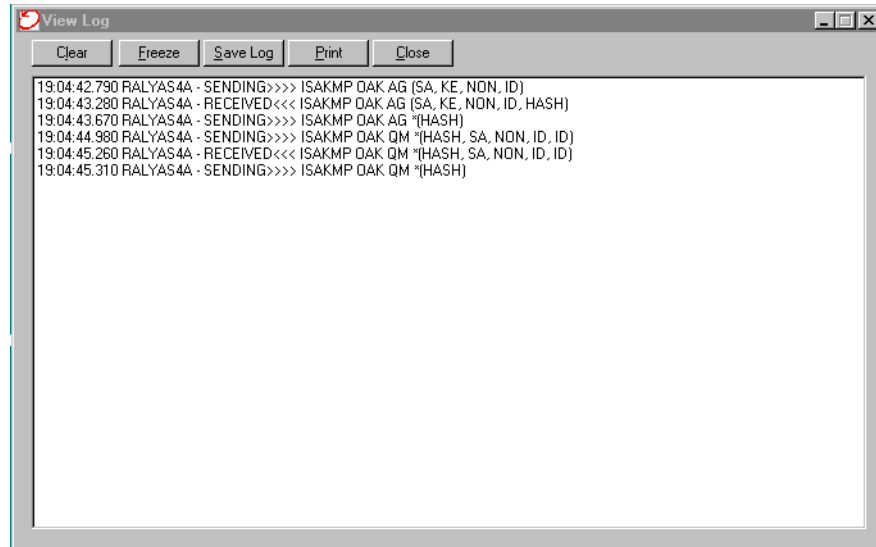


Figure 620. SafeNet Soft-PK - Log Viewer

The log contains the following information:

- **Time stamp:** The time stamp is written into the left-most position of the log and specifies the time that the message was issued.
- **Connection name:** The next column in the log contains the connection name as defined in the Security Policy Editor.
- **Direction:** The third column represents the direction of the message flow.
- **Message:** On the last column, you find the messages. In the log shown in Figure 620, all messages are `ISAKMP OAK` (Oakley) messages. That means, they report the IKE negotiation process. The first three messages are IKE phase 1 messages. They are identified by `AG`, which means aggressive mode. The last three messages belong to IKE phase 2. The abbreviation `QM` means quick mode, which is used for phase 2, regardless if phase 1 is negotiated in aggressive or main mode. The last part of the message contains the message payload. Further information about the ISAKMP message format and payload can be found in the IETF RFCs RFC2407, RFC2408, and RFC2409.

IKE negotiation in aggressive mode is achieved with an exchange of six messages. Figure 620 shows a successful IKE negotiation.

Chapter 12. Don't forget a firewall: Protecting your VPN server

For the sake of simplicity, previous chapters in this redbook do not discuss firewalls protecting the AS/400 system acting as a security gateway. By no means does this imply that you should forget a firewall.

This chapter builds upon scenarios discussed in other chapters by adding a firewall between the corporate gateway and the Internet. It explores changes that are necessary for the TCP/IP configuration of the AS/400 security gateway when a firewall is placed between the AS/400 system VPN server and the Internet. This chapter also explains how to configure the firewall filters to allow VPN protocols to flow through it.

12.1 Choosing the VPN gateway platform

Currently OS/400 has a strong set of IP security features and functions commonly found in firewalls, such as:

- IP filtering
- Network Address Translation (NAT)
- Proxy server (part of IBM HTTP Server for AS/400, 5769-DG1)
- VPN

However, there are still some functions available in firewalls not yet supported on OS/400, such as SOCKS server and split DNS.

There are some scenarios where implementing the security functions listed above on OS/400 and connecting the AS/400 system to the Internet through a router may be sufficient. You can use the router security features as an extra level of protection. It may be that, with future functional enhancements, the AS/400 system will become a fully viable firewall. When using an LPAR partition dedicated to IP security functions, protecting the rest of the system may become an alternative to a dedicated firewall.

It may be viable to connect smaller branch office AS/400 systems directly to the Internet using a VPN to provide a secure link to the central site. If you are connecting an AS/400 system to the Internet directly without the protection of a firewall, consider the following points:

- Implement a tight system security on the AS/400 system. Perform regular security audits. Refer to *Tips and Tools for Securing Your AS/400*, SC41-5300, and *OS/400 Security - Reference V4R4*, SC41-5302, for information on AS/400 security.
- Use a dial-up connection to connect the AS/400 system to the ISP (Internet Service Provider). This provides the added security that the AS/400 is always getting a different IP address, which makes it difficult to follow.
- Use two physical interfaces (lines) on the AS/400 system that act as a gateway. They are:
 - The secure interface that connects the system to the internal network. No IP filters are necessary on this interface.

- The non-secure interface that connects the system to the public network (Internet). Implement the IP filters carefully on this interface, and verify that only the services that you want to allow are permitted.
- Use the connection to the Internet only to establish a VPN tunnel to the central site. Access to other Internet services (Web surfing, e-mail, etc.) is allowed only through the corporate firewall.
- If you are allowing direct access to the Internet for the branch office users through the AS/400 gateway, be sure to properly configure IP filters so that incoming requests are not allowed.

If you are connecting your network to the Internet through a firewall with VPN support, the firewall is the natural choice for the VPN gateway. In this case, you may wonder what is the role of your AS/400 system VPN support.

For gateway-to-gateway connections, there are some reasons why you may need to use your AS/400 system as a VPN gateway, even if you are protecting it with a firewall:

- Lack of VPN IPSec and L2TP support on your current firewall. Not all firewalls (or routers) support the newer VPN IPSec and L2TP standards. You may need to upgrade or replace existing equipment.
- Interoperability problems. You need to consider compatibility carefully. The term Virtual Private Networking means different things to some suppliers. IPSec is an emerging set of standards that different products, even from the same manufacturer, can implement differently. As an example, consider the IBM Firewall for AS/400 and native OS/400 VPN implementations. They are *not* compatible. One way you can guarantee compatibility is to use the same product at local and remote sites. This also rationalizes the skill sets that you require. Different products may inevitably have different configuration interfaces and structures and may use different terminology. IPSec is not a simple subject to master for one product implementation, to say nothing of multiple products.

Note

VPN support was introduced in IBM Firewall for AS/400 in V4R3. However, OS/400 native VPN support introduced in V4R4 and Firewall for AS/400 VPN support do *not* interoperate.

- For host-to-host connections between, for example, business partners and suppliers, the use of iterated (nested) tunnelling may be an ideal solution. You could set up a gateway-to-gateway tunnel using AH for authentication between firewalls and then a host-to-host transport connection using ESP between your AS/400 system and specific hosts in the business partner's network.

This chapter considers scenarios where an AS/400 VPN connection is to be configured through a firewall. The information in this chapter can be used if you want to add a firewall to the scenarios discussed in other chapters of this redbook.

12.2 Gateway-to-gateway VPN through a firewall

This section repeats the scenario discussed in Chapter 6, “Gateway-to-gateway VPN” on page 199, but now there is a firewall protecting the network at the corporate site.

Figure 621 shows a corporate office connected to the Internet through a firewall. Here, the AS/400 security gateway is at the branch office and is connected directly to the Internet through a router, but the same principles apply if there was a firewall at both ends. Similarly, while IBM Firewall for AS/400 is used in this example, it is intended to represent a *generic* firewall. The AS/400 system and firewall configurations discussed here are valid even if another firewall is used.

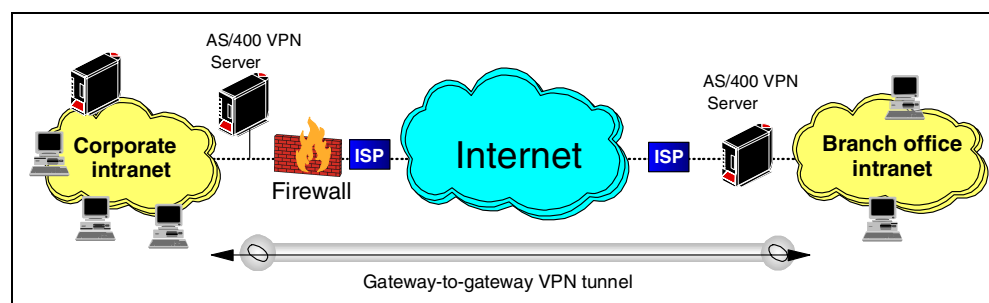


Figure 621. Gateway-to-gateway VPN through firewall

Note: To simplify the example, we do not include a firewall in front of the branch office network. However, the configuration of the branch office AS/400 system can mirror the corporate AS/400 configuration.

12.2.1 Scenario characteristics

The characteristics of this scenario are:

- The corporate network is connected to the Internet through IBM Firewall for AS/400.
- The branch office network is connected to the Internet through an AS/400 security gateway and a router. Both the AS/400 system and the router are carefully configured to provide maximum protection to the branch office network.
- VPN support in IBM Firewall for AS/400 is not compatible with the VPN support in OS/400 V4R4. Therefore, a VPN tunnel cannot be established between the firewall at the corporate office and the AS/400 system at the branch office.

12.2.2 Scenario objectives

The objectives of this scenario are:

- All traffic between the corporate network and the branch office network must be protected by a VPN tunnel.
- Due to interoperability limitations of the firewall, the VPN tunnel must be established between the AS/400 VPN servers at the corporate office and branch office. IP forwarding must be enabled in the firewall. The firewall filters must be configured to allow the IPsec protocols to flow through it.

- All traffic can flow in the clear inside the corporate and branch office intranets. Both networks belong to the same company and they fully trust each other. Therefore, only the VPN servers need to provide VPN functions.
- All clients and hosts on each network have full access to the partner's network, including all applications (Telnet, FTP, LPR/LPD, HTTP, etc.).

12.2.3 Firewall requirements

To configure the firewall to permit IPSec protocols through it, you must create filter rules to permit:

- IKE negotiations using protocol UDP on port 500
- ESP protocol
- AH protocol

Notice that ESP (protocol number 50) and AH (protocol number 51) are separate from TCP, UDP, or ICMP. The firewall or router filter rules need to support filtering of these relatively new protocols to permit them. IBM Firewall for AS/400 V4R3 and later allows you to specify protocols AH and ESP in the filter rules.

12.2.4 Implementing a gateway-to-gateway VPN through a firewall

This section describes the tasks that you must perform to configure a gateway-to-gateway VPN scenario where an intermediate firewall is employed. Many of the steps are identical to those in Chapter 6, "Gateway-to-gateway VPN" on page 199. However, some changes in the routing configuration and addressing schemes are required. In addition, IP forwarding and filter rules must be configured on the firewall.

Figure 622 shows the test network used for this scenario.

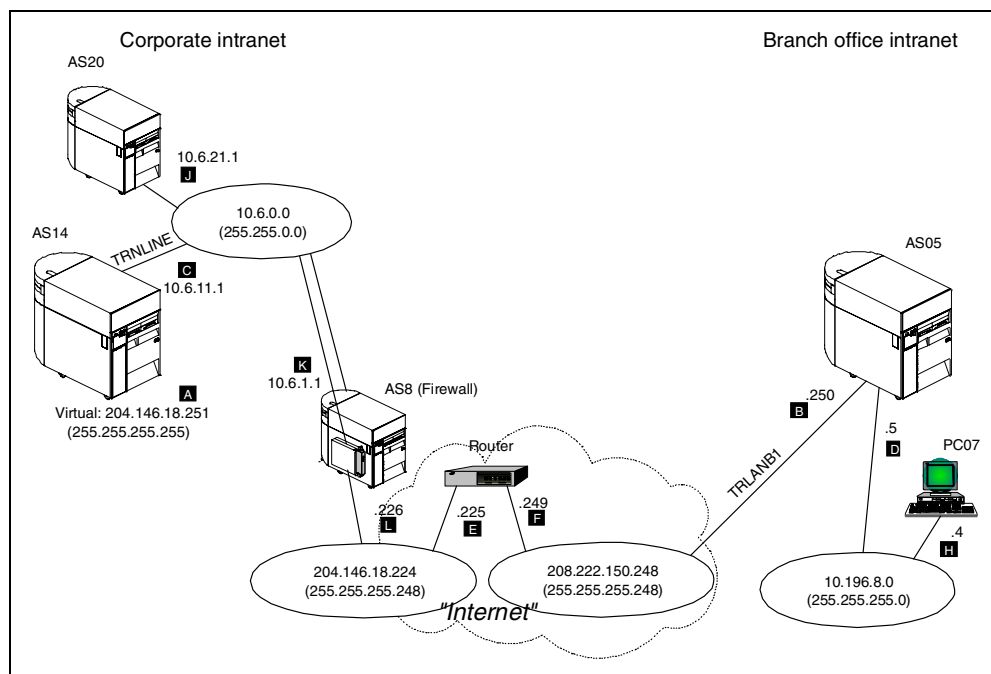


Figure 622. Gateway-to-gateway VPN through a firewall - Scenario test network

The characteristics of the test network are:

- AS8 is an AS/400 system with an Integrated Netfinity Server (previously known as Integrated PC Server or IPCS) running IBM Firewall for AS/400 V4R3.
- AS14 is an AS/400 system running OS/400 V4R4. AS14 represents the corporate office VPN server.
- AS05 is an AS/400 system running OS/400 V4R4. AS05 represents the branch office VPN server.
- AS20 is an AS/400 system running standard TCP/IP applications. VPN functions are not configured on this system. It represents a generic TCP/IP host in the corporate network. For all practical purposes, it does not support VPN.
- PC07 represents a generic client (also referred to as a *host* in TCP/IP terminology) on the other remote subnet. PC7 will access the TCP/IP applications on AS20 through the VPN tunnel.
- At the corporate office, the network administrator assigns a portion of a class C network to connect to the Internet. The corporate office Demilitarized Zone (DMZ) is assigned the network address 204.146.18.224, with subnet mask 255.255.255.248.
- At the branch office, the network administrator assigns a portion of a class C network to connect to the Internet. The branch office DMZ is assigned the network address 208.222.150.248, with subnet mask 255.255.255.248.
- The corporate office uses the subnet 10.6.0.0, with subnet mask 255.255.0.0 in its intranet. This subnet represents the data endpoint of the VPN tunnel at the corporate office site.
- The branch office uses the subnet 10.196.8.0, with subnet mask 255.255.255.0 in its intranet. This subnet represents the data endpoint of the VPN tunnel at the branch office site.
- TRNLINE is the Token-Ring line description connecting AS14 to the corporate intranet subnet 10.6.0.0.
- TRLANB1 is the Token-Ring line description connecting AS05 to the Internet router in subnet 208.222.150.248.
- AS14 is assigned a public IP address 204.146.18.251, with subnet mask 255.255.255.255. This IP address is configured as a Virtual IP address on AS14 and is used to route all the VPN traffic that traverses the firewall to be processed by the VPN server (AS14).

12.2.5 Subnetting considerations

Comparing Figure 622 on page 518 with Figure 198 on page 201 in Chapter 6, “Gateway-to-gateway VPN” on page 199, it becomes clear that the difference between them is the presence of a firewall in the current chapter’s scenario. In this chapter, we introduce a firewall between the corporate office intranet (10.6.0.0 network) and the corporate office public network or DMZ (204.146.18.224 network in Figure 198 on page 201). This firewall is an IBM Firewall for AS/400 running on an Integrated Netfinity Server under the cover of AS8.

The firewall must be able to route the VPN traffic to AS14 to be processed by the VPN server. After applying the IPSec protocols to the inbound (and outbound) datagrams, AS14 must route the incoming traffic to the destination host in the intranet and the outgoing traffic to the firewall.

Because the firewall must act as a router between the DMZ and AS14 in this scenario, it is necessary to subnet the original 204.146.18.224 network assigned by the ISP to the corporate office into two separate networks.

In the scenario described in Chapter 6, “Gateway-to-gateway VPN” on page 199, we assume that the ISP allocates a portion of a class C network to the corporate office (204.146.18.224 network address, with a subnet mask of 255.255.255.224). This represents a maximum of 30 hosts. For the firewall to route IP packets between the DMZ and AS14, we need to split the portion of the class C network assigned into smaller subnetworks.

Using mask 255.255.255.248 results in the following network and hosts:

- Network: 204.146.18.224 Hosts: 204.146.18.225 to 230, that is 6 hosts
- Range of host IP addresses Hosts: 204.146.18.232 to 255, that is 24 hosts

You can use any of the host IP addresses as a virtual IP as explained in 12.2.6, “Virtual IP addressing and routing: VPN gateway behind a firewall” on page 520.

Note: The individual host addresses do not need to be contiguous. They can be any disjointed set of addresses (or only one) as long as they are not in the same network as the DMZ.

For this example, we only require two subnets and use 204.146.18.224 and 204.146.18.248. The other host addresses are reserved for internal clients that require the use of Network Address Translation (NAT) through the firewall. When you need to subnet the IP addresses assigned by the ISP, avoid wasting globally routable IP addresses.

The 204.146.18.224 subnet is used in the DMZ between the non-secure port of the firewall and the *Internet* router. The non-secure port of the firewall (□ in Figure 622 on page 518) is assigned the IP address 204.146.18.226.

Subnet 204.146.18.248 is used as a *virtual* network running over the same physical LAN as the 10.6.0.0 network, which is on the secure side of the firewall.

A routing entry must be added to the Internet router to route traffic for the 204.146.18.248 network to the firewall non-secure port 204.146.18.226.

12.2.6 Virtual IP addressing and routing: VPN gateway behind a firewall

Figure 623 on page 521 shows the technique that we used here to route IPSec traffic through the firewall to the AS/400 VPN server, AS14, on the secure network. It uses virtual IP addresses to avoid creating a separate physical network between AS14 and the firewall.

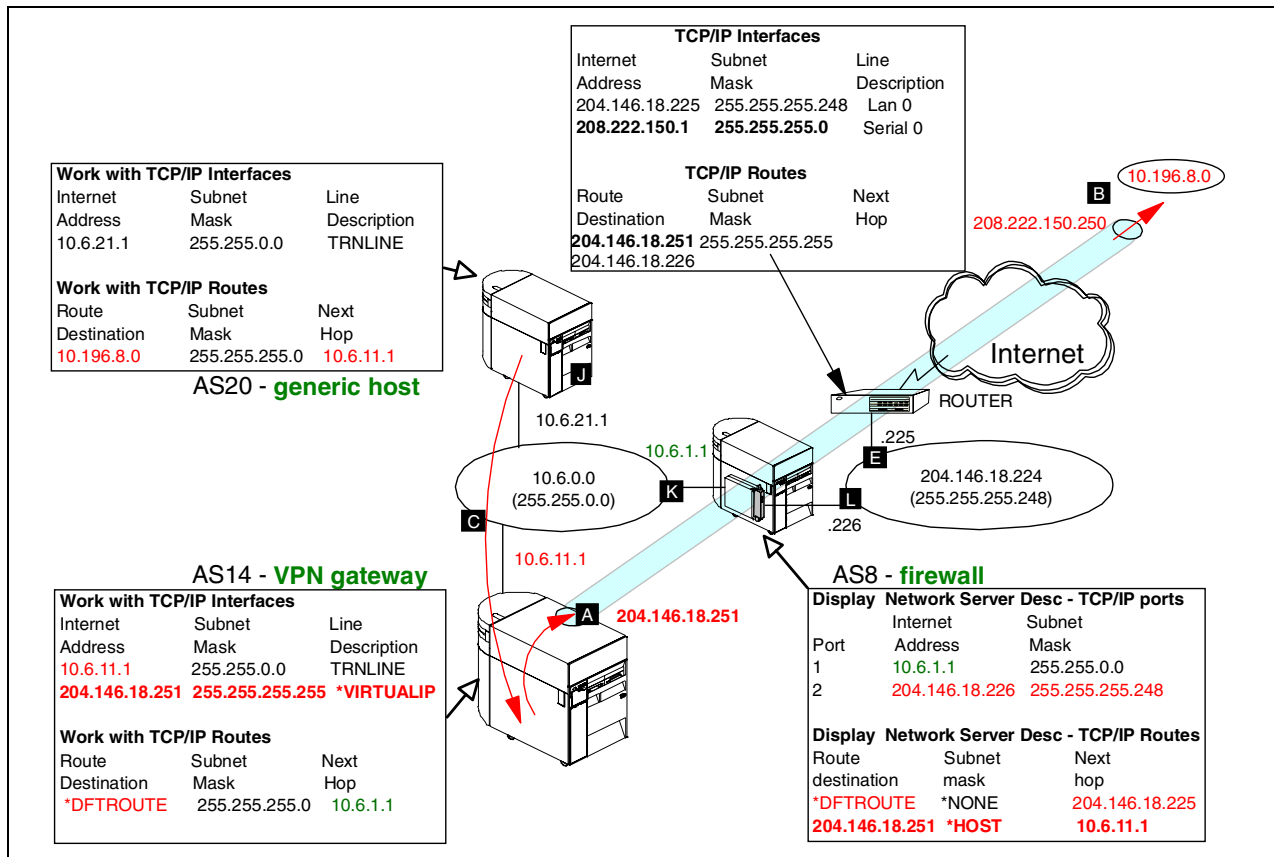


Figure 623. AS/400 VPN server behind a firewall - IP addressing and routing with a virtual IP

In this scenario, AS14 has only one physical interface, TRNLINE, that connects it to the intranet subnet using IP address 10.6.11.1 (G in Figure 623). We strongly recommend that you have two separate physical interfaces for the security gateway: one attached to the internal network and the other to the Internet. However, in this scenario, AS14 is not directly connected to the Internet.

You must assign a public IP address to AS14 since NAT cannot be used with IPSec protocols. NAT changes the addresses in the IP header and causes authentication failures. VPN NAT cannot be used here since the AS/400 VPN server does *not* border the public network.

In V4R3, OS/400 introduced support for virtual IP interfaces. You can configure an IP addresses on your AS/400 system that is not bound to a single physical interface, but is globally local to the system regardless of the physical interface the datagram came from. The following series describes how to use this feature to provide routing in this environment:

1. The interfaces and routing table on AS20 are the same as in the scenario described in Chapter 6, "Gateway-to-gateway VPN" on page 199. All traffic for the remote VPN partner, 10.196.8.0, is routed to 10.6.11.1 G, that is AS14.
2. AS14 now has a single physical line into the internal network with the same IP address, 10.6.11.1. It also has a public address, 204.146.18.251 A, defined as *VIRTUALIP. The subnet mask is now 255.255.255.255.

3. The firewall secure port address is 10.6.1.1 **K**, and the non-secure port is 204.146.18.226 **L**.
4. The firewall default route points to the Internet router **E** 204.146.18.225.
5. The firewall has an explicit route that directs traffic for host 204.146.18.251 (*VIRTUALIP) to physical IP address 10.6.11.1. This way, datagrams coming from the external network, with destination public IP address 204.146.18.251, are routed to AS14 across the private network (10.6.0.0).

The technique we just described allows AS14 to be a single-homed VPN gateway, which means a single network interface for both local and VPN traffic. In this case, you need to add extra filter rules to avoid the default DENY rule that prevents local traffic from using the interface (we return to this later). In this example, the following rule was added after the IPSEC rule to permit all traffic with a source and destination address of 10.*.*.*:

```
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = * SRCADDR = Net10 DSTADDR = Net10 PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
```

Net10 is defined as follows:

```
ADDRESS Net10 IP = 10.0.0.0 MASK = 255.0.0.0 TYPE = TRUSTED
```

12.2.7 Task summary

The following series summarizes the tasks you need to perform to implement the gateway-to-gateway connection through a firewall in this scenario:

1. Configure the firewall to permit IPSec protocols through it.
2. Verify end-to-end connectivity. Before starting the VPN connection, ensure that normal TCP/IP routing is working so that:
 - The gateway AS/400 systems can communicate with each other across the intervening Internet (and through the firewall).
 - Hosts on each subnet route datagrams to their respective gateway for access to the remote subnet.
3. Complete the planning worksheet for AS/400 VPN server behind the firewall (AS14).
4. Configure VPN and IP filtering on the AS/400 VPN server at the corporate office behind the firewall (AS14).
5. Complete the planning worksheet for the AS/400 VPN server at the branch office (AS05).
6. Configure VPN and IP filtering on the AS/400 VPN server at the branch office (AS05).
7. Activate the VPN connections.
8. Perform final verification tests between both subnets.

12.2.8 Configuring the firewall to permit IPSec protocols

It is beyond the scope of this document to cover all the steps and options involved in setting up the IBM Firewall for AS/400 product. For information about IBM Firewall for AS/400 implementation and configuration, refer to *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162, and *IBM Firewall for AS/400: VPN and NAT Support*, SG24-5376.

The following series of events is a high level summary of the main tasks used to create a basic firewall configuration suitable for this scenario. If the firewall is already in use, omit the steps for installing the firewall and for creating the basic settings.

Note: In this scenario, we use IBM Firewall for AS/400 as a generic firewall. The same configuration applies to any firewall installed between the AS/400 VPN server and the Internet.

To configure the firewall in this scenario, complete these steps:

1. Install IBM Firewall for AS/400 using the browser interface.

Figure 624 shows the firewall installation summary. Note that the secure port is configured as 10.6.1.1 (subnet mask 255.255.0.0), and the non-secure port is configured as 204.146.18.226 (255.255.255.248). The external router IP address is 204.146.18.225.

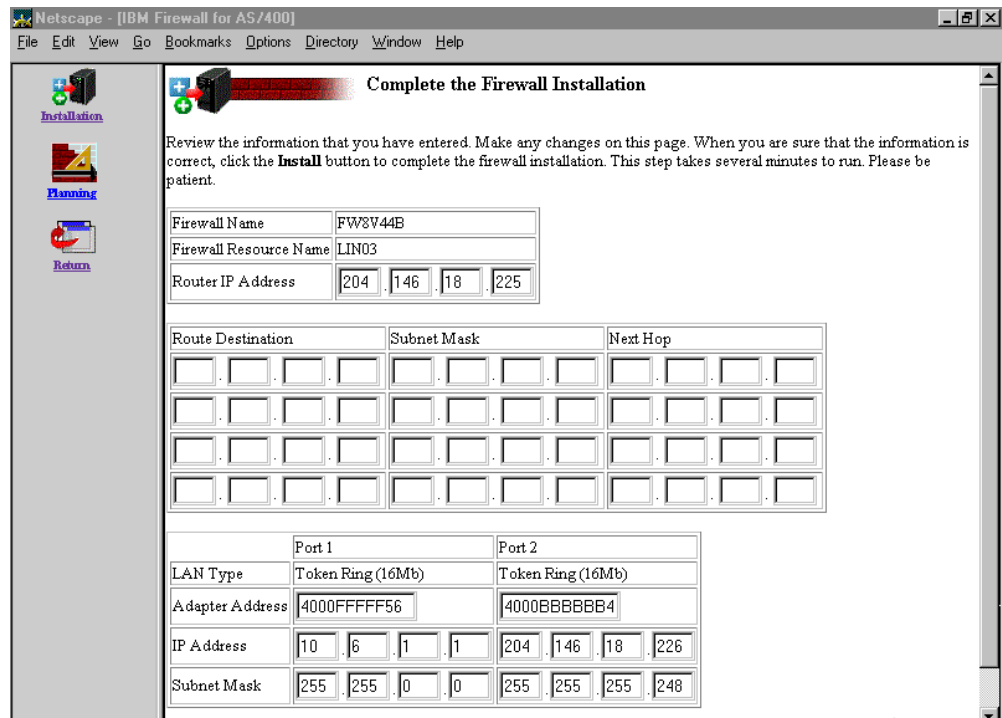


Figure 624. Firewall installation summary

2. Add an explicit route to the AS14 virtual IP address. Add a route to 204.146.18.251, with a next hop of 10.6.11.1 (AS14's physical IP address). Use the Change Network Server Description (CHGNWSD) command to change the firewall network server description. Enter the command:

```
CHGNWSD NWS(FW8V44B) TCPROUTE ((*DFTRROUTE *NONE '204.146.18.225 ' )
('204.146.18.251' *HOST '10.6.11.1'))
```

Note: The default route to the external router at 204.146.18.225, configured during the firewall installation, is also shown in this command.

3. Vary on the network server description. Use the following command:

```
VRYCFG CFGOBJ (FW8V44B) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)
```

4. Start the firewall network server application using the following command:

STRNWSAPP NWSAPP (*FIREWALL) NWS (FW8V44B)

5. Access the Configuration and Administration functions interface through the firewall secure port as shown in Figure 625.
6. Use the firewall Basic configuration option to create the basic firewall settings. For this example, very few functions are selected. Only the proxy and SOCKS server for HTTP are selected since the firewall configuration is beyond the scope of this redbook.

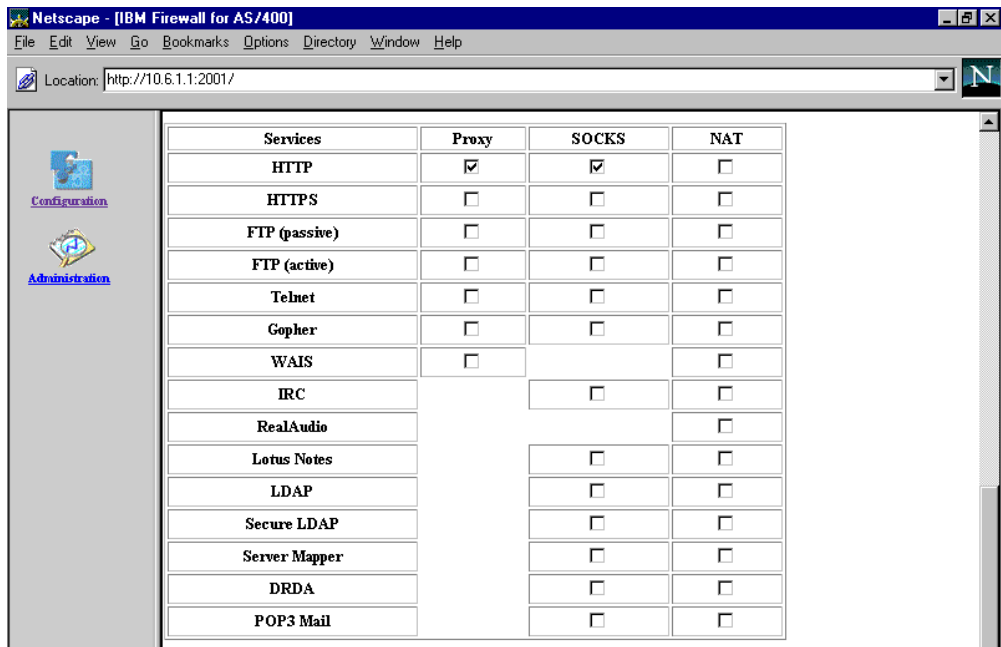


Figure 625. Firewall Basic configuration - Outgoing services

7. Use the Status page to start (permit) IP Packet Forwarding as shown in Figure 626.

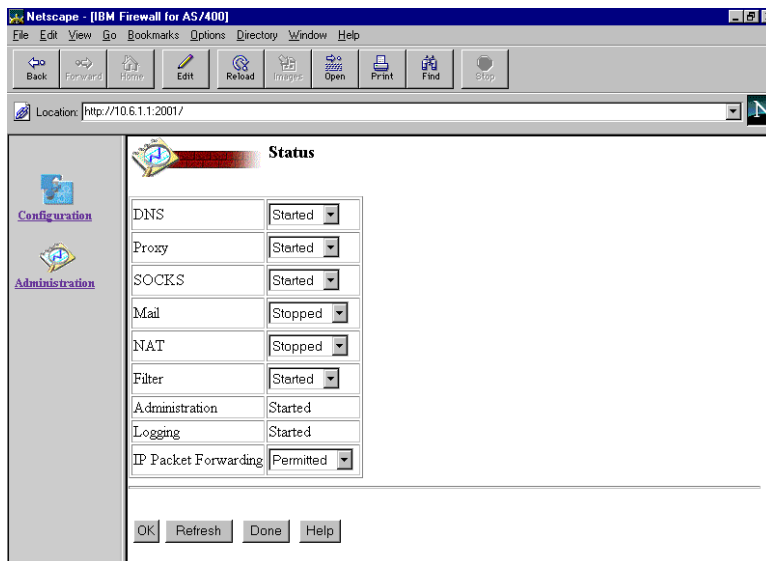


Figure 626. Start IP packet forwarding

8. Use the Autostart Settings page to enable IP Packet Forwarding every time the firewall is started as shown in Figure 627.

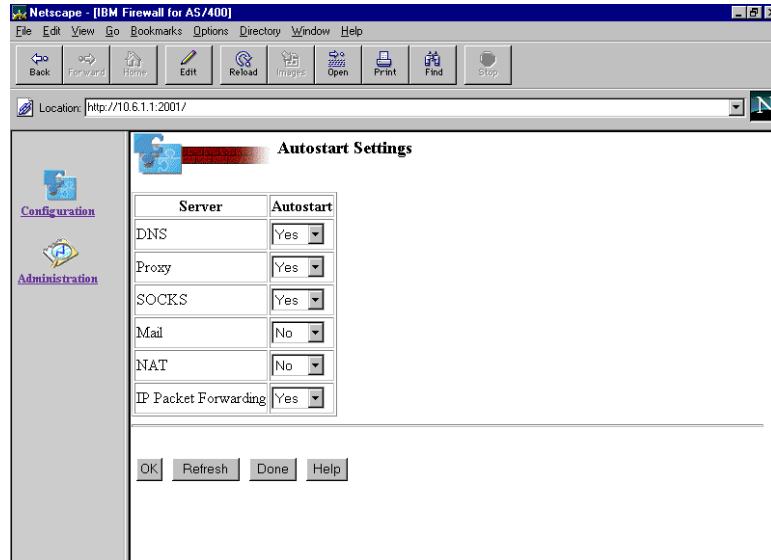


Figure 627. Firewall autostart settings

9. Use the Filters page to edit the firewall filter rules.

You need to add three sets of rules to permit the IPSec protocols IKE (UDP 500), AH, and ESP.

- The IKE rules permit traffic using UDP with source and destination ports 500. Four filters are required:
 - Permit datagrams with source address 204.146.18.251 and destination address 208.222.150.250 inbound on the secure port.
 - Permit datagrams with source address 204.146.18.251 and destination address 208.222.150.250 outbound on the non-secure port.
 - Permit datagrams with source address 208.222.150.250 and destination address 204.146.18.251 inbound on the non-secure port.
 - Permit datagrams with source address 208.222.150.250 and destination address 204.146.18.251 outbound on the secure port.
- The AH and ESP rules are the same as the four rules described previously, but the protocol field changes to AH and ESP respectively.

Note: For testing and verification purposes, we specified logging in the filter rules (log (y)). In a production environment, you should log only when necessary.

Figure 628 on page 526 shows the IPSEC filter rules added to the firewall filters configuration to allow IPSec protocols to flow through it.

```

#
# #####
# Filters added to permit IPSEC tunnel though Firewall. Local AS/400 VPN gateway has IP address of 204.146.18.251,
remote AS400 VPN gateway
# has address 208.222.150.250
# #####
#
0008:action(permit) from(204.146.18.251) to(208.222.150.250) protocol(udp eq 500/eq 500)
interface(secure) routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit IKE
Exchanges")
0009:action(permit) from(204.146.18.251) to(208.222.150.250) protocol(udp eq 500/eq 500)
interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit IKE
exchange")
0010:action(permit) from(208.222.150.250) to(204.146.18.251) protocol(udp eq 500/eq 500)
interface(non-secure) routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit IKE
exchange")
0011:action(permit) from(208.222.150.250) to(204.146.18.251) protocol(udp eq 500/eq 500)
interface(secure) routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit IKE
exchange")
#
0012:action(permit) from(204.146.18.251) to(208.222.150.250) protocol(ah any 0/any 0) interface(secure)
routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit AH tunnel")
0013:action(permit) from(204.146.18.251) to(208.222.150.250) protocol(ah any 0/any 0) interface(non-secure)
routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit AH tunnel")
0014:action(permit) from(208.222.150.250) to(204.146.18.251) protocol(ah any 0/any 0) interface(non-secure)
routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit AH tunnel")
0015:action(permit) from(208.222.150.250) to(204.146.18.251) protocol(ah any 0/any 0) interface(secure)
routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit AH tunnel")
#
0016:action(permit) from(204.146.18.251) to(208.222.150.250) protocol(esp any 0/any 0) interface(secure)
routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit ESP tunnel")
0017:action(permit) from(204.146.18.251) to(208.222.150.250) protocol(esp any 0/any 0) interface(non-secure)
routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit ESP tunnel")
0018:action(permit) from(208.222.150.250) to(204.146.18.251) protocol(esp any 0/any 0) interface(non-secure)
routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit ESP tunnel")
0019:action(permit) from(208.222.150.250) to(204.146.18.251) protocol(esp any 0/any 0) interface(secure)
routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit ESP tunnel")
#
#####

```

Figure 628. IPSEC filter rules added to the firewall

The above rules only permit IPSec protocols. To test basic TCP/IP routing between the VPN gateways before activating the VPN connection, it is useful to enable PING through the firewall, temporarily at least. Figure 629 shows the ICMP filters built in IBM Firewall for AS/400 by the Basic configuration program. Change the default value of routing(local) to routing(both) to allow PING through the firewall as shown in Figure 629.

```

#
0022:action(permit) from(any) to(any) protocol(icmp eq 8/eq 0) interface(both) routing(both) direction(both)
fragment(y) log(n) VPN(0) description(" Permit ping requests")
0023:action(permit) from(any) to(any) protocol(icmp eq 0/eq 0) interface(both) routing(both) direction(both)
fragment(y) log(n) VPN(0) description(" Permit ping replies")

```

Figure 629. Firewall ICMP filter rules

10.Restart the IP filters from the firewall administration Status link.

12.2.9 Verifying end-to-end connectivity

Before activating filters and VPN, you must be sure that connectivity and routing between the two VPN servers is working properly.

The routing requirements for this scenario are discussed in 12.2.6, “Virtual IP addressing and routing: VPN gateway behind a firewall” on page 520. Having a firewall in the configuration clearly complicates matters because:

- It adds an extra hop that routing tables must reflect.
- By default, IP filtering in the firewall blocks traffic. When testing, your TCP/IP routing may actually be correct. However, it may appear not to work because datagrams are being stopped at the firewall.

Check TCP/IP routing before activating your VPN connection (and the associated OS/400 filter rules). This is possible if you permit PING requests and replies through the firewall as described in 12.2.8, “Configuring the firewall to permit IPSec protocols” on page 522.

In this example network, test PING from AS05 to AS14 using the command:

```
PING RMTSYS('204.146.18.251')
```

To test PING from AS14 to AS05, you need to specify the AS14 virtual IP address in the optional Local Internet address parameter. This is because TCP/IP defaults to using a source IP address from the physical interface from which it routes. In this case, this is 10.6.11.1. The external network router cannot route 10.*.* addresses. Therefore, the source address must be overridden to the virtual IP address:

```
PING RMTSYS('208.222.150.250') LCLINTNETA('204.146.18.251')
```

To test PING from AS20 to PC7, issue the following command:

```
PING RMTSYS('10.196.8.4') LCLINTNETA('10.6.21.1')
```

Note: We tested connectivity between the private 10.x.x.x networks because our systems were not in a real Internet environment. Routers in the Internet do not forward IP packets with 10.x.x.x destination IP addresses.

12.2.10 Configuring the AS/400 VPN server behind the firewall (AS14)

The following sections explain how to configure a gateway-to-gateway VPN on the AS/400 VPN server behind the firewall (AS14) at the corporate office.

12.2.10.1 Planning worksheets for the corporate AS/400 system

Complete the planning worksheets to gather the information that you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 53 shows the planning worksheet for this scenario from the perspective of the VPN server behind the firewall (AS14 in Figure 622 on page 518).

Table 53. AS14 New Connection Wizard planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	GtoGFW14to05

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest
How will you identify your local server?	IP address
What is the IP address of your local server?	204.146.18.251 A
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	208.222.150.250 B
What is the pre-shared key?	qacbezlrxiq
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest

This time, the wizard uses the IPSec protocols that provide highest security at the expense of lowest performance for protecting both key and data information. The main configuration object, the *connection group*, is named GtoGFW14to05, and the pre-shared key is a "random" string of characters (qacbezlrxiq).

Table 54 shows the planning worksheet to gather the information that you need to create the IP filters for this scenario.

Table 54. AS14 Planning worksheet - IP filter rules

This is the information you need to create your IP filters to support your VPN	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.	Gateway
Is the <i>remote</i> VPN server acting as a host or gateway ?	Gateway
What name do you want to use to group together the set of filters that will be created?	VPNIFC
If <i>your</i> server is acting as a gateway ... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	10.6.0.0 255.255.0.0 AS14subnets
If the <i>remote</i> server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	10.196.0.0 255.255.0.0 AS05subnets

This is the information you need to create your IP filters to support your VPN	Scenario answers
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound IKE filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	204.146.18.251 A
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	208.222.150.250 B
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRNLINE
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	All 10.*.* addresses All protocols All ports

Note

The main difference between this scenario and others in this redbook is that, when placing the VPN server behind the firewall, we use a single physical line (TRNLINE in this scenario) that is shared between intranet and extranet (VPN) traffic. For this reason, you must configure an additional filter rule to permit traffic to and from the internal network over the single physical interface.

The other scenarios show the AS/400 gateway connected to the Internet and intranet using two separate physical interfaces (lines).

12.2.10.2 VPN connection and IP filters on the corporate AS/400 system

This section presents only the configuration summary for the gateway-to-gateway VPN and the IP filters configuration in this scenario. Refer to Chapter 6, “Gateway-to-gateway VPN” on page 199, for step-by-step configuration instructions.

Figure 630 on page 530 shows the New Connection Wizard Summary window. This is the last window displayed by the VPN configuration wizard when configuring the gateway-to-gateway VPN on AS14.

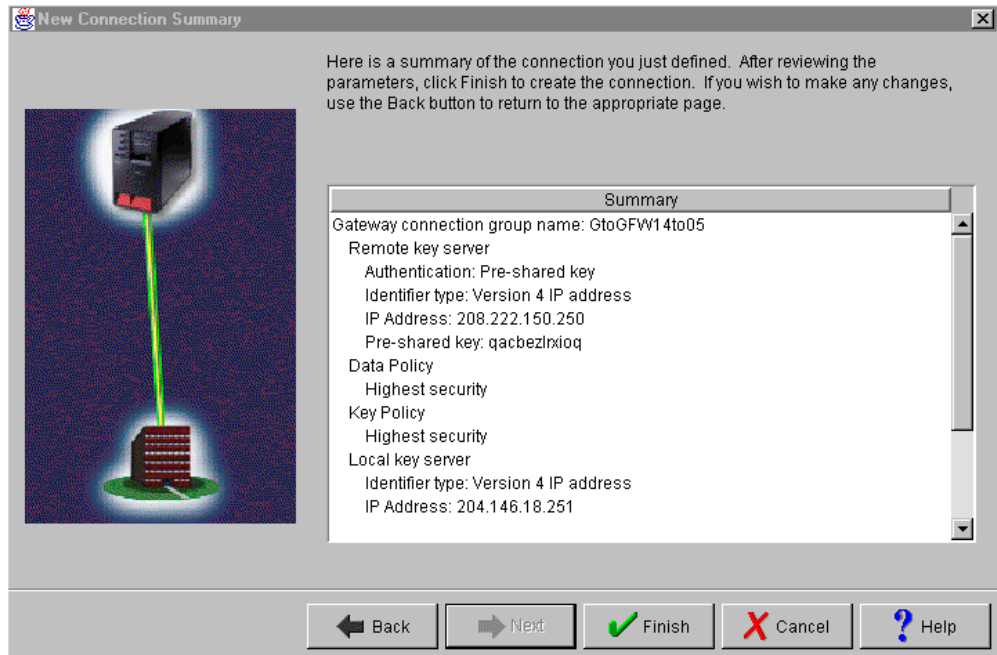


Figure 630. AS14 New Connection Summary window

Figure 631 shows the summary of the IP filters configured on AS14 for this scenario.

```

*****
#Filter rules for VPN traffic
*****
#Intranet subnet - All subnets at corporate
ADDRESS Net10 IP = 10.0.0.0 MASK = 255.0.0.0 TYPE = TRUSTED
#Branch office VPN partner's subnet
ADDRESS AS05subnets IP = 10.196.0.0 MASK = 255.255.0.0 TYPE = UNTRUSTED
#Local VPN endpoint subnet
ADDRESS AS14subnets IP = 10.6.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
#IKE filter rules
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.251
  DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 208.222.150.250
  DSTADDR = 204.146.18.251 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC filter rule
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS14subnets DSTADDR = AS05subnets
  PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
  CONNECTION_DEFINITION = GtoGFW14to05
#Filter interface
FILTER_INTERFACE LINE = TRNLIN SET = VPNIFC
#Permit internal traffic to use TRNLIN for all protocols and services
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = * SRCADDR = Net10 DSTADDR = Net10 PROTOCOL = *
  DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF

```

Figure 631. AS14 IP filter rules - Summary

The first and last filter rules refer to address *Net10* and allow any traffic with a source and destination address of 10.*.* using any protocol or port to use the line TRNLIN. This is required because AS14 is behind the firewall and a single line is being shared by both internal traffic from the local network and the VPN

tunnel. The permit rule for internal traffic must be placed *after* the IPSEC rule so that *outbound* datagrams on TRNLIN with a source address of 10.6.*.* and a destination address of 10.196.*.* are processed by the IPSEC rule. If you place the PERMIT rule for internal traffic *before* the IPSEC rule, the intended VPN datagrams will also match it and not reach the IPSEC rule.

At first sight, you may think that the permit rule for internal traffic should allow only 10.6.*.* addresses since that is the local network address. However, remember that datagrams destined for the VPN gateway have destination addresses of 10.196.*.* and must first enter AS14 before they can be sent out again through the tunnel. Similarly, datagrams that have been received through the tunnel have a source address of 10.196.*.*, and they must be allowed out over the local network.

12.2.11 Configuring the AS/400 security gateway at the branch office

The following sections explain how to configure a gateway-to-gateway VPN on the AS/400 VPN server at the branch office (AS05).

12.2.11.1 A planning worksheet for the branch office AS/400 system

Complete the planning worksheet to gather the information that you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 55 shows the planning worksheet for this scenario from the perspective of the VPN server at the branch office (AS05 in Figure 622 on page 518).

Table 55. AS05 New Connection Wizard planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	GtoGFW05to14
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest
How will you identify your local server?	IP address
What is the IP address of your local server?	208.222.150.250 B
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	204.146.18.251 A
What is the pre-shared key?	qacbezlrxiog

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Highest

The level of key and data protection match AS14, as does the pre-shared key. The connection group is named GtoGFW05to14.

Table 56 shows the planning worksheet to gather the information you need to create the IP filters for this scenario.

Table 56. AS05 Planning worksheet - IP filter rules

This is the information you need to create your IP filters to support your VPN	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ?	Gateway
Is the <i>remote</i> VPN server acting as a host or gateway ?	Gateway
What name do you want to use to group together the set of filters that will be created?	VPNIFC
If <i>your</i> server is acting as a gateway ... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	10.196.0.0 255.255.0.0 AS05subnets
If the <i>remote</i> server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	10.6.0.0 255.255.0.0 AS14subnets
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound IKE filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	208.222.150.250 B
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	204.146.18.251 A
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRLANB1
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

The IP addresses in the AS05 IP filters are essentially the reverse of those configured on AS14. The Token-Ring line name on AS05 is TRLANB1. Unlike AS14, this line is directly connected to the external network and only VPN traffic is permitted on it.

12.2.12 Configuring VPN connection and IP filters on AS05

This section presents only the configuration summary for the gateway-to-gateway VPN and the IP filters configuration in this scenario. Refer to Chapter 6, “Gateway-to-gateway VPN” on page 199, for step-by-step configuration instructions.

Figure 632 shows the New Connection Wizard Summary window. This is the last window displayed by the VPN configuration wizard when configuring the gateway-to-gateway VPN on AS05.

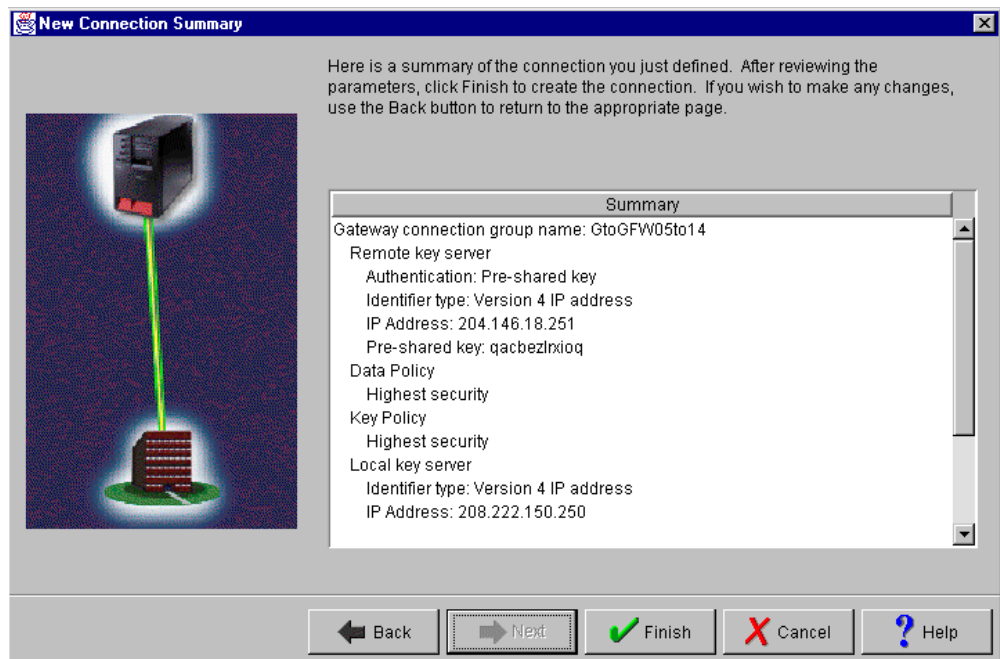


Figure 632. AS05 New Connection Summary window

Figure 633 on page 534 shows the summary of the IP filters configured on AS14 for this scenario.

```

*****
#Filter rules for VPN traffic
*****
ADDRESS AS05subnets IP = 10.196.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
ADDRESS AS14subnets IP = 10.6.0.0 MASK = 255.255.0.0 TYPE = UNTRUSTED
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 208.222.150.250
  DSTADDR = 204.146.18.251 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 204.146.18.251
  DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS05subnets DSTADDR = As14subnets
  PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
  CONNECTION_DEFINITION = GtoGFW05to14
FILTER_INTERFACE LINE = TRLANB1 SET = VPNIFC

```

Figure 633. AS05 IP filter rules - Summary

The filter rules on the branch office AS/400 system are similar to those in other scenarios in this redbook where the AS/400 VPN gateway is connected directly to the external network.

12.2.13 Activating the VPN connection

Perform the following steps to start the VPN tunnel on both AS/400 VPN servers:

1. Activate the IP filters.
2. Start the VPN server jobs by starting Virtual Private Networking.
3. Activate the connection from one of the AS/400 systems.

Refer to 3.8, “VPN operations and management” on page 84, for detailed information on how to start a VPN connection.

Figure 634 shows the Active Connections window on AS14.

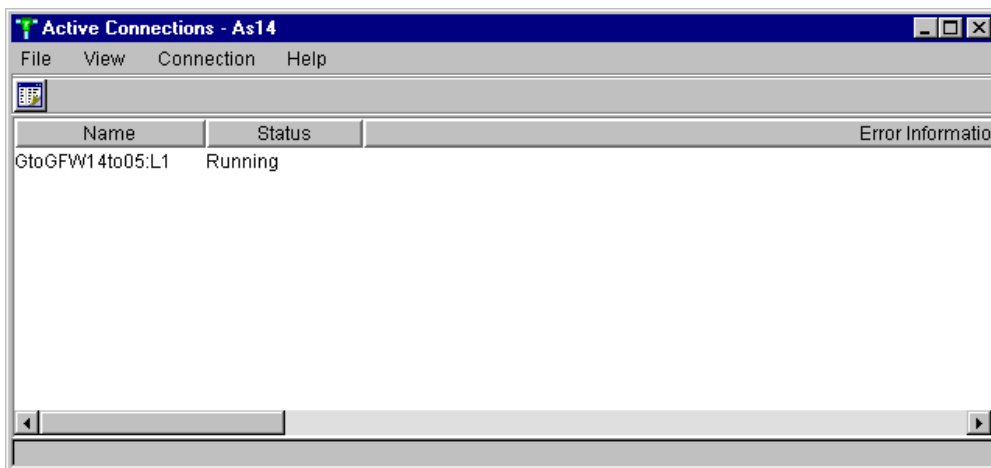


Figure 634. AS14 Active Connections window

12.2.14 Performing verification tests

Table 57 shows a summary of the verification tests performed for this scenario.

Table 57. Gateway to gateway through a firewall - Verification tests

From	To	To IP address	Application	Success
AS20	PC07	10.196.8.4 (H)	PING	Yes
AS20	AS05	10.196.8.5 (D)	PING	Yes
AS20	AS05	10.196.8.5 (D)	FTP	Yes
AS20	AS05	10.196.8.5 (D)	TELNET	Yes
PC07	AS20	10.6.21.1 (J)	TELNET	Yes
PC07	AS20	10.6.21.1 (J)	Client Access PC5250	Yes
PC07	AS20	10.6.21.1 (J)	Operations Navigator	Yes
PC07	AS20	10.6.21.1 (J)	FTP	Yes
PC07	AS14	10.6.11.1 (C)	FTP	Yes
AS20	AS05	208.222.150.250 (B)	PING	No
AS14	AS05	10.196.8.5 (D)	TELNET	Yes

The tests shown in Table 57 were performed in our example network to validate a selection of TCP/IP applications and IP addresses. Notice that the connections to the AS05 208.222.150.250 address did not work. This is because this IP address is not within the range of IP addresses configured as a data endpoint of the VPN connection. Refer to 6.5, “Adding host-to-gateway and gateway-to-host connection groups” on page 238, for further information.

However, note that AS14 was able to connect to the AS05 private address 10.196.8.5. This is because AS14 has a physical address of 10.6.11.1 on the interface, TRNLINE. This is the interface that datagrams are initially routed out of and, therefore, 10.6.11.1 is inserted as the source address. With a source address of 10.6.11.1 and a destination address of 10.196.8.5, the datagrams match the IPSEC filter rule and are permitted through the VPN tunnel.

12.2.15 Additional TCP/IP configuration information

This section shows additional TCP/IP configuration information on the systems in this scenario’s network.

Beware of fragmentation

One problem that we encountered when testing this firewall configuration concerned fragmentation and MTU (Maximum Transmission Unit) sizes.

The default for native OS/400 filter rules does not permit fragments (FRAGMENTS = NONE) since only the first fragment contains the identifying header for higher level protocols such as TCP and UDP. Later fragments can override header fields such as the source and destination address. This allows attackers to use this technique as a way to infiltrate a network.

Small datagrams, for example, PING requests and replies, passed through the VPN tunnel and firewall successfully. However, larger packets, for example when using Telnet, failed, and ICMP DESTINATION UNREACHABLE messages with a header code of 04 (*Fragmentation needed, but the do not fragment bit was set*) were seen on the line trace. The solution involved changing the MTU sizes for sending and receiving interfaces to a common value (the minimum supported is 576). Because all interfaces on the route supported at least 576 bytes, no fragmentation occurred.

When an IP datagram travels from one host to another, it can cross different physical networks and pass through different routers and links. Each of these may support a different MTU size that limits the maximum size of a datagram that can be placed in one physical frame. Fragmentation is the process that breaks long datagrams into a number of smaller ones and reassembles them at the destination host. If you don't allow fragments, all pieces of the network fabric shouldn't fragment. Otherwise, packets will be lost.

Fragmentation can be used with AH and ESP, but we did not test it here. AH and ESP are only applied to unfragmented packets. However, IP packets can be fragmented by intermediate routers. In this case, the destination first reassembles the packet, and then applies AH or ESP processing to it. If a packet that appears to be a fragment is input to AH or ESP processing, it is discarded. This prevents the *overlapping fragment* attack, which misuses the fragment assembly algorithm to create forged packets and force them through a firewall.

12.2.16 AS14 TCP/IP interfaces and routes configuration

Figure 635 on page 537 shows the TCP/IP interfaces on AS14 that are relevant to this scenario.


```

Work with TCP/IP Interfaces
System: AS14
Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

Internet      Subnet      Line      Line
Opt Address    Mask        Description Type
....
10.6.11.1     255.255.0.0 TRNLINE   *TRLAN
....
127.0.0.1     255.0.0.0   *LOOPBACK *NONE
204.146.18.251 255.255.255.255 *VIRTUALIP *NONE

```

Figure 635. AS14 TCP/IP interfaces - Gateway to gateway through the firewall

Figure 636 shows the TCP/IP routes on AS14 that are relevant to this scenario.

```

Work with TCP/IP Routes
System: AS14
Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display

Route      Subnet      Next      Preferred
Opt Destination Mask        Hop        Interface
....
*DFROUTE   *NONE       10.6.1.1  *NONE
....

```

Figure 636. AS14 TCP/IP routes

12.2.17 AS05 TCP/IP interfaces and routes configuration

Figure 637 shows the TCP/IP interfaces on AS05 that are relevant to this scenario.

```

Work with TCP/IP Interfaces
System: AS05
Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

Internet      Subnet      Line      Line
Opt Address    Mask        Description Type
....
10.196.8.5     255.255.255.0 TRLANC    *TRLAN
127.0.0.1     255.0.0.0   *LOOPBACK *NONE
....
208.222.150.250 255.255.255.248 TRLANB1   *TRLAN

```

Figure 637. AS05 TCP/IP interfaces

Figure 638 on page 538 shows the TCP/IP routes on AS05 that are relevant to this scenario.

```

Work with TCP/IP Routes
System: AS05
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display
Route      Subnet      Next      Preferred
Opt  Destination  Mask      Hop      Interface
....
*DFTROUTE *NONE      208.222.150.249 *NONE

```

Figure 638. AS05 TCP/IP routes

12.2.18 AS20 TCP/IP interfaces and routes configuration

Figure 639 shows the TCP/IP interfaces on AS20 that are relevant to this scenario.

```

Work with TCP/IP Interfaces
System: AS20
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  9=Start  10=End
Internet  Subnet      Line      Line
Opt  Address    Mask      Description  Type
....
10.6.21.1 255.255.0.0 TRNLINE    *TRLAN
....
127.0.0.1 255.0.0.0  *LOOPBACK *NONE

```

Figure 639. AS20 TCP/IP interfaces

Figure 640 shows the TCP/IP routes on AS20 that are relevant to this scenario.

```

Work with TCP/IP Routes
System:S20
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display
Route      Subnet      Next      Preferred
Opt  Destination  Mask      Hop      Interface
....
10.196.8.0 255.255.255.0 10.6.11.1 *NONE
208.222.150.250 *HOST      10.6.11.1 *NONE

```

Figure 640. AS20 TCP/IP routes

12.2.19 Router configuration

The router that connects the corporate office to the Internet must have a static route to the network 204.146.18.248, with mask 255.255.255.248, or to the host 204.146.18.251. This route is used to route datagrams to the AS/400 VPN server behind the firewall with *VIRTUALIP address 204.146.18.251.

The next hop for this route must be the firewall non-secure port as shown in Figure 641.

Generic router configuration		
Route	Subnet	Next
Destination	Mask	Hop
204.146.18.248	255.255.255.248	204.146.18.226

Figure 641. Corporate router static route

12.2.20 PC07 TCP/IP configuration

The TCP/IP properties on PC07 are defined as follows:

- **IP address:** 10.196.8.4
- **Subnet mask:** 255.255.255.0
- **Default gateway:** 10.196.8.5

12.2.21 Firewall configuration

Figure 642 shows the TCP/IP ports configured in the firewall used during our tests for this scenario.

Display Network Server Desc				AS8
Network server description				FW8V44B
Option				*TCP/IP
TCP/IP port configuration				
-----TCP/IP port configuration-----				
	Internet	Subnet		Maximum
Port	address	mask		transmission
				unit
1	10.6.1.1	255.255.0.0		1500
2	204.146.18.226	255.255.255.248		1500
*INTERNAL	192.168.3.34	255.255.255.0		15400

Figure 642. FW8V44B TCP/IP ports

Figure 643 on page 540 shows the TCP/IP routes configured in the firewall used during our tests for this scenario.

```

Display Network Server Desc                               AS8
Network server description . . . . . : FW8V44B
Option . . . . . : *TCPIP
TCP/IP route configuration . . . . . :

-----TCP/IP route configuration-----
Route          Subnet          Next
destination    mask             hop
*DFTRROUTE     *NONE           204.146.18.225
204.146.18.251 *HOST           10.6.11.1

```

Figure 643. FW8V44B TCP/IP routes

12.3 Remote access to an AS/400 VPN gateway behind a firewall

This section pulls together information from Chapter 10, “Secure remote access for PC clients over the Internet” on page 419, and from all previous sections in this chapter. There is no new information added here. Concepts that were already discussed in previous sections of this redbook are presented in this section’s example. This section does not document the sample scenario step-by-step, but presents configuration summaries.

Figure 644 shows remote PC clients accessing the corporate AS/400 VPN server over the Internet. This is the same scenario as the one discussed in Chapter 10, “Secure remote access for PC clients over the Internet” on page 419, The only difference is that now there is a firewall in front of the AS/400 VPN gateway.

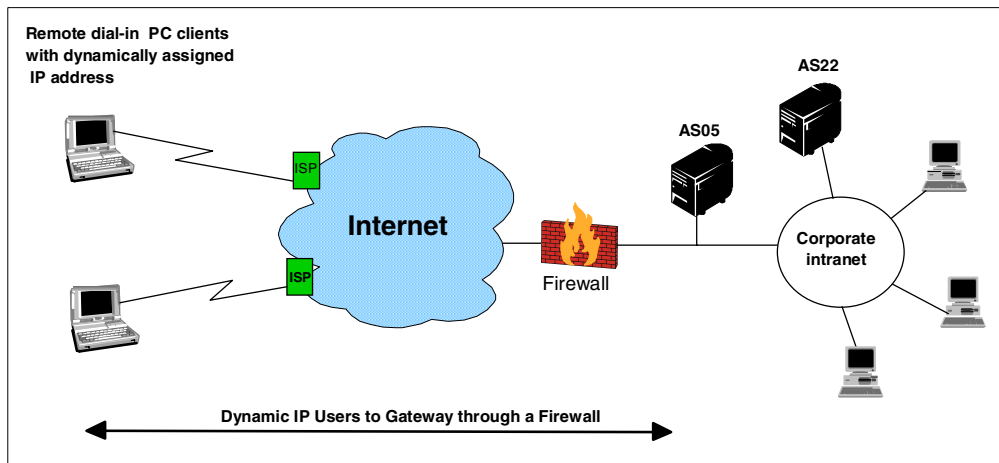


Figure 644. Remote clients access to AS/400 VPN gateway through a firewall - Scenario overview

The characteristics and objectives of this scenario are the same as in Chapter 10, “Secure remote access for PC clients over the Internet” on page 419. The differences in this section are:

- The corporate network is connected to the Internet through a firewall.
- The AS/400 VPN gateway is connected to the firewall secure port and to the corporate intranet through the same physical line. The single line on AS05 shares VPN traffic and corporate intranet traffic.

12.3.1 Scenario test network

Figure 645 shows the test network used in this scenario.

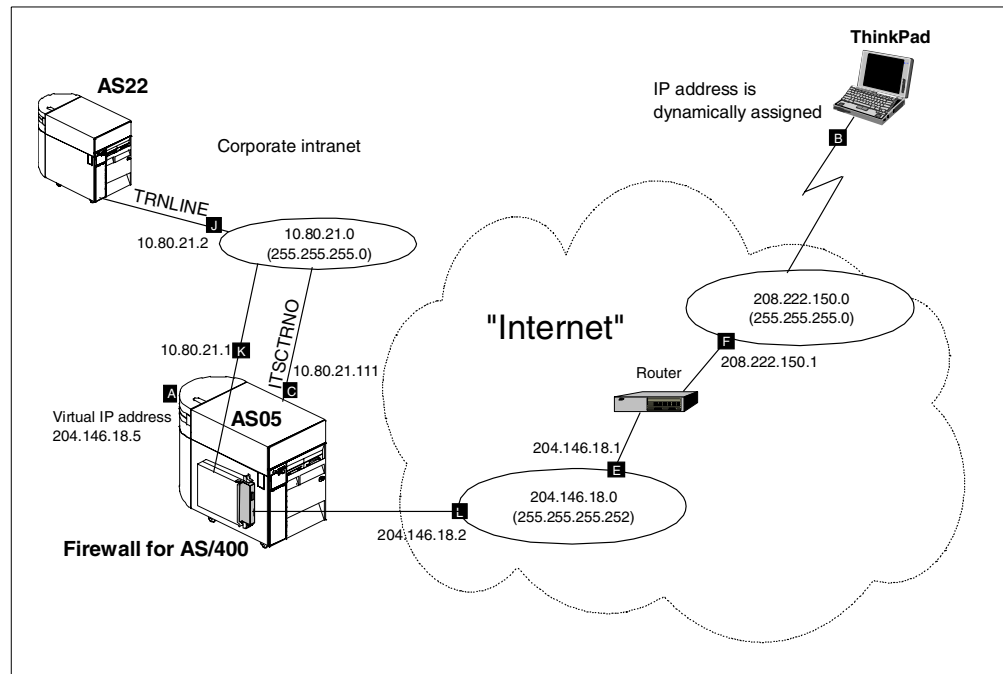



Figure 645. Remote client access to AS/400 VPN gateway - Scenario test network

The characteristics of the test network are:

- AS05 is an AS/400 system running OS/400 V4R4. AS05 represents the corporate office VPN server.
- AS05 is connected to the corporate office intranet through the physical interface ITSCTRNO and IP address 10.80.21.111 **C**.
- AS05 is assigned a public IP address (204.146.18.5 subnet mask 255.255.255.252 **A**). This IP address is configured as a Virtual IP address on AS05 and is used to route all the VPN traffic that traverses the firewall to be processed by the VPN server (AS05).
- AS05 is an AS/400 system with an Integrated Netfinity Server (previously known as Integrated PC Server or IPCS) running IBM Firewall for AS/400 V4R4.
- The secure port of the firewall is connected to the corporate office intranet with IP address 10.80.21.1 **K**.
- The non-secure port of the firewall is connected to the *Internet* with IP address 204.146.18.2 **L**.
- ThinkPad is a remote dial-in client with IPSec support. Refer to Chapter 10, “Secure remote access for PC clients over the Internet” on page 419, for information on Windows VPN clients and configuration details.
- The dial-in client (ThinkPad) is dynamically assigned an IP address by the ISP. In our test network, the randomly assigned IP addresses are from the pool 208.222.150.0, with mask 255.255.255.0 **B**.

- AS22 is an AS/400 system running standard TCP/IP applications. VPN functions are not configured on this system. It represents a generic TCP/IP host in the corporate network. For all practical purposes, it does not support VPN. AS22 is connected to the corporate intranet through line TRNLINE and IP address 10.80.21.2 .
- At the corporate office, the network administrator assigns a portion of a class C network to connect to the Internet. The corporate office DMZ is assigned the network address 204.146.18.0, with subnet mask 255.255.255.252.
- The corporate office uses the subnet 10.80.21.0, with subnet mask 255.255.255.0 in its intranet. This subnet represents the data endpoint of the VPN tunnel at the corporate office site.

12.3.2 Subnetting considerations

In this scenario, we assume that the ISP assigns to the corporate office the network address 204.146.18.0, with a subnet mask of 255.255.255.248. This is a network of six hosts (addresses that have all 0s or all 1s are special cases and cannot be used). The assigned address range can be subdivided into two networks of two hosts each, using a mask of 255.255.255.252 as follows:

- Network: 204.146.18.0 Hosts: 204.146.18.1 to 2, that is 2 hosts
- Range of host IP addresses Hosts: 204.146.18.4 to 5, that is 2 hosts

The 204.146.18.0 subnet is used between the non-secure port of the firewall and the external network router. You can use any of the hosts IP addresses as a virtual IP as explained in 12.2.6, “Virtual IP addressing and routing: VPN gateway behind a firewall” on page 520.

Note: The individual host addresses do not need to be contiguous. They can be any disjointed set of addresses (or only one), as long as they are not in the same network as the DMZ.

A routing entry must be added to the firewall to route traffic for the 204.146.8.5 virtual IP address to the physical IP interface 10.80.21.111. The router must also have a routing entry for the 204.146.8.5 IP address that routes the traffic to the firewall non-secure port at 204.146.18.2.

12.3.3 Virtual IP and routing: Access to VPN gateway behind a firewall

Figure 646 on page 543 shows the technique used here to route IPSec traffic through the firewall to the AS/400 VPN server, AS05, on the secure network. It uses virtual IP addresses to avoid creating a separate physical network between AS05 and the firewall.

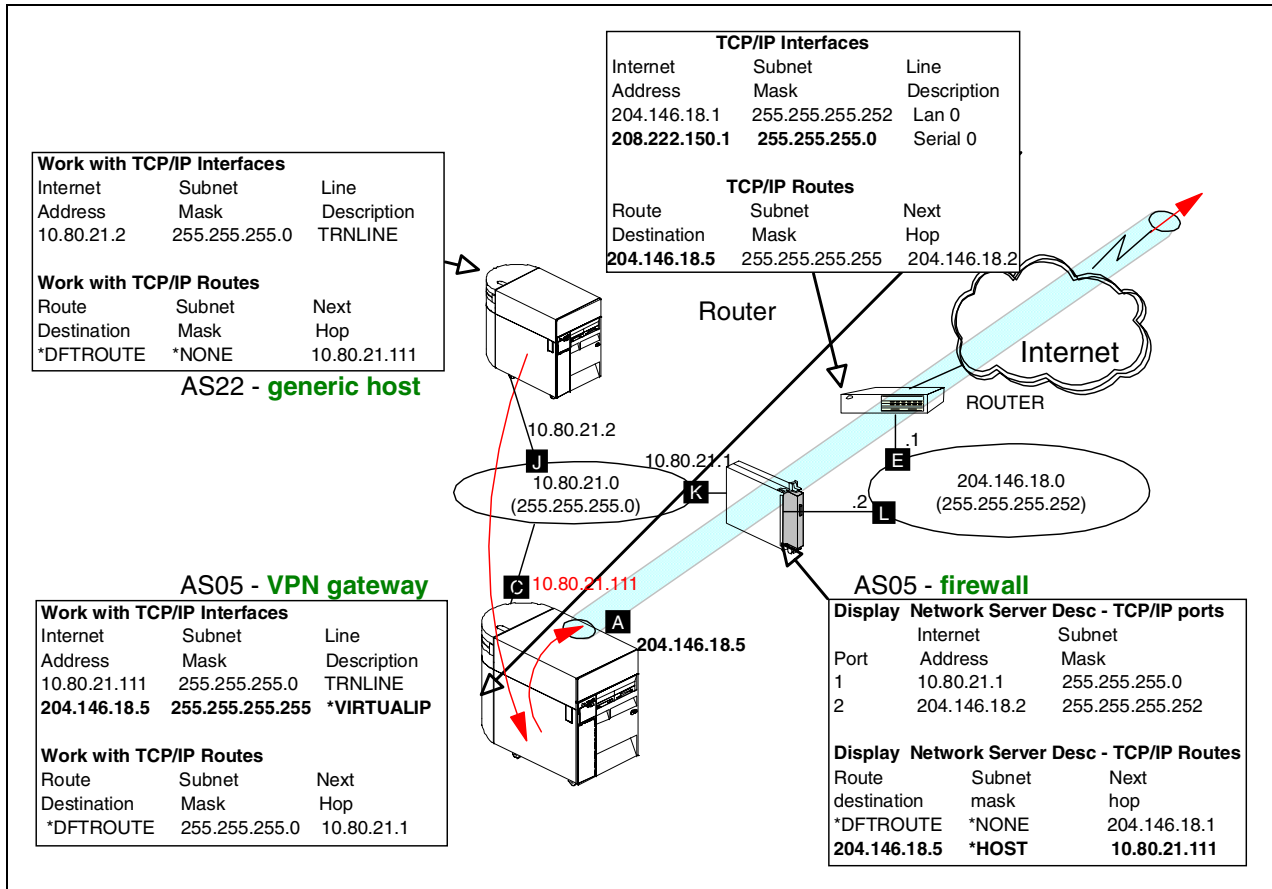


Figure 646. AS/400 VPN gateway behind the firewall - IP addressing and routing remote access

The technique shown in Figure 646 is explained in 12.2.6, "Virtual IP addressing and routing: VPN gateway behind a firewall" on page 520.

12.3.4 Firewall configuration summary

Figure 647 on page 544 shows IBM Firewall for AS/400 installation summary page.

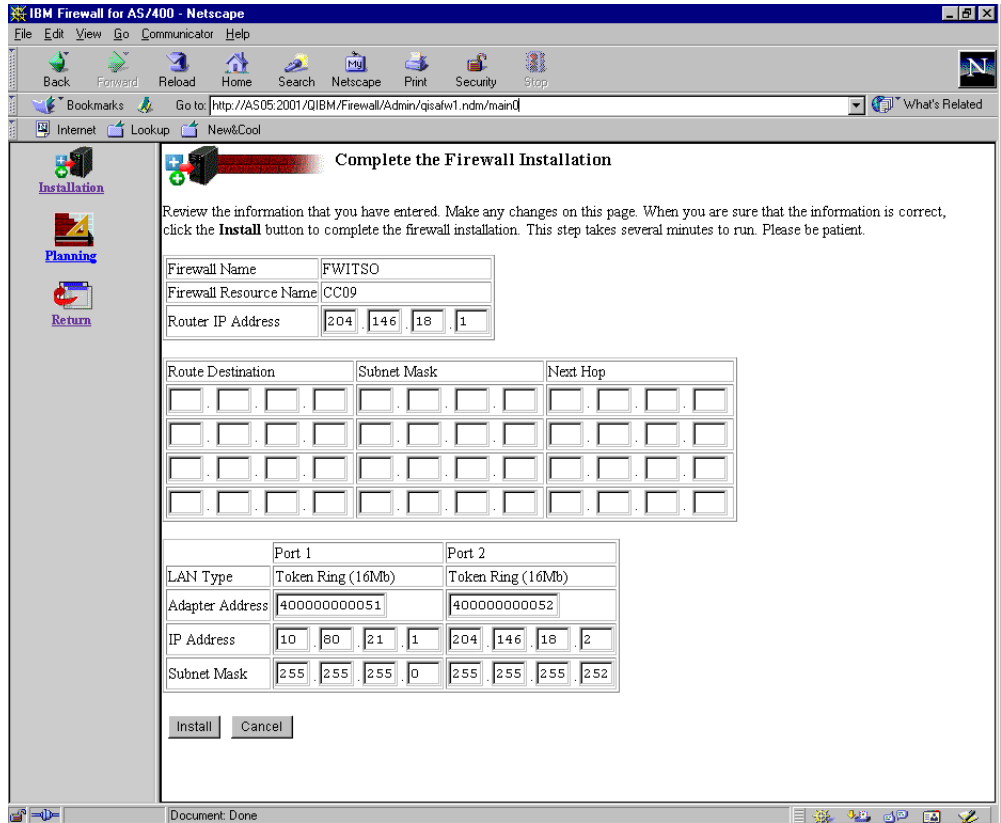


Figure 647. Firewall installation summary - Remote access to a VPN gateway behind the firewall

Notice the IP addresses assigned to the secure port (10.80.21.1, with subnet mask 255.255.255.0) and non-secure port (204.146.18.2, with subnet mask 255.255.255.252).

Figure 648 shows the TCP/IP ports configured in the firewall used during our tests for this scenario.

```

Display Network Server Desc                               AS05

Network server description . . . . . : FWITSO
Option . . . . . : *TCPIP
TCP/IP port configuration . . . . . :

-----TCP/IP port configuration-----

Port          Internet          Subnet          Maximum
              address         mask            transmission
              10.80.21.1      255.255.255.0  unit
1             10.80.21.1      255.255.255.0  1500
2             204.146.18.2   255.255.255.252 1500
*INTERNAL    192.168.9.2    255.255.255.0  15400

```

Figure 648. FWITSO Firewall TCP/IP ports

Figure 649 on page 545 shows the TCP/IP routes configured in the firewall used during our tests for this scenario.


```
Display Network Server Desc AS05
Network server description . . . . : FWITSO
Option . . . . . : *TCPIP
TCP/IP route configuration . . . . :

-----TCP/IP route configuration-----
Route          Subnet          Next
destination    mask            hop
*DFROUTE      *NONE          204.146.18.1
204.146.18.5  *HOST          10.80.21.111
```

Figure 649. FWITSO Firewall TCP/IP routes

12.3.4.1 Configuring firewall filters to permit IPSec protocols

The filters for the remote access to a VPN gateway behind the firewall scenario are similar to those described in 12.2.8, “Configuring the firewall to permit IPSec protocols” on page 522. The difference is that, in the remote access scenario, the dial-in client is dynamically assigned an IP address. For this reason, the remote IP address that represents the dial-in clients must be a wildcard (*).

Opening the firewall to IPSec protocols does not represent a security exposure, since the IPSec protocols themselves guarantee authentication of the remote partner.

Figure 648 on page 544 shows the filter rules added to the firewall in this scenario to allow IPSec protocols through it.

```

#
# #####
# Filters added to permit IPSEC tunnel though Firewall. Local AS/400 VPN gateway has IP address of 204.146.18.5,
# remote client
# has address dynamically assigned
# #####
#
0008:action(permit) from(204.146.18.5) to(0.0.0.0) protocol(udp eq 500/eq 500) interface(secure)
routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit IKE Exchanges")
0009:action(permit) from(204.146.18.5) to(0.0.0.0) protocol(udp eq 500/eq 500) interface(non-secure)
routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit IKE exchange")
0010:action(permit) from(0.0.0.0) to(204.146.18.5) protocol(udp eq 500/eq 500) interface(non-secure)
routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit IKE exchange")
0011:action(permit) from(0.0.0.0) to(204.146.18.5) protocol(udp eq 500/eq 500) interface(secure)
routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit IKE exchange")
#
0012:action(permit) from(204.146.18.5) to(0.0.0.0) protocol(ah any 0/any 0) interface(secure) routing(route)
direction(inbound) fragment(y) log(y) VPN(0) description(" Permit AH tunnel")
0013:action(permit) from(204.146.18.5) to(0.0.0.0) protocol(ah any 0/any 0) interface(non-secure) routing(route)
direction(outbound) fragment(y) log(y) VPN(0) description(" Permit AH tunnel")
0014:action(permit) from(0.0.0.0) to(204.146.18.5) protocol(ah any 0/any 0) interface(non-secure) routing(route)
direction(inbound) fragment(y) log(y) VPN(0) description(" Permit AH tunnel")
0015:action(permit) from(0.0.0.0) to(204.146.18.5) protocol(ah any 0/any 0) interface(secure) routing(route)
direction(outbound) fragment(y) log(y) VPN(0) description(" Permit AH tunnel")
#
0016:action(permit) from(204.146.18.5) to(0.0.0.0) protocol(esp any 0/any 0) interface(secure) routing(route)
direction(inbound) fragment(y) log(y) VPN(0) description(" Permit ESP tunnel")
0017:action(permit) from(204.146.18.5) to(0.0.0.0) protocol(esp any 0/any 0) interface(non-secure) routing(route)
direction(outbound) fragment(y) log(y) VPN(0) description(" Permit ESP tunnel")
0018:action(permit) from(0.0.0.0) to(204.146.18.5) protocol(esp any 0/any 0) interface(non-secure) routing(route)
direction(inbound) fragment(y) log(y) VPN(0) description(" Permit ESP tunnel")
0019:action(permit) from(0.0.0.0) to(204.146.18.5) protocol(esp any 0/any 0) interface(secure) routing(route)
direction(outbound) fragment(y) log(y) VPN(0) description(" Permit ESP tunnel")
#
#####

```


Figure 650. Remote access to a VPN gateway behind a firewall - Filter rules added to firewall to permit IPSec protocols

12.3.5 AS/400 VPN gateway behind a firewall: IP filters summary

Table 58 shows the planning worksheet to gather the information you need to create the IP filters on AS05 for this scenario.

Table 58. AS05 IP filter rules - Planning worksheet

This is the information you need to create your IP filters to support your VPN	Scenario answers
<p>Is <i>your</i> VPN server acting as a host or gateway?</p> <p>Is the data endpoint the same as the authentication or encryption endpoint?</p> <p>If yes, your VPN server acts as a host.</p> <p>If no, your VPN server acts as a gateway.</p>	Gateway
<p>Is the <i>remote</i> VPN server acting as a host or gateway?</p>	Host
<p>What name do you want to use to group together the set of filters that will be created?</p>	VPNIFC
<p>If <i>your</i> server is acting as a gateway...</p> <ul style="list-style-type: none"> – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? <p>Use this name as the <i>source address</i> on the IPSEC filter.</p>	<p>10.80.21.0</p> <p>255.255.255.0</p> <p>Corporate</p>

This is the information you need to create your IP filters to support your VPN	Scenario answers
If the <i>remote</i> server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound IKE filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	204.146.18.5 
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	Dynamically assigned
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	ITSCTRNO
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	All 10.80.21.* addresses All protocols All ports

The IP filters in the VPN gateway behind the firewall in this scenario are almost the same as those configured in 10.1.9, “Configuring IP filters on the AS/400 system (AS05)” on page 430. The only difference is that, in the current scenario, the same physical interface in the VPN gateway is shared by VPN and intranet traffic. For this reason, you must configure an additional filter rule to permit traffic to and from the internal network over the single physical interface.

Figure 651 shows the IP filters configured in AS05 for this scenario.

```

#Corporate internal network
ADDRESS securenet IP = 10.80.21.0 MASK = 255.255.255.0 TYPE = TRUSTED
FILTER_INTERFACE LINE = ITSCTRNO SET = DynIP
#IKE negotiations
FILTER SET DynIP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.5 DSTADDR = * PROTOCOL
= UDP DSTPORT = 500 SRCPOR = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET DynIP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = 204.146.18.5 PROTOCOL =
UDP DSTPORT = 500 SRCPOR = 500 FRAGMENTS = NONE JRN = OFF
#Permit internal network traffic
FILTER SET DynIP ACTION = PERMIT DIRECTION = * SRCADDR = securenet DSTADDR = securenet PROTOCOL = * DSTPORT
= * SRCPOR = * FRAGMENTS = NONE JRN = OFF
#VPN traffic
FILTER SET DynIP ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = securenet DSTADDR = * PROTOCOL = * DSTPORT
= * SRCPOR = * FRAGMENTS = NONE JRN = OFF CONNECTION_DEFINITION = DYNAMICIP
#Permit VPN traffic in and out of the VPN server to the internal network
FILTER SET DynIP ACTION = PERMIT DIRECTION = * SRCADDR = * DSTADDR = * PROTOCOL = *
DSTPORT = * SRCPOR = * FRAGMENTS = NONE JRN = OFF

```

Figure 651. AS/400 VPN gateway behind the firewall - IP filters configuration

Tip

The order of the filter rules is important. The rule that permits inbound and outbound traffic from the internal network must be placed before the IPSEC rule to avoid internal traffic being processed by the IPSEC filter rule.

The last filter rule is required to route packets from the remote clients to the internal network and vice versa.

The VPN configuration on AS05 is the same as the one described in 10.1.8, “Configuring Gateway to Dynamic IP Users VPN on AS05” on page 424.

Figure 652 shows a communication trace taken over line ITSCTRNO on AS05. The figure shows the flow of a datagram from the remote client (ThinkPad) to AS22 and the response from AS22 to the remote client. The trace shows the following sequence of events:

1. Packet 452 is received (R) from the remote client (Src Addr 208.222.150.4) by the VPN server. The destination address is the *VIRTUALIP address defined in AS05 (Dest Addr 204.146.18.5). The packet is encrypted. Protocol is ESP.
2. Packet 458 shows the same packet being sent (S) over the line to AS22 (Dest Addr 10.80.21.2). The packet is in the clear. Protocol is TCP, and you can see the information in the packet.
3. Packet 459 is received (R) by the VPN server (AS05) from AS22 (Src Addr 10.80.21.2) with the destination of the remote client (Dest Addr 208.222.150.4). The packet is in the clear. It has not been processed by IPSEC yet.
4. Packet 460 shows the same packet being sent (S) by the VPN server (Src Addr 204.146.18.5) to the remote client (Dest Addr 208.222.150.4). The packet is encrypted. Protocol is ESP.

The routing is determined by the routing configuration on each system as shown in Figure 646 on page 543.

```

452 R      109      1068.8          400000011005 C00000000051 LLC UI
Routing Info . : 02F0
Frame Type : IP          TOS: NORMAL          Length: 104 Protocol: ESP
                        Src Addr: 208.222.150.4  Dest Addr: 204.146.18.5  Fragment Flags: MAY ,LAST
SNAP Header: 0000000800
IP Header : 45000068001200001E3256D8D0DE9604CC921205
IP Options : NONE
ESP header : SPI: 'FF91C6CD'X SNF: 18
Data . . . . . : 0C4821453DCCE15 19E577D69E93E9DE 940942386512093F B583F8A988266CF5 *. . . . .V.O. . . .
                  F1ECAAFD1F792F80 F18E039E28BFF777 C2FCE5CAD4276581 7F4A0A486DF794A0 *1. . . . .1. . . . .
                  DE7D45829230A69F 082F9EDA *. . . . .BK.W. . . . .

458 S      61      1063.8          0020357A1ECC C00000011005 LLC UI
Routing Info . : 0270
Frame Type : IP          TOS: NORMAL          Length: 56 Protocol: TCP
                        Src Addr: 208.222.150.4  Dest Addr: 10.80.21.2  Fragment Flags: DON'T
SNAP Header: 0000000800
IP Header : 450000386F0240001F066689D0DE96040A501502
IP Options : NONE
TCP . . . . : Src Port: 1027,Unassigned  Dest Port: 21,FTP
                SEQ Number: 22497757 ('015749DD'X) ACK Number: 1047320398 ('3E6CD74E'X)
                Code Bits: ACK PSH Window: 5717 TCP Option: NONE
TCP Header : 04030015015749DD3E6CD74E50181655446B0000
Data . . . . . : 73697465206E616D 65666D7420310D0A * . . . . .>/_ . . . .

459 R      80      1063.8          400000011005 8020357A1ECC LLC UI
Routing Info . : 02F0
Frame Type : IP          TOS: NORMAL          Length: 75 Protocol: TCP
                        Src Addr: 10.80.21.2  Dest Addr: 208.222.150.4  Fragment Flags: DON'T
SNAP Header: 0000000800
IP Header : 4500004B3C0C40004006786C0A501502D0DE9604
IP Options : NONE
TCP . . . . : Src Port: 21,FTP  Dest Port: 1027,Unassigned
                SEQ Number: 1047320398 ('3E6CD74E'X) ACK Number: 22497773 ('015749ED'X)
                Code Bits: ACK PSH Window: 8192 TCP Option: NONE
TCP Header : 001504033E6CD74E015749ED5018200099EF0000
Data . . . . . : 32353020204E6F77 207573696E67206E 616D696E6720666F 726D617420223122 * . . . . .+? . . . . .
                  2E0D0A * . . . .

460 S      133      1063.8          400000000051 C00000011005 LLC UI
Routing Info . : 0270
Frame Type : IP          TOS: NORMAL          Length: 128 Protocol: ESP D
                        Src Addr: 204.146.18.5  Dest Addr: 208.222.150.4  Fragment Flags: DON'T,
SNAP Header: 0000000800
IP Header : 450000803C0C40003E32BAC5CC921205D0DE9604
IP Options : NONE
ESP header : SPI: '5D17A58A'X SNF: 10
Data . . . . . : FB8DD4A7DD6E8DED 0F3320368CE2CCCC FCA793048EC18F52 17BE8E0074B941DA * . . . . .MX. > . . . . .S
                  E4CB69BD703C4F50 0E5697F2E61F90AA 8D8435B54C1338B5 E028D40D436EE77D *U. . . . .|&. . . . .P2W.
                  D4E5FA2EEDA095BA F7643711D10D5F05 F45E5CBF06291F1A 6DFF782113548319 *MV. . . . .N. 7. . . . .J.
                  D969828D *R.B.

```

Figure 652. Communication trace on AS05 ITSCTRNO line

12.4 L2TP considerations

In L2TP tunnels protected by IPSec, the outer headers include IPSec protocols, as explained in Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263 and Chapter 9, “L2TP compulsory tunnel” on page 351. Therefore, there is basically no difference in the firewall filters configuration to allow L2TP tunnels protected by IPSec to flow through it. You must open the filters to the IPSec protocols IKE (protocol UDP port 500), AH, and ESP as shown in the previous sections of this chapter.

Only the range of IP addresses configured for the clients may raise some questions. This section explores the special considerations for each L2TP tunnel type.

12.4.1 Firewall filters for L2TP voluntary tunnel protected by IPSec

In the voluntary tunnel scenario discussed in Chapter 7, “L2TP host-to-gateway voluntary tunnel” on page 263, and Chapter 8, “L2TP gateway-to-gateway voluntary tunnel” on page 323, the remote client is assigned IP addresses dynamically. The client IP addresses must be a wildcard (*). The filter configurations are the same as those shown in 12.3.4.1, “Configuring firewall filters to permit IPSec protocols” on page 545, in the remote access to a VPN gateway.

12.4.2 Firewall filters for L2TP compulsory tunnel protected by IPSec

In the compulsory tunnel scenario discussed in Chapter 9, “L2TP compulsory tunnel” on page 351, the L2TP tunnel between the LNS (L2TP Network Server) and the ISP is authenticated with the IPSec protocol AH. Therefore, the same filters apply as those described in 12.3.4.1, “Configuring firewall filters to permit IPSec protocols” on page 545.

If the L2TP tunnel is not authenticated with AH, the IPSec headers do not wrap the L2TP packet. In this case, you must open the firewall filters to L2TP. L2TP uses protocol UDP, port 1701 on the LNS, and wildcard (any port) on the initiator.

Note: The AS/400 system as an L2TP initiator uses protocol UDP port 1701.

Chapter 13. VPN Network Address Translation (VPN NAT)

There are some cases where it may be desirable or necessary to translate the original IP address of hosts that participate in a VPN connection. The main reasons for address translation are:

- Both networks that need to communicate over the VPN use private IP address and they collide.
- You don't fully trust your VPN partner and want to hide your internal network IP address information.

Conventional Network Address Translation (NAT), allows you to translate one IP address into another IP address. NAT allows you to connect two private networks with incompatible addressing structures or hide addresses in a subnetwork from a less trusted network. NAT is one of the TCP/IP security components that the AS/400 packet security feature provides since V4R3.

Unfortunately, conventional NAT cannot be used with IPSec protocols, because:

- In tunnel mode, ESP encrypts the inner IP addresses. Therefore, they cannot be translated by NAT.
- AH authenticates inner and outer IP addresses. Therefore, they cannot be translated.
- Even in transport mode, where ESP does not encrypt nor authenticates the IP addresses, the Security Associations (SAs) are defined in terms of the destination IP address. Therefore, it cannot be changed.

AS/400 VPN provides a unique solution that is its own version of NAT, called Virtual Private Network Network Address Translation (VPN NAT), to support successful VPN connection configuration.

This chapter explores the use of VPN NAT through two practical scenarios:

- Scenario 1 discusses resolving IP address conflicts in a VPN connection (see the following section).
- Scenario 2 is presented in 13.4, "Hiding IP addresses from your VPN partner: VPN NAT for servers" on page 584.

13.1 Resolving IP address conflicts in a VPN connection

VPN NAT can be used to resolve IP address conflicts between networks that need to communicate over a VPN but they use private IP addresses and they collide.

To understand the problem, refer to Figure 653 on page 553. The figure shows two networks: network A (10.196.0.0, with mask 255.255.0.0), and network B (10.196.8, with mask 255.255.255.0). Network A is divided into two subnets: network A1 (10.196.11.0, with mask 255.255.255.0), and network A2 (10.196.8.0, with mask 255.255.255.0). This address scheme raises two problems:

- It is not possible to exchange IP datagrams between network B and Network A1. A packet sent from network A1 with destination IP address 10.196.8.* and mask 255.255.255.0 is always routed to the local network A2 even if it is meant for network B. This problem can be solved by configuring VPN NAT

either on the manufacturer's AS/400 gateway (AS14) or on the distributor's (AS05).

- It is not possible to exchange datagrams between network A2 and network B. In both cases, packets with destination IP address 10.196.8.* and mask 255.255.255.0 are always routed to a local host. This address conflict *cannot* be resolved.

Note

VPN NAT can solve address collision problems that arise when one of the network's address space is a subset of the other one. However, hosts in exact-match subnets cannot communicate with each other even after configuring VPN NAT.

To enable communication between network A1 and network B, you can configure VPN NAT either on AS14 or on AS05. If you configure VPN NAT on AS14, network B's *source* IP address is translated on *inbound* traffic to prevent collisions with network A2's IP addresses. This configuration is called *source inbound*, and AS14 must be the responder of the VPN connection.

If you configure VPN NAT on AS05, network B's *source* IP address is translated on *outbound* traffic to prevent collisions with network A2's IP addresses. This configuration is called *source outbound*, and AS05 must be the initiator of the VPN connection.

VPN NAT is an AS/400-unique solution. In the network presented in Figure 653 on page 553, we can choose to configure VPN NAT on either end of the VPN since both VPN gateways are AS/400 systems. In a more general environment, you may be forced to configure VPN NAT to resolve address collisions on the end of the VPN where an AS/400 system is installed.

This scenario shows how to configure VPN NAT source inbound on AS14 and source outbound on AS05. Naturally, only one of the two methods should be implemented in a real network.

13.1.1 Scenario characteristics

The characteristics of this scenario are:

- Network A is a Class A network with a 16-bit subnet mask creating the address space of 10.196.0.0. This network is further divided into two subnetworks: network A1 and A2 with a 24-bit subnet mask.
- Network B is a Class A network with a 24-bit subnet mask creating the address space of 10.196.8.0.
- Network B's address space is a subset of network A's address space.
- Both networks have assigned their internal hosts IP address out of the 10.196.8.0 subnet address space as shown Figure 653 on page 553. This is not a problem until both networks are connected.
- The collision between network A2 and network B address space makes it impossible to route traffic between hosts in network A1 and network B.

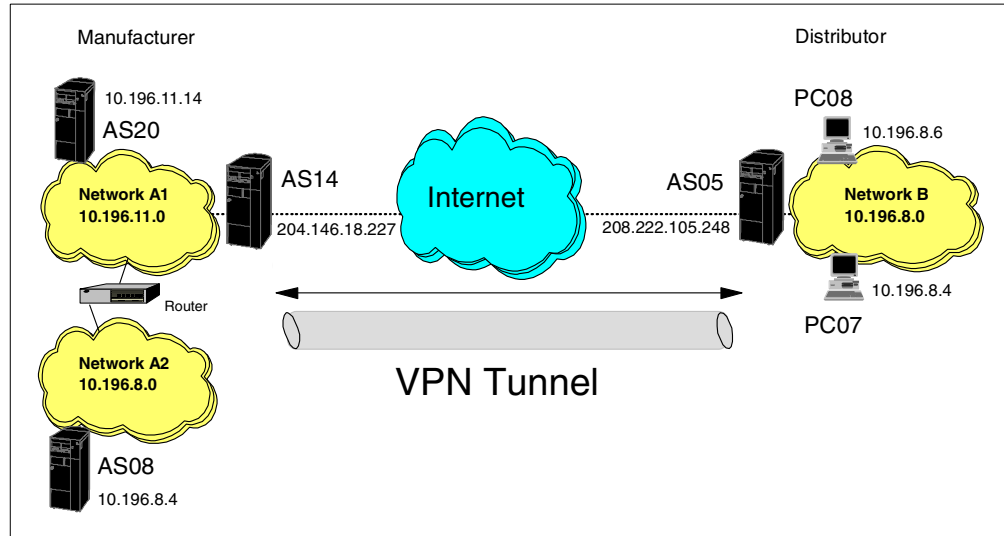


Figure 653. Connecting networks with colliding IP address space

13.1.2 Scenario objectives

The objectives of this scenario are:

- Allow all hosts in network B access to all hosts in network A1. Network A1's hosts cannot start TCP/IP connections on network B1 because the public addresses of network B's clients are *randomly* assigned from the VPN NAT pool.

Note: Since you must configure a single VPN connection for each single address that is translated, this requires you to configure one Dynamic Key Connection (:L connections) on AS05 for each host on network B with a maximum of up to 255 connections.

- Resolve IP address and routing conflicts caused by collisions between Network B and subnetwork A2 address spaces using VPN NAT.

Note: As explained in 13.1, “Resolving IP address conflicts in a VPN connection” on page 551, VPN NAT cannot resolve collisions between two subnetworks whose address spaces match exactly. In this scenario, hosts in network B cannot communicate with hosts in network A2 over the VPN connection.

13.2 VPN NAT source inbound implementation (AS14)

This section describes the tasks that you must perform to configure a gateway-to-gateway scenario where one of the AS/400 VPN servers (AS14) is configured to support VPN NAT source inbound.

13.2.1 Scenario network configuration

Figure 654 on page 554 shows our simple network configuration for this scenario.

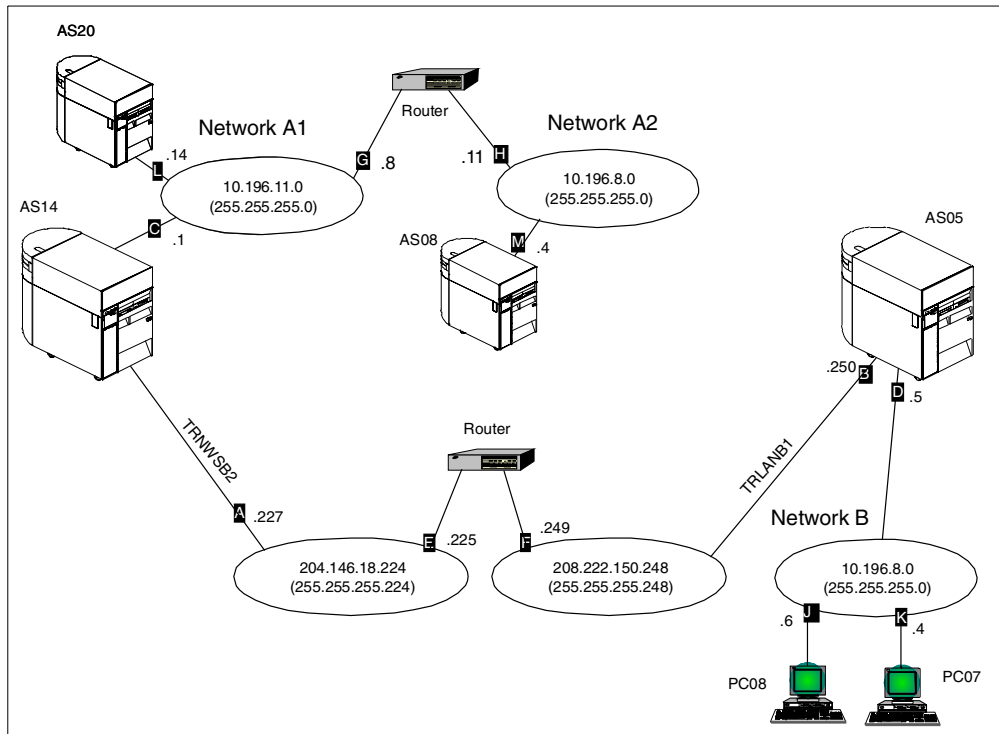


Figure 654. Gateway to gateway - VPN NAT source inbound

The test network has the following characteristics:

- AS14 is the VPN gateway for network A. VPN NAT source inbound is configured on this AS/400 system.
- AS20 represents hosts on network A1 (10.196.11.0, with mask 255.255.255.0) that communicate over the VPN with hosts on network B.
- AS08 represents hosts on network A2. AS08 cannot communicate with hosts on network B.
- PC07 and PC08 represent hosts on network B that can communicate with hosts on network A1.
- The addresses chosen for VPN NAT (192.168.1.* in this scenario) must be globally unique and routable within the private network (network A1).
- Even though this is a gateway-to-gateway VPN, you must set up a separate dynamic key connection for each client in network B that needs to access network A1. The filter rules can be subnets as shown in this scenario.

13.2.2 Task summary

Complete the following tasks to implement the gateway-to-gateway VPN with VPN NAT source inbound:

1. Verify TCP/IP routing before implementing the VPN connection.
2. Configure VPN on the network A's gateway AS/400 system (AS14).
3. Configure VPN NAT source inbound on AS14.
4. Configure IP filtering on AS14 (refer to the VPN connection group configured in the previous steps).

5. Configure VPN on the network B's gateway AS/400 system (AS05).
6. Make configuration changes to the base VPN configuration objects created by the wizard on AS05.
7. Configure IP filtering on AS05 (refer to the VPN connection group configured in the previous steps).
8. Start VPN servers.
9. Activate filters.
10. Start the VPN connections from the initiator AS05.

13.2.3 Verifying TCP/IP routing

Defining basic TCP/IP routing is beyond the scope of this document. However, it is vital that routing be configured and tested before attempting to implement a VPN connection. Because you will likely use data encryption under VPN (which, by design, means line traces cannot be fully interpreted), problem determination can be particularly difficult if you have not established routes beforehand.

In the case of the Internet, your gateway AS/400 systems must be able to communicate with each other using public addresses. However, if you are using private network addresses on your local networks, these will not route across the Internet. Therefore, you must configure local routing so that any request for the remote network routes to the gateway AS/400 systems.

Note: You cannot test end-to-end routing until you have established the VPN tunnel.

Tip

Rather than adding routing information to all hosts (including PC clients) that use the VPN tunnel, it may be possible to make the VPN gateway AS/400 the default TCP/IP gateway. Alternatively, if you use routers on the local network, you may only need to add the necessary routing information once to a suitable router.

Table 59 summarizes the routes configured on AS14 for our test scenario.

Table 59. VPN gateway: AS14 routes

Destination network	Next hop
*DFTRROUTE	204.146.18.225 (E) - the 'Internet' router

Table 60 summarizes the routes configured on AS20 for our test scenario.

Table 60. AS20 routes

Destination network	Next hop
*DFTRROUTE	10.196.11.1 (C) - AS14
10.196.8.0 255.255.255.0	10.196.11.8 (G)

Table 61 summarizes the routes configured on AS08 for our test scenario.

Table 61. AS08 routes

Destination network	Next hop
*DFTRROUTE	10.196.8.11 (H) - Internal router

Table 62 summarizes the routes configured on AS05 for our test scenario.

Table 62. VPN gateway AS05 routes

Destination network	Next hop
*DFTRROUTE	208.222.150.249 (F) - the 'Internet' router

Table 63 summarizes the routes configured on PC08 for our test scenario.

Table 63. PC08 routes

Destination network	Next hop
*DFTRROUTE	10.196.8.5 (D) - AS05

13.2.4 Completing the planning worksheets for AS14

Complete the planning worksheets to gather the information you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 64 shows the wizard configuration planning worksheet for this scenario from the perspective of the VPN gateway at the manufacturer's network (AS14).

Table 64. AS14 New Connection Wizard planning worksheet

This is the information you need to create the VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Gateway to Host – Gateway to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	SourceInbound14to05
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	204.126.18.227 (A)
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	208.222.150.250 (B)
What is the pre-shared key?	28oey94w3w
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

This is the information you need to create the VPN with the New Connection Wizard	Scenario answers
Is this AS/400 system resolving IP address conflicts?	Yes
Are the address being translated in the local network? – Yes. Configure VPN NAT source outbound. – No. Configure VPN NAT source inbound.	Responder
What is the VPN NAT address pool?	192.168.1.1 - 192.168.1.254

To complete the VPN configuration, you must configure IP filters. Table 65 shows the IP filter rules configuration planning worksheet for this scenario from the perspective of the VPN gateway at the manufacturer's network (AS14).

Table 65. AS14 Planning worksheet - IP filter configuration

This is the information you need to create the IP filters to complete the VPN with VPN NAT source inbound	Scenario answers
What name do you want to use to group together the set of filters that will be created?	VPNIFC
– What is the Network address of the <i>local</i> network that can use the VPN tunnel? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	10.196.0.0 255.255.0.0 AS14subnets
– What is the IP address of the <i>remote</i> network that can use the VPN tunnel? If the remote system is resolving the address conflict and is using Source Outbound, this is the IP address range of the NAT pool. – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	10.196.8.0 255.255.255.0 AS05subnets
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	204.146.18.227 (A)
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	208.222.150.250 (B)
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRNWSB2
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

Note: The IP addresses of the data endpoints (network A and network B) are the real IP addresses of both networks when you use VPN NAT source inbound to resolve IP address conflicts.

13.2.5 Configuring the gateway-to-gateway VPN on AS14

Configure the gateway-to-gateway VPN using the configuration planning worksheet in Table 65 on page 557. Follow the steps described in 13.6.2, “Configuring the gateway-to-gateway VPN on AS14” on page 592.

Figure 655 shows the New Connection Summary window that the wizard presents at the end of the configuration.

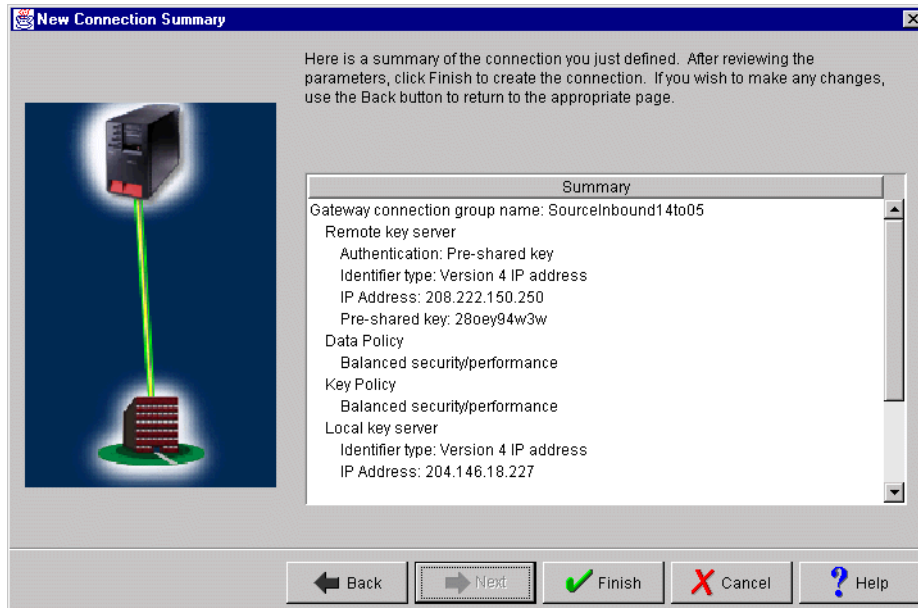


Figure 655. AS14 New Connection Summary window

13.2.6 Configuring the VPN NAT source inbound on AS14

To configure VPN NAT source inbound, you must make the following changes to the default gateway-to-gateway configuration created by the new connection wizard:

- Configure the local gateway (AS14) to be the responder of the VPN connection.
- Configure the address translation pool in the key connection group to translate the remote hosts IP addresses.

To configure VPN NAT source inbound, perform the following steps:

1. On the Virtual Private Networking window, expand **Data Connections->Dynamic Key Groups**.
2. Right-click the dynamic key (connection) group created by the wizard, which is **SourceInbound14to05** in this example.
3. Select **Properties** from the pull-down menu.
4. On the General page, select **Only the remote system can initiate this connection** as shown in Figure 656 on page 559. AS14 is configured to perform VPN NAT source inbound. Therefore, it must be the responder of the connection.

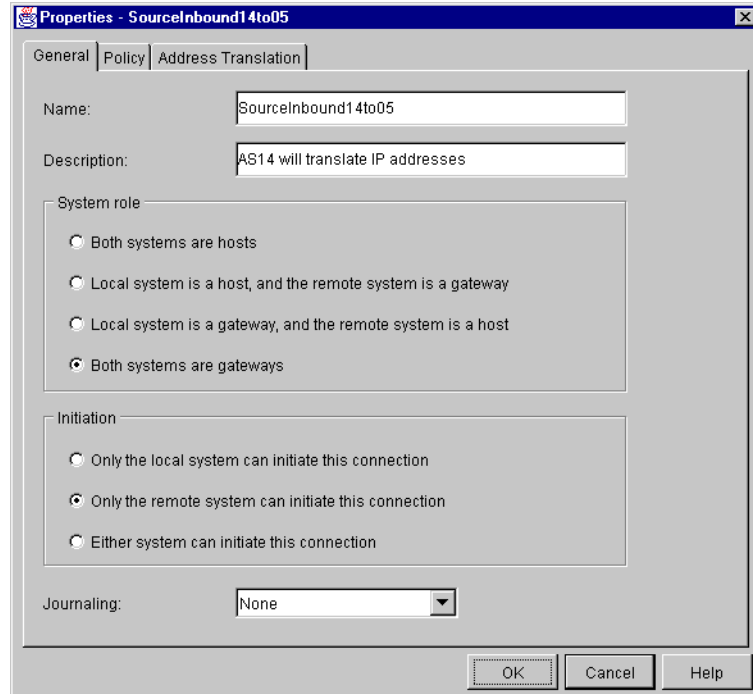


Figure 656. AS14 connection responder

5. Click the **Policy** tab.
6. Select **Connection** or **Single value** for the connection of the Remote addresses as shown in Figure 657.

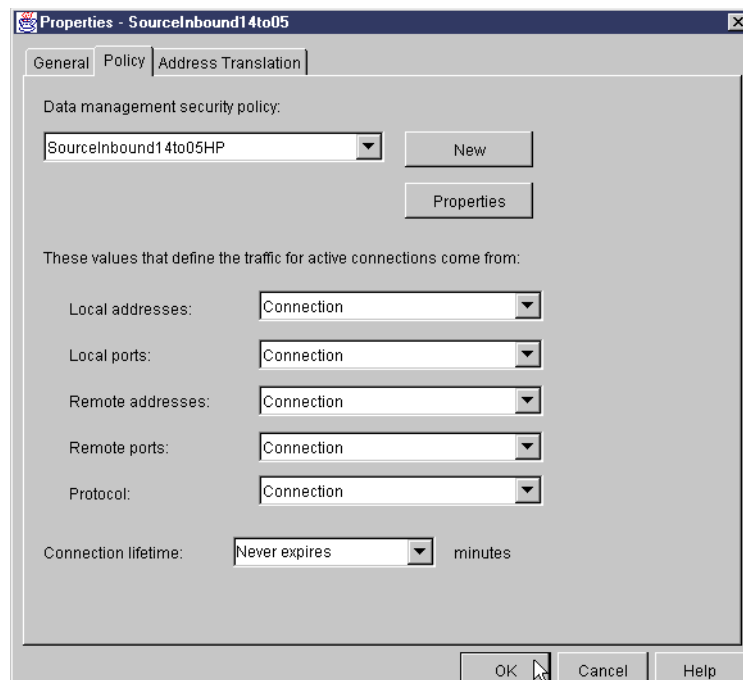


Figure 657. AS14 Configuring a connection for remote addresses

7. Click the **Address Translation** tab.

8. Select **Remote addresses using addresses from the remote key server pool** as shown in Figure 658.

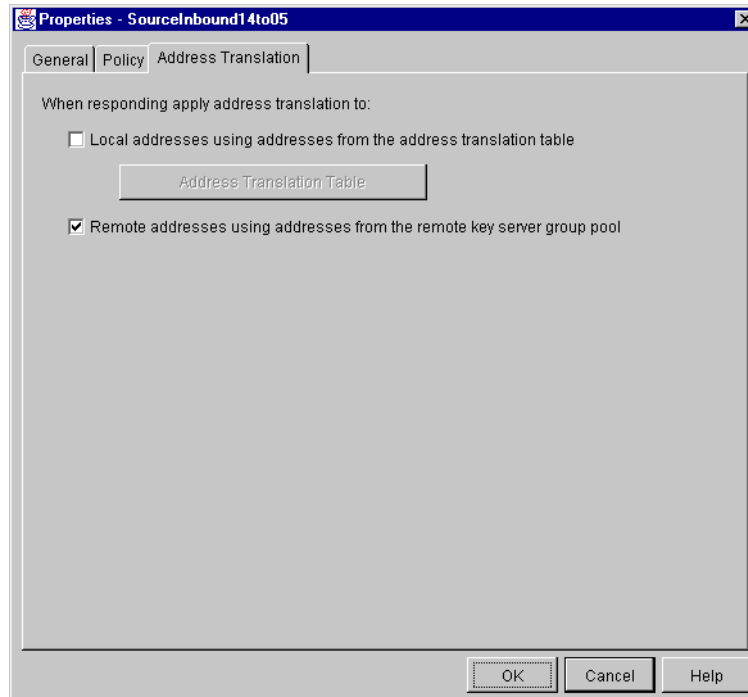


Figure 658. Specifying translation for remote address - VPN NAT source inbound

9. Click **OK** to close the properties pages and save your configuration changes.
10. Right-click the key connection group created by the wizard (**SourceInbound14to05**), and select **Properties** as shown in Figure 659 on page 561.

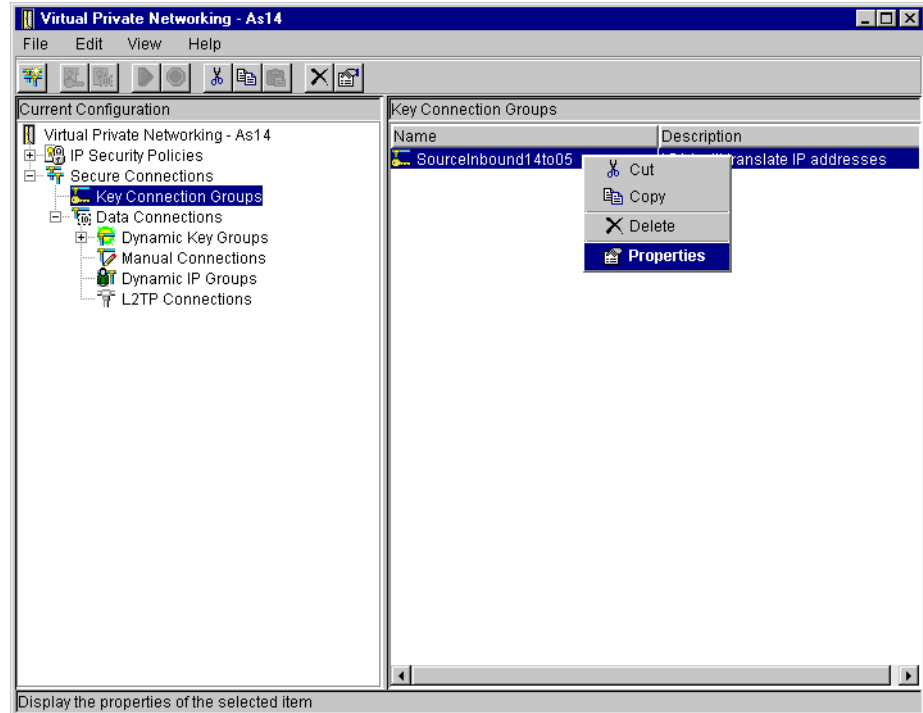


Figure 659. AS14 SourceInbound14to05 key connection group properties

11. Click the **Address Translation** tab.

12. Click **Add** to enter the range of IP addresses in the address translation pool as shown in Figure 660.

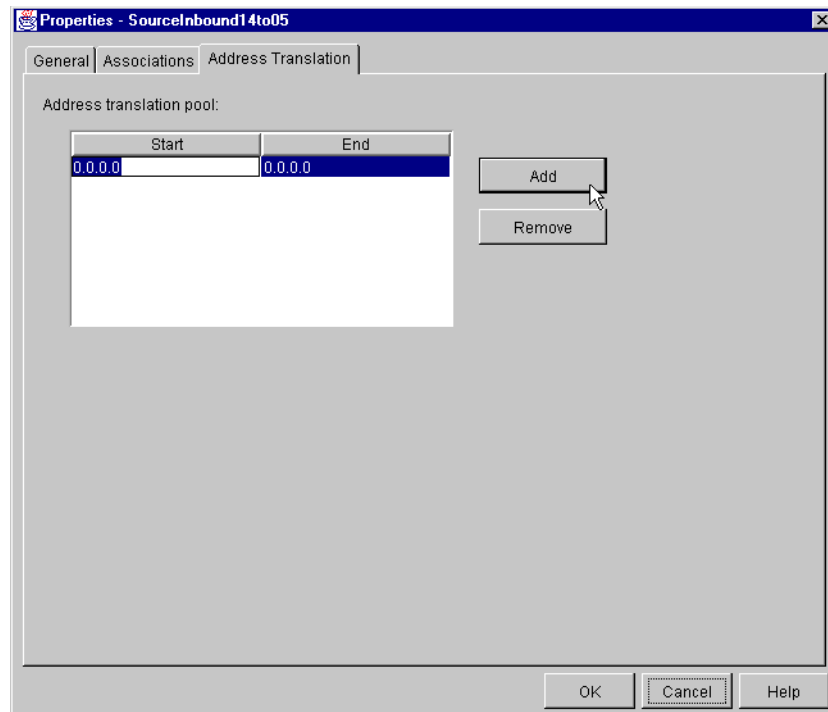


Figure 660. AS14 Address translation pool configuration

13. Specify the Start and End IP addresses used to translate the conflicting addresses in the remote network (Figure 661).

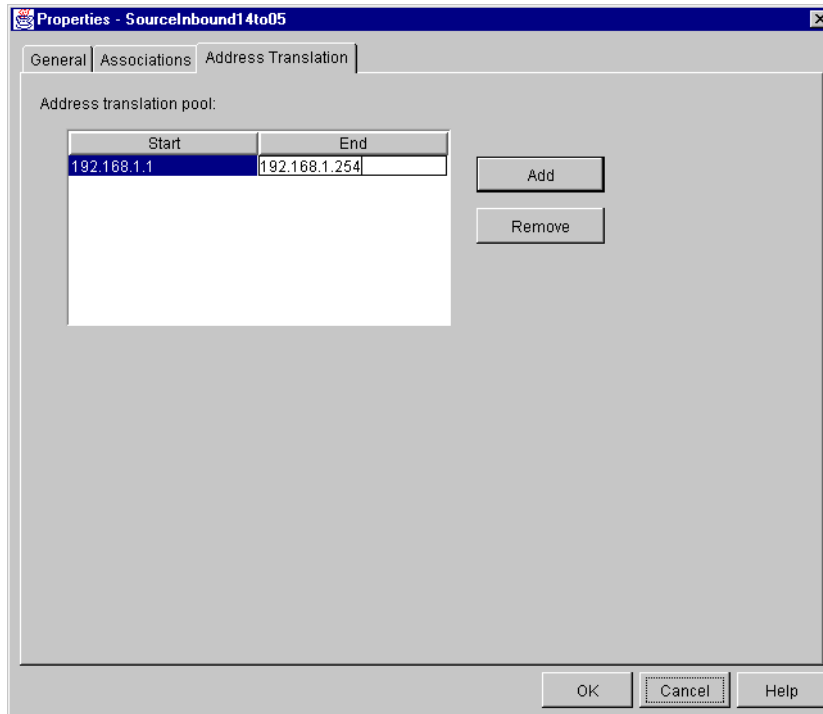


Figure 661. Specifying the address range for the address translation pool

14. Click **OK** to close the Properties pages and save your configuration.

13.2.7 Configuring IP filtering on AS14

Figure 662 shows the IP filters configuration summary on AS14 for VPN NAT source inbound.

```

IP Packet Security: All Security Rules
#Defined address for the local network
ADDRESS subnet14 IP = 10.196.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
#Defined address for the remote network
ADDRESS subnet05 IP = 10.196.8.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
#Filter interface
FILTER_INTERFACE LINE = TRNWSB2 SET = VPNIFC
#IKE filter rules
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.227
DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS =
NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 208.222.150.250
DSTADDR = 204.146.18.227 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS =
NONE JRN = OFF
#IPSEC filter rule
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = subnet14
DSTADDR = subnet05 PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE
JRN = FULL CONNECTION_DEFINITION = SourceInbound14to05

```

Figure 662. AS14 VPN NAT source inbound IP filter configuration summary

13.2.8 Completing the planning worksheets for AS05

Complete the planning worksheets to gather the information you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 66 shows the wizard configuration planning worksheet for this scenario from the perspective of the VPN gateway at the distributor's network (AS05).

Table 66. AS05 New Connection Wizard planning worksheet

This is the information you need to configure the VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Gateway to Host – Gateway to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	SourceInbound05to14
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	208.222.150.250 (B)
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	204.146.18.227 (A)
What is the pre-shared key?	28oey94w3w
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
Is this AS/400 system resolving the address conflict?	No
Are the address being translated in the local network? – Yes. Configure VPN NAT source outbound. – No. Configure VPN NAT source inbound.	N/A
What is the NAT address pool?	N/A

To complete the VPN configuration, you must configure IP filters. Table 67 on page 564 shows the IP filter rules configuration planning worksheet for this scenario from the perspective of the VPN gateway at the manufacturer's network (AS14).

Table 67. AS05 Planning worksheet - IP filter configuration

This is the information you need to create the IP filters to complete the VPN configuration	Scenario answers
What name do you want to use to group together the set of filters that will be created?	VPNIFC
<ul style="list-style-type: none"> – What is the network address of the LOCAL network that can use the VPN tunnel? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter. 	10.196.8.0 255.255.255.0 AS05subnets
<ul style="list-style-type: none"> – What is the IP address of the <i>remote</i> network that can use the VPN tunnel? If the remote system is resolving the address conflict and is using Source Outbound, this is the IP address range of the NAT pool. – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter. 	10.196.0.0 255.255.0.0 AS14subnets
What is the IP address of your VPN server? <ul style="list-style-type: none"> – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host. 	208.222.150.250 (B)
What is the IP address of the remote VPN server? <ul style="list-style-type: none"> – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host. 	204.146.18.227 (A)
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRLANB1
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

13.2.9 Configuring the gateway-to-gateway VPN on AS05

Use the New Connection Wizard to configure the gateway-to-gateway VPN using the configuration planning worksheet in Table 66 on page 563. Figure 663 on page 565 shows the New Connection Summary window for AS05.

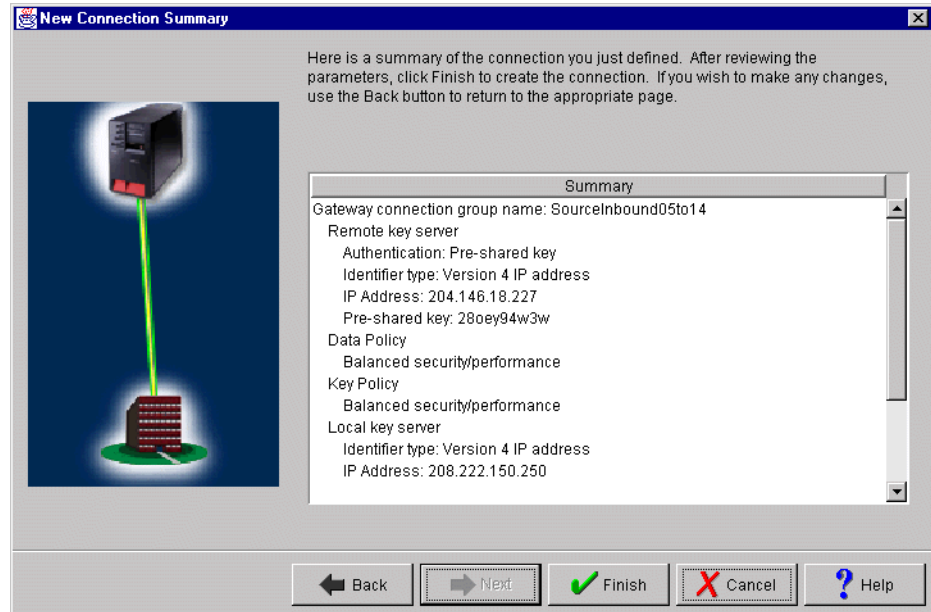


Figure 663. AS05 New Connection Summary window

13.2.10 Configuration changes for VPN NAT source inbound on AS05

Although AS14 performs the address translation in this scenario, the following changes to the VPN configuration created by the wizard are required on AS05:

- Configure AS05 as the initiator of the connection.
- Configure a dynamic key connection for each host on network B that needs to communicate with hosts on network A1. Specify the real local IP address of the hosts in the connection configuration.

Perform the following steps to update the configuration created by the wizard:

1. On the Virtual Private Networking window, expand **Data Connections->Dynamic Key Groups** (Figure 664 on page 566).
2. Right-click the dynamic key (connection) group created by the wizard, which is **SourceInbound05to14** in this example.
3. Select **Properties** from the pull-down menu as shown in Figure 664 on page 566.

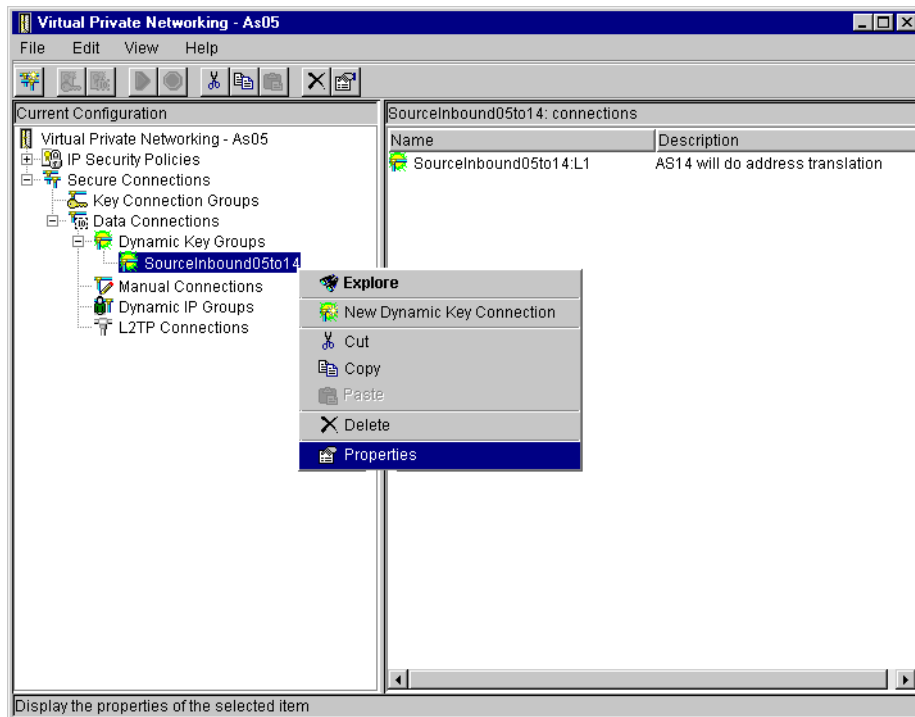


Figure 664. AS05 SourceInbound05to14 dynamic key connection group properties

4. On the General page, select **Only the local system can initiate this connection** as shown in Figure 665. VPN NAT source inbound requires the remote VPN server (AS05) to initiate the connection.

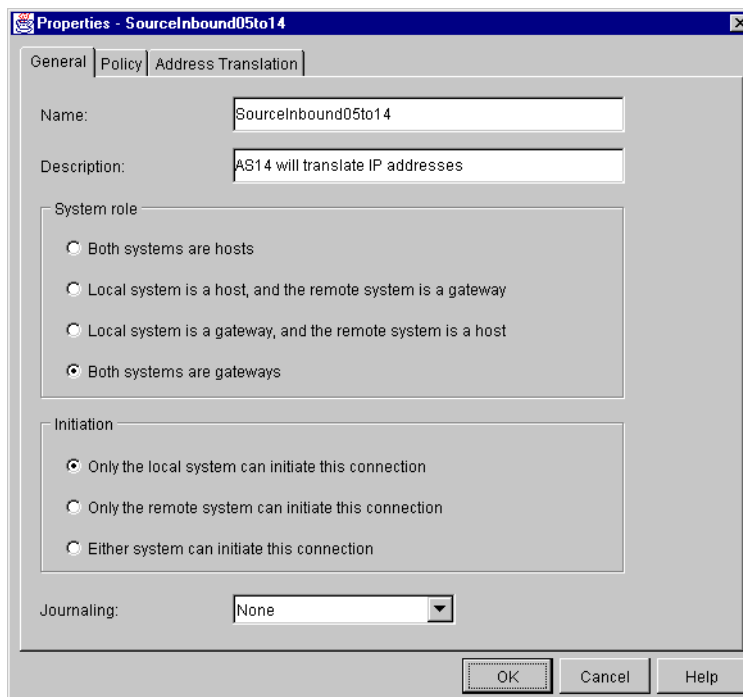


Figure 665. AS05 connection initiator

5. Click the **Policy** tab.

6. On the Policy window, select **Connection** for Local address as shown in Figure 666. Since AS05 is the connection initiator, the value for this parameter is defined in the dynamic key connection. Refer to 4.3, “Refining the traffic for active connections: Connection granularity” on page 129, for more information.

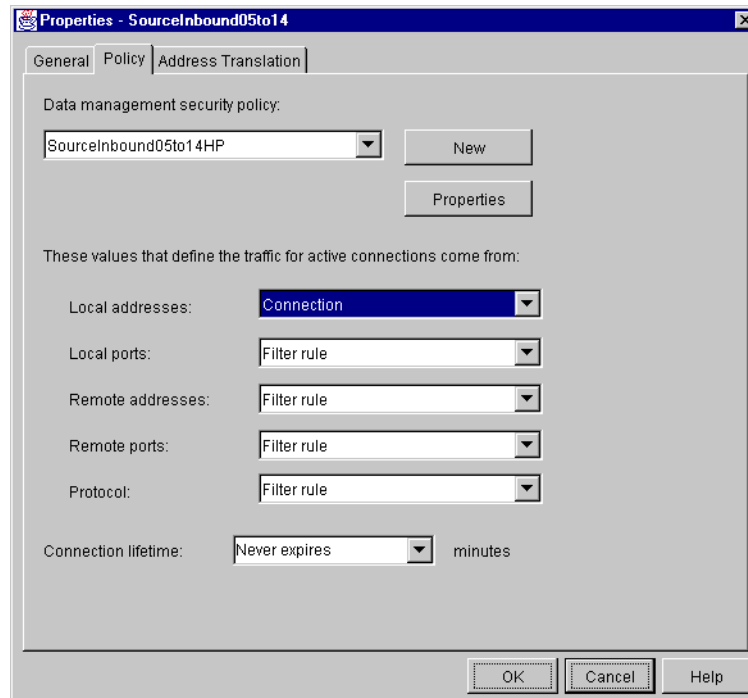


Figure 666. AS05 policy for SourceInbound05to14

7. Click **OK** to close the properties pages and save your configuration.

The following steps describe the configuration of the individual dynamic key connections required for each host on network B that needs access to network A1 in the VPN NAT source inbound scenario. Complete this process:

1. Right-click the dynamic key connection created by the wizard, which is **SourceInbound04to14:L1** in this scenario.
2. Select **Properties** from the pull-down menu as shown in Figure 667 on page 568.

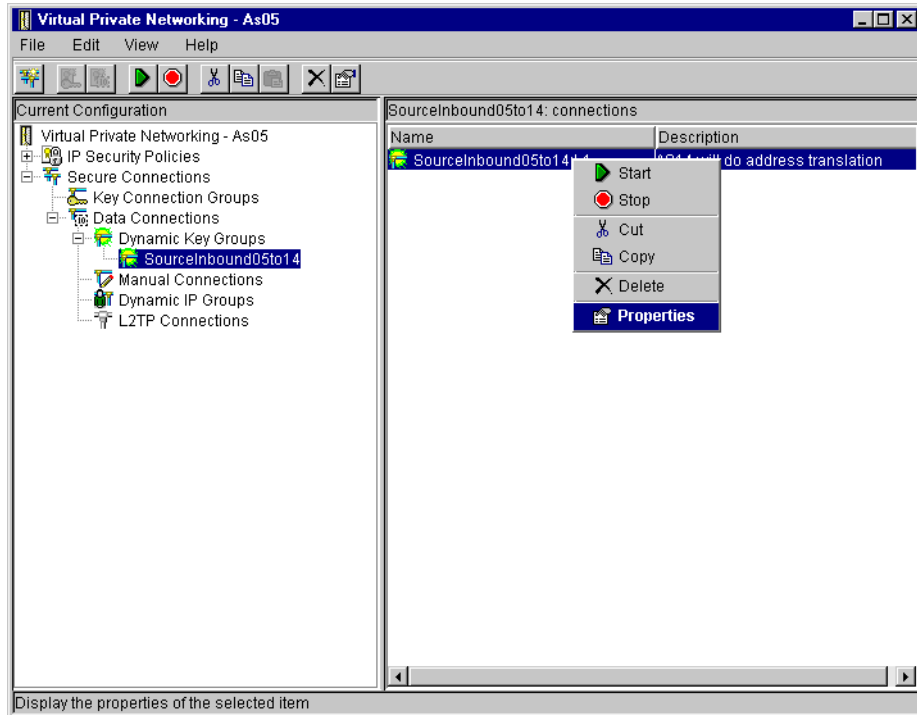


Figure 667. AS05 Configuring the dynamic key connection for local host PC08

3. Select the **Local Addresses** tab.
4. Select **Version 4 IP Address** for Identifier type as shown in Figure 668.

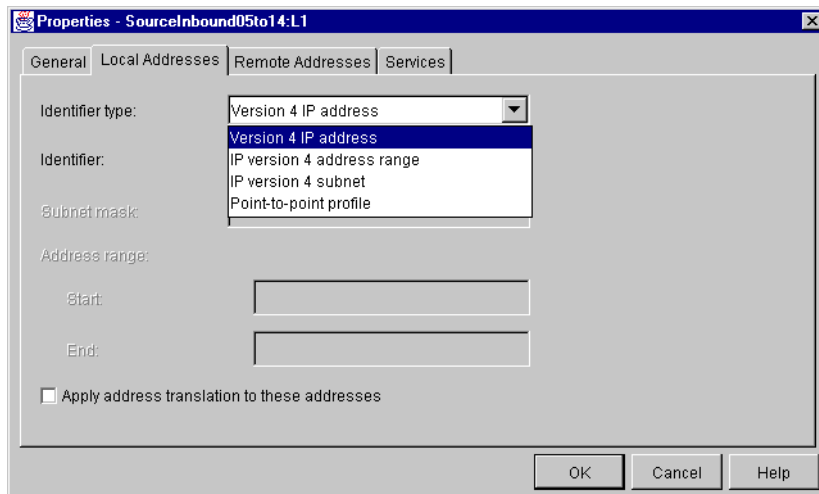


Figure 668. AS05 Configuring the dynamic key connection for local host PC08

5. Specify the single IP address of the local host as shown in Figure 669 on page 569. This is the local data endpoint for this specific dynamic key connection. In this scenario, it is PC08 IP address 10.196.8.6 (J).

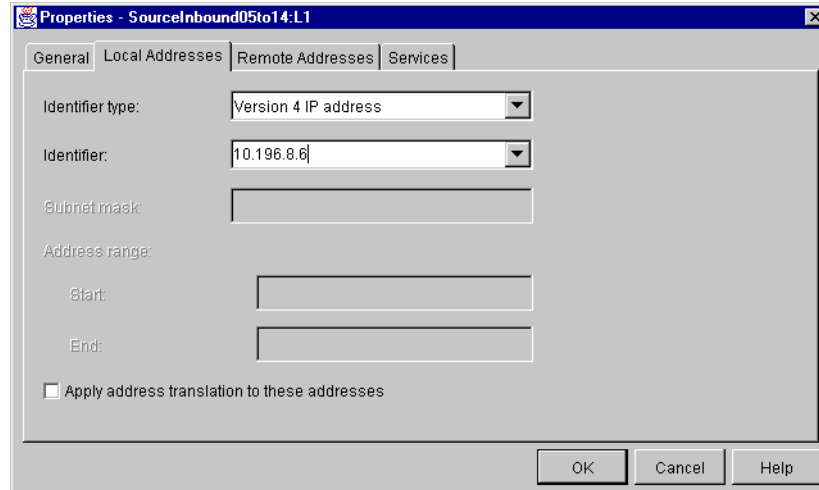


Figure 669. Configuring the Local Address for the SourceInbound05to14:L1 connection

6. Click **OK** to close the properties window and save the configuration.
7. Configure a new dynamic key connection for PC07. To simplify the configuration of the connection for PC07, copy and paste the dynamic key connection for PC08. This creates a second dynamic key connection, which is SourceInbound05to14:L2.
8. Right-click **SourceInbound0514:L2**, and select **Properties**.
9. Click the **Local Addresses** tab.
10. Select **Version 4 IP Address** for Identifier type.
11. Enter the PC07 local IP address 10.196.8.4 for Identifier as shown in Figure 670.

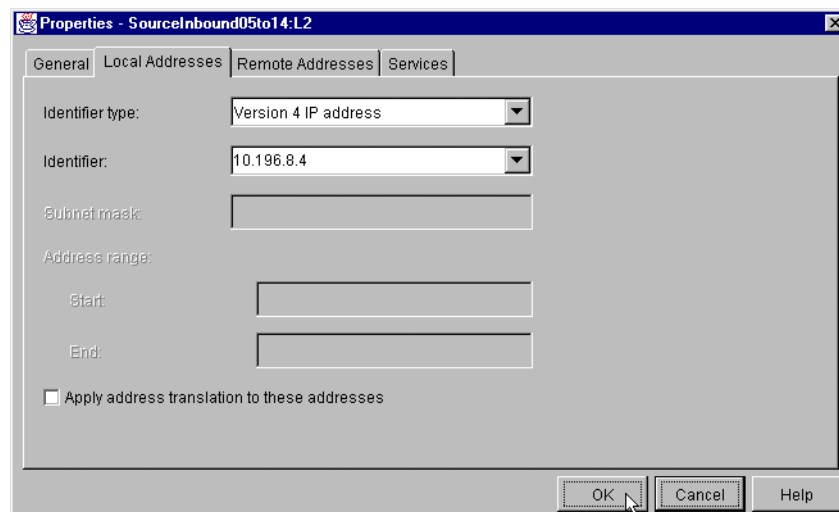


Figure 670. AS05 Configuring dynamic key connection for local host PC07

12. Click **OK** to save the configuration.

13.2.11 Configuring IP filtering on AS05

Figure 671 shows the IP filters configuration summary on AS05 for this scenario.

```
All Security Rules
#Defined Address for local network
ADDRESS AS05subnets IP = 10.196.8.0 MASK = 255.255.255.0 TYPE = TRUSTED
#Defined Address for remote network
ADDRESS AS14subnets IP = 10.196.0.0 MASK = 255.255.0.0 TYPE = UNTRUSTED
#Filter interface
FILTER_INTERFACE LINE = TRLANB1 SET = VPNIFC
#IKE filter rules
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 208.222.150.250
  DSTADDR = 204.146.18.227 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 204.146.18.227
  DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC filter rules
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS05subnets
  DSTADDR = AS14subnets PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = SourceInbound05to14
```

Figure 671. AS05 IP filter configuration summary for VPN NAT source inbound scenario

13.2.12 Starting the VPN connections

For a complete description on activating IP filters and starting VPN connections, refer to 3.8, “VPN operations and management” on page 84.

The following list summarizes the steps you must perform to start the VPN connections:

1. Activate IP filters on both AS/400 systems (AS14 and AS05).
2. Start Virtual Private Networking on both AS/400 systems (AS14 and AS05).
3. On the initiator AS/400 system, AS05, start the dynamic key connections for the local hosts PC08 and PC07. In this scenario, start the connections **SourceInbound05to14:L1** and **SourceInbound05to14:L2**.
4. Click **View**, and select **Active Connections** to view the status of the dynamic key connections as shown in Figure 672.

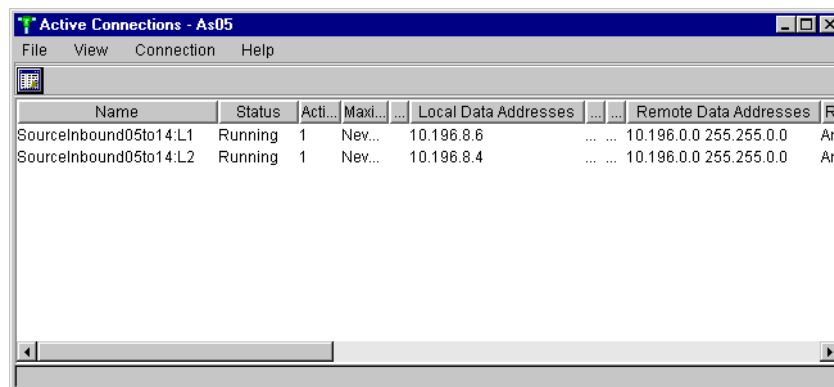


Figure 672. AS05 Active Connections window

13.3 VPN NAT source outbound implementation

In this section, we resolve the same address collisions described in 13.2, “VPN NAT source inbound implementation (AS14)” on page 553, but implement VPN NAT source outbound on AS05. Notice that source outbound can be used to resolve address collisions and hide internal addresses. Since you control the configuration on the machine that is translating the source outbound address (using VPN NAT), you can hide your internal network address information. Where source inbound only resolves an address conflict since to configure VPN NAT on the gateway performing the address translation, both the public and private IP addresses of the partner must be known.

This section does *not* include step-by-step instructions, but offers a summary of the configuration required to implement VPN NAT source outbound. Figure 654 on page 554 shows the test network for this scenario.

Complete the planning worksheets to gather the information you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 68 shows the wizard configuration planning worksheet for this scenario from the perspective of the VPN gateway on network B, AS05.

Table 68. AS05 New Connection Wizard configuration planning worksheet

This is the information you need to create your VPN using the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Gateway to Host – Gateway to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	SourceOutbound05to14
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	208.222.150.250 (B)
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	204.126.18.227 (A)
What is the pre-shared key?	28oey94w3w
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
Is this AS/400 system resolving IP address conflicts?	Yes
Are the address being translated in the local network? - Yes. Configure VPN NAT source outbound. - No. Configure VPN NAT source inbound.	Initiator

This is the information you need to create your VPN using the New Connection Wizard	Scenario answers
What is the VPN NAT address pool?	192.168.1.1 - 192.168.1.254

To complete the VPN configuration, you must configure IP filters. Table 69 shows the IP filter rules configuration planning worksheets for this scenario from the perspective of the VPN gateway at the distributor's network (AS05).

Table 69. AS05 Planning worksheet - IP filter rules configuration AS05

This is the information you need to create the IP filters to complete the VPN configuration	Scenario answers
What name do you want to use to group together the set of filters that will be created?	VPNIFC
<ul style="list-style-type: none"> – What is the Network address of the <i>local</i> network that can use the VPN tunnel? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter. 	10.196.8.0 255.255.255.0 AS05subnets
<ul style="list-style-type: none"> – What is the IP address of the <i>remote</i> network that can use the VPN tunnel? If the remote system is resolving the address conflict and is the <i>initiator</i> (using Source Outbound), this is the IP address range of the NAT pool. – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter. 	10.196.0.0 255.255.0.0 AS14subnets
<ul style="list-style-type: none"> What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host. 	208.222.150.250 (B)
<ul style="list-style-type: none"> What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host. 	204.146.18.227 (A)
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRLANB1
<ul style="list-style-type: none"> What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i>. 	

Complete the planning worksheets to gather the information you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 70 on page 573 shows the wizard configuration planning worksheet for this scenario from the perspective of the VPN gateway on network A, AS14.

Table 70. AS14 New Connection Wizard planning worksheet -

This is the information you need to create your VPN using the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Gateway to Host – Gateway to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	SourceOutbound14to05
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	204.146.18.227 (A)
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	208.222.150.250 (B)
What is the pre-shared key?	28oey94w3w
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
Is this AS/400 system resolving IP address conflicts?	No
Are the address being translated in the local network? – Yes. Configure VPN NAT source outbound. – No. Configure VPN NAT source inbound.	N/A
What is the VPN NAT address pool?	N/A

To complete the VPN configuration, you must configure IP filters. Table 71 shows the IP filter rules configuration planning worksheet for this scenario from the perspective of the VPN gateway on network A (AS14).

Table 71. AS14 Planning worksheet - IP filter rules configuration

This is the information you need to configure IP filters to support the VPN with VPN NAT source outbound	Scenario answers
What name do you want to use to group together the set of filters that will be created?	VPNIFC
– What is the Network address of the <i>local</i> network that can use the VPN tunnel? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	10.196.0.0 255.255.0.0 AS14subnets

This is the information you need to configure IP filters to support the VPN with VPN NAT source outbound	Scenario answers
<ul style="list-style-type: none"> – What is the IP address of the <i>remote</i> network that can use the VPN tunnel? If the remote system is resolving the address conflict and it is the <i>initiator</i> (using Source Outbound), this is the IP address range of the NAT pool. – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter. 	192.168.1.1 -192.168.1.254 255.255.0.0 AS05subnets
<ul style="list-style-type: none"> What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for <i>destination address</i> on inbound filters – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host. 	204.146.18.227 (A)
<ul style="list-style-type: none"> What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host. 	208.222.150.250 (B)
<ul style="list-style-type: none"> What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied? 	TRNWSB2
<ul style="list-style-type: none"> What other IP addresses, protocols, and ports do you wish to permit on this interface? <p>Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i>!</p>	

Note: The remote data endpoint IP address in the IPSEC filter rule is the set of IP addresses in the VPN NAT pool.

13.3.1 Configuring the gateway-to-gateway VPN on AS05

Configure the gateway-to-gateway VPN using the configuration planning worksheet in Table 68 on page 571 and the New Connection Wizard.

Figure 673 on page 575 shows the New Connection Summary window that the wizard presents at the end of the configuration.

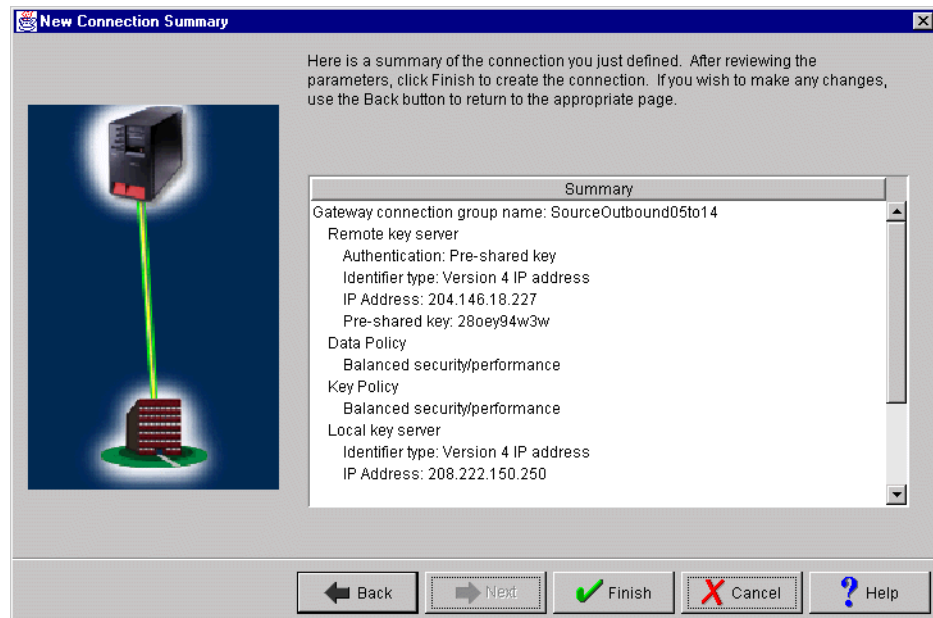


Figure 673. AS05 New Connection Summary window

13.3.2 Configuring VPN NAT source outbound on AS05

To configure VPN NAT source outbound, you must make the following changes to the default gateway-to-gateway configuration created by the New Connection Wizard:

- Configure the address translation pool in the key connection group to translate the local hosts IP addresses.
- Configure a connection for each local host that needs to access the remote network through the VPN.
- Configure the local gateway (AS05) to be the initiator of the VPN connection.

To configure VPN NAT source outbound, perform the following steps:

1. From the VPN GUI, expand **Secure Connections**, and click **Key Connection Groups**.
2. In the right panel, right-click the key connection group **SourceOutbound05to14** configured by the wizard, and select **Properties** as shown in Figure 674 on page 576.

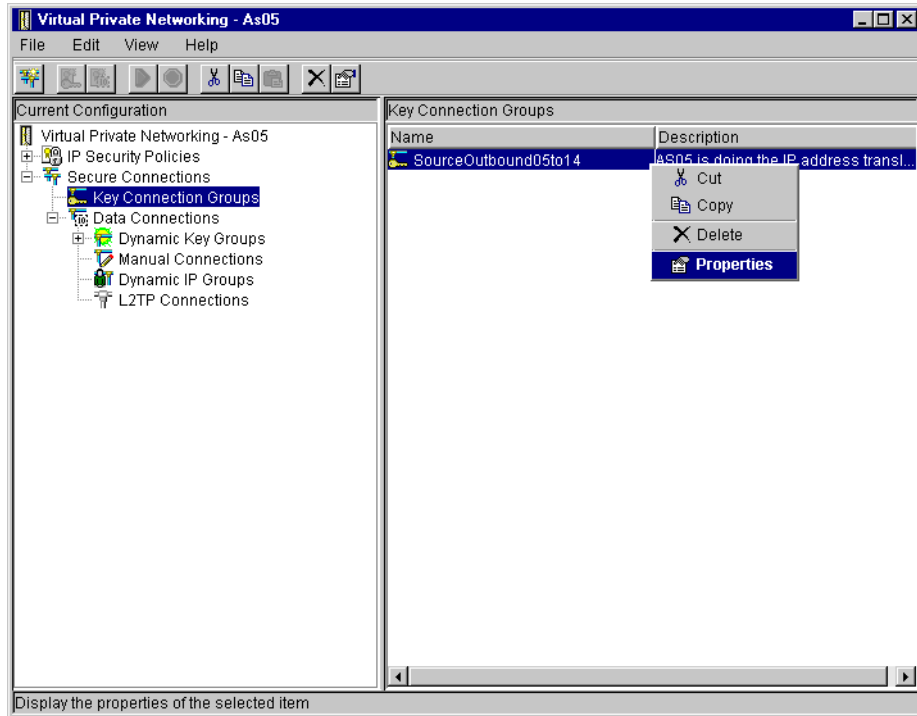


Figure 674. AS05 SourceOutbound05to14 key connection group properties

3. From the Properties window, select the **Address Translation** tab to add the address translation pool.
4. Click **Add** to display a new field in the list box as shown in Figure 675.

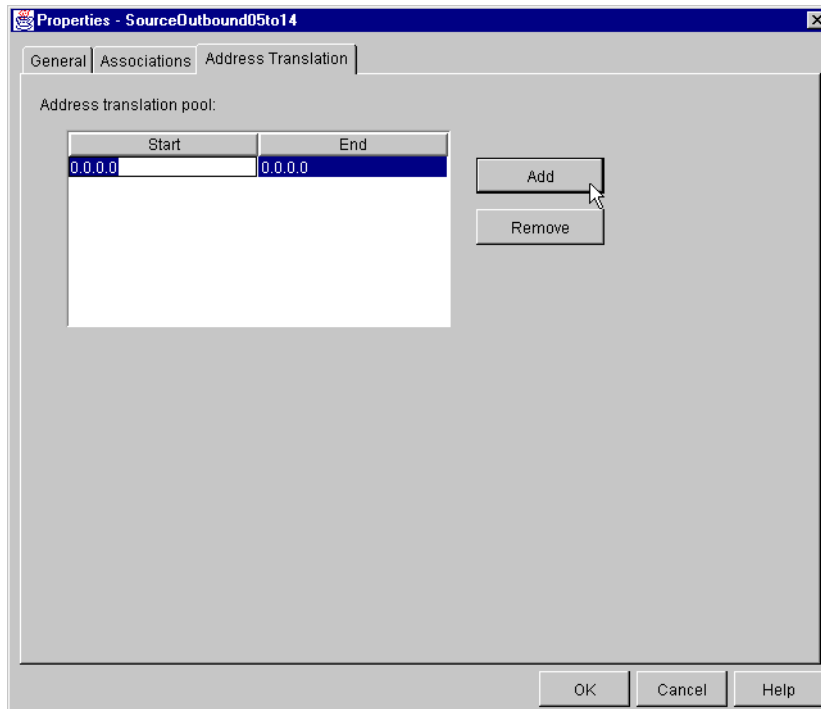


Figure 675. AS05 Configuring the address translation pool

5. Enter the Start and End IP addresses for the pool of addresses that will be used to translate local hosts IP addresses (Figure 676).

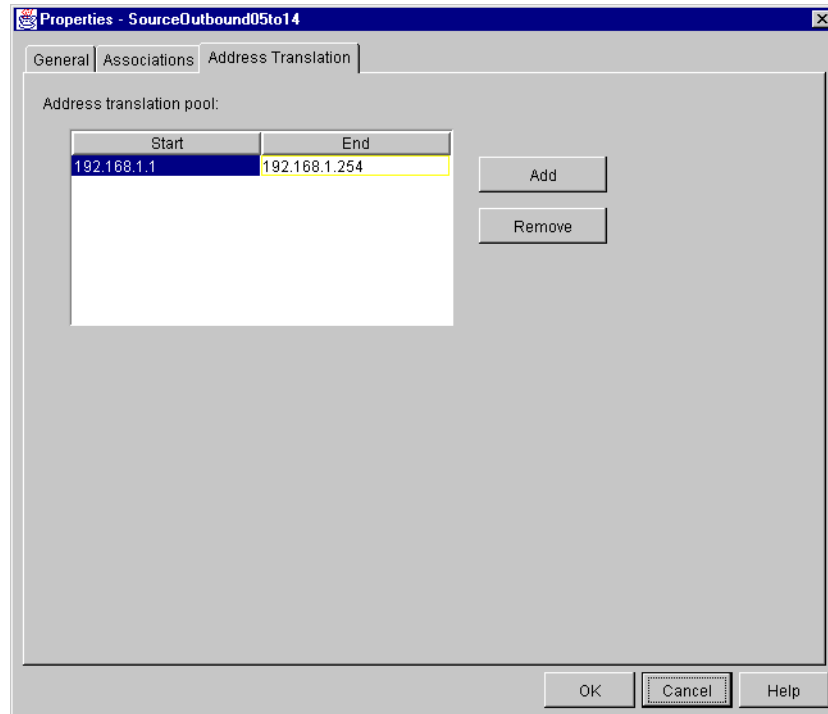


Figure 676. AS05 Setting the address range for address translation pool

6. Click **OK** to close properties pages and save your configuration.

You must now configure AS05 to be the connection initiator and the individual dynamic key connection for each local host. Follow these steps:

1. On the Virtual Private Networking window, expand **Data Connections->Dynamic Key Groups**.
2. Right-click the dynamic key (connection) group created by the wizard, which is **SourceOutbound05to14** in this example.
3. Select **Properties** from the pull-down menu as shown in Figure 677 on page 578.

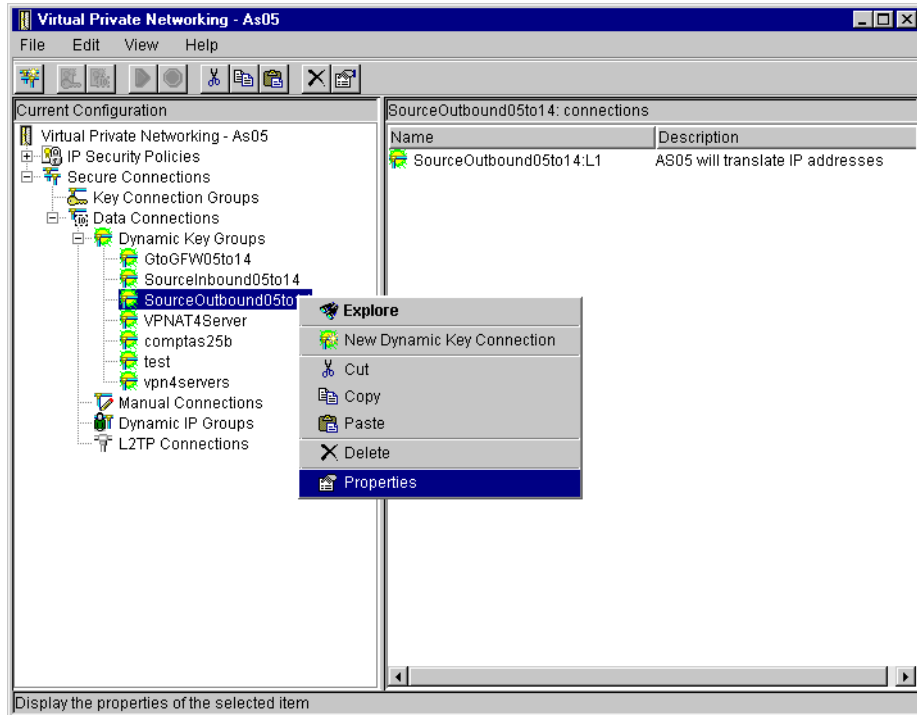


Figure 677. AS05 Selecting properties for the dynamic key connection group

4. On the General page, select **Only the local system can initiate this connection** as shown in Figure 678. AS05 is configured to perform VPN NAT source outbound. Therefore, it must be the initiator of the connection.

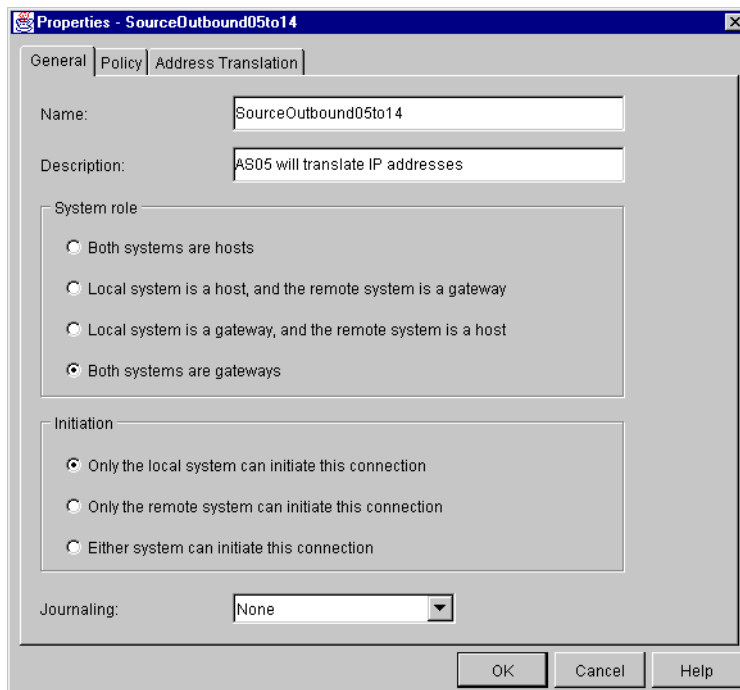


Figure 678. AS05 connection initiator

5. Click the **Policy** tab.

6. On the Policy window, select **Connection** for Local addressed as shown in Figure 679. Since AS05 is the connection initiator, the value for this parameter is defined in the dynamic key connection. Refer to 4.3, “Refining the traffic for active connections: Connection granularity” on page 129, for more information.

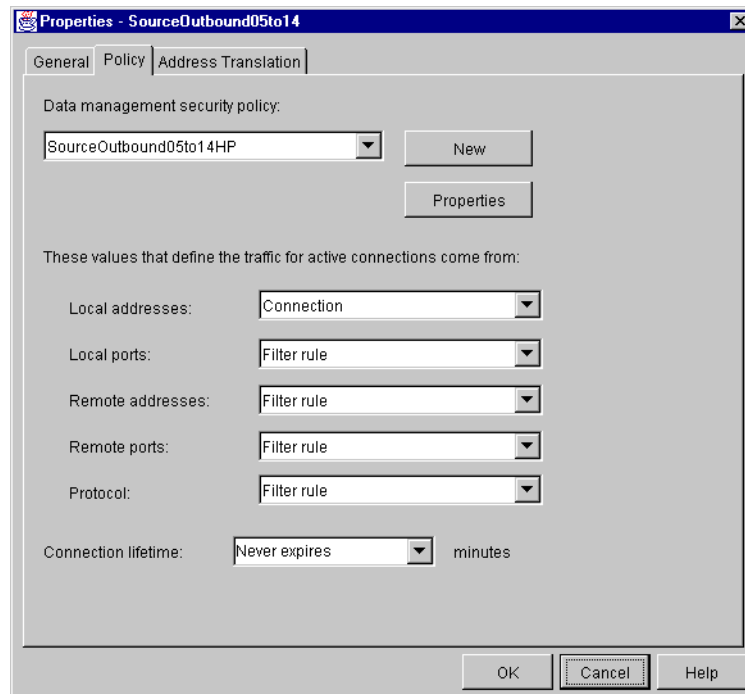


Figure 679. Policy for SourceOutbound05to14

7. Click **OK** to close the Properties window and save the configuration changes.

The following steps describe the configuration of the individual dynamic key connections required for each host on network B that needs access to network A1 in the VPN NAT source outbound scenario. Complete these steps:

1. Right-click the dynamic key connection created by the wizard, which is **SourceOutbound05to14:L1** in this scenario.
2. Select **Properties** from the pull-down menu.
3. Click **Local Address**.
4. Select **Version 4 IP address** for Identifier type.
5. Enter PC08 local IP address 10.196.8.6 (J) for Identifier.
6. Check **Apply addresses translation to these addresses** as shown in Figure 680 on page 580.

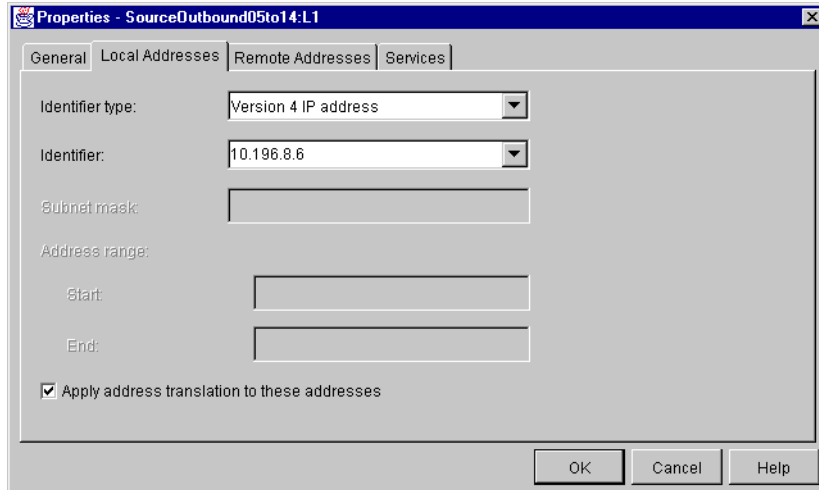


Figure 680. PC08 connection configuration

7. Click **OK** to close the Properties window and save your configuration changes.
8. Copy and paste the dynamic key connection to create SourceOutbound05to14:L2 for PC07.
9. On the Local Address window, change Identifier to PC07's local IP address 10.196.8.4, and check **Apply addresses translation to these addresses** as shown in Figure 681.

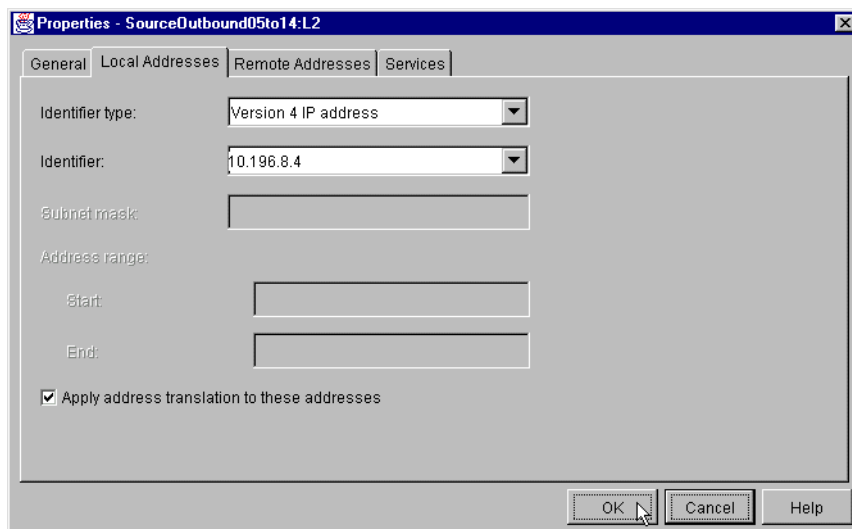


Figure 681. PC07 connection configuration

13.3.3 Configuring IP filtering on AS05

Figure 682 on page 581 shows the IP filters configuration summary on AS05 for this scenario.

```

IP Packet Security: All Security Rules
#Defined Address for local network
ADDRESS AS05subnets IP = 10.196.8.0 MASK = 255.255.255.0 TYPE = TRUSTED
#Defined Address for remote network
ADDRESS AS14subnets IP = 10.196.0.0 MASK = 255.255.0.0 TYPE = UNTRUSTED
#Filter interface
FILTER_INTERFACE LINE = TRLANB1 SET = VPNIFC
#IKE filter rules
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 208.222.150.250
  DSTADDR = 204.146.18.227 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 204.146.18.227
  DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC Filter rules
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS05subnets
  DSTADDR = AS14subnets PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = SourceOutbound05to14

```

Figure 682. AS05 VPN NAT source outbound IP filter rules configuration summary

13.3.4 Configuring the gateway-to-gateway VPN on AS14

Configure the gateway-to-gateway VPN using the configuration planning worksheet in Table 70 on page 573. Figure 683 shows the New Connection Summary window that the wizard presents at the end of the configuration.

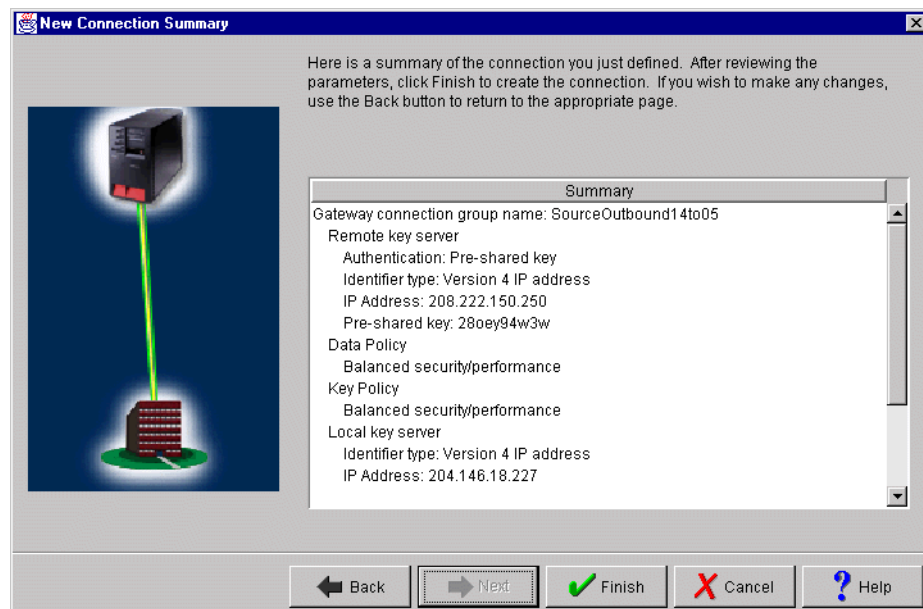


Figure 683. AS14 New Connection Summary window

13.3.5 Configuration changes for VPN NAT source outbound on AS14

Perform the following configuration changes to the VPN configuration objects created by the wizard on AS14:

1. Configure AS14 as a connection responder. Change the dynamic key (connection) group `SourceOutbound14to05`, and select **Only the remote system can initiate the connection** as shown in Figure 684 on page 582.

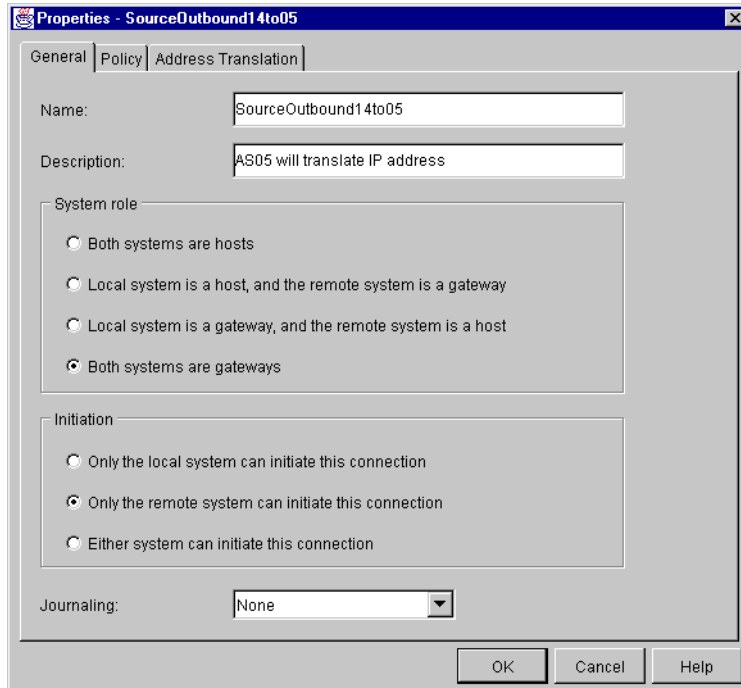


Figure 684. AS14 connection responder

2. Click the **Policy** tab.
3. On the Policy window, select **Connection** for Remote address as shown in Figure 685 on page 583. As the responder of this connection, AS14 accepts the value proposed by the initiator within the limits of the IPSEC filter rule associated with this connection group. Refer to 4.3, "Refining the traffic for active connections: Connection granularity" on page 129, for more information.

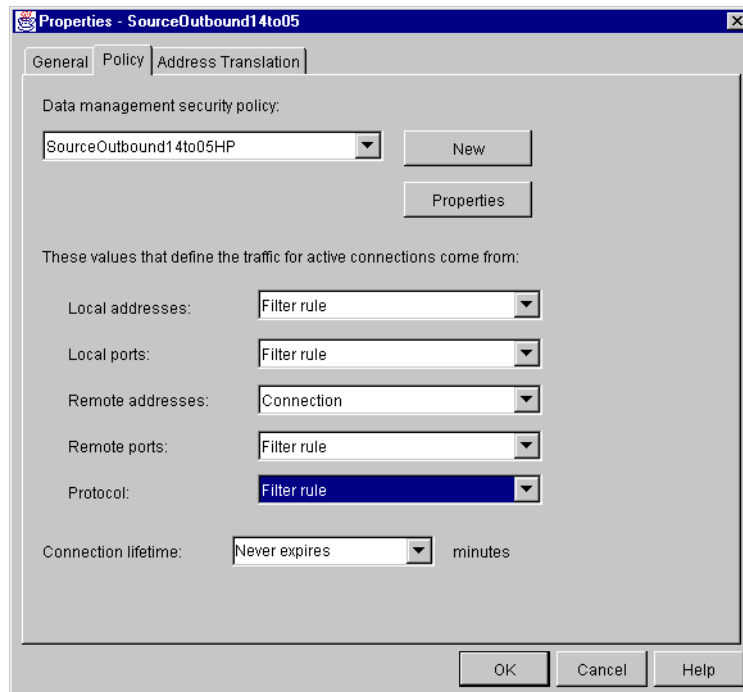


Figure 685. AS14 dynamic key group policy

4. Click **OK** to close the properties pages and save your configuration.

13.3.6 Configuring IP filtering on AS14

Figure 686 shows the IP filters configuration summary on AS14 for this scenario.

```

IP Packet Security: All Security Rules
#Defined Address for local network
ADDRESS subnet14 IP = 10.196.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
#Defined Address for remote network
ADDRESS subnet05 IP = 192.168.1.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
#Filter interface
FILTER_INTERFACE LINE = TRNWSB2 SET = VPNIFC
#IKE Filter rules
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.227
  DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPOR = 500 FRAGMENTS = NONE JRN = FULL
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 208.222.150.250
  DSTADDR = 204.146.18.227 PROTOCOL = UDP DSTPORT = 500 SRCPOR = 500 FRAGMENTS = NONE JRN = FULL
#IPSEC filter rule
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = subnet14
  DSTADDR = subnet05 PROTOCOL = * DSTPORT = * SRCPOR = * FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = SourceOutbound14to05

```

Figure 686. AS14 IP filtering configuration summary - VPN NAT source outbound scenario

13.3.7 Starting the VPN connections

For a complete description on activating IP filters and starting VPN connections, refer to 3.8, “VPN operations and management” on page 84. The following list summarizes the steps you must perform to start the VPN connections.

1. Activate IP filters on both AS/400 systems (AS14 and AS05).
2. Start Virtual Private Networking on both AS/400 systems (AS14 and AS05).
3. On the initiator AS/400 system, AS05 start the dynamic key connections for the local hosts PC08 and PC07. In this scenario, start the connections **SourceOutbound05to14:L1** and **SourceOutbound05to14:L2**.
4. Click **View**, and select **Active Connections** to view the status of the dynamic key connections as shown in Figure 687.

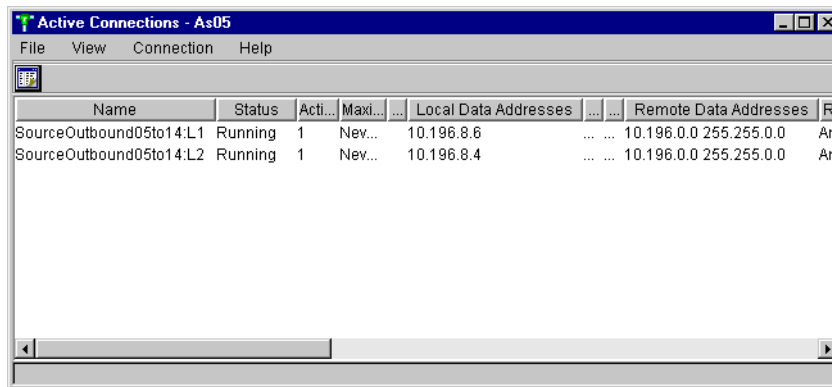


Figure 687. AS05 Active Connections window

13.4 Hiding IP addresses from your VPN partner: VPN NAT for servers

VPN NAT for servers allows you to hide the *real* IP addresses of your local systems by translating these addresses to another address that you make publicly available. When you configure VPN NAT, you can specify that each publicly known IP address be translated to one of a pool of hidden addresses. Your AS/400 system must act as the responder for the VPN connection to use VPN NAT for servers. You should use VPN NAT for servers if you answer *yes* to these questions:

- Do you have one or more servers that you want remote partners to access by using a VPN?
- Do you want to hide the real address of your internal servers?
- Does (or could) your AS/400 system act as the responder of the VPN connection?

VPN NAT for servers is also called *destination inbound*. In this configuration, the AS/400 VPN gateway acting as a *responder* performs the network address translation for hosts that are data endpoints of the VPN connection.

When we discuss VPN NAT and how it is applied to IP traffic, we need to understand the direction (inbound or outbound) and the addresses (source or destination) that may be affected. This describes the kind of VPN NAT that will be applied to IP traffic. In VPN NAT for servers, IP traffic is generated outside of this AS/400 gateway, in the external network, by clients requesting services of the hosts inside the private network. Therefore, from the gateway perspective, the IP packets are *inbound* and the address that will be translated is the *destination*, which results in the term *destination inbound*. Each publicly known IP address is configured to be translated to a single or a pool of hidden addresses.

Note: The publicly known IP address is the IP address revealed to the partially trusted VPN partner. Since it is a gateway-to-gateway configuration, it does *not* need to be a globally routable or registered IP Address. However, the public IP address of the gateways must be globally routable.

VPN NAT for servers (or destination inbound) imposes some restriction on the AS/400 VPN gateway that performs the address translation. The restrictions are:

- The VPN gateway where VPN NAT for servers is configured must be the responder of the VPN connection (AS14 in Figure 688 on page 586).
- The AS/400 gateway performing VPN NAT must have network addressability (must be able to route IP datagrams) to the internal servers using the real IP addresses (after translation).
- The system initiating the VPN connection must specify a remote data endpoint of a single IP address. In this scenario, AS05 is the initiator. It must specify the publicly known IP address of the server (AS08 or AS20 in Figure 688 on page 586) to initiate the connection. This allows the local AS/400 VPN gateway where VPN NAT is configured (AS14) to perform a one-to-one lookup of the public address in the address translation table.

Tip

The IP addresses that you make publicly available to the partially trusted network do not need to be globally routable IP addresses. Since the two gateways are in tunnel mode, these addresses will be encapsulated and considered part of the payload on the public Internet.

This scenario presents two independent companies that need to communicate securely over the Internet. The *manufacturer* wants to give the *distributor* access to two servers in their internal network (network A in Figure 688 on page 586) over a VPN connection. The manufacturer wants to protect the privacy of their network structure and hide the real IP addresses of the servers in the internal network.

13.4.1 Scenario characteristics

Figure 688 on page 586 shows the network in this scenario. The characteristics of this scenario are:

- Network A (manufacturer's) and Network B (distributor's) belong to different companies and don't fully trust each other.
- The manufacturer wants to give the distributor access to the AS/400 servers AS20 and AS08 on network A over a VPN connection.
- The VPN gateway on network A is the AS/400 system AS14. The VPN gateway on network B is the AS/400 system AS05. To simplify this scenario, we don't show the AS/400 gateways behind a firewall. Refer to Chapter 12, "Don't forget a firewall: Protecting your VPN server" on page 515, for information on how to configure AS/400 VPN servers behind a firewall.
- The VPN gateway performing VPN NAT for servers (AS14) is in the same network as the servers AS08 and AS20.

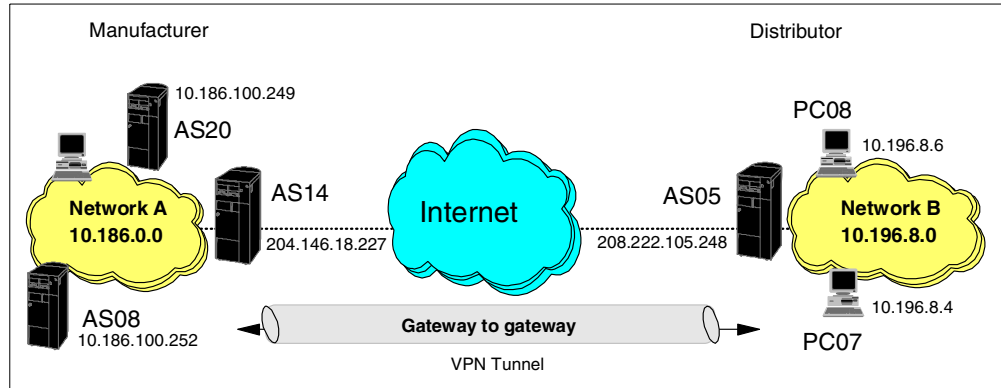


Figure 688. Connecting partially trusted partners through a VPN

13.4.2 Scenario objectives

The objectives of this scenario from the manufacturer's perspective are:

- Allow access to AS20 and AS08 on network A from all clients on network B over a VPN connection.
- Hide the internal IP addresses of AS20 and AS08 by translating them to public (global) IP addresses.
- Block all outside traffic going into the gateway AS/400 systems (AS14) other than the VPN tunnel.

13.5 VPN NAT for servers implementation

This section describes the tasks that you must perform to configure a gateway-to-gateway scenario where one of the AS/400 VPN servers (AS14) is configured to support VPN NAT for servers (destination inbound).

13.5.1 Scenario network configuration

Figure 689 on page 587 shows our simple network configuration for this scenario. The testing environment is similar to the one described in Chapter 6, "Gateway-to-gateway VPN" on page 199. Only the internal network on network A is different.

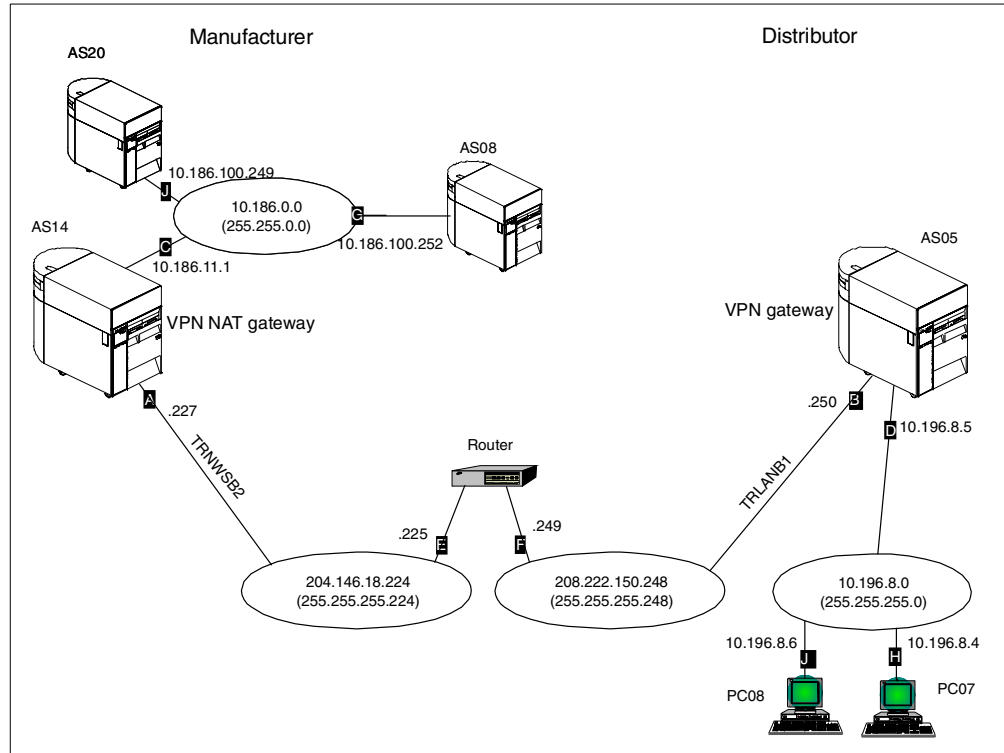


Figure 689. Gateway to gateway - VPN NAT for servers (destination inbound)

The characteristics of the testing network are:

- The AS/400 VPN gateway AS14 is configured to perform VPN NAT for servers.
- AS20 and AS08 are the hosts in network A to be accessed from network B over the VPN. VPN NAT destination inbound must hide these server's internal IP addresses.
- AS08's internal IP address (10.186.100.252) is translated into the public IP address 172.16.150.101. In other words, AS08 is to be known and accessible through the AS14 gateway as 172.16.150.101.
- AS20's internal IP address (10.186.100.249) is translated into the public IP address 172.16.150.100. In other words, AS20 is to be known and accessible through the AS14 gateway as 172.16.150.100.

Note

The public IP addresses 172.16.150.* are *only* configured on the AS14 gateway Address Translation Table (later in this scenario). They are not real interfaces on the internal hosts AS08 and AS20.

- AS05 is the remote VPN gateway. There is a connection configured on this server for each remote host (AS08 and AS20).
- AS20 and AS08 are the connection data endpoints. They do not need to implement VPN support.

13.5.2 Task summary

Complete the following tasks to implement the gateway to gateway with VPN NAT for servers scenario:

1. Verify TCP/IP routing.

Ensure that normal TCP/IP routing is working so that:

- The gateway AS/400 systems can communicate with each other across the intervening Internet or intranet.
 - Hosts on each subnet route traffic to their respective gateway for access to the remote subnet.
2. Configure VPN on network A's gateway AS/400 system (AS14).
3. Configure VPN NAT for servers on AS14.
4. Configure IP filtering on AS14 (refer to the VPN *connection group* configured in the previous steps).
5. Configure VPN on network B's AS/400 system (AS05).
6. Make configuration changes to the VPN configuration objects created by the wizard on AS05. The configuration changes required are:
- AS05 must be the initiator of the connection.
 - There must be one connection per remote host with a single IP address specified on each connection. Both connections are under the same connection group.
7. Configure IP filtering on AS05 (refer to the VPN connection group configured in the previous steps).
8. Start VPN servers.
9. Activate filters.
10. Start the VPN connections from the initiator AS05.

13.5.3 Verifying TCP/IP routing

Defining basic TCP/IP routing is beyond the scope of this document. However, it is vital that routing be configured and tested before attempting to implement a VPN connection. Because you may likely use data encryption under VPN (which, by design, means line traces cannot be fully interpreted), problem determination can be particularly difficult if you have not established routes beforehand.

In the case of the Internet, your gateway AS/400 systems must be able to communicate with each other using public addresses. However, if you are using private network addresses on your local networks, these do not route across the Internet. Therefore, you must configure local routing so that any request for the remote network routes to the gateway AS/400 systems.

Note: You cannot test end-to-end routing until you have established the VPN tunnel.

Tip

Rather than adding routing information to all hosts (including PC clients) that use the VPN tunnel, it may be possible to make the VPN gateway AS/400 system the default TCP/IP gateway. Alternatively, if you use routers on the local network, you may only need to add the necessary routing information once to a suitable router.

Table 72 summarizes the routes configured on AS14 for our test scenario.

Table 72. VPN gateway - AS14 routes

Destination network	Next hop
*DFTRROUTE	204.146.18.225 (E) - the 'Internet' router

Table 73 summarizes the routes configured on AS20 for our test scenario.

Table 73. 'AS20 routes

Destination network	Next hop
*DFTRROUTE	10.186.11.1 (C) - AS14

Table 74 summarizes the routes configured on AS08 for our test scenario.

Table 74. AS08 routes

Destination network	Next hop
*DFTRROUTE	10.186.11.1 (C) - AS14

Table 75 summarizes the routes configured on AS05 for our test scenario.

Table 75. VPN gateway AS05 routes

Destination network	Next hop
*DFTRROUTE	208.222.150.249 (F) - the 'Internet' router

Table 76 summarizes the routes configured on PC08 for our test scenario.

Table 76. PC08 routes

Destination network	Next hop
*DFTRROUTE	10.196.8.5 (D) - AS05

Note

The distributor's clients (PC08 and PC07 in our test environment) must be able to route traffic to the public IP addresses of the manufacturer's servers. In our tests, this is accomplished by configuring the gateways as the default router. You can use explicit routes or other routing techniques beyond the scope of this book.

Client applications on the distributor's network either know the IP addresses of the servers at the remote partner's network or their internal DNS resolves the server's name to their publicly known IP addresses. Additional details on these topics are beyond the scope of this redbook.

13.6 Configuring the manufacturer's AS/400 VPN gateway (AS14)

The following sections take you step-by-step through the configuration of the VPN and filters on the AS/400 VPN gateway in the manufacturer's network (network A).

13.6.1 Planning worksheets for the manufacturer AS/400 gateway (AS14)

Complete the planning worksheets to gather the information that you need to create a gateway-to-gateway connection with the VPN configuration wizard. Table 77 shows the wizard configuration planning worksheet for this scenario from the perspective of the VPN gateway at the manufacturer's network (AS14). Refer to Figure 689 on page 587 for an overview of the network configuration for this scenario.

Table 77. AS14 New Connection Wizard planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Gateway to Host – Gateway to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	vpn4servers
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	204.146.18.227 (A)
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	208.222.150.250 (B)
What is the pre-shared key?	bdcfhhnprotvqa

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
What is the publicly known IP address of the internal host? What is the associated hidden (private) address of the internal host?	172.16.150.100 10.186.100.249 (J)
What is the publicly known IP address of the internal host? What is the associated hidden (private) address of the internal host?	172.16.150.101 10.186.100.252 (G)

To complete the VPN configuration, you must configure IP filters. Table 78 shows the IP filter rules configuration planning worksheet for this scenario from the perspective of the VPN gateway at the manufacturer's network (AS14). Notice the following points:

- The policy (action IPSEC) filter rule allows traffic between subnet 172.16.150.* on the local network and the subnet 10.196.8.* address on the remote network.
- You must configure defined addresses for these subnets and give each of them a name. In this example, specify *AS14subnets* and *AS05subnets* respectively.
- The filter set name that groups the filter rules together is *VPNIFC*.
- Apply the filter rules to the gateway public interface *TRNWSB2*.
- Only VPN traffic is allowed on the public interface.

Refer to Chapter 4, "AS/400 IP filtering overview" on page 103, for information on how to configure IP filters on the AS/400 system.

Table 78. AS14 Planning worksheet - IP filter configuration

This is the information you need to create your IP filters to complete the VPN configuration using VPN NAT for servers	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway. You must answer <i>Gateway</i> to this question.	Gateway
Is the <i>remote</i> VPN server acting as a host or gateway ?	Gateway
What name do you want to use to group together the set of filters that will be created?	VPNIFC
– What is the Network address of your ("TRUSTED") network that can use the VPN tunnel? Specify the publicly known addresses. – What is the subnet mask? – What name do you want to give these address(es)? Use this name as the <i>source address</i> on the IPSEC filter.	172.16.150.0 255.255.255.0 AS14subnets

This is the information you need to create your IP filters to complete the VPN configuration using VPN NAT for servers	Scenario answers
If the remote server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the VPN tunnel? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	10.196.8.0 255.255.255.0 AS05subnets
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	204.146.18.227 (A)
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	208.222.150.250 (B)
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRNWSB2
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

13.6.2 Configuring the gateway-to-gateway VPN on AS14

Perform the following steps to configure a gateway-to-gateway VPN on AS14:

1. Start Operations Navigator from your desktop.
2. Expand your AS/400 system, which in this case **AS14**. Sign on when prompted.
3. Expand **Network**.
4. Double-click **IP Security** to reveal two server names in the right window: IP Packet Security and Virtual Private Networking. You must configure both of these, but start with *Virtual Private Networking* as shown in Figure 690 on page 593.

Note

At this stage, Virtual Private Networking may already have a status of *started* since the default is for the server to automatically start when TCP/IP starts. The server can be either *started* or *stopped* during the following steps.

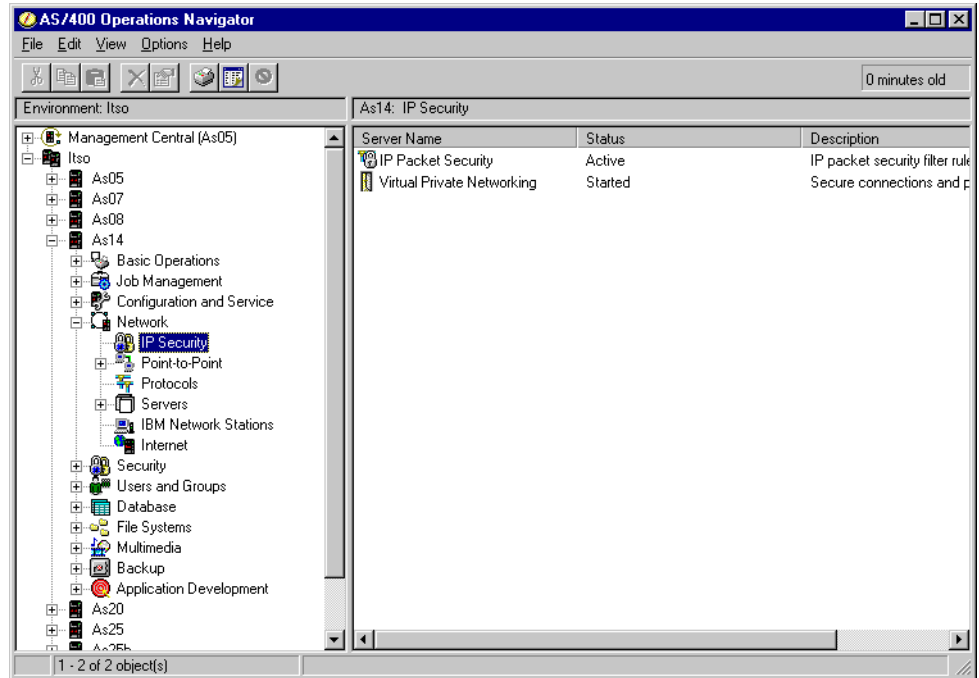


Figure 690. IP Security

5. Double-click **Virtual Private Networking** to start the VPN GUI as shown in Figure 691.

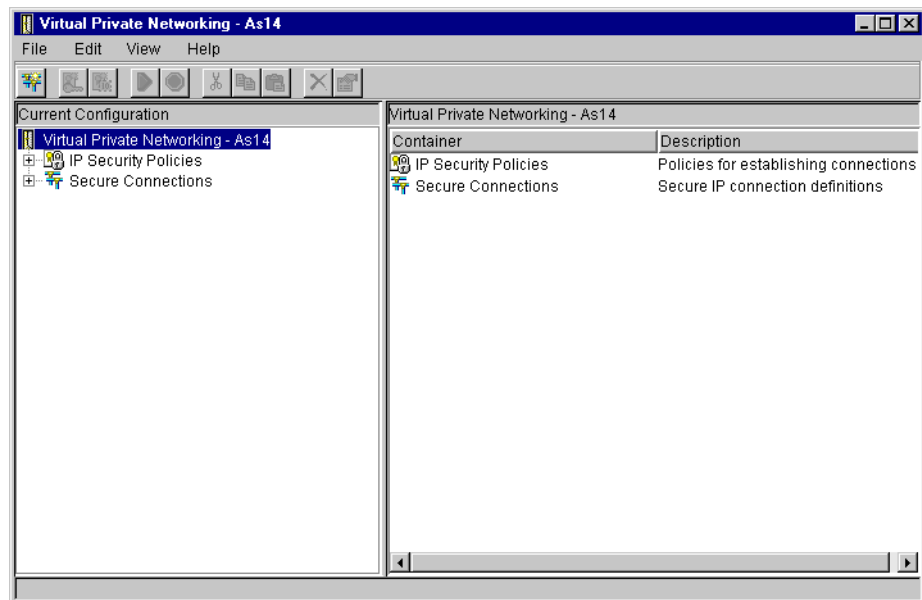


Figure 691. VPN GUI configuration interface

6. Select **File->New Connection**.
7. Select **Gateway To Gateway** from the drop-down menu as shown in Figure 692 on page 594.

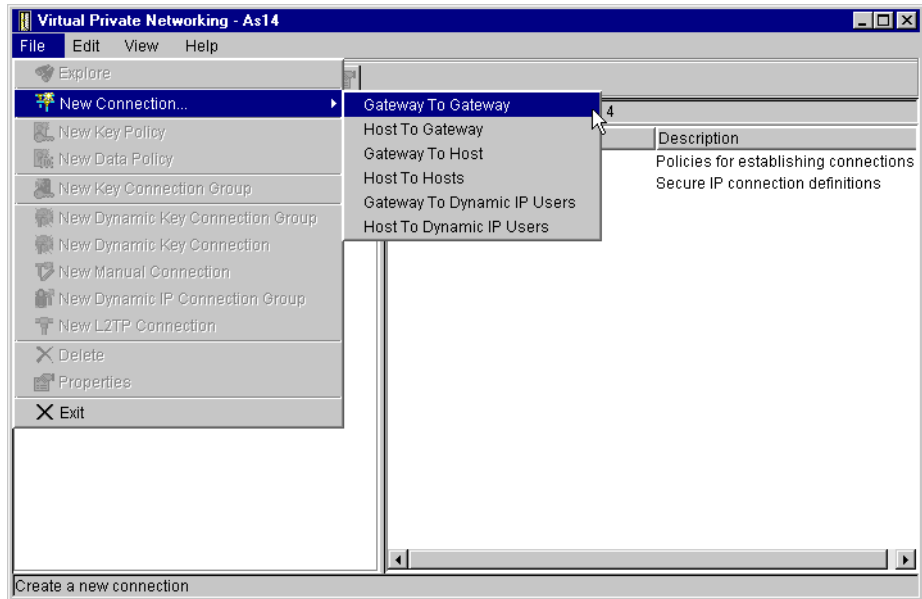


Figure 692. New Connection -> Gateway to Gateway

This starts the New Connection Wizard for a gateway-to-gateway connection (Figure 693).

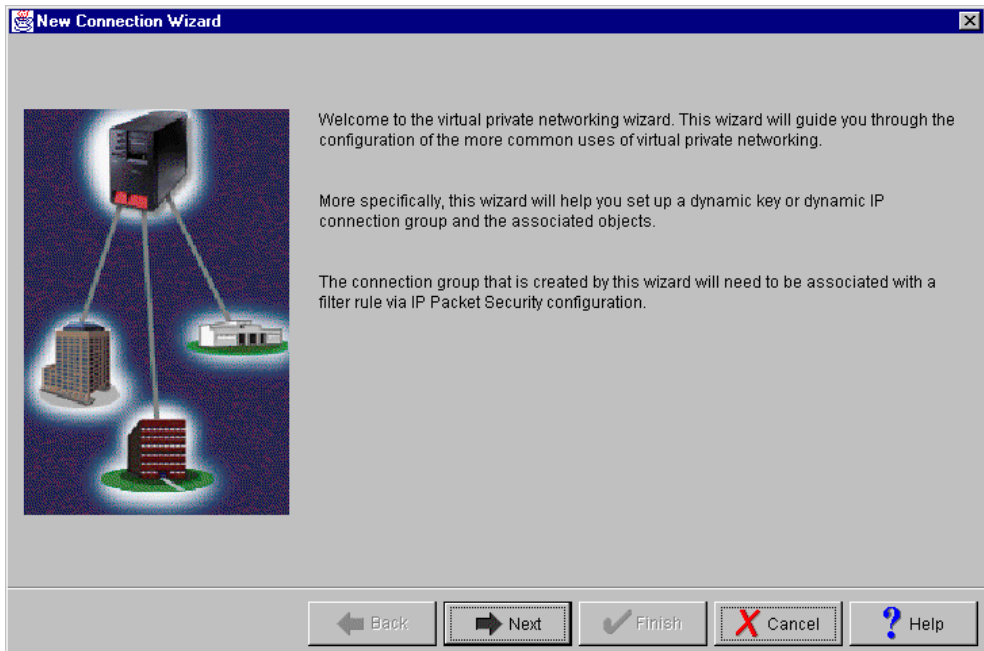


Figure 693. New Connection Wizard welcome window

8. Click **Next** after reading the welcome window.
9. At the Connection Name window, enter `vpnat4servers` for the name of the connection group, and enter a description as shown in Figure 694 on page 595.

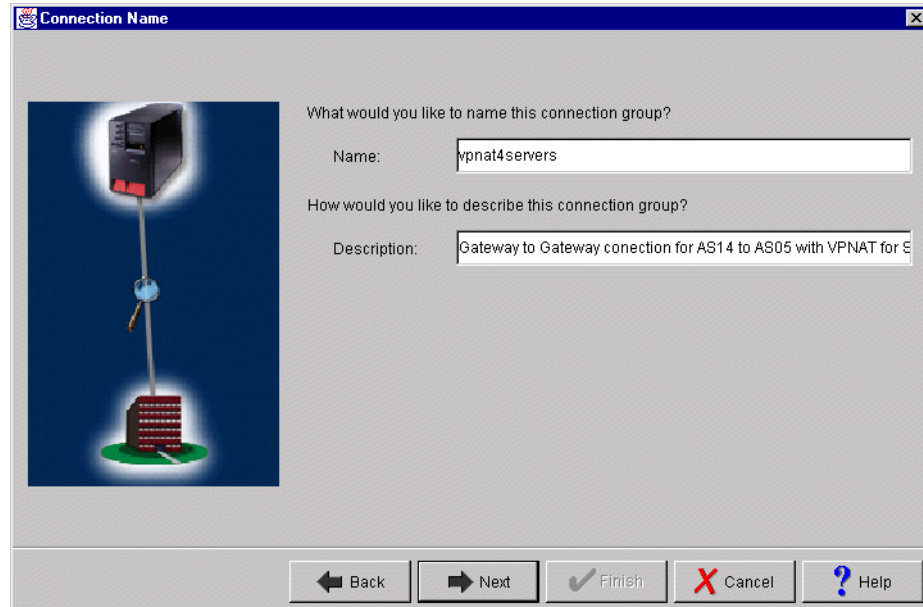


Figure 694. Connection Name window

10. Click **Next**.

11. On the Key Policy window (Figure 695), specify the level of authentication or the encryption protection that IKE uses during phase 1 negotiations. Select **Balance security and performance** as specified on the planning worksheet (Table 78 on page 591). The wizard chooses the appropriate encryption and authentication algorithms based on the selection you make here.

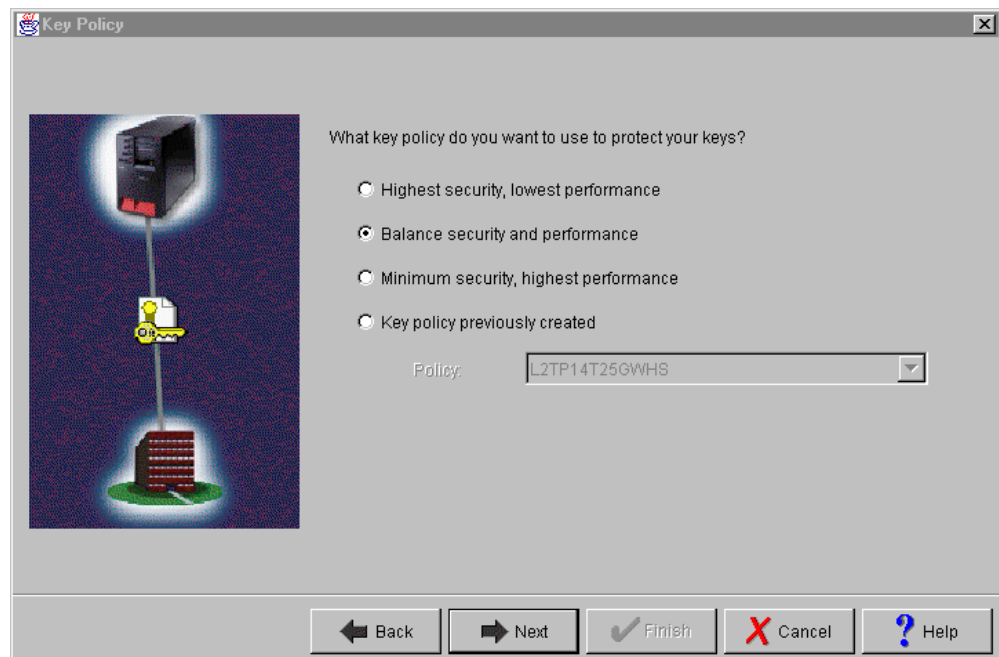


Figure 695. Key Policy window

12. Click **Next**.

13. On the Local Identifier window (Figure 696), specify the identity of the local key server. In other words, specify the local AS/400 system that acts as the VPN gateway, which in this case, is AS14. Leave Identifier type as the default value **Version 4 IP address**. For IP Address, use the pull-down list to select the IP address of the interface that is connecting to the remote gateway AS/400 system (AS05) as shown in Figure 696 on page 596. Refer to the planning worksheet in Table 78 on page 591 and to the network configuration in Figure 689 on page 587. For AS14, this IP address is 204.146.18.227 (interface **A** in Figure 689 on page 587).

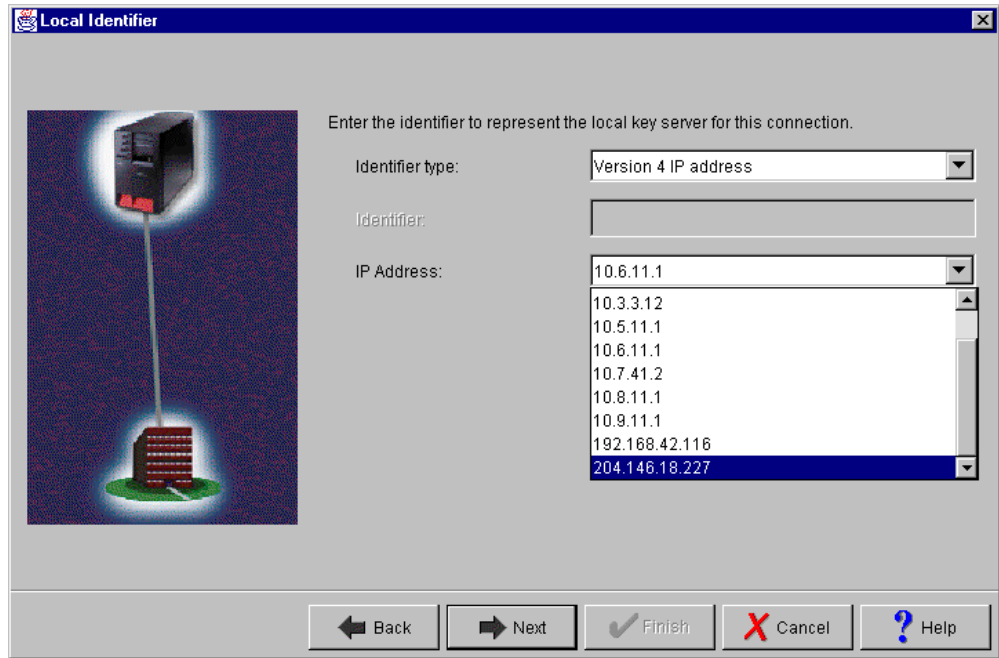


Figure 696. Local Identifier window pull-down list

Figure 697 on page 597 shows the completed Local Identifier window.

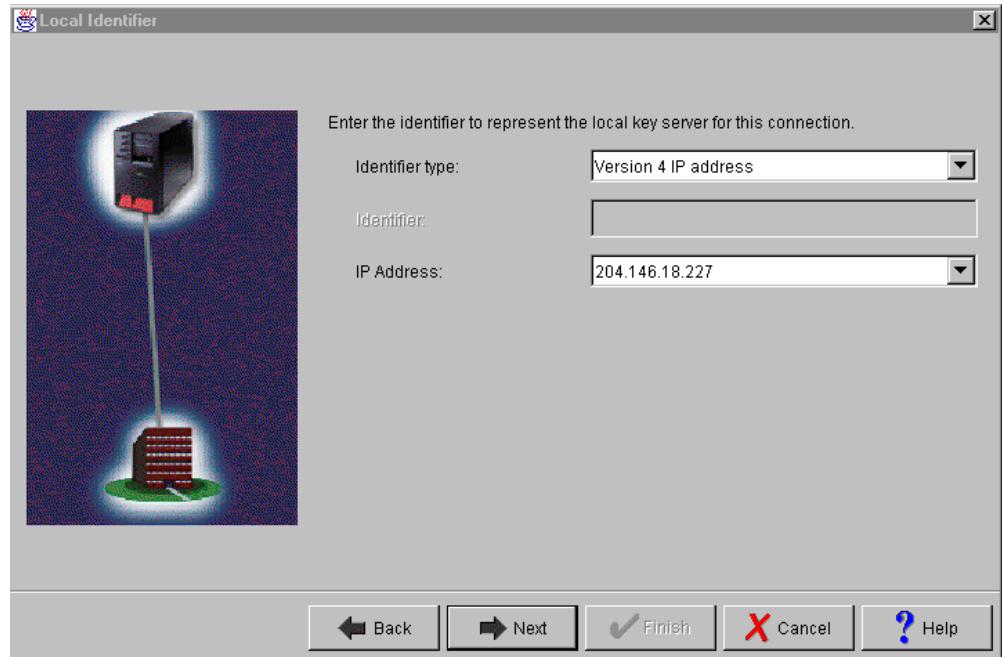


Figure 697. Local Identifier window

14. Click **Next**.

15. On the Remote Network window (Figure 698), enter details about the remote key server, as well as the pre-shared key. The remote key server is AS05 with IP Address 208.222.150.250 (interface **B** in Figure 689 on page 587). Specify `bdcfhnpvqvqa` in the Pre-shared key field. The same pre-shared key must be entered when configuring VPN on the remote AS/400 VPN gateway.

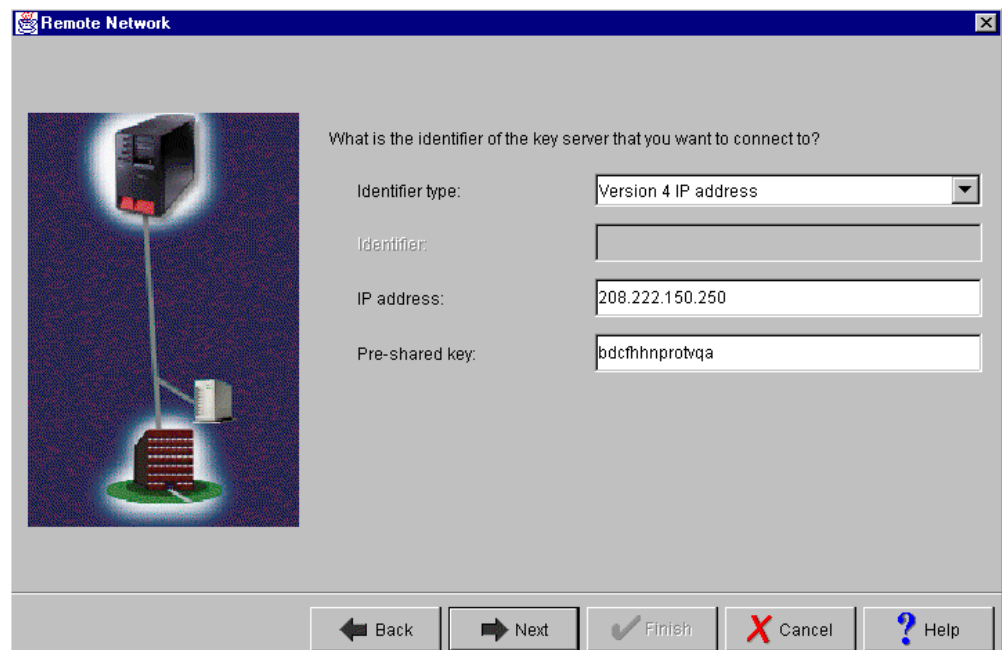


Figure 698. Remote Network window

16. Click **Next**.

17. On the Data Policy window (Figure 699), select **Balance security and performance**.

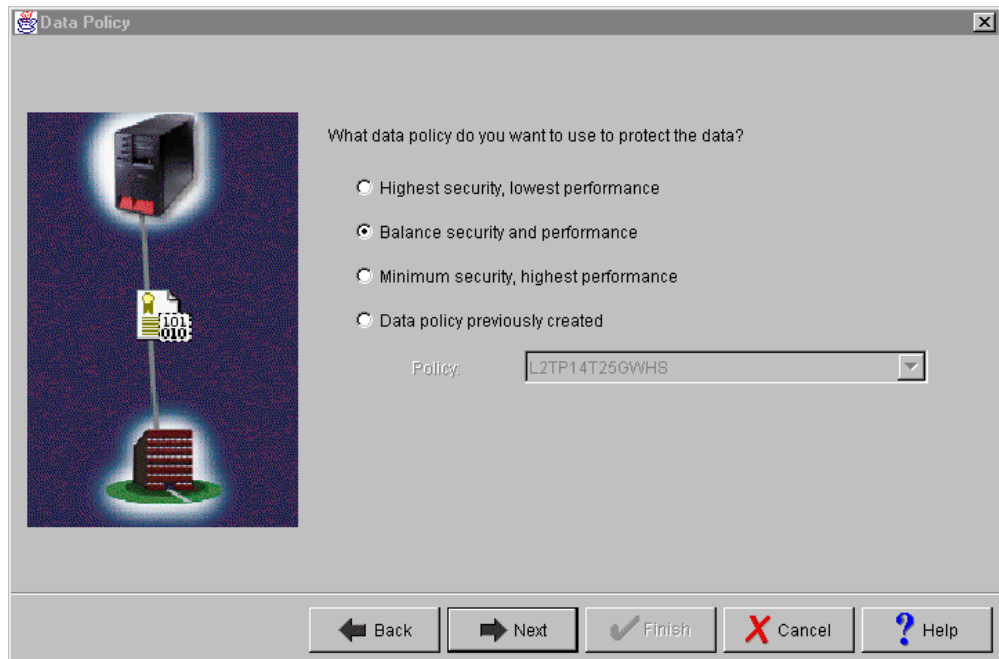


Figure 699. Data Policy window

18. Click **Next**.

19. The New Connection Summary window (Figure 700 on page 599) summarizes the configuration values you entered. Scroll down to see a list of the configuration objects that the wizard creates when you click the Finish button. Check the configuration values against your worksheets. If changes need to be made, click **Back**. Otherwise, click **Finish**.

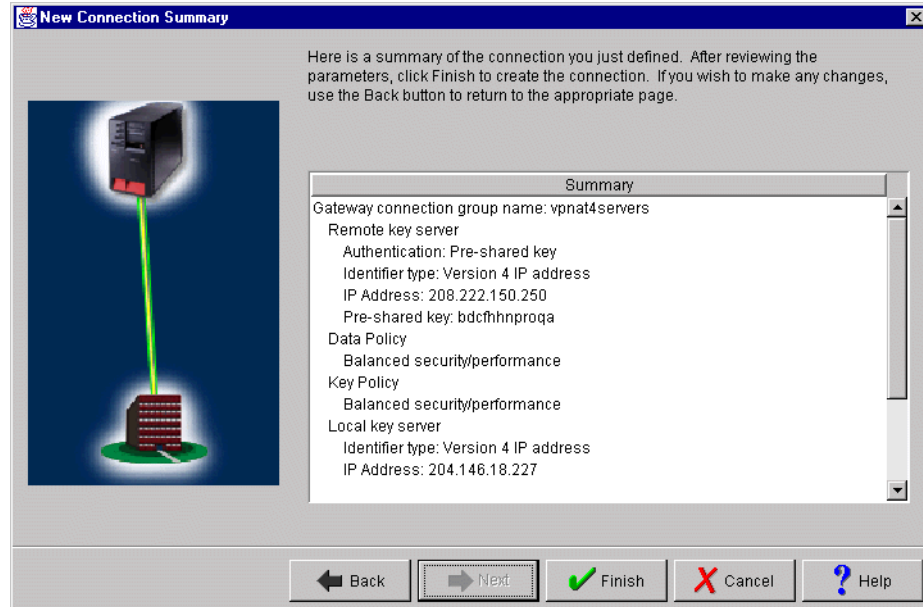


Figure 700. New Connection Summary window AS14

The wizard now creates the various objects you configured for this VPN connection. After a short delay (and assuming there are no errors), you return to the initial VPN GUI Configuration window as shown in Figure 691 on page 593.

At this stage, you can make the changes to the base gateway-to-gateway configuration objects that the wizard created to add the VPN NAT for Servers configuration.

13.6.3 Configuring VPN NAT for servers on AS14

To configure VPN NAT for servers (destination inbound), you must make the following changes to the default gateway-to-gateway configuration created by the new connection wizard:

- Configure the local gateway (AS14) to be the responder of the VPN connection.
- Configure Address Translation to translate the public addresses of the servers into the local (private) addresses of the internal network where the servers are actually located.

To configure VPN NAT for server, perform the following steps:

1. On the Virtual Private Networking window, expand **Data Connections->Dynamic Key Groups** (Figure 701 on page 600).
2. Right-click the dynamic key (connection) group created by the wizard, which is **vpn4servers** in this example.
3. Select **Properties** from the pull-down menu as shown in Figure 701 on page 600.

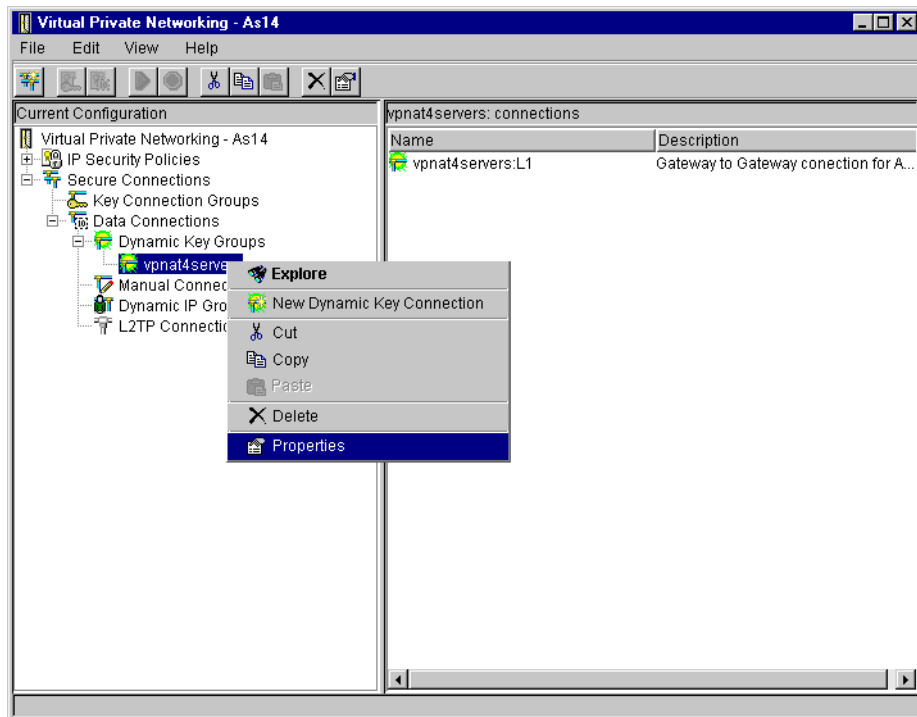


Figure 701. AS14 vpnat4servers dynamic key group properties

4. On the General page, select **Only the remote system can initiate this connection** as shown in Figure 702. VPN NAT for servers destination inbound requires that the gateway performing the address translation be configured as the responder of the VPN connection.

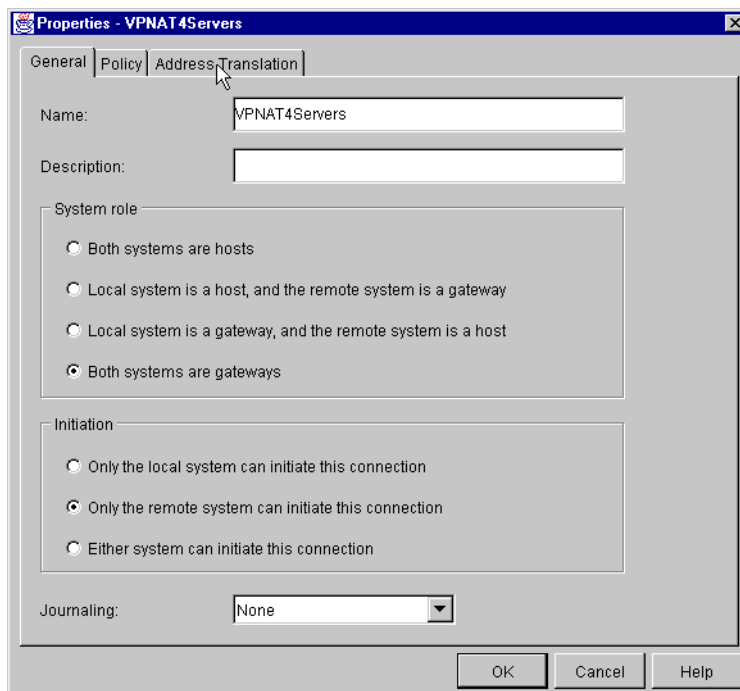


Figure 702. AS14 connection responder

5. Click the **Address Translation** tab to configure the address translation table.
6. Select **Local addresses using addresses from the address translation table** as shown in Figure 703.

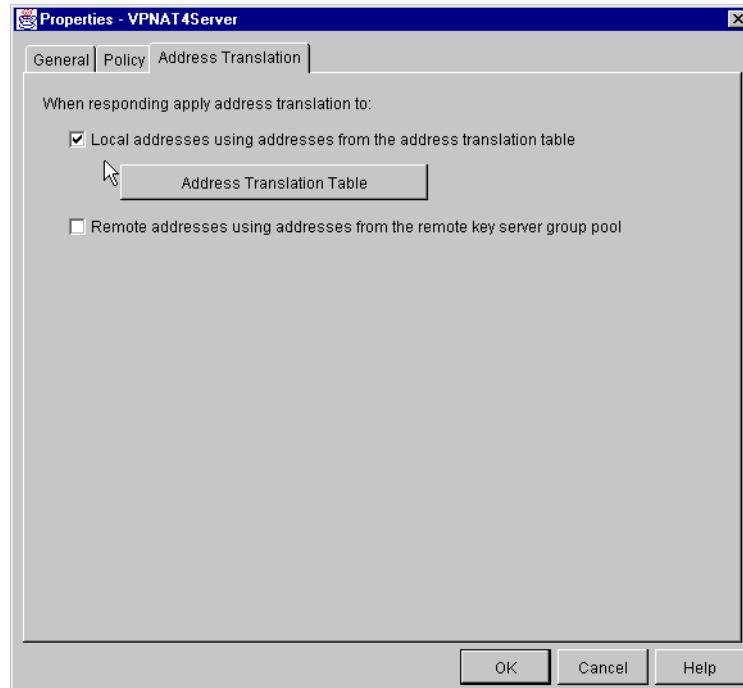


Figure 703. Specifying translation for local addresses

7. Click the **Address Translation Table** button to display the Address Translation Table dialog box as shown in Figure 704.

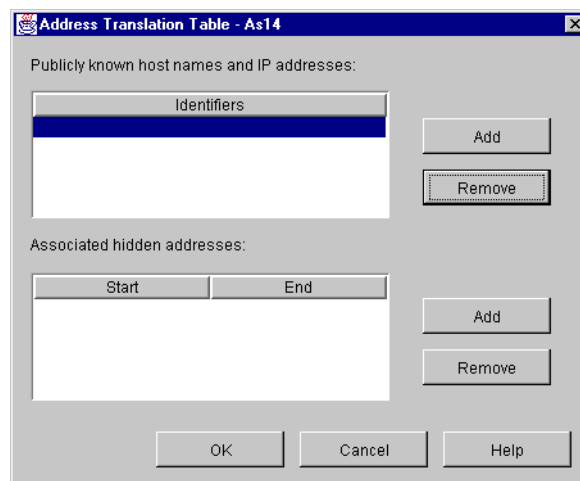


Figure 704. Configuring the Address Translation Table for VPN NAT for servers

The Address Translation Table window has two sections:

- **Identifier:** Contains the list of publicly known IP addresses.
- **Associated hidden addresses:** Contains the corresponding list of private addresses for each host.

- Click **Add** next to the Identifiers list box to add the first internal host public address (Figure 705). Enter the AS20 public address of 172.16.150.100. Refer to the planning worksheet in Table 78 on page 591. Repeat this step for every host publicly known IP address. In this scenario, AS08 is the second host.

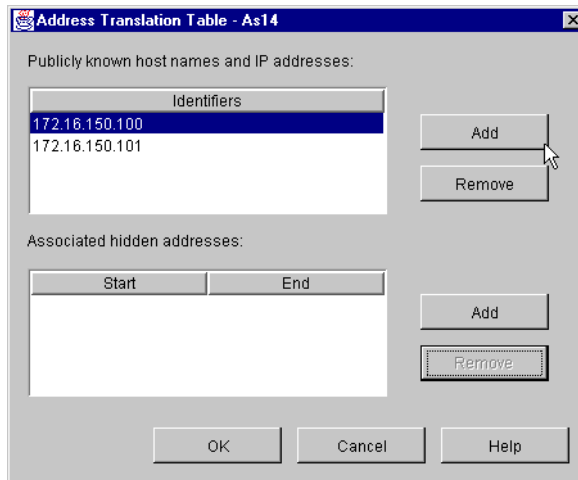


Figure 705. Adding a server identifier to the Address Translation Table

- Select the first publicly known IP address in the Identifiers dialog box, and ensure it is highlighted as shown in Figure 705.
- Click **Add** next to the Associated hidden addresses list box to add the first internal host private address (Figure 706). Enter AS20 private address, 10.186.100.249. Refer to the planning worksheet in Table 78 on page 591. Repeat this step for every host private (hidden) IP address. In this scenario, AS08 is the second host.

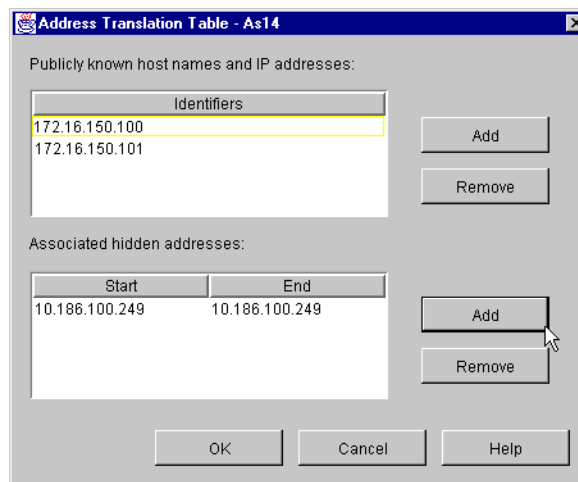


Figure 706. Adding hidden addresses to the Address Translation Table

Note

If the Associated hidden addresses is a single address and not a pool, enter the single IP address for Start and End.

Tip

Use a pool of addresses when you have multiple servers providing the same service for increased availability. Associate the service with a single public address (for example, 172.16.150.102). To do this, the current scenario requires some changes.

First, server addresses for the same service need to be contiguous for example: servers addresses 10.186.100.253 and 10.186.100.254.

Next, change the Address Translation Table to associate public address 172.16.150.102 with the hidden address range 10.186.100.253 through 10.186.100.254. Then, when a VPN connection is requested to server 172.16.150.102, the next available private address (10.186.100.253) is assigned to that VPN connection. If a second VPN connection request is received before the first VPN connection is stopped, the second server address (10.186.100.254) is assigned to that connection.

11. Click **OK** on the Address Translation Table window.

12. Select the **Policy** Tab as shown in Figure 707.

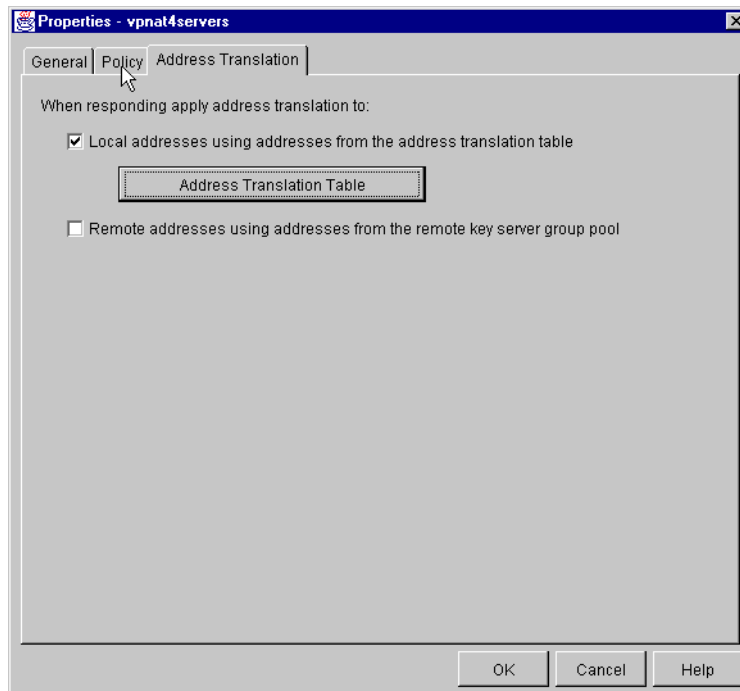


Figure 707. Selecting the Policy tab

13. On the Policy window, select **Connection** or **Single value from connection** for Local address as shown in Figure 708 on page 604. As the responder of this connection, AS14 will accept the value proposed by the initiator within the limits of the IPSEC filter rule associated with this connection group. Refer to 4.3, "Refining the traffic for active connections: Connection granularity" on page 129, for more information.

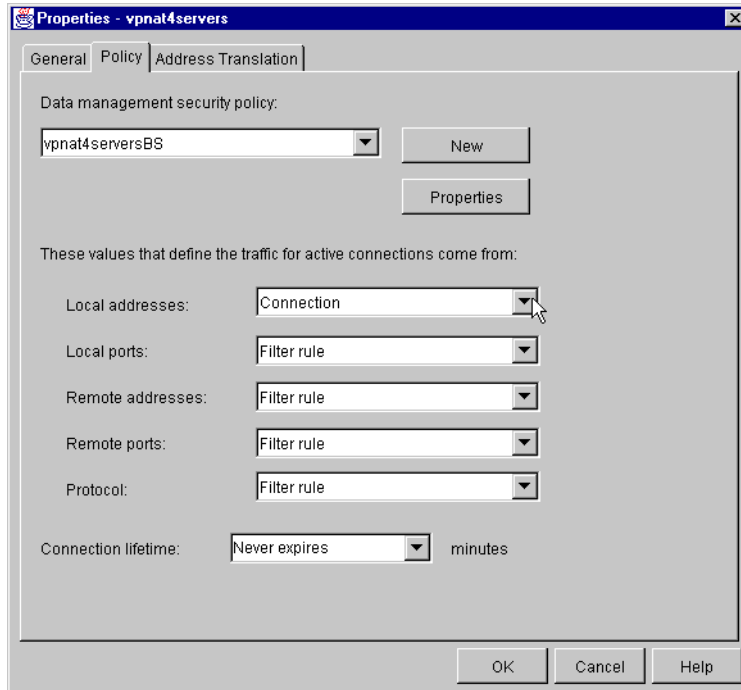


Figure 708. Policy for the vpn4servers connection group

14. Click **OK** to close the properties window and save the configuration changes.

13.6.4 Configuring IP filtering on AS14

The wizard does *not* configure IP filtering. You must complete this task manually by using Operations Navigator. In this example, no filters currently exist. However, if IP filtering is already configured and active, the active filters must be stopped and any new filters must be integrated with those already in existence. Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for more information. Follow these steps:

1. From Operations Navigator, double-click **IP Packet Security** as shown in Figure 709 on page 605. The IP Packet Security configuration GUI starts. You can configure IP filtering and conventional Network Address Translation support using this GUI. However, conventional NAT is incompatible with VPN. Therefore, you cannot configure NAT here to hide the private IP addresses of hosts that participate in a VPN connection.

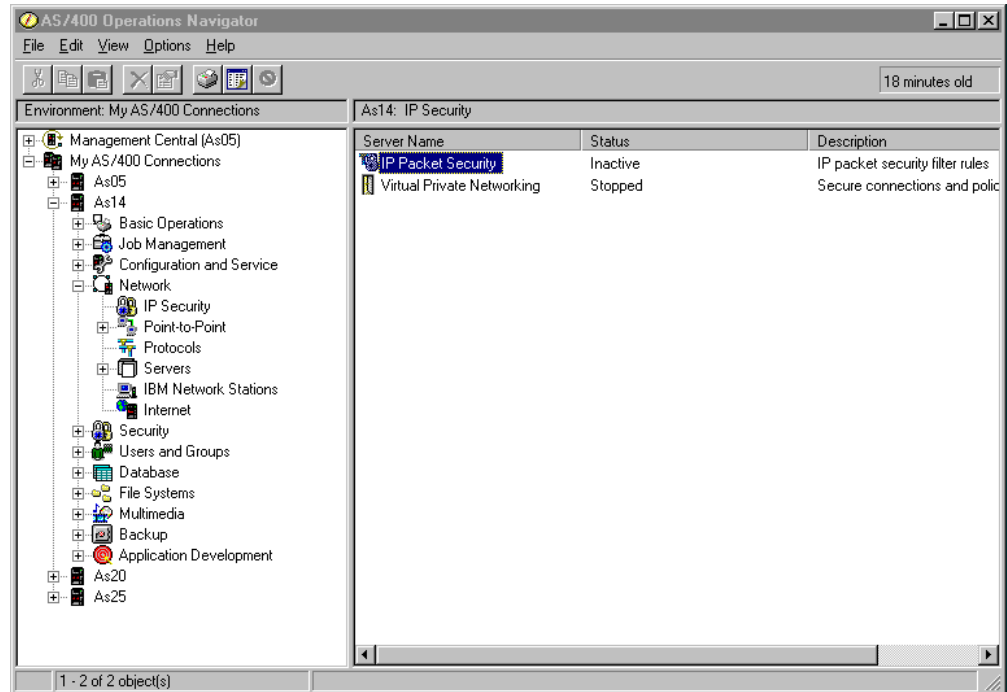


Figure 709. IP Packet Security

In this scenario, we are starting a new IP packet security configuration. All Security Rules displays an empty window (Figure 710).

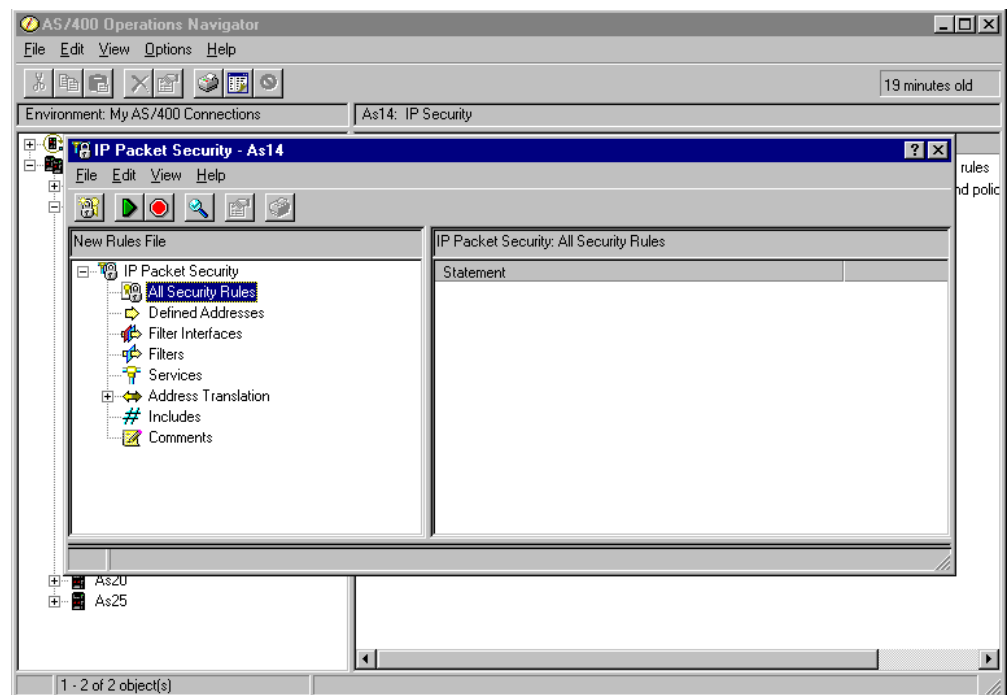


Figure 710. All Security Rules empty

2. Configure the subnets that can use the VPN tunnel. Right-click **Defined Addresses**, and select **New Defined Address** as shown in Figure 711 on page 606.

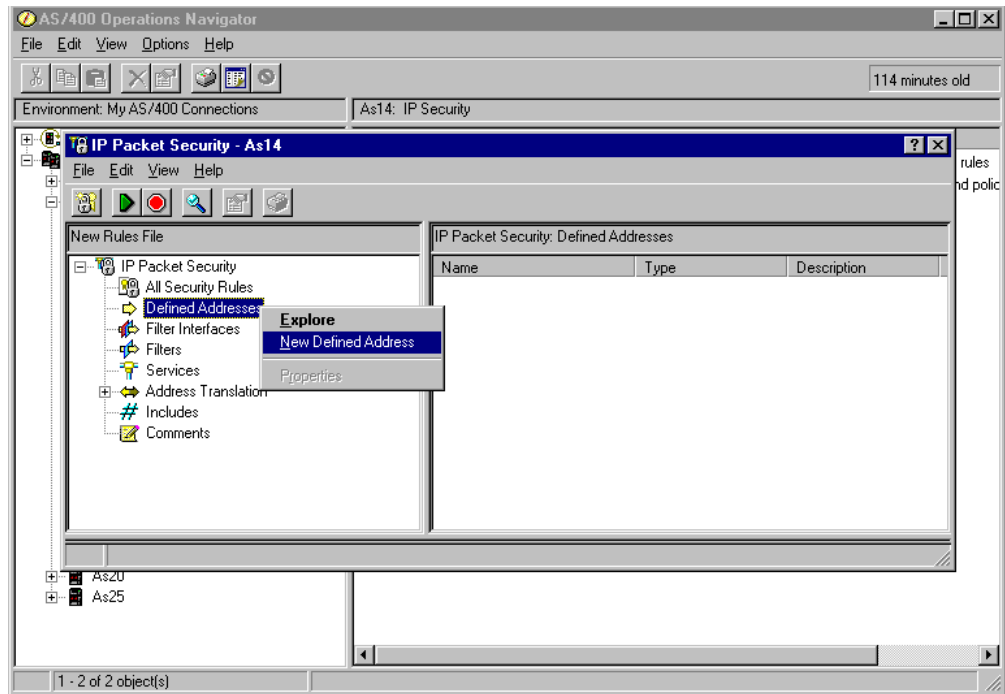


Figure 711. Configuring subnets - New Defined Address

3. The Address name is referenced by other rules using this defined address. You are creating a subnet. Therefore, select **IP specification**, and enter a subnet mask.
4. Click **Add**, and enter the **IP address** of the subnet. You can optionally add a description to document the rules file that you are creating as shown in Figure 712 on page 607.

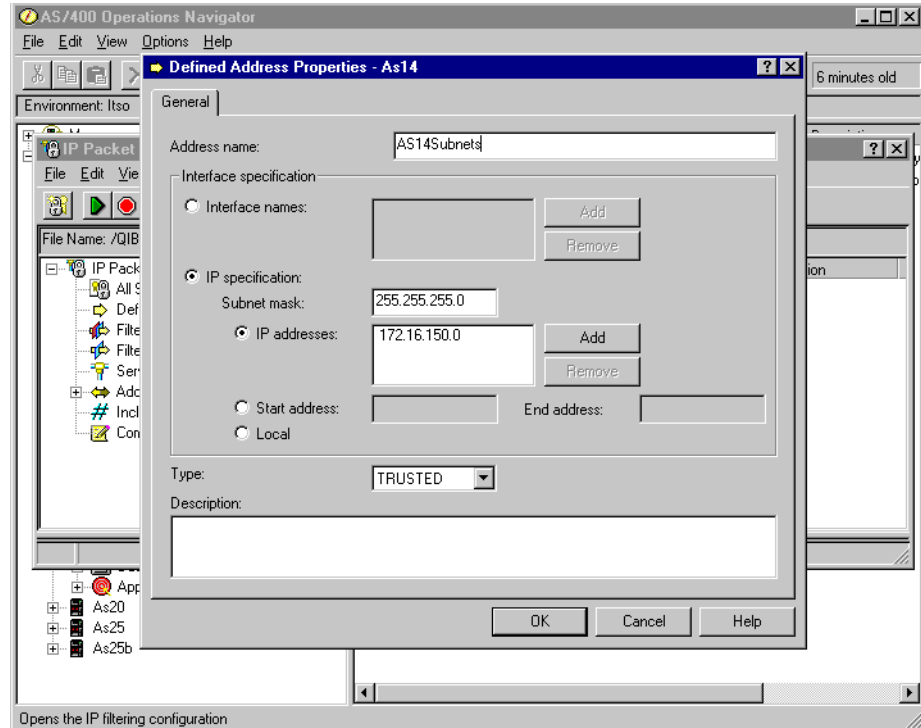


Figure 712. Defined addresses AS14 subnets

Refer to the example worksheet for AS14 in Table 78 on page 591 for the appropriate address name for this subnet. These addresses define the subnet that you are allowing to use the VPN tunnel. In this case, the subnet is 172.16.150.0 with a subnet mask of 255.255.255.0. Since this subnet is the local network to AS14, select the default **TRUSTED** for Type. Complete the remaining fields.

5. Click **OK**.
6. Repeat step 2 through step 5 to create a defined address for the subnet behind the remote VPN gateway. In our example, the address name is AS05subnets, with subnet 10.196.8.0 and subnet mask 255.255.255.0. Because this is the remote subnet, select **UNTRUSTED** for Type as shown in Figure 713 on page 608.

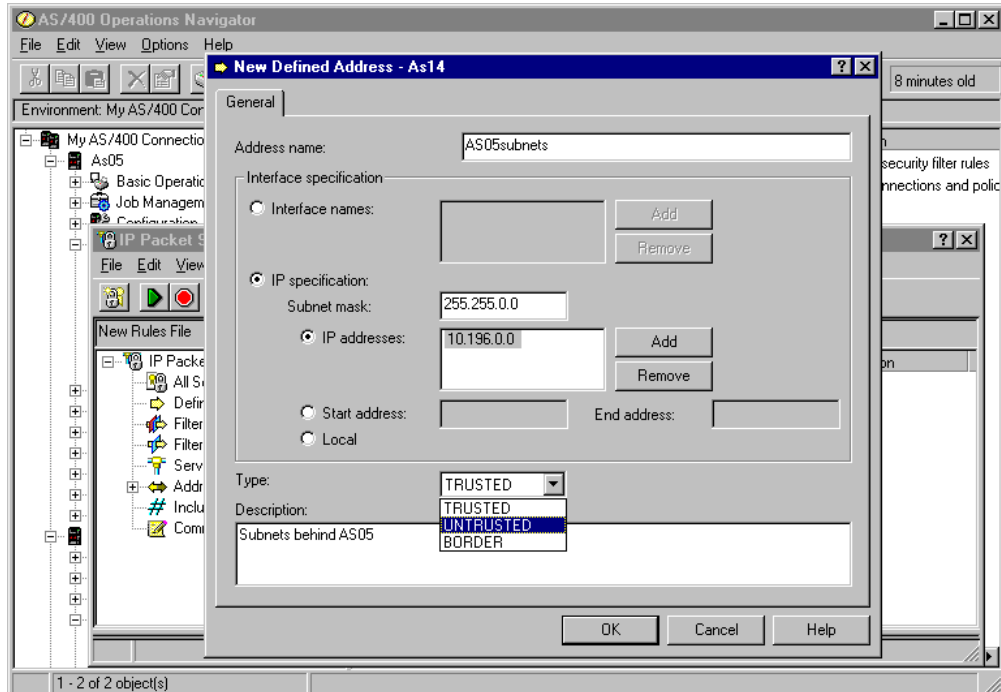


Figure 713. Defined addresses AS05 subnets

- Right-click **Filters**, and select **New Filter**. All associated filter rules (for example, all rules for one interface) should have the same Set name. In this example, we use `VENIFC` for the Set name.

You need to add two rules to allow IKE traffic to flow into and out of the AS/400 system. Select **PERMIT** for Action, and for the first rule, select **OUTBOUND** for Direction. Specify the local AS/400 system's address `204.146.18.227` in the Source address name field, and the remote AS/400 system's address `208.222.150.250` in the Destination address name field.

Leave the other fields on the General page set to their defaults as shown in Figure 714 on page 609.

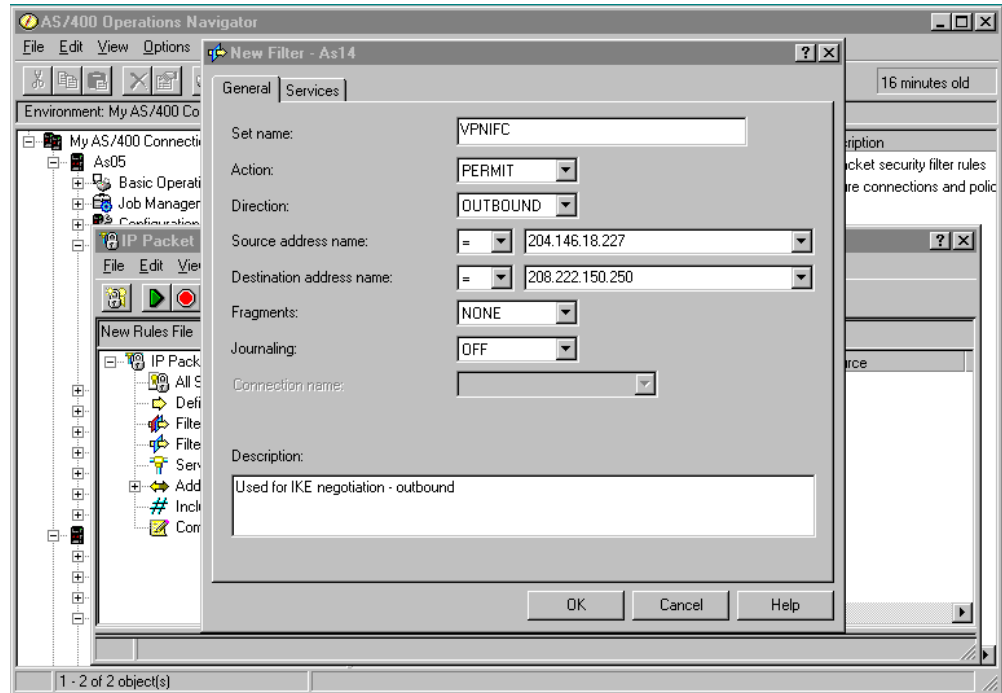


Figure 714. AS14 Outbound IKE filter rule

8. Click the **Services** tab to display the Services window as shown in Figure 715.

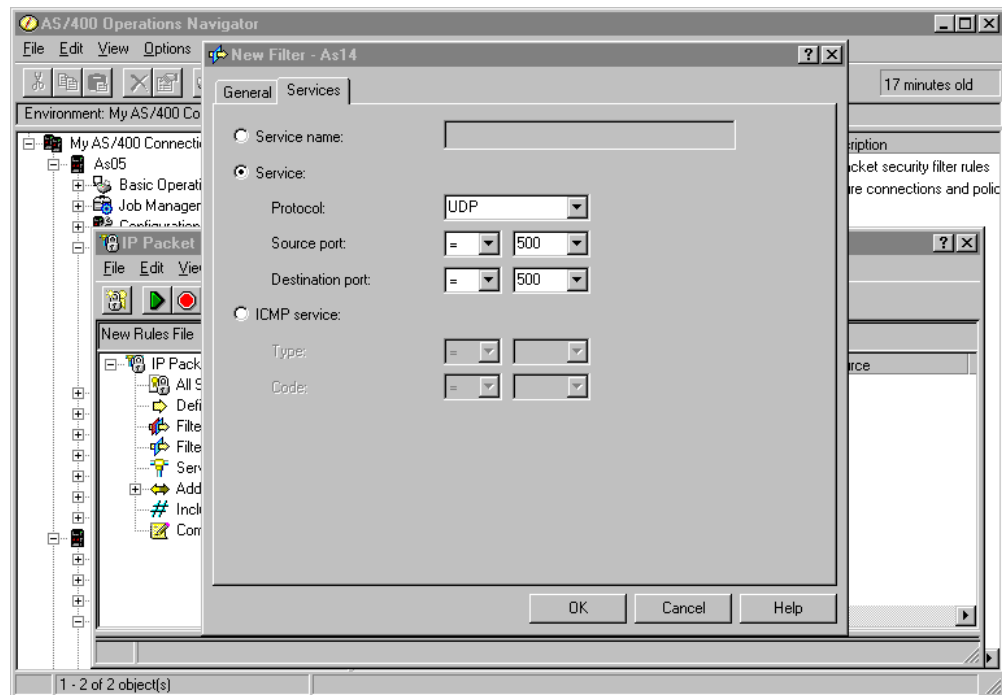


Figure 715. AS14 Outbound IKE filter rule services

9. Select the **Services** tab. In the Protocol field, select **UDP**. In the Source and Destination port fields, specify 500. IKE uses the UDP protocol with source port 500 and destination port of 500 as shown in Figure 715 on page 609.

10. Click **OK**.

11. Repeat steps 7 through 10 to configure the IKE *inbound* filter rule. Remember to reverse the Source and Destination address names. Refer to Figure 716 and Figure 717.

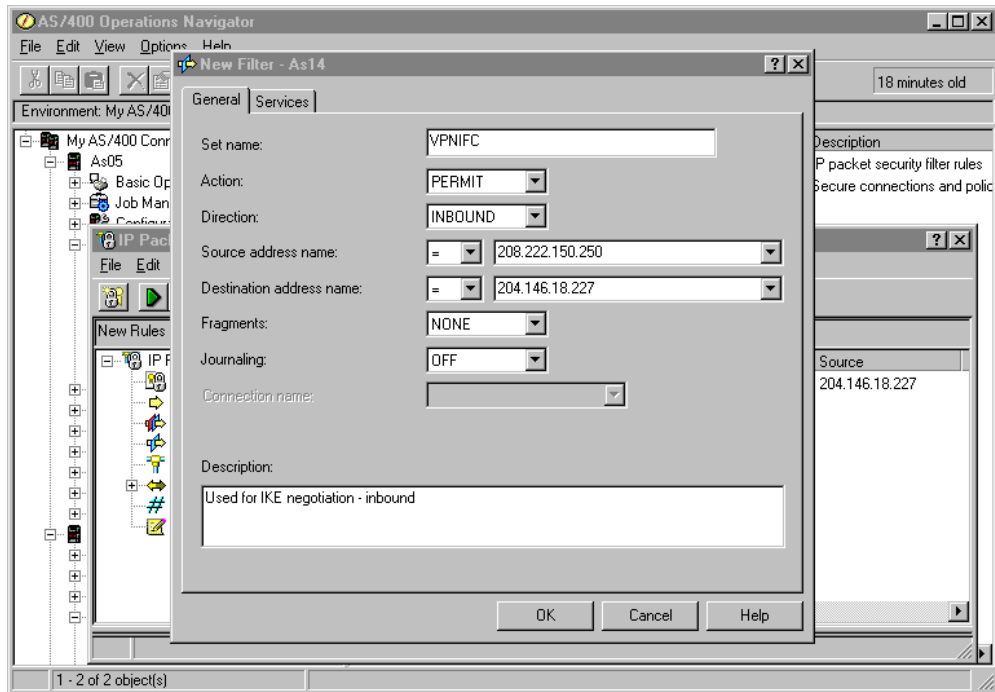


Figure 716. AS14 Inbound IKE filter rule

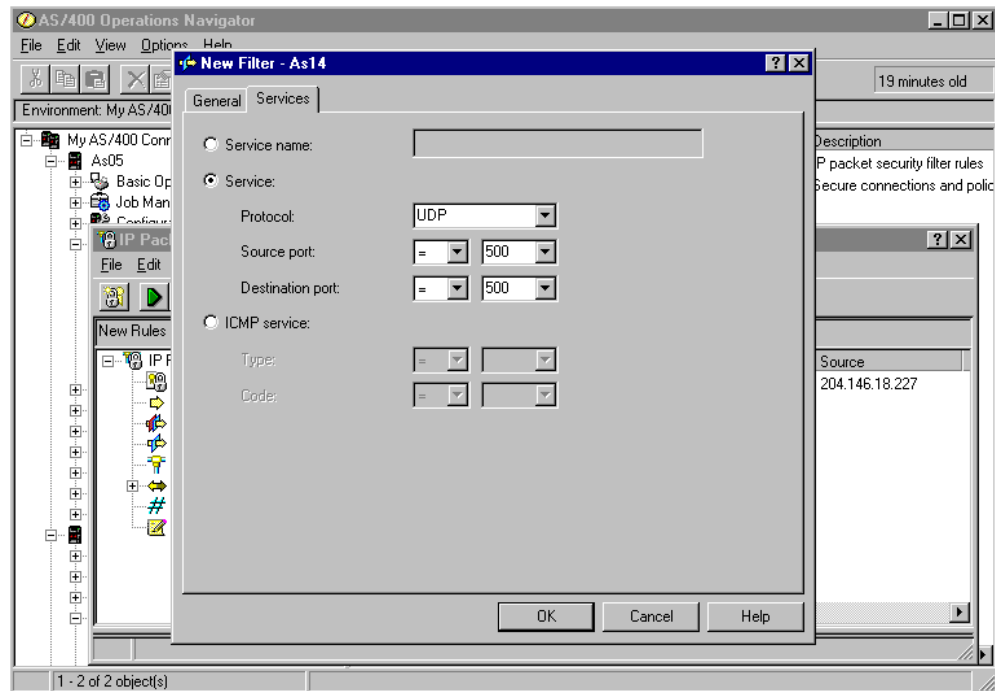


Figure 717. AS14 Inbound IKE filter rule services

12. Create a new filter rule that allows data traffic to use the VPN tunnel. Use the same filter `VPNIFC` for Set name, but select **IPSEC** in the Action field. With an IPSEC filter rule, Direction is always set to **OUTBOUND** and grayed out. In the Source and Destination address name fields, enter the defined address names you created earlier, which is `AS14subnets` and `AS05subnets` in this example. Make sure that the source and destination addresses are in the correct direction. The source address for the local subnets is connected directly to the AS/400 system (AS14 in this scenario) as shown in Figure 718.

Key step

At this stage, you tie the IP filters back to the VPN configuration that you built in the previous task. The *Connection name* is the name of the dynamic key connection *group*. Use the pull-down list to view all the data connection names that have been configured on this system and select the one that is required. In this example, select **vpnat4servers**.

Because IP filters refer to the VPN data connection name, the VPN configuration must be created before configuring the filters.

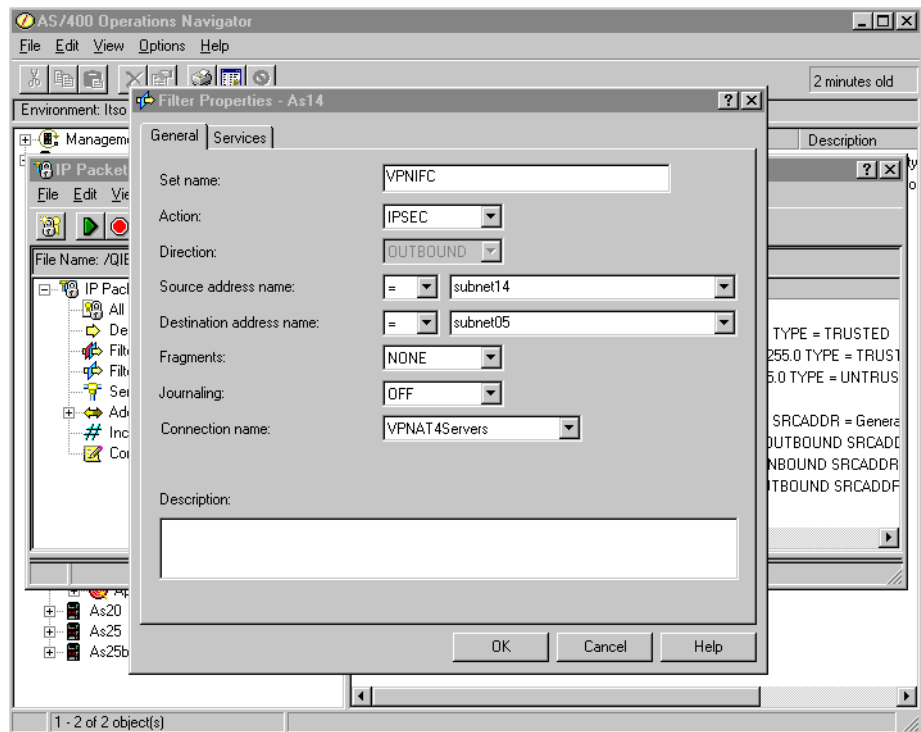


Figure 718. AS14 IPSEC filter rule

13. Click the **Services** tab.
14. Select **Service**, and enter a wildcard (*) for the Protocol, Source port, and Destination port fields. This allows any protocol using any port to use this filter rule and, therefore, the VPN tunnel as shown in Figure 719 on page 612.

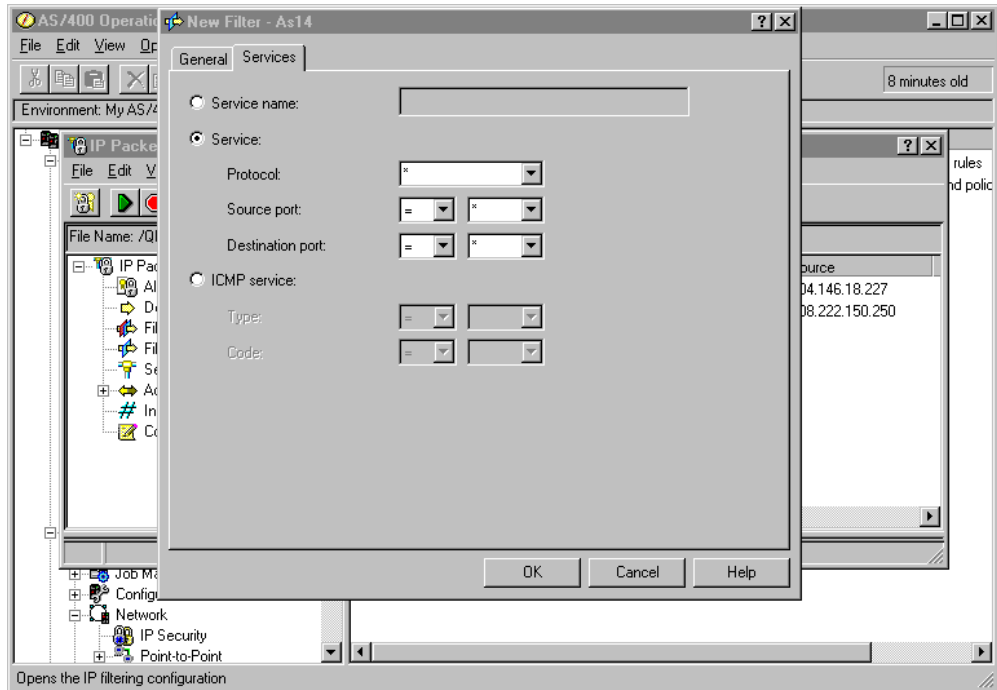


Figure 719. IPSEC filter rule services

15. Click **OK**.

16. The final rule, which ties the filter set that you just created to the required interface, is a filter interface rule. Right-click **Filter interfaces**, and select **New filter interface**. Select **Line name**, and use the pull-down menu to view a list of all the AS/400 line descriptions on the system (for example, created by CRTLINTRN or CRTLINETH). Select the line description that connects *out* to the remote gateway AS/400 system across the Internet or intranet. For this example, select **TRNWSB2**.

Click **Add** to add the filter set name of the filter rules you created previously, which is `VPNIFC` in this example as shown in Figure 720 on page 613.

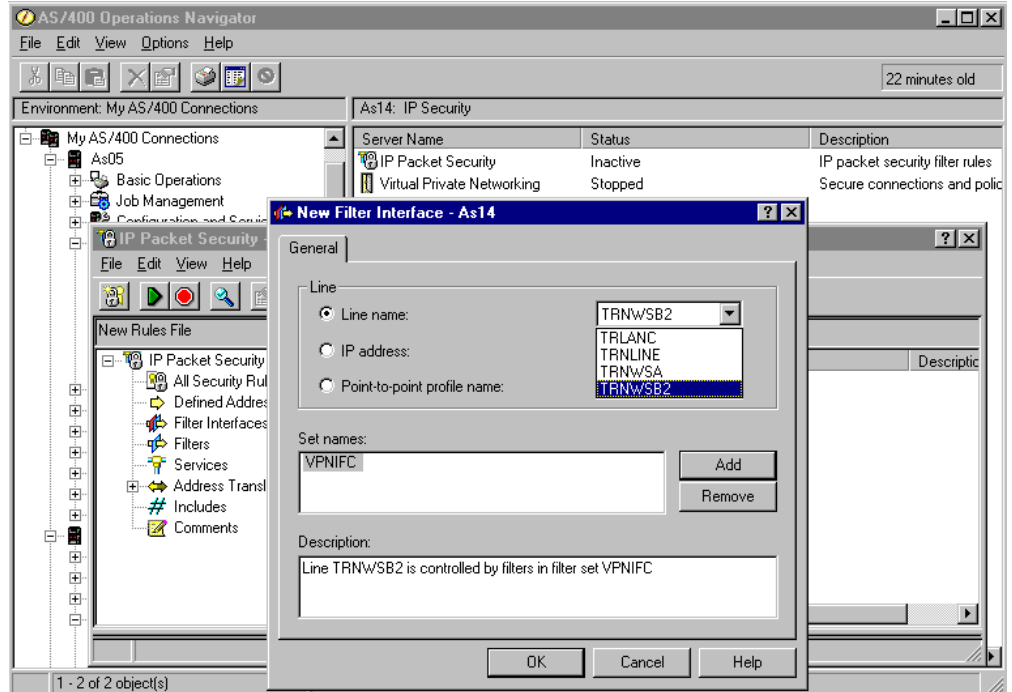


Figure 720. Filter interface rule

17. Once you complete entering filter rules, select **File** from the main menu, and then select **Verify** as shown in Figure 721. Alternatively, there is a verify icon (a magnifying glass) on the toolbar.

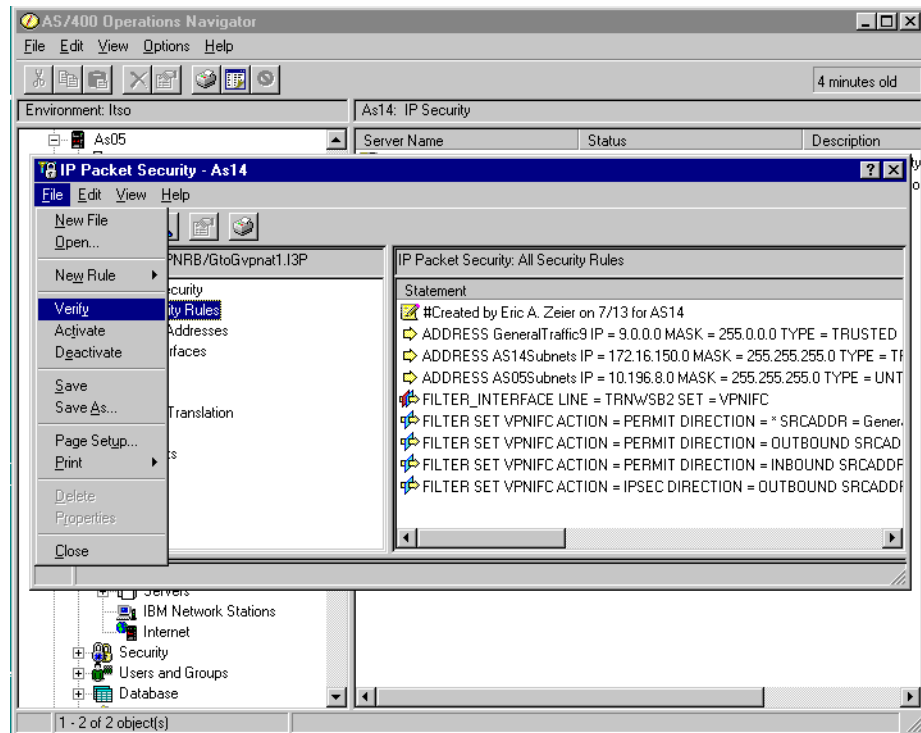


Figure 721. Verify filter rules

18. You can now activate the rules file. Select **File** from the main menu, and then select **Activate** as shown in Figure 722. Alternatively, there is an activate icon (a green triangle) on the toolbar. Look for the message: The rules file was successfully activated.

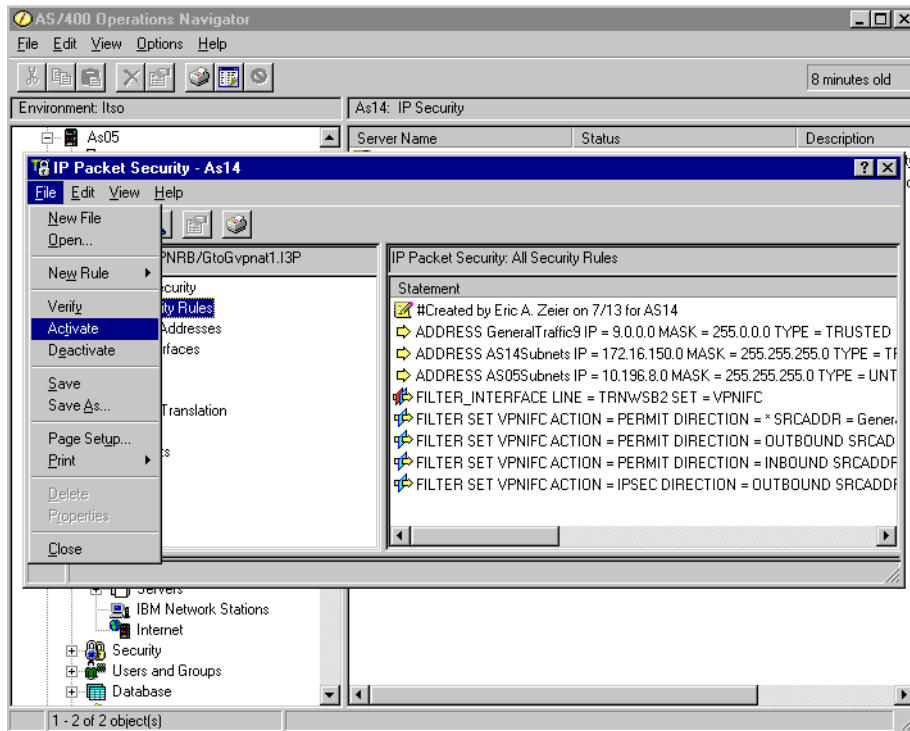


Figure 722. Activating filter rules

19. Save your filter rules file. Select **File** from the main menu, and then select **Save**. The file is saved into the IFS with an extension of *i3p*. In this example, we created a subdirectory, *VPNRB* under the directory *QIBM*. Save the filter rules as *GtoGvpnat1.i3p* into */QIBM/VPNRB*.

Figure 723 shows the summary of the IP filter rules created in this section.

```
IP Packet Security: All Security Rules
#Defined Address AS14Subnets
ADDRESS AS14Subnets IP = 172.16.150.0 MASK = 255.255.255.0 TYPE = TRUSTED
#Defined Address AS05Subnets
ADDRESS AS05Subnets IP = 10.196.8.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
#Filter interface
FILTER_INTERFACE LINE = TRNWSB2 SET = VPNIFC
#IKE filter rules
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.227
  DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 208.222.150.250
  DSTADDR = 204.146.18.227 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC filter rule
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS14Subnets
  DSTADDR = AS05Subnets PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = vpmat4servers
```

Figure 723. AS14 IP filter rules summary

13.7 Configuring the distributor's AS/400 VPN gateway (AS05)

The following sections take you step-by-step through the configuration of VPN and filters on the AS/400 VPN gateway at the distributor's network.

13.7.1 Planning worksheets for the distributor AS/400 gateway (AS05)

Complete the planning worksheets to gather the information you need to create a gateway-to-gateway connection with the VPN configuration wizard on AS05. Table 79 shows the wizard configuration planning worksheet for this scenario from the perspective of the VPN gateway at the manufacturer's network (AS14). Refer to Figure 689 on page 587 for an overview of the network configuration for this scenario.

Table 79. AS05 New Connection Wizard configuration planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Gateway to Gateway
What will you name the connection group?	vpn4servers
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	208.222.150.250 (B)
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	204.146.18.227 (A)
What is the pre-shared key?	bdcfhhnprotvqa
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

To complete the VPN configuration, you must configure IP filters. Table 80 on page 616 shows the IP filter rules configuration planning worksheet for this scenario from the perspective of the VPN gateway at the distributor's network (AS05). Notice the following points:

- The policy (action IPSEC) filter rule allows traffic between subnet 10.196.8.* on the local network and the subnet 172.16.150.* address on the remote network. The publicly known remote network IP address is used. The private addresses of the manufacturer's hosts remains hidden.

- You must configure defined addresses for these subnets and give each of them a name. In this example, specify `AS05subnets` and `AS14subnets` respectively.
- The filter set name that groups the filter rules together is `VPNIFC`.
- Apply the filter rules to the gateway public interface, `TRNLAB1`.
- Only VPN traffic is allowed on the public interface.

Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for information on how to configure IP filters on the AS/400 system.

Table 80. AS05 Planning worksheet - IP filter rules configuration

This is the information you need to create your IP filters to support your VPN	Scenario answers
Is <i>your</i> VPN server acting as a host or gateway ?	Gateway
Is the <i>remote</i> VPN server acting as a host or gateway ?	Gateway
What name do you want to use to group together the set of filters that will be created?	VPNIFC
If <i>your</i> server is acting as a gateway ... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	10.196.8.0 255.255.255.0 AS05subnets
If the remote server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	172.16.150.0 255.255.255.0 AS14subnets
What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	208.222.150.250 (B)
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	204.146.18.227 (A)
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRLANB1
What other IP addresses, protocols, and ports do you wish to permit on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied!</i>	

13.7.2 Configuring the gateway-to-gateway VPN (AS05)

Repeat the steps described in 13.6.2, “Configuring the gateway-to-gateway VPN on AS14” on page 592, but use the configuration values specified in Table 79 on page 615.

Figure 724 shows the New Connection Summary window that the wizard presents at the end of the AS05. Compare this with the equivalent window for AS14 in Figure 700 on page 599.

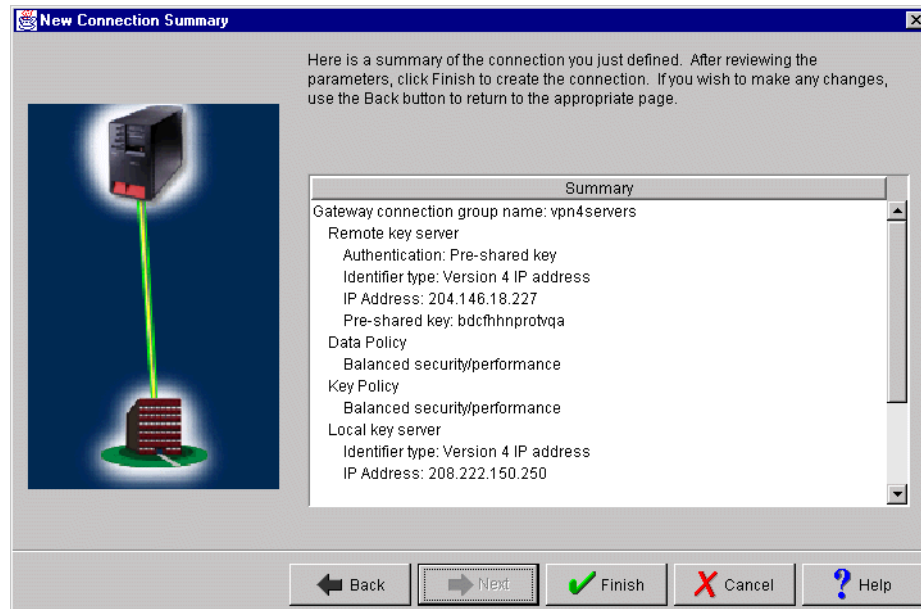


Figure 724. AS05 New Connection Summary window

13.7.3 Making configuration changes for VPN NAT for servers on AS05

Although AS05 is unaware of the VPN NAT for servers configuration on AS14 to hide the private IP address of the hosts at manufacturer’s network, there are some changes that are required to the VPN default configuration created by the wizard. The changes are:

- Configure AS05 as the initiator of the VPN connection.
- Configure two connections, one for each remote host, and specify a single value for the remote IP address.

Perform the following steps to update the configuration created by the wizard:

1. On the Virtual Private Networking window, expand **Data Connections->Dynamic Key Groups**.
2. Right-click the dynamic key (connection) group created by the wizard, which is **vpn4servers** in this example.
3. Select **Properties** from the pull-down menu as shown in (Figure 725 on page 618).

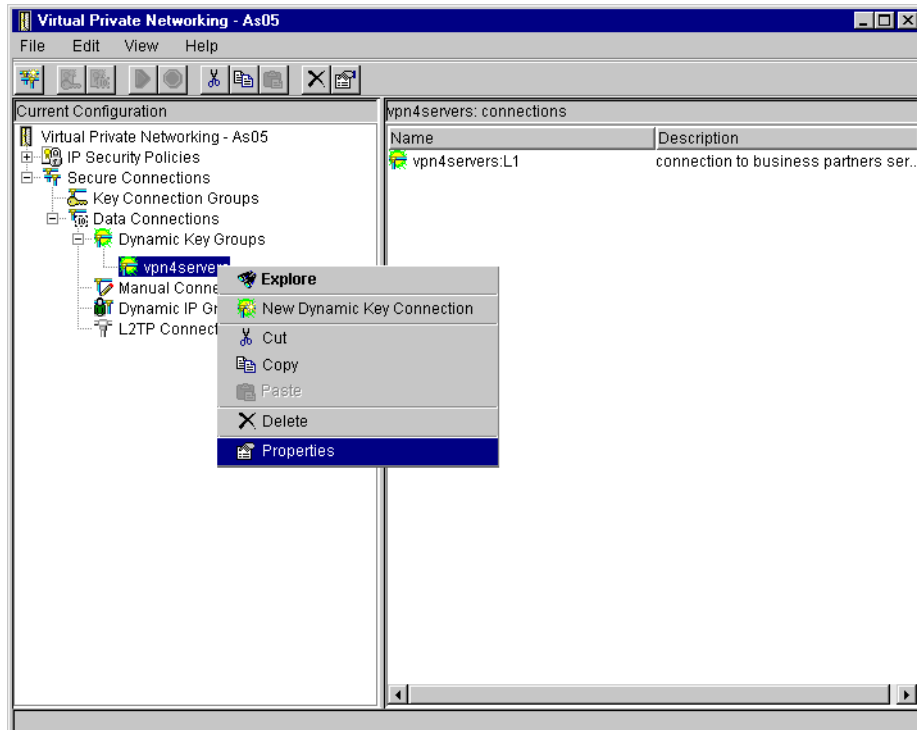


Figure 725. AS05 vpn4servers dynamic key group properties

4. On the General page, select **Only the local system can initiate this connection** as shown in Figure 726. VPN NAT for servers destination inbound requires the remote VPN server (AS05) to initiate the connection.

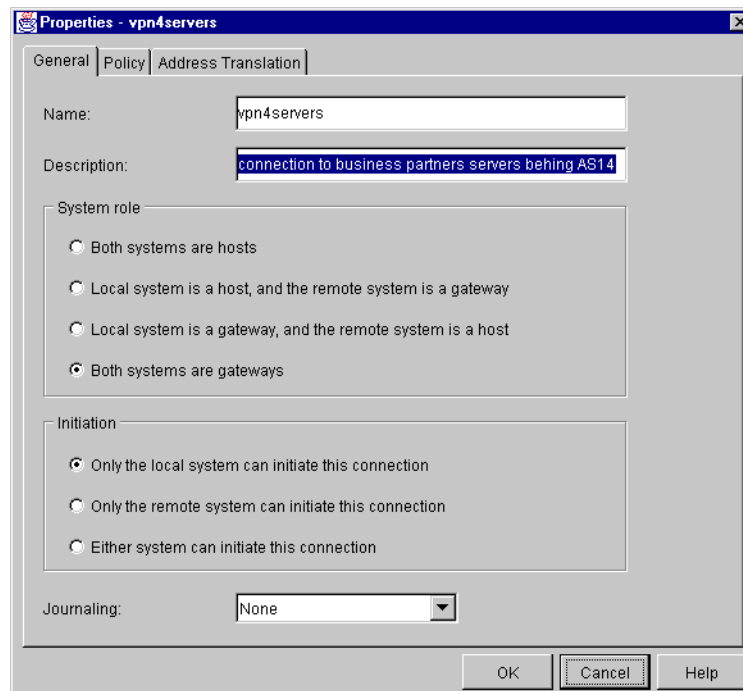


Figure 726. AS05 connection initiator

5. Select the **Policy** tab.

6. On the Policy window, select **Connection** or **Single value from connection** for Remote addresses as shown in Figure 727. Since AS05 is the connection initiator, the value for this parameter is defined in the dynamic key connection. Refer to 4.3, “Refining the traffic for active connections: Connection granularity” on page 129, for more information.

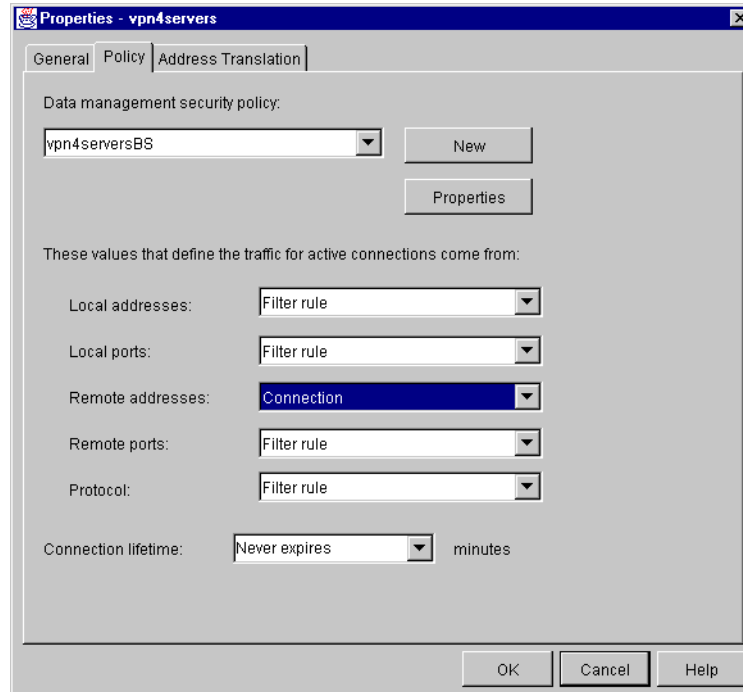


Figure 727. AS05 Policy for vpn4server connection group

7. Click **OK** to close the properties window and save your configuration.

The following steps describe the configuration of the individual dynamic key connections required to access each host in the manufacturer’s network in the VPN NAT for servers scenario. Follow this process:

1. Right-click the dynamic key connection created by the wizard, which is **vpn4servers:L1** in this scenario.
2. Select **Properties** from the pull-down menu as shown in Figure 728 on page 620.

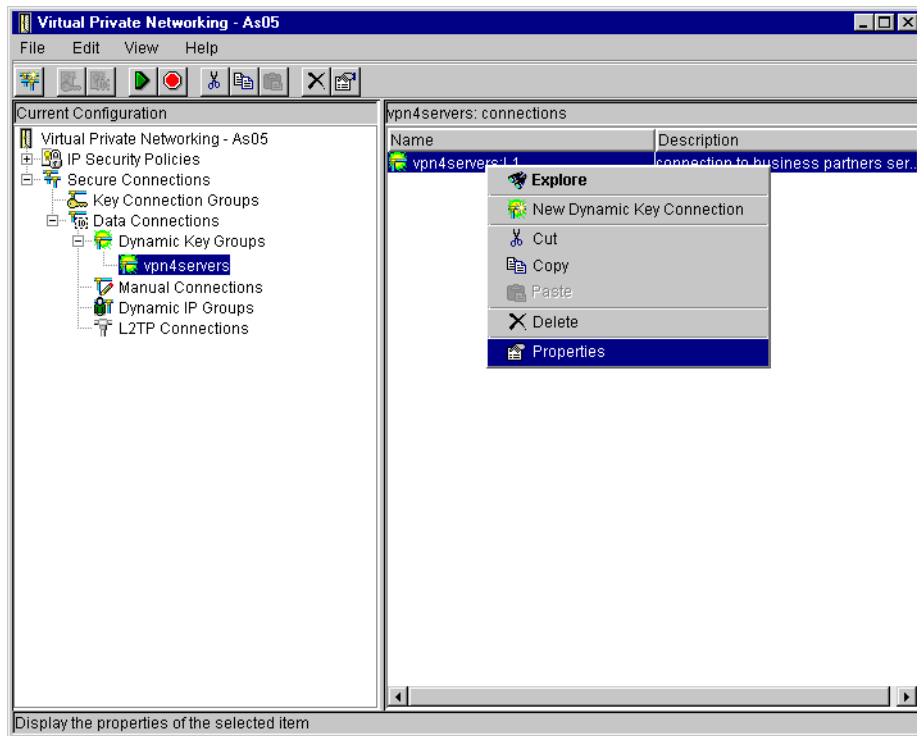


Figure 728. AS05 Dynamic key connection properties

3. Click the **Remote Addresses** tab.
4. Select **Version 4 IP Address** for Identifier type as shown in Figure 729.

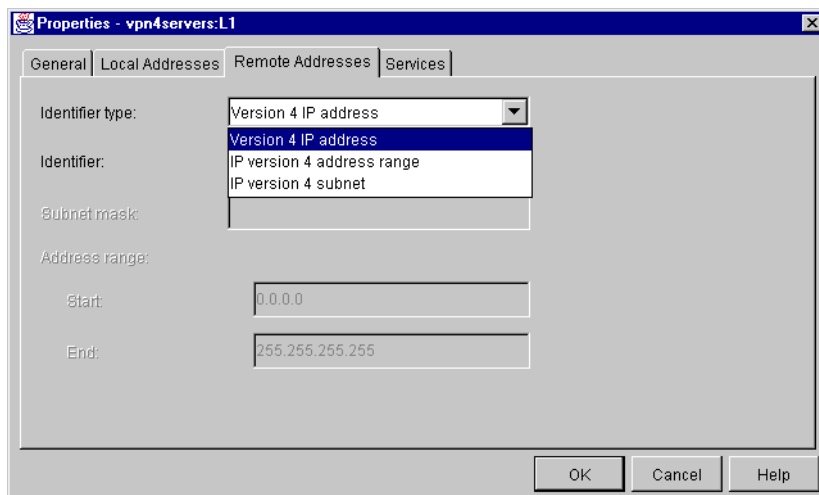


Figure 729. AS05 Configuring the remote host address

5. Specify the single publicly known IP address for the remote server AS20. In this scenario, enter 172.16.150.100 as shown in Figure 730 on page 621. This is the remote data endpoint for this dynamic key connection.

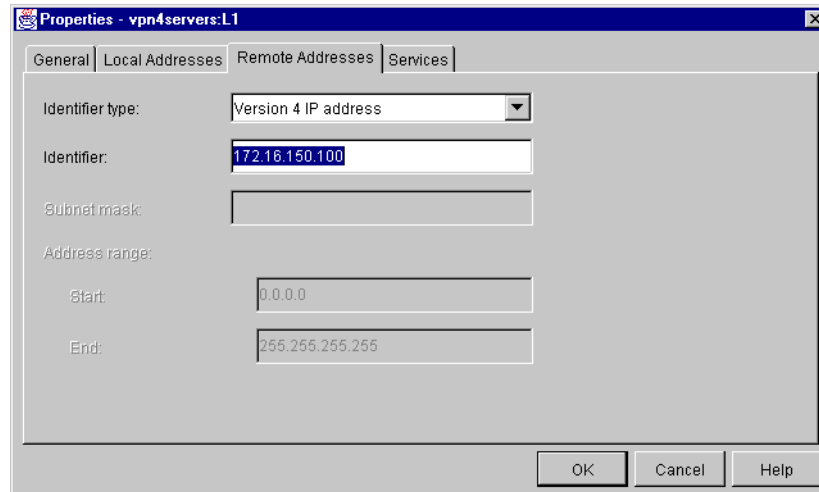


Figure 730. AS05 Specifying AS20 IP address for connection

6. Click **OK** to close the properties pages and save the configuration.
7. To simplify the configuration of the connection to AS08, copy and paste the dynamic key connection to AS20, vpn4servers:L1. Figure 731 and Figure 732 on page 622 show how to copy and paste an existing connection using the VPN GUI.

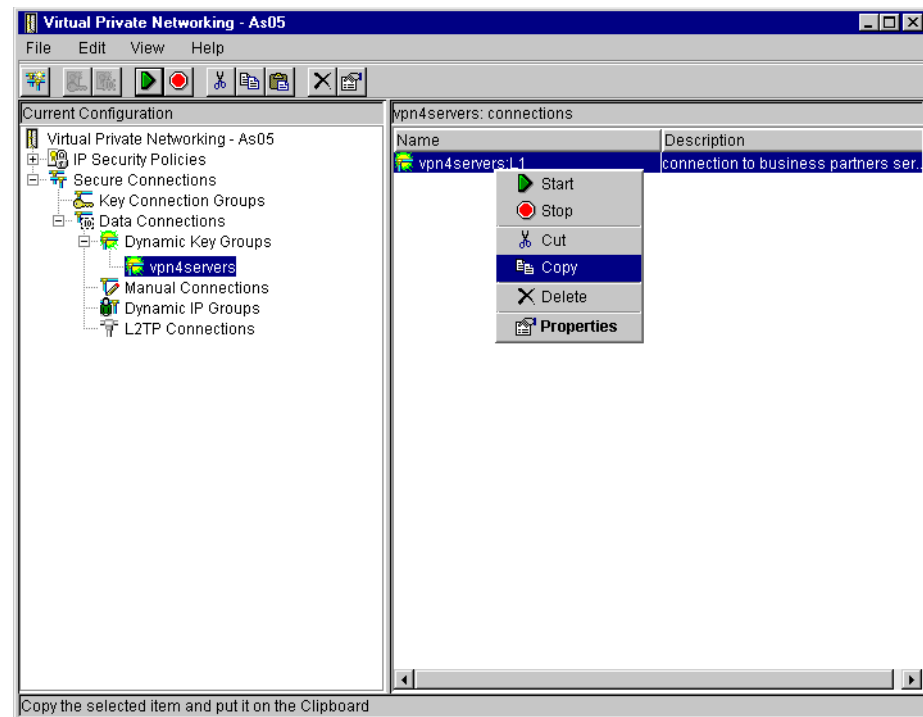


Figure 731. AS05 Copying a dynamic key connection

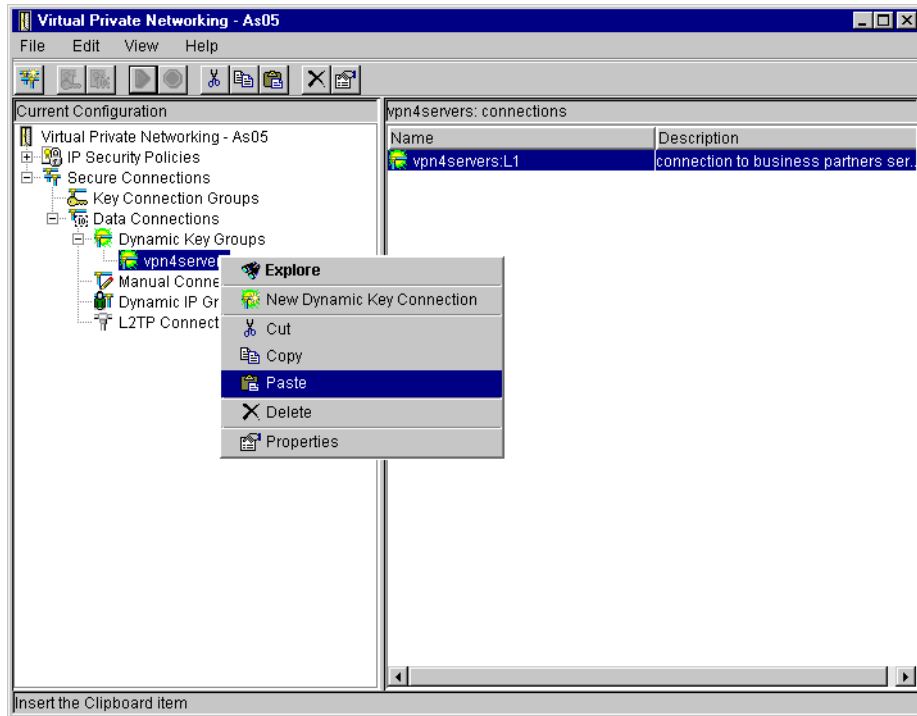


Figure 732. AS05 Pasting a dynamic key connection

8. Right-click the second connection, **vpn4servers:L2**, and select **Properties** from the pull-down menu as shown in Figure 733.

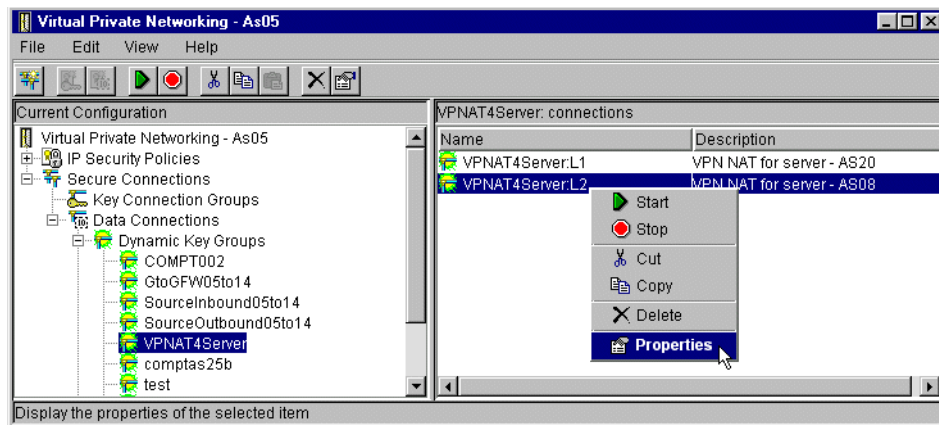


Figure 733. AS05 Dynamic key connections to access remote hosts in the VPN NAT scenario

9. Change the Remote Addresses field to AS08's publicly known IP address 172.16.150.101 as shown in Figure 734 on page 623.

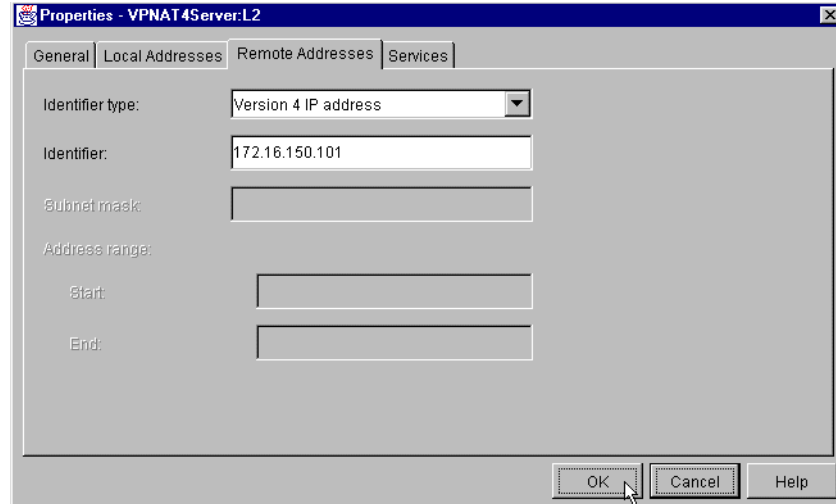


Figure 734. AS05 Specifying AS08 IP address for connection

10. Click **OK** to save the changes.

13.7.4 Configuring IP filtering on AS05

The wizard does not configure IP filtering. You must complete this task manually. Repeat the steps described in 13.6.4, “Configuring IP filtering on AS14” on page 604, but reverse the IP addresses.

Figure 735 shows All Security Rules for the IP filters configured on AS05 for this scenario.

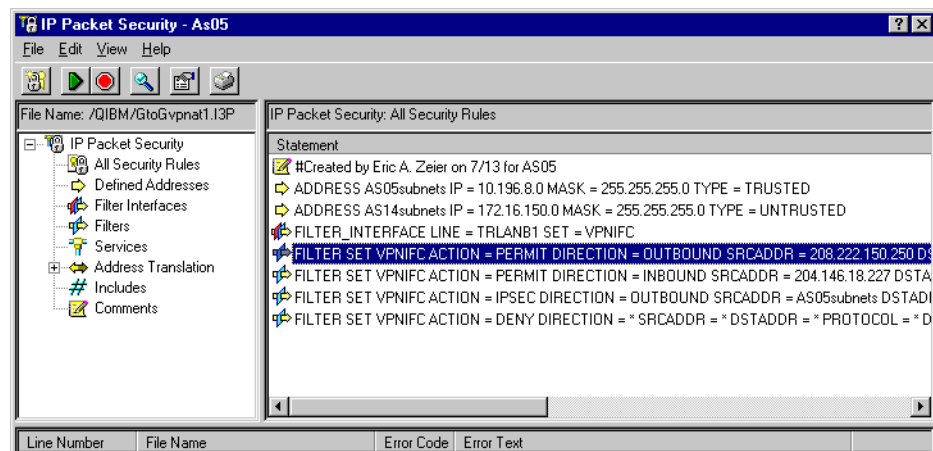


Figure 735. AS05 All Security Rules

Figure 736 on page 624 shows the summary of the IP filter rules created in this section.

```

IP Packet Security: All Security Rules
#Defined address local network
ADDRESS AS05subnets IP = 10.196.8.0 MASK = 255.255.255.0 TYPE = TRUSTED
#Defined address remote network
ADDRESS AS14subnets IP = 172.16.150.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
#Filter interface
FILTER_INTERFACE LINE = TRLANB1 SET = VPNIFC
#IKE filter rules
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 208.222.150.250
    DSTADDR = 204.146.18.227 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 204.146.18.227
    DSTADDR = 208.222.150.250 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC filter rule
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS05subnets
    DSTADDR = AS14subnets PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = VPNAT4Server

```

Figure 736. AS05 IP filter configuration summary

13.7.5 Starting the VPN connections

For a complete description on activating IP filters and starting VPN connections, refer to 3.8, “VPN operations and management” on page 84.

The following list summarizes the steps you must perform to start the VPN connections:

1. Activate IP filters on both AS/400 systems (AS14 and AS05).
2. Start Virtual Private Networking on both AS/400 systems (AS14 and AS05).
3. On the initiator AS/400 system, AS05, start the dynamic key connections to AS20 and to AS08. In this scenario, start the connections **vpn4servers:L1** and **vpn4servers:L2** as shown in Figure 737 on page 625.

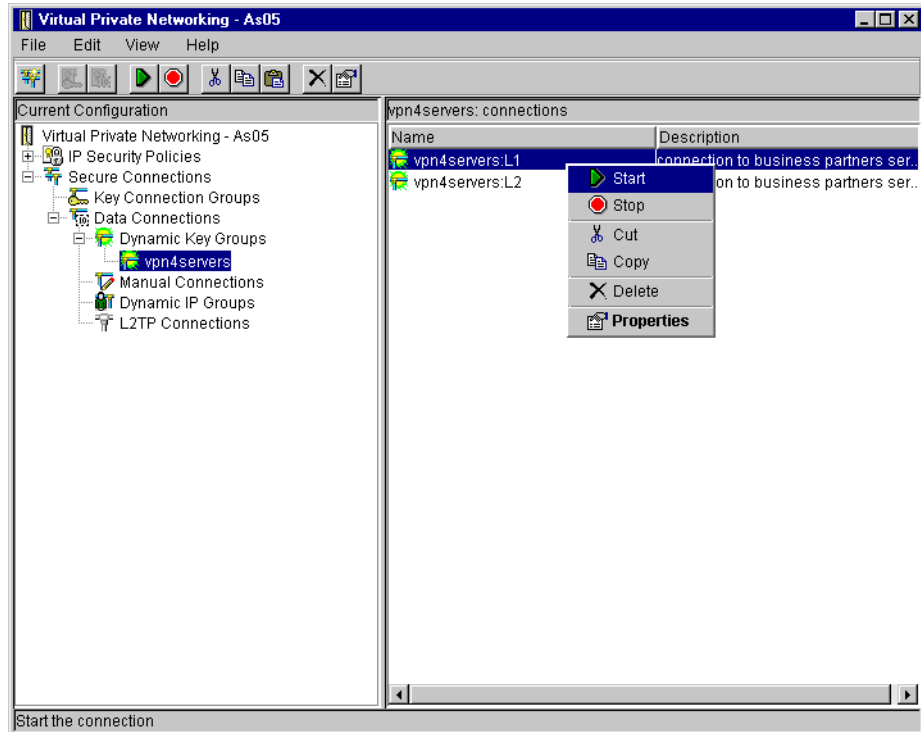


Figure 737. AS05 Starting dynamic key connections from the initiator AS/400 system

4. Click **View**, and select **Active Connections** as shown in Figure 738.

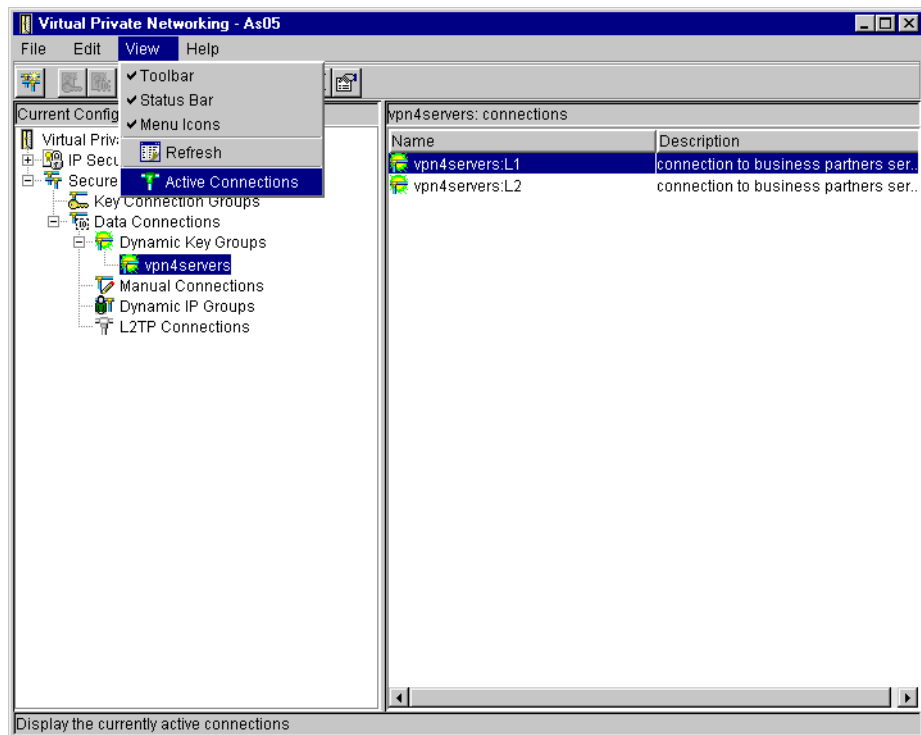


Figure 738. View Active Connections

The Active Connections window displays two connections with the status as Running, which is shown in Figure 739.

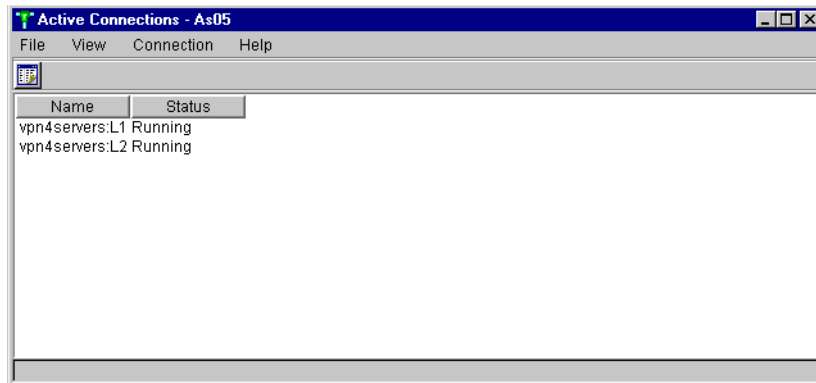


Figure 739. AS05 Active Connections window

Chapter 14. AS/400 VPN problem determination

Problem determination in a communications network is never an easy task. It becomes more complex when protocols such as the IPSec protocols are implemented since they add authentication, cryptography, key negotiation, key refresh, and usually a multivendor environment.

To implement VPN successfully on a TCP/IP network, you should have a working knowledge of the following subjects:

- TCP/IP protocol and routing
- IP packet filtering
- VPN architecture

This chapter introduces the tools available to troubleshoot AS/400 VPNs. It provides some general guidelines on problem determination techniques that you can apply when implementing AS/400 VPNs.

It is important to remember that there are two endpoints in any VPN connection. One endpoint may not show any problems or errors, but it may be indirectly cause a failure. You need to keep the two endpoints in mind when troubleshooting. This chapter assumes that at least one endpoint of the VPN connection is an AS/400 system. The following recommendations can help you avoid common pitfalls:

- Ensure that the latest VPN PTFs are installed and applied on your AS/400 system.
- Verify end-to-end network connectivity and routing before starting filters and VPN connections. This eliminates several variables that may introduce errors.
- If possible, use PING to verify end-to-end connectivity. PING is a common tool that network administrators use to verify system connectivity. However, there may be filtering routers or hosts that do not allow or do not respond to PING requests (based on ICMP messages). Telnet and FTP are other commonly used protocols to test end-to-end connectivity. Always make sure that all the elements in the path allow the protocols and services you use for testing.
- If PING worked before you attempted the VPN connection, and it doesn't work afterwards, make sure your filter rules and VPN connection allow PING to work afterwards (if this is the technique you're using to verify connectivity).
- Since you are dealing with two endpoints, it is possible to configure filter rules and connections that are uni-directional. That is, you may be able to establish a Telnet session from System A to System B, but not from System B to System A.
- If you don't have previous experience with IP filter and VPN configurations, start with as few IP filters as possible. Configure only the filters required for the VPN. That is, permit IKE traffic and apply IPSEC to all other traffic. Examples of such filter rules are shown in several scenarios in this redbook.
- Keep in mind that you may need to permit internal TCP/IP traffic to allow at least the PC running Operations Navigator to access the AS/400 system where you are configuring VPN.

- After you configure successfully the simplest VPN connection, you can build more restrictive IP filters or VPN connections depending on what your security policy specifies.

The information in this chapter complements the *Troubleshooting Guide for AS/400 VPN* in the AS/400 Information Center on the Web at <http://www.as400.ibm.com/infocenter> under the **Internet and Secure Networks** category. It also complements the information on the Web at: <http://www.as400.ibm.com/vpn>

Tip

For late breaking news, frequently asked questions (FAQs), known problems, latest VPN PTFs, and other up-to-the-minute information on AS/400 VPN support, log on to: <http://www.as400.ibm.com/vpn>

14.1 AS/400 VPN problem determination tools

This section describes the tools available on the AS/400 system to troubleshoot VPN problems. These tools include:

- Active Connections window
- IP filter journal
- VPN journal
- Trace TCP/IP Application (TRCTCPAPP) command
- Job logs
- Communication trace
- NETSTAT command
- QSYSOPR message queue

14.1.1 Active Connections window

Use the Active Connections window as the entry point to find AS/400 VPN problems. By default, the Active Connections window displays basic information that lists the connections running, and in error, on this AS/400 VPN server. The Active Connections window does not list stopped connections. To take advantage of the Active Connections window, customize its settings to include the information you want to display. Refer to 3.8.6, “Checking the VPN connections status” on page 97, for information on how to start and customize the Active Connections window.

To add more fields to display by the Active Connections window, click on the **Columns** tab as shown in Figure 740 on page 629.

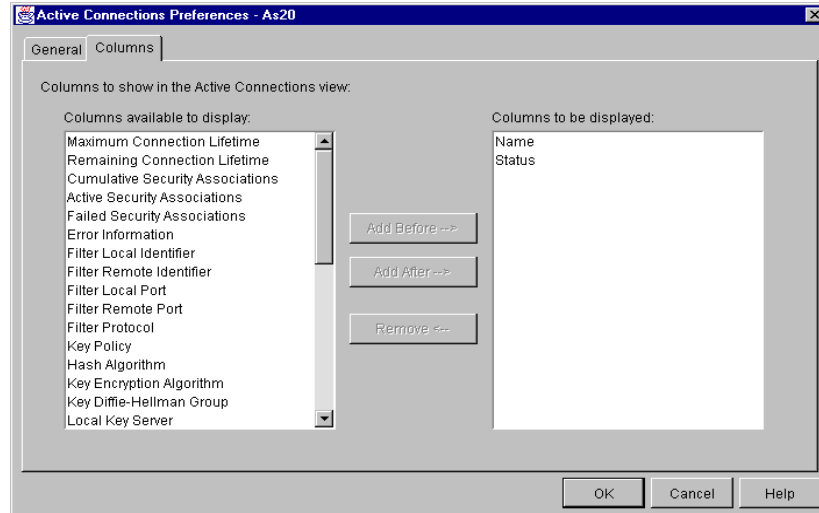


Figure 740. Active Connections Window columns to be displayed

The Active Connection window shows only the Name and Status columns by default. There are many columns that you may add to the Active Connections window. However, this section focuses on those that provide information to aid you with problem solving. These include:

- Failed Security Association
- Local Key Server IP Address
- Remote Key Server IP Address
- Local Data Addresses
- Remote Data Addresses

Tip

You can retrieve connection error information by right-clicking the connection in error. Figure 741 shows the error information.

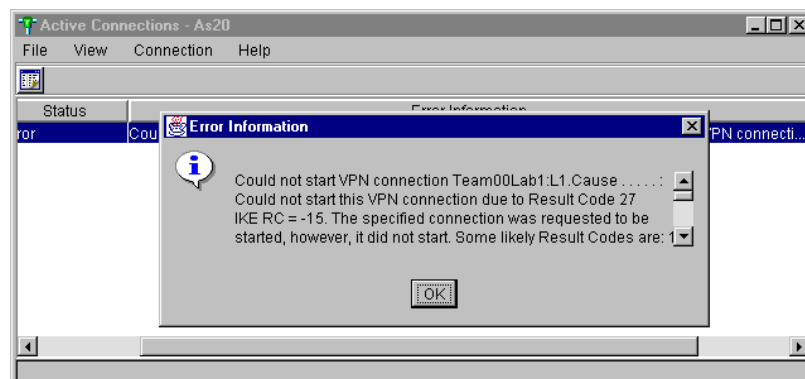


Figure 741. Active Connections window detailed error information

The message does not contain a message ID. However, if you report the problem to IBM software service, you must also provide the message ID. You can find the message ID and other message details in the QTOKVPNIKE and QTOVMAN job logs on the AS/400 system.

Add other columns to the Active Connections window, depending on the information you want to see or need to isolate due a problem. For example, if you defined several proposals within one data policy and you don't know which proposal is actually in use, add the following columns to the Active Connections window:

- Security Protocol
- ESP Authentication
- ESP Encryption
- AH Authentication
- Encapsulation

The information in these columns allows you to determine which proposal was chosen from the data policy.

14.1.2 IP filter journal

IP filter logging is useful tool in problem determination. OS/400 uses *journaling* to log packet activity. Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, for information on AS/400 IP filtering implementation.

The QIPFILTER journal in the QUSRSYS library contains information about activation and deactivation of filter sets, as well as information about whether an IP datagram was permitted or denied. The logging is performed based on the journaling option specified in a filter rule.

14.1.2.1 Enabling IP packet filter journaling

Journaling is enabled individually for each filter rule. Before you can enable journaling for a particular filter rule, you must deactivate filters. Perform the following steps to enable journaling for a filter rule:

1. In Operations Navigator, expand your AS/400 system.
2. Expand **Network**, and click **IP Security**.
3. Double-click **IP Packet Security**.
4. Double-click the filter rule you want to journal as shown in Figure 742.

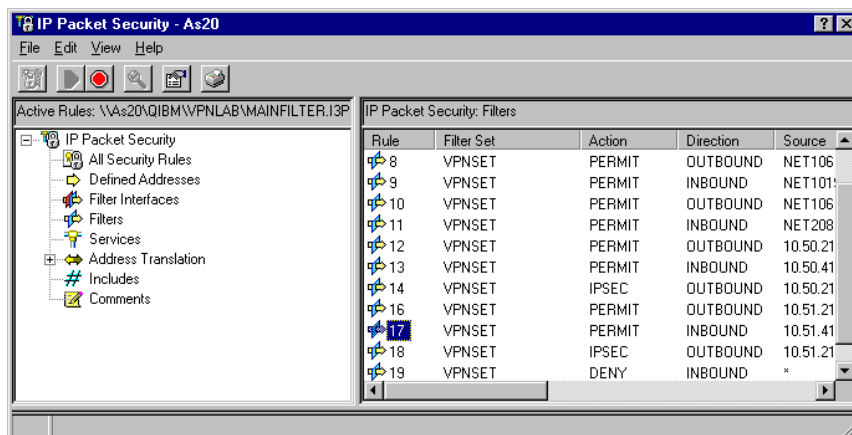


Figure 742. IP Packet Security - Editing a filter rule

5. Select **FULL** in the Journaling field to enable logging for this particular filter rule as shown in Figure 743 on page 631.

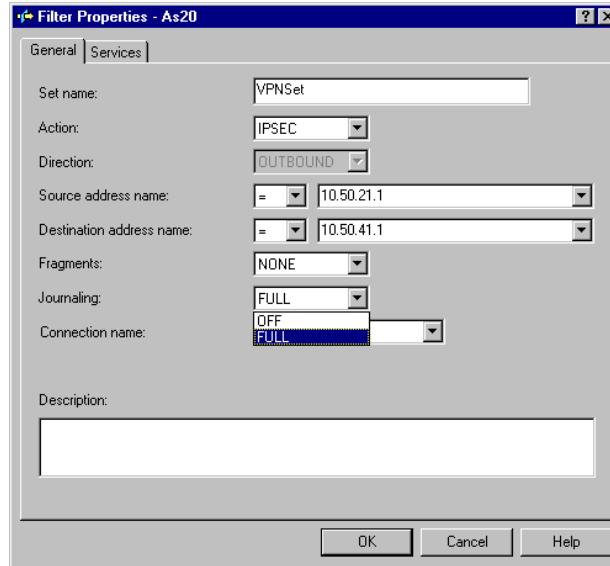


Figure 743. Filter Rule Journal Options

6. Click **OK**.
7. Save and activate the changed filter rule file.

When an IP datagram matching a filter rule with Journaling set to FULL flows through the interface on which the filter is active, an entry is logged in the QIPFILTER journal.

Tip

The last rule in a filter rules file is an implicit DENY *ALL rule. Since it is an *unwritten* rule, no logging (journaling = OFF) takes place when packets match the implicit DENY *ALL. To log packets that match the DENY *ALL rule, you must explicitly add a written rule at the end of the file. Specify FULL for Journaling in the explicit DENY *ALL rule.

14.1.2.2 Using the QIPFILTER journal

The AS/400 system automatically creates the QUSRSYS/QIPFILTER journal the first time you activate IP packet filtering. To view the entry-specific details in the journal, you can display the raw journal entries on the screen using the Display Journal (DSPJRN) command. To view the journal entries, at the command entry screen, enter:

```
DSPJRN JRN(QUSRSYS/QIPFILTER) JRNCD((M)) ENTYP(TF)
```

Figure 744 and Figure 745 on page 632 display entries in the QIPFILTER journal that show an IKE request packet being denied.

```

Display Journal Entries

Journal . . . . . : QIPFILTER      Library . . . . . : QUSRSYS

Type options, press Enter.
5=Display entire entry

Opt   Sequence Code Type Object      Library      Job          Time
-----
      6299  M   TF          Object      Library      Job          Time
      6300  M   TF          Object      Library      Job          Time
      6301  M   TF          Object      Library      Job          Time
      6302  M   TF          Object      Library      Job          Time
      6303  M   TF          Object      Library      Job          Time
      6304  M   TF          Object      Library      Job          Time
      6305  M   TF          Object      Library      Job          Time
      6306  M   TF          Object      Library      Job          Time
      6307  M   TF          Object      Library      Job          Time
      6308  M   TF          Object      Library      Job          Time
      6309  M   TF          Object      Library      Job          Time
      6310  M   TF          Object      Library      Job          Time

F3=Exit  F12=Cancel

```

Figure 744. Displaying the QIPFILTER journal

```

Display Journal Entry

Object . . . . . :                      Library . . . . . :
Member . . . . . :                      Sequence . . . . . : 6308
Code . . . . . : M - Network management data
Type . . . . . : TF - IP filter rules actions
Incomplete data . . : No

Entry specific data
Column *...1...2...3...4...5
00001 'NLINE A I 19DENY 1710.50.41.1 50010.5'
00051 '0.21.1 500
00101 '

Bottom

Press Enter to continue.

F3=Exit F6=Display only entry specific data
F10=Display only entry details F12=Cancel F24=More keys

```

Figure 745. Displaying the QIPFILTER journal - Entry-specific data

By copying the journal entries to an outfile, you can easily view the entries using query utilities such as Query/400 or SQL. You can also write your own HLL programs to process the entries in the outfile.

Use the following steps to copy the IP packet filtering journal entries to the outfile:

1. Create a copy of the system supplied file QSYS/QATOFIPF into a user library by using the Create Duplicate Object (CRTDUPOBJ) command. The following command shows an example of using the CRTDUPOBJ command:

```
CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
NEWOBJ(myfile)
```

2. Use the Display Journal (DSPJRN) command to copy the entries from the QUSRSYS/QIPFILTER journal to the outfile you created in the previous step:

```
DSPJRN JRN(QIPFILTER) JRNCD((M)) ENTYP((TF)) OUTPUT(*OUTFILE) +
OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*CALC)
```

Table 81 describes the fields in the QATOFIP file.

Table 81. QATOFIPF file layout

Field name	Field length	Numeric	Description	Comments
TFENTL	5	Y	Length of entry	
TFSEQN	10	Y	Sequence number	
TFCODE	1	N	Journal code	Always 'M'
TFENTT	2	N	Entry type	Always 'TF'
TFTIME	26	N	SAA timestamp	
TFJOB	10	N	Job name	
TFUSER	10	N	User profile	
TFNBR	6	Y	Job number	
TFPGM	10	N	Program name	
TFRES1	51	N	Reserved	
TFUSPF	10	N	User	
TFSYMN	8	N	System name	
TFRES2	20	N	Reserved	
TFRESA	50	N	Reserved	
TFLINE	10	N	Line description	"*ALL" if TFREVT is "U*". Blank if TFREVT is "L*". Line name if TFREVT is "L".
TFREVT	2	N	Rule event	"L*" or "L" when rules are loaded. "U*" when rules are unloaded. "A" when filter action.
TFPDIR	1	N	IP packet direction	"O" is outbound. "I" is inbound.
TFRNUM	5	N	Rule number	Applies to the rule number in the active rules file.

Field name	Field length	Numeric	Description	Comments
TFFACT	6	N	Filter action taken	"PERMIT", "DENY" or "IPSEC"
TFPROT	4	N	Transport protocol	1 is ICMP 6 is TCP 17 is UDP 50 ESP 51 AH
TFSRCA	15	N	Source IP Address	
TFSRCP	5	N	Source Port	Disregard if TFPROT = 1 (ICMP)
TFDSTA	15	N	Destination IP Address	
TFDSTP	5	N	Destination Port	Disregard if TFPROT = 1 (ICMP)
TFTEXT	76	N	Additional Text	Contains description if TFREVT = "L*" or "L" or "U*"

Note that there is a second journal for IP packet security. This is the QIPNAT journal that contains entries for conventional Network Address Translation (NAT) and is not related to VPN.

Figure 746 shows a simple view of the filters file. This view was created using the *Database* function in Operations Navigator. We copied the entries of the QUSRSYS/QIPFILTER journal to the outfile ADAN/IPFILTER. Then, we used the Database function in Operations Navigator to create a view that provides an easy-to-read format of the entries logged in the journal.

TFLINE	TFFACT	TFPROT	TFSRCA	TF SRCP	TFDSTA	TFDSTP	TFTEXT
TRLANB1	PERMIT	17	204.146.18.22	500		500	
TRLANB1	PERMIT	17	204.146.18.22	500		500	
TRLANB1	PERMIT	17		500	204.146.18.227	500	
TRLANB1	PERMIT	17		500	204.146.18.227	500	
TRLANB1	PERMIT	17	204.146.18.22	500		500	
TRLANB1	PERMIT	17		500	204.146.18.227	500	
TRLANB1	PERMIT	17		500	204.146.18.227	500	
TRLANB1	PERMIT	17	204.146.18.22	500		500	
TRLANB1	PERMIT	17	204.146.18.22	500		500	
TRLANB1	IPSEC	6	10.196.8.6	1025	10.196.11.14	23	SourceInbow
TRLANB1	IPSEC	6	10.196.8.6	1025	10.196.11.14	23	SourceInbow
TRLANB1	IPSEC	6	10.196.8.6	1025	10.196.11.14	23	SourceInbow
TRLANB1	IPSEC	6	10.196.8.6	1025	10.196.11.14	23	SourceInbow
TRLANB1	IPSEC	6	10.196.8.6	1025	10.196.11.14	23	SourceInbow
*ALL	Unload						

Figure 746. IP filter view

14.1.3 VPN journal

VPN uses a separate journal, QVPN in library QUSRSYS, to log information about VPN connections. The journal code is M, and the journal type is TS.

Journal entries are rarely used as an everyday tool. Instead, they are useful for troubleshooting and verifying that your system, keys, and connections are functioning in the manner that you specified. For example, journal entries help you understand what happens to your data packets. They also keep you informed of your current VPN status.

14.1.3.1 Enabling the VPN journal

Use the Virtual Private Networking option of Operations Navigator to activate the VPN journal. You have to enable the logging function for a single connection group.

The VPN journal function can be activated for the following types of data connections:

- Dynamic Key Groups
- Manual Connections
- Dynamic IP Groups
- L2TP Connections

The following steps show how to enable journal logging for a Dynamic Key Group:

1. Start Operations Navigator.
2. Expand the desired AS/400 system to **Network->IP Security**, and click **IP Security**.
3. Double-click **Virtual Private Networking**.
4. Expand **Secure Connections** and then **Data Connections** as shown in Figure 747.

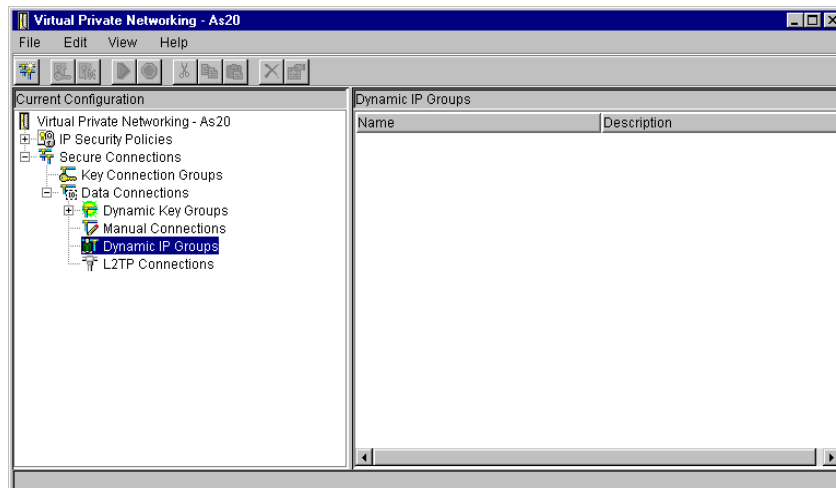


Figure 747. Virtual Private Networking window

5. Expand the **Dynamic Key Groups** as shown in Figure 748 on page 636.

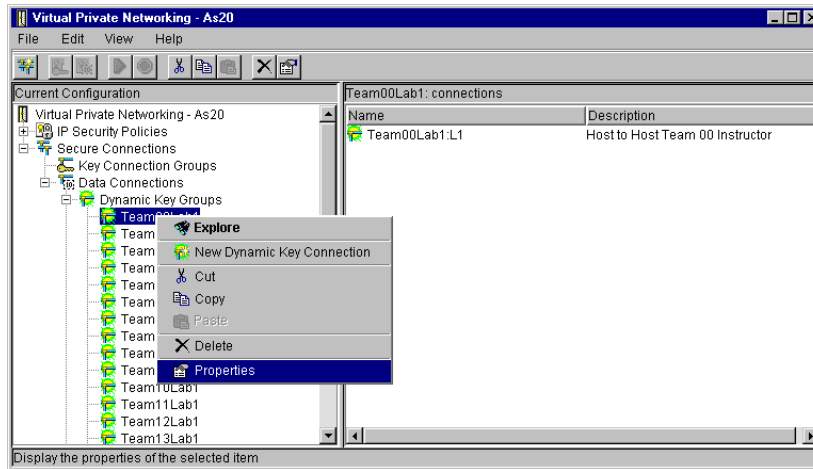


Figure 748. Virtual Private Networking window - Dynamic Key Groups

6. Right-click the Dynamic Key Group for which you want to enable journaling, and select **Properties** as shown in Figure 748.

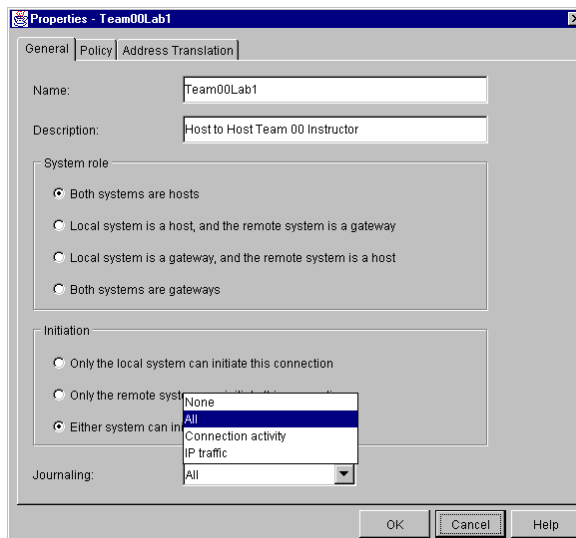


Figure 749. Dynamic Key Group properties - Enabling journaling

7. Select the level of logging you require in the Journaling field as shown in Figure 749.

You can choose between four options. These are:

- **None:** The VPN journal function is turned off for this connection group.
- **All:** All connection activities, such as starting or stopping a connection, or key refreshes, and so on as well as IP traffic information are logged in the VPN journal.
- **Connection activity:** Specifies that the system logs such connection activity as starting or stopping a connection.
- **IP traffic:** Specifies that the system logs all of the VPN traffic associated with this connection. A log entry is made every time a filter rule is invoked.

The system records IP traffic information in the journal QIPFILTER, which is located in the QUSRSYS library.

8. Click **OK**.
9. Start the changed connection to activate the journaling.

Note
Before changing the Journaling field, you must stop active connections.

14.1.3.2 Using the QVPN journal

To view the entry-specific details in the journal, you can display the raw journal entries on the screen using the Display Journal (DSPJRN) command. To view the journal entries, at the command entry screen, enter the following command:

```
DSPJRN JRN(QUSRSYS/QVPN) JRNCD( (M) ) ENTYP(TF)
```

Figure 750 and Figure 751 on page 638 display entries in the QVPN journal that show an entry for a dynamic connection.

Display Journal Entries							
Journal : QVPN				Library : QUSRSYS			
Type options, press Enter.							
5=Display entire entry							
Opt	Sequence	Code	Type	Object	Library	Job	Time
	61	M	TS			QTOVMAN	18:14:58
	62	M	TS			QTOVMAN	18:15:01
	63	M	TS			QTOVMAN	18:15:23
	64	M	TS			QTOVMAN	18:15:23
	65	M	TS			QTOVMAN	18:15:27
	66	M	TS			QTOVMAN	18:16:04
	67	M	TS			QTOVMAN	18:16:04
	68	M	TS			QTOVMAN	18:16:04
	69	M	TS			QTOVMAN	18:16:05
	70	M	TS			QTOVMAN	18:16:08
	71	M	TS			QTOVMAN	18:16:27
	72	M	TS			QTOVMAN	18:16:31
							+
F3=Exit F12=Cancel							

Figure 750. Displaying the QVPN journal

```

Display Journal Entry

Object . . . . . :                               Library . . . . . :
Member . . . . . :                               Sequence . . . . . : 65
Code . . . . . : M - Network management data
Type . . . . . : TS - VPN information
Incomplete data . . : No

Entry specific data
Column *...+....1....+....2....+....3....+....4....+....5
00001 'CM Team00Lab1:L1 '
00051 'DYNAMIC RUNNING 19990309181528 AN'
00101 'Y 0.0.0.10 '
00151 ' 0 0.0.0.10 '
00201 ' 0 10.50.21.1 '
00251 ' 10.50.41.1 '
00301 ' 1 199903091835285000 2SHA 3DES '
00351 ' 0 '

More...

Press Enter to continue.

F3=Exit F6=Display only entry specific data
F10=Display only entry details F12=Cancel F24=More keys

```

Figure 751. Displaying the QVPN journal - Entry-specific data

By copying the journal entries to an outfile, you can easily view the entries by using such query utilities as Query/400 or SQL. You can also write your own HLL programs to process the entries in the outfiles.

Use the following steps to copy the VPN journal entries to the outfile:

1. Create a copy of the system supplied file QSYS/QATOVSOFF into a user library by using the Create Duplicate Object (CRTDUPOBJ) command. The following command shows example of using the CRTDUPOBJ command:

```

CRTDUPOBJ OBJ(QATOVSOFF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
NEWOBJ(myfile)

```

2. Use the Display Journal (DSPJRN) command to copy the entries from the QUSRSYS/QVPN journal to the outfile you created in the previous step:

```

DSPJRN JRN(QVPN) JRNCDE((M)) ENTYP((TF)) OUTPUT(*OUTFILE) +
OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)

```

Table 82 describes the fields in the QATOVSOFF file:

Note

The model outfile shipped with OS/400 V4R4M0 is missing some header fields. It will be corrected in the next release. Meanwhile, a fixed model outfile is available on the Web site at: <http://www.as400.ibm.com/vpn>

Table 82. QATOVSOFF file layout

Field name	Field length	Numeric	Description	Comments
TFENTL	5	Y	Length of entry	
TFSEQN	10	Y	Sequence number	

Field name	Field length	Numeric	Description	Comments
TFCODE	1	N	Journal code	Always 'M'
TFENTT	2	N	Entry type	Always 'TS'
TFTIME	26	N	SAA timestamp	
TFRES	95	N	Reserved	
TSCMPN	10	N	VPN component	
TSCONM	40	N	Connection name	
TSCOTY	10	N	Connection type	
TSCOS	10	N	Connection state	
TSCOSD	8	N	Start date	
TSCOST	6	N	Start time	
TSCOED	8	N	End date	
TSCOET	6	N	End time	
TSTRPR	10	N	Transport protocol	
TSLCAD	43	N	Local client address	
TSLCPR	11	N	Local ports	
TSRCAD	43	N	Remote client addr.	
TSRCPR	11	N	Remote ports	
TSLEP	43	N	Local endpoint	
TSREP	43	N	Remote endpoint	
TSCORF	6	N	Times refreshed	
TSRFDA	8	N	Date of next refresh	
TSRFTI	6	N	Time of next refresh	
TSRFLS	8	N	Refresh life-size	
TSSAPH	1	N	SA Phase	
TSAUTH	10	N	Authentication type	
TSENCR	10	N	Encryption type	
TSDHGR	2	N	Diffie-Hellman-Group	
TSERRC	8	N	Error code	
TSSPI1	32	N	Phase 1 SPI	
TSSP2I	8	N	Phase 2 SPI In	
TSSP2O	8	N	Phase 2 SPI Out	
TSIDPR	1	N	Identity protect	

14.1.4 Trace TCP/IP Application (TRCTCPAPP) command

The Trace TCP/IP Application (TRCTCPAPP) command is used by service personnel when trace information needs to be captured for one of the following TCP/IP applications:

- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP) server
- SMTP client
- TELNET/Virtual Terminal Application Programming Interface (VTAPI)
- Host Servers (*CENTRAL, *DTAQ, *RMTCMD, *SIGNON, *NETPRT, and *SVRMAP)
- Distributed Data Management (DDM)
- Virtual Private Networking (VPN)
- Layer 2 Tunneling Protocol (L2TP)
- Digital Certificate Services

The user profile under which TRCTCPAPP runs requires *SERVICE special authority. For a given application, there can only be one trace active at a time on the system.

Many error messages in the VPN server job logs recommend that you use the TRCTCPAPP command to provide the necessary information needed by IBM software service to debug the problem. This section explores the options available for the VPN trace. Your IBM service representative will direct you to run TRCTCPAPP with some of these options when you report a VPN-related problem.

Note

The trace output produced by the TRCTCPAPP command is intended to be used by IBM software support personnel to debug and isolate problems.

14.1.4.1 Starting the TCP/IP application trace

The trace information captured by the TRCTCPAPP command depends on the parameter specified during the start of the trace. You can choose to trace only the connection manager job, only the key manager job, or both VPN server jobs. The following example shows how to start the VPN trace:

```
TRCTCPAPP APP(*VPN) SET(*ON) MAXSTG(*APP) TRCFULL(*WRAP)
```

The following parameters can be used when starting a TCP/IP application trace:

- APP** TCP/IP application. The APP parameter specifies the TCP/IP application that you want to trace. *VPN specifies tracing for the VPN server jobs. *L2TP specifies tracing the Layer 2 Tunnel Protocol servers.
- SET** Trace option setting. *ON starts the TCP/IP application trace selected in the APP parameter.
- MAXSTG** Maximum storage for trace. Specifies the maximum amount of storage in kilobytes (K) used for collected trace information. Values can range

from 1 to 16,000. On this parameter, you specify the buffer size for the trace. The default value is *APP. Each application type defines a default buffer size. The predefined default value for APP(*VPN) is 16000 KB per server job. For APP(*L2TP), the default buffer size is 4096 KB per job.

RMTNETADR

Remote network address. The user may limit the amount of information captured by specifying the remote TCP/IP address of the L2TP peer. In most cases, the IP address should be left blank unless there is a large amount of traffic with multiple L2TP peers.

TRCFULL Trace full action. Specify *WRAP to wrap the trace records (replace oldest records with new records). Specify *STOPTRC to stop the trace when all of the storage specified by the MAXSTG parameter has been used. As a general rule, define the buffer size always big enough to store all the trace records. If the trace wraps, you may lose important trace information. If you experience a highly intermittent problem, define the trace buffer big enough, so that wrapping the buffer does not cause the loss of important information.

ARGLIST Argument list. Only trace information associated with this specific argument list is included in the trace information captured. The argument list contains debug level data and special trace requests. Some common arguments used when tracing the VPN key manager job are P2SAS and NETWORK. The IBM support personnel will provide the arguments if necessary. This parameter is *not* valid for L2TP.

VPNSVR Virtual private network server. Specifies whether the trace information is to be collected for the VPN key manager (*KEYMGR) job, the VPN connection manager (*CNNMGR) job, or both. If you leave the parameter blank, both VPN servers are traced. This parameter is *not* valid for L2TP.

14.1.4.2 Stopping the TCP/IP application trace

As a general guideline, you should stop the trace as soon as the error condition you want to capture occurs. For example, if you have problems establishing a VPN connection, stop the trace after you receive an error message.

The following example shows how to stop the VPN trace:

```
TRCTCPAPP APP(*VPN) SET(*OFF) TITLE('VPN Trace for connection problems')
```

The following parameters can be used when stopping a TCP/IP application trace:

APP TCP/IP application. The APP parameter specifies the TCP/IP application for which you want to stop the trace. *VPN specifies stop trace for the VPN server jobs. *L2TP specifies stop trace for the Layer 2 Tunnel Protocol servers.

SET Trace option setting. *OFF stops the TCP/IP application trace selected in the APP parameter. The trace information is written to a spooled file. The TRCTCPAPP command creates a separate spooled file for each VPN server job. The VPN trace output is in the printer file QPTOCSERVE. The output for the L2TP trace is in the printer file QTOC2TRC.

TITLE Trace title. Give a meaningful title to identify the reason for the trace.

Additional options on the TRCTCPAPP command

There are two more values that you can specify on the SET parameter of the TRCTCPAPP command when tracing VPN server jobs. They are:

- *END** This value stops the TCP/IP application trace and deletes all trace data captured. No spooled file is created.
- *CHK** The status of tracing for the specified application is checked. Messages are returned indicating whether tracing is active for the specified TCP/IP application, the command parameters specified from the last time that TRCTCPAPP was started for this application, and other information related to the collection of trace information. The messages are written into the job log of the job that issued the TRCTCPAPP SET(*CHK) command.

14.1.5 Job logs

The AS/400 system's job logs always include useful information that can be used for problem determination. If you are experiencing problems establishing a VPN connection between two AS/400 systems, study the job logs on both sides. The AS/400 VPN server, whether it is initiator or responder, writes error information to its respective job log. You must study error information on both sides of the VPN to debug problems properly.

Tip

If you are debugging problems in a VPN connection between an AS/400 system and another platform, designate the AS/400 system to act as the responder in the connection and study the joblogs discussed in this section. These job logs often report the problem information that will help you to determine the problem cause.

If you have problems setting up a VPN connection, look for error information in the job logs produced by the following jobs running in the QSYSWRK subsystem:

QTCPIP This job is the base job that starts all the TCP/IP interfaces. If you have fundamental problems with TCP/IP in general, analyze the QTCPIP job log.

QTOKVPNIKE

The QTOKVPNIKE job is the Virtual Private Networking key manager job. The VPN key manager listens to UDP port 500 to perform the Internet Key Exchange (IKE) protocols.

QTOVMAN

This job is the connection manager for VPN connections. The related job log contains messages for every connection attempt that fails.

QTPPANSxxx

This job is used for PPP dial-up connections. It answers to connection attempts where *ANS is defined in a PPP profile.

QTPPPCTL

PPP job for dial-out connections. The PPP control job handles the starting and ending of the L2TP server job and the controlling L2TP

and PPP profiles. Problems in this job log are part of PPP problem determination.

QTPPPL2TP

Layer Two Tunneling Protocol (L2TP) manager's job. The L2TP server logs informational and error messages in this job log. It sends a few selected messages to QSYSOPR message queue. The informational messages include normal operations such as `L2TP Tunnel established` and `L2TP Tunnel ended`. The error messages indicate a problem such as `AS L2TP server unable to bind to port 1701` and include the recovery action required to resolve the problem. If you have problems starting an L2TP tunnel, look for messages in this job log first.

QTPPPL2SSN

The L2TP pre-start job is invoked to handle the (virtual) PPP session data after the L2TP tunnel is established and call negotiations complete successfully. This job defaults to the QUSRWRK subsystem, but you can configure the subsystem from Operations Navigator. Problems in this job log are part of PPP problem determination.

Use the `Work with Active Jobs (WRKACTJOB)` command or `Work with Subsystem Jobs (WRKSBSJOBS)` command to display the jobs and job logs from a command entry 5250 session. The following command displays the VPN key manager job that is currently active:

```
WRKACTJOB SBS (QSYSWRK) JOB (QTOKVPNIKE)
```

The following command displays all the VPN key manager jobs on the system, whether they are in the out queue or active:

```
WRKJOB JOB (QTOKVPNIKE)
```

14.1.5.1 Working with job logs using Operations Navigator

This section shows you how to use the Operations Navigator GUI to work with the TCP/IP and VPN server job logs.

To access all job logs for jobs that run under the QTCP user profile from Operations Navigator, perform the following steps:

1. Start Operations Navigator, and expand your AS/400 system.
2. Expand **Job Management**, and click on **Jobs** as shown in Figure 752 on page 644.

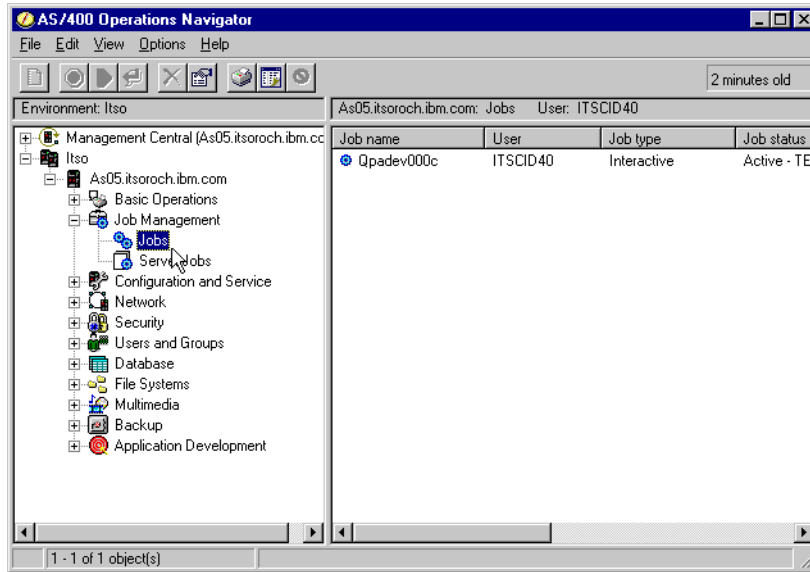


Figure 752. Operations Navigator - Job management

3. Select **Options->Include** from the menu bar to open the Jobs - Include window as shown in Figure 753.

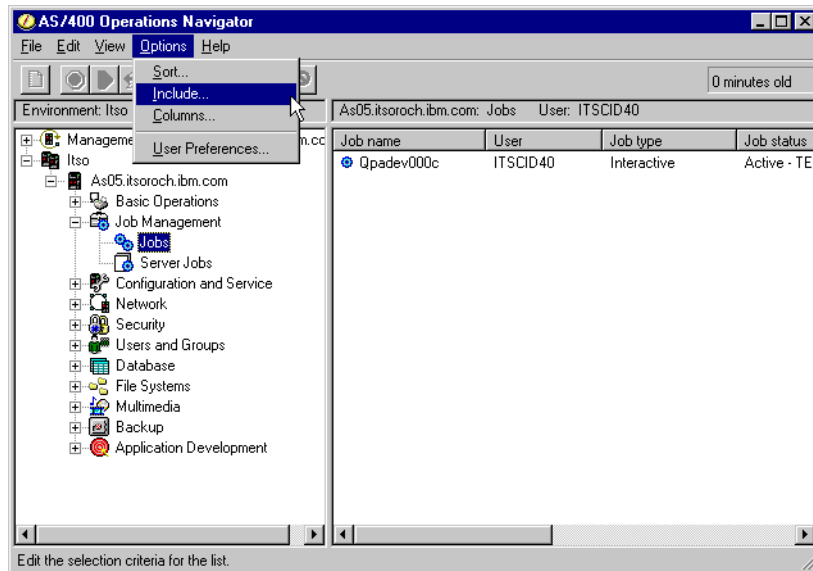


Figure 753. Operations Navigator task bar selection

4. Click on the button in the User field as shown in Figure 754 on page 645.

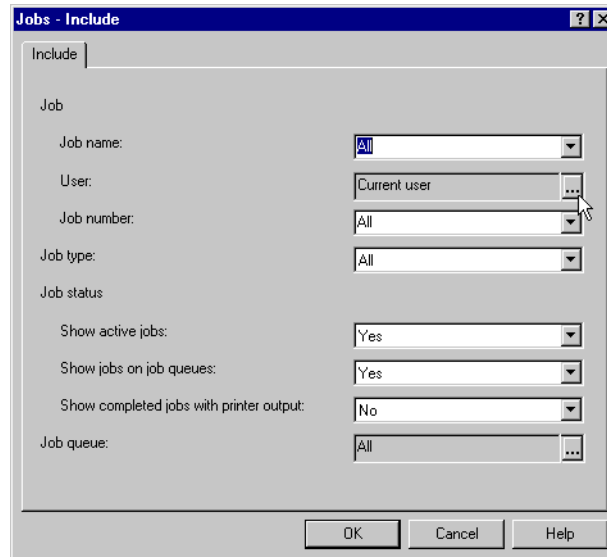


Figure 754. Operations Navigator Jobs - Include window

5. At the User dialog window, select the **User** radio button, and enter QTCP as shown in Figure 755.

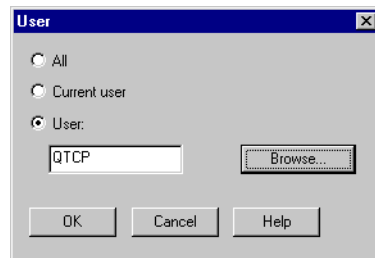


Figure 755. Operations Navigator User dialog box

6. Click **OK** to display all active jobs for the user QTCP as shown in Figure 756 on page 646.

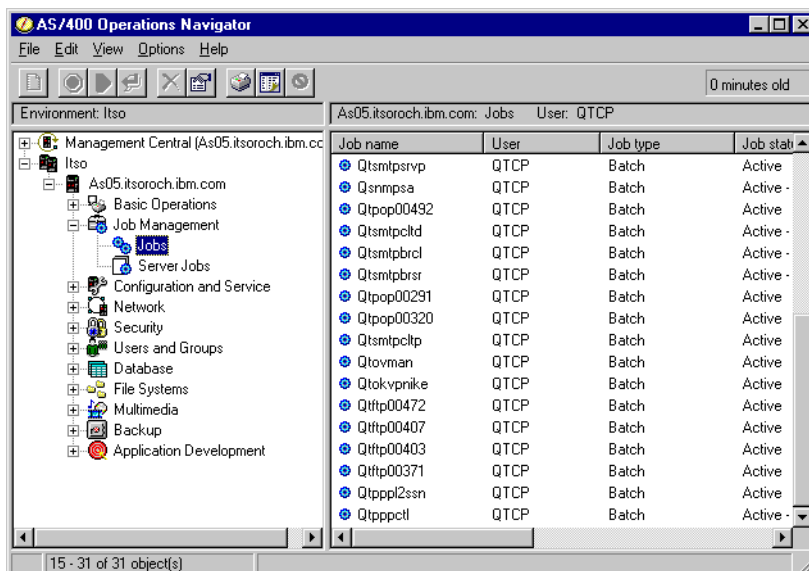


Figure 756. Operations Navigator job list for user profile QTCP

If you are interested *only* on the VPN server jobs QTOKVPNIKE and QTOVMAN, perform the following steps:

1. Start Operations Navigator, and expand your AS/400 system.
2. Expand **Network**, and click on **IP Security** as shown in Figure 757. Two servers are displayed on the right panel: IP Packet Security and Virtual Private Networking.

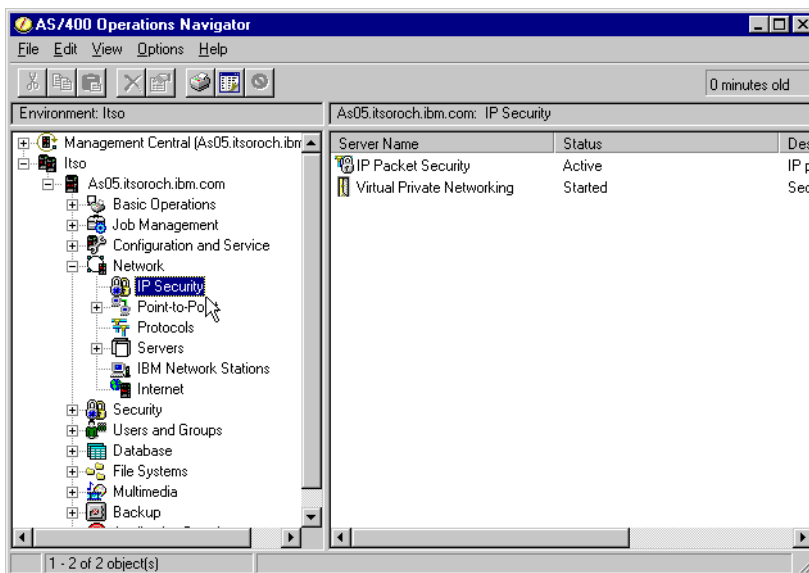


Figure 757. Operations Navigator - IP Security

3. Right-click **Virtual Private Networking**, and select **Server Jobs** as shown in Figure 758 on page 647.

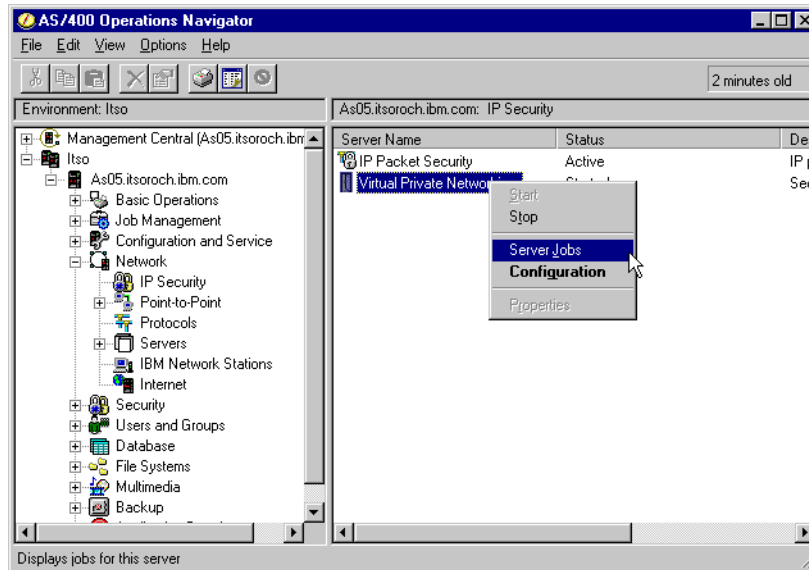


Figure 758. Operations Navigator - Displaying Virtual Private Networking server jobs

Two separate job windows open: one for each server job QTOVMAN and QTOKVPNIKE. The jobs window is independent of Operations Navigator and can be left open after shutting down Operations Navigator. Figure 759 shows the job window for the QTOKVPNIKE server job.

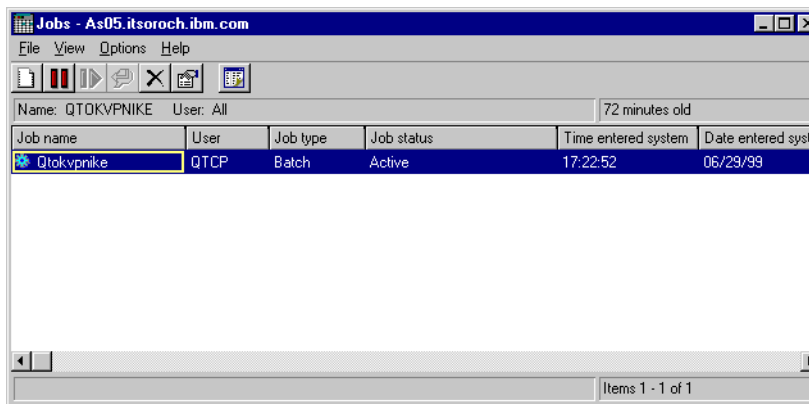


Figure 759. QTOKVPNIKE job window

4. Right-click **Job Log** as shown in Figure 760 on page 648.

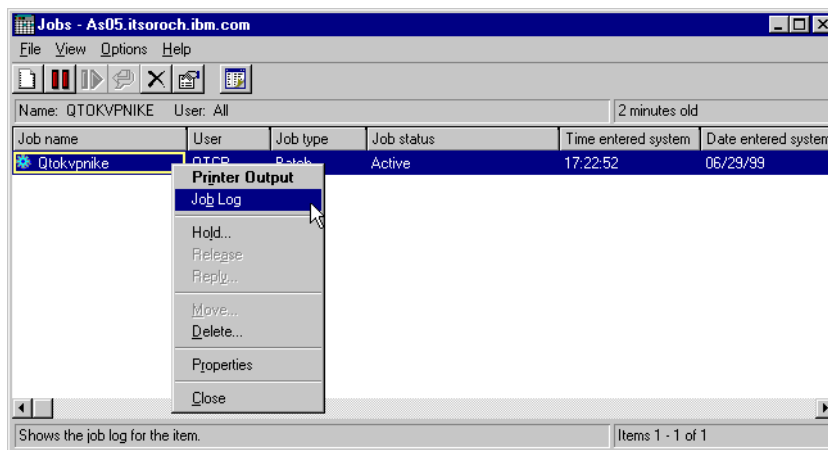


Figure 760. Selecting a job log for QTOKVPNIKE

The job log for the active server job is displayed as shown in Figure 761.

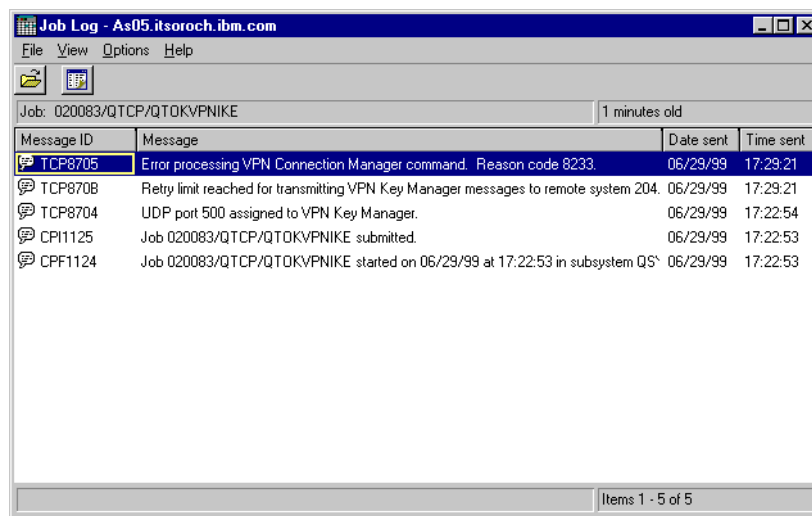


Figure 761. QTOKVPNIKE job log

5. Double-click a specific message ID to open the Detailed Message Information window as shown in Figure 762 on page 649.

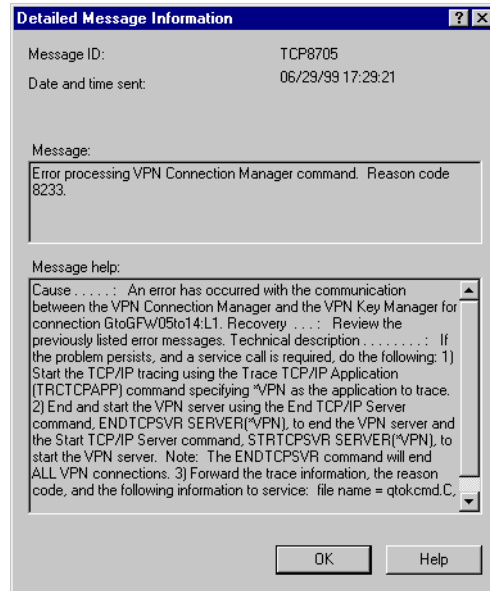


Figure 762. Detailed Message Information window

14.1.6 Communications trace

The AS/400 system also provides the capability to trace data on a communications line, such as a Local Area Network (LAN) or Wide Area Network (WAN) interface. The average user may not understand the entire contents of the trace data. However, you can use the trace entries to determine whether a data exchange between the local and the remote systems took place.

14.1.6.1 Starting the communications trace

Use the Start Communications Trace (STRCMNTRC) command to initiate the communications trace for a particular line. The following example shows the STRCMNTRC command:

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('VPN Problems')
```

The command has several parameters. Refer to the online help in the STRCMNTRC command for a complete description of the parameters. Some of the most commonly used parameters are:

- CFGOBJ** Configuration object. Specifies the name of the configuration object to trace. The object is either a line description, a network interface description, or a network server description.
- CFGTYPE** Type. Specifies whether a line (*LIN), a network interface (*NWI), or a network server (*NWS) is being traced.
- MAXSTG** Buffer size. Specifies the buffer size for the trace. The default value is set to 128 KB. The range goes from 128 KB to 64 MB. The actual maximum system wide buffer size is defined within the System Service Tools (SST). Therefore, you may receive an error message when using a larger buffer size on the STRCMNTRC command than defined in the SST. Keep in mind that the sum of buffer sizes specified on all started communications traces must not exceed the maximum buffer size defined in the SST.

- DTADIR** Data direction. Specifies the direction of data traffic to be traced. The direction can be outbound traffic only (*SND), inbound traffic only (*RCV), or both directions (*BOTH).
- TRCFULL** Trace full. This parameter specifies the action the system takes when the trace buffer is full of data. The default value is *WRAP, which indicates that the trace continues and overwrites the data in the buffer. *STOPTRC stops the trace when the trace buffer, specified in the MAXSTG parameter, is full of a trace record. As general rule, define the buffer size always big enough to store all the trace records. If the trace wraps, you may lose important trace information. If you experience an intermittent problem, define the trace buffer big enough, so that a wrap of the buffer does not discard any important information.
- USRDTA** Number of user bytes to trace. Defines the quantity of data to be traced in the user data part of the data frames. By default, only the first 100 bytes of user data are captured for LAN interfaces. For all other interfaces, all user data is captured. Make sure you specify *MAX if you suspect problems in the user data of a frame.
- TEXT** Trace description. Provide a meaningful description of the trace.

14.1.6.2 Stopping the communications trace

As a general guideline, you should stop the trace as soon as the error condition you want to capture occurs. Use the End Communications Trace (ENDCMNTRC) command to stop the trace. The following command is an example of the ENDCMNTRC command:

```
ENDCMNTRC CFGOBJ (TRNLINE) CFGTYPE (*LIN)
```

The command has two parameters:

- CFGOBJ** Configuration object. Specifies the name of the configuration object for which the trace is running. The object is either a line description, a network interface description, or a network server description.
- CFGTYPE** Type. Specifies whether a line (*LIN), a network interface (*NWI), or a network server (*NWS) is traced.

14.1.6.3 Printing the trace data

After stopping the communications trace, print the trace data. Use the Print Communications Trace (PRTCMNTRC) command to perform this task. Since all line traffic is captured during the trace period, you have multiple filter options to generate the output. We recommend that you keep the spooled file as small as possible. This makes the analysis faster and more efficient. In the case of a VPN problem, you are advised to filter on IP traffic only and if possible, on a specific IP address. In V4R4 you also have the option of filtering on a specific IP port number. The following command shows an example of the PRTCMNTRC command:

```
PRTCMNTRC CFGOBJ (TRNLINE) CFGTYPE (*LIN) FMTCIP (*YES) TCPIPADR ('10.50.21.1)
SLIPORT (500) FMTBCD (*NO)
```

In this example, the trace is formatted for IP traffic and contains only data for the IP address where the source or destination address is 10.50.21.1 and the source or destination IP port number is 500.

The command has several parameters, which are the most important parameters for VPN troubleshooting. These parameters are explained in the following list:

- CFGOBJ** Configuration object. Specifies the name of the configuration object for which the trace is running. The object is either a line description, a network interface description, or a network server description.
- CFGTYPE** Type. Specifies whether a line (*LIN), a network interface (*NWI), or a network server (*NWS) is traced.
- FMTTCP** Format TCP/IP data. Specify *YES to format the trace for IP data. The name of this parameter is misleading in that it not only formats TCP/IP data. It also formats UDP/IP data.
- TCPIPADR** Format TCP/IP data by address. This parameter consists of two elements. If you specify IP addresses on both elements, only IP traffic between those addresses is printed.
- SLTPORT** IP Port Number. Specifies the IP port number to filter.
- FMTBCD** Format broadcast data. By default, this parameter is set to *YES, which means that all broadcast frames are also printed. If you are not interested in Address Resolution Protocol (ARP) requests, for example, specify *NO. Otherwise, you may be overwhelmed with broadcast messages.

14.1.7 Work with Connection Status (NETSTAT) command

Use the `NETSTAT` command to view the status of TCP/IP interfaces, routes, and connections. For example, you can use `NETSTAT` to determine if a route to a particular destination is available.

14.2 Common problems

This section describes some common problems encountered by early users of AS/400 VPN support.

14.2.1 Unable to encrypt keys. QRETSVRSEC must be set to 1

Symptoms:

The following error appears:

```
Unable to encrypt keys. QRETSVRSEC must be set to 1.
```

Possible cause:

QRETSVRSEC is a system value that indicates if encrypted keys can be stored on the AS/400 system. If this value is set to 0, then pre-shared keys and the keys for the algorithms in a manual connection cannot be stored in the VPN policy database. To fix this problem, from a 5250 session to the AS/400 system, perform the following steps:

1. Enter the following command statement:

```
WRKSYSVAL SYSVAL(QRETSVRSEC)
```

Press **Enter**.

2. Type 2 (change) next to it.
3. On the next panel, type 1, and press **Enter**.

14.2.2 All keys are blank

Symptom:

All pre-shared keys and the algorithm keys for manual connections are blank.

Possible cause:

If the system value QRETSVRSEC is set to 0, no encrypted data can be stored on the AS/400 system. When you specify pre-shared keys, they are stored in encrypted form. Therefore, if you are configuring VPN on an AS/400 system using Operations Navigator, and QRETSVRSEC is set to "0", Operations Navigator reports this condition. You will not be allowed to continue until QRETSVRSEC is set back to "1".

Most likely, QRETSVRSEC was set to 1, you configured VPN, and then backed up the VPN configuration objects in QUSRSYS. Then, QRETSVRSEC was set back to "0". Setting this system value to 0 causes all of the keys in the VPN Policy Database to be erased. You can try changing QRETSVRSEC to 1 if your security policy allows it, and then restoring the VPN configuration objects again. If this doesn't work, the only resolution is to re-enter all of the keys after the system value is set back to "1".

14.2.3 CPF9821: Not authorized to program QTFRPRS in QSYS library

Symptom:

When selecting IP Security in Operations Navigator, the CPF9821 message pops up:

Not authorized to program QTFRPRS in QSYS library.

Possible cause:

The user does not have the required authority to retrieve the current status of IP packet security or the VPN Connection Manager. *IOSYSCFG authority is required.

14.2.4 Unable to communicate with the remote system

Symptoms:

- TCP870B Retry limit reached for transmitting VPN Key Manager messages to remote system in either the initiator or responder job log.
- TCP8705 Error processing VPN Connection Manager command. Reason code 8233 in the initiator's job log.

Possible causes:

- Base TCP/IP or TCP/IP routing problems. Sometimes the obvious is easy to overlook. For IKE to function, the two systems must have base IP connectivity between them. This can be verified by deactivating filtering rules on both systems and testing connectivity using PING.
- A firewall may be running on either system or some system between the two VPN servers that is either not allowing UDP port 500 traffic or is using NAT to translate addresses.
- Filtering rules are not properly configured. All UDP port 500 PERMIT filter rules must appear before any IPSEC filter rules. Refer to Chapter 4, "AS/400 IP filtering overview" on page 103, for information on how to configure IP filtering for VPN.

- Dead gateway detection. The AS/400 system attempts to recognize routes that are no longer valid and shut them down. If a dead gateway is suspected (that is, a TCP connection failure), the AS/400 system will PING (ICMP echo request) the associated router. If no response is received, the route is marked as unavailable. The system will attempt other alternative routes. If filter rules are blocking ICMP traffic, routes may be inappropriately disabled causing VPN problems and other TCP/IP communication problems.

14.2.5 No remote phase 1 policy

Symptoms:

- TCP870B Retry limit reached for transmitting VPN Key Manager messages to remote system in the initiator job log.
- TCP8705 Error processing VPN Connection Manager command. Reason code 8221 in the initiator's job log.
- If the remote system is not an AS/400 system, TCP8705 Error processing VPN Connection Manager command. Reason code 8233 in the initiator's job log.
- TCP870C Proposal not accepted with remote system in responder's job log.
- TCP8709 VPN policy processing error for connection x. Reason code 5 in initiator's job log. The error points to a database item type of REMOTE_ID_GROUP.

Possible causes:

- The responder was not able to locate a key connection group for this system.
- The exchange does not match. For example, identity protection is proposed, but the responder requires the aggressive mode.
- FQDN (hostname) is being used as the identity, and the exchange is identity protection (main mode). Hostname can be misleading by making you think that it is interchangeable with the IP address. This is true with most TCP/IP applications, but it is *not* true when used as an identifier for a dynamic key connection. Hostname as an identifier can only be used in aggressive mode. In this case, the hostname must be configured on both the local and remote system.
- Lifetime or lifesize is not negotiable. Lifetime must always be proposed and can be combined with life-size. If lifesize is proposed, the policy must contain both lifesize and lifetime. In other words, if the responder's policy only contains time, and time plus size is proposed, the proposal will not match (will be rejected by the responder). If size (bytes) is proposed, the responder's policy must specify something other than *No Size Limit*. Refer to 3.6.7, "Key policy (IKE phase 1) and data policy (IKE phase 2) lifetime and size limits" on page 65, for more information.

14.2.6 No remote phase 2 policy

Symptoms:

- TCP8705 Error processing VPN Connection Manager command. Reason code 8241 in the initiator's job log.
- If the remote system is not an AS/400 system, TCP8705 Error processing VPN Connection Manager command. Reason code 8233 may appear in the initiator's job log.
- TCP870C Proposal not accepted with remote system in the responder's job log.

- TCP8709 VPN policy processing error for connection RESPONDER. Reason code 5 in the responder's job log. The error points to a database item type of CONNECTION_DEFINITION.

Possible causes:

- Filter rules are not loaded (active) on the responder side. Activating the filter rules causes the VPN connection definitions to be updated to indicate *loaded*. Until connection definitions are loaded, they will not be found by the key manager. A filter rules file with an IPSEC filter rule pointing to the appropriate connection group must be active.
- Connection on the initiator is not contained with the connection or filter rules on the responder. For example, the local connection specifies a range for local addresses. However, this does not fit with the granularity of the connection on the responding system.
- Granularity proposed does not match granularity on the responder system. Granularity is defined in the connection definition. Refer to 4.3, "Refining the traffic for active connections: Connection granularity" on page 129, for more information on connection granularity.
- Lifetime or lifesize are not negotiable. Lifetime must always be proposed and can be combined with lifesize. If lifesize is proposed, the policy must contain both lifesize and lifetime. In other words, if the responder's policy only contains time, and time plus size is proposed, the proposal will not match (will be rejected by the responder). If size (bytes) is proposed, the responder's policy must specify something other than *No Size Limit*. Refer to 3.6.7, "Key policy (IKE phase 1) and data policy (IKE phase 2) lifetime and size limits" on page 65, for more information.

14.2.7 Pre-shared key not found on local system

Symptoms:

- TCP8709 VPN policy processing error for connection x. Reason code 5 in initiator's job log. The error points to a database item type of P1_PREKEY.
- TCP8705 Error processing VPN Connection Manager command. Reason code 8220 in the initiator's job log.
- TCP8703 Authentication failed with remote system x may be seen in the responder's job log.

Possible cause:

The pre-shared key has not been configured on the local the local system for the remote system.

14.2.8 Preshared key not found on remote system

Symptoms:

- TCP8705 Error processing VPN Connection Manager command. Reason code 8222 in the initiator's job log.
- If the remote system is not an AS/400 system, TCP8705 Error processing VPN Connection Manager command. Reason code 8233 may be seen in the initiator's job log.
- TCP8703 Authentication failed with remote system x may be seen in the initiator's job log along with TCP8705 Error processing VPN Connection Manager command. Reason code 24.

Possible causes:

- The pre-shared key has not been configured on the remote system.
- The pre-shared key was configured with an ID type other than IP for identity protection (Main Mode) exchange. The only time that a pre-shared key can be identified by a non-IP ID (key identifier or user@fqdn) is in an aggressive mode.
- FQDN (hostname) is being used as the identity and the exchange is identity protection (main mode). Hostname can be misleading by making you think that it is interchangeable with IP address. This is true with most TCP/IP applications, but it is *not* true when used as an identifier for a dynamic key connection. Hostname as an identifier can only be used in aggressive mode. In this case, the hostname must be configured on both the local and remote system.

14.2.9 Pre-shared key is invalid

Symptoms:

- TCP8705 RC=82xx on initiator
- TCP8703 Authentication failure

Possible causes:

- The pre-shared key is different on local and remote systems.
- The value of the pre-shared key is the ASCII representation of the string entered on the GUI. Some other implementations allow or require you to enter the pre-shared key in hexadecimal format. Refer to 17.2.2, “Configuring a host-to-host VPN in the AIX server” on page 772, for an example of matching pre-shared keys in ASCII and hexadecimal formats.

14.2.10 Filters not loaded correctly on WAN interfaces

Symptom:

TCP8604 RC=111 on initiator or responder

Possible cause:

Filter rules for the WAN interface are loaded (activated) *after* the dial-up connection is established. End the dial-up connection and restart it after the filter rules are active.

14.2.11 Invalid filter rule name

Symptom:

TCP5A11 on initiator or responder

Possible causes:

- Invalid character in filter rule name
- Space in filter rule name

14.2.12 Active filter rules fail to deactivate

Symptom:

When you try to deactivate the current set of IP packet security rules, the message `The active rules failed to be deactivated` appears in the results.

Possible cause:

The most common reason for this error is that there is at least one active VPN connection. To fix this, open the Active Connections Monitor, and stop each of the

connections that have a status of Running, by right-clicking them and selecting Stop.

14.2.13 3DES not a choice for encryption

Symptom:

When working with a key policy transform, data policy transform, or a manual connection, the 3DES encryption algorithm is not offered as a choice.

Possible cause:

Most likely, you only have the Cryptographic Access Provider 5769-AC2 product installed, and not Cryptographic Access Provider 5769-AC3. AC2 only allows for the DES encryption algorithm due to restrictions on key lengths.

14.2.14 Key policy not a choice in a Dynamic IP Connection Group

Symptom:

A key policy that is shown in the VPN main dialog in the key policies container is not offered as a choice for a Dynamic IP Connection Group on the Associations page.

Possible cause:

The key policy used in a Dynamic IP Connection Group cannot allow identity protection. The property window for Dynamic IP Connection Groups handles this by only offering key policies that do not allow identity protection.

To get a particular key policy to be available as a choice, select **Key Policies** from the VPN main dialog, and open the properties pages for the policy. On the General page, deselect **Identity protection** for Initiator negotiation, and then select **Do not allow identity protection** for Responder negotiation.

14.2.15 Item not found

Symptom:

When you right-click an object in the main VPN dialog and select Properties or Delete, the following message appears:

Item not found

Possible causes:

- The object was deleted or renamed elsewhere in the VPN GUI and you have not refreshed the window yet. Therefore, the object still appears in the VPN main dialog. To see if this is the case, simply select **View** from the main menu, and then select **Refresh**. If the object still appears in the VPN main window, continue to the next item in this list.
- There is a loss of synchronization between a VPN object and one or more objects in the VPN policy database. Since many of the objects that appear in the VPN GUI relate to more than one object in the VPN policy database, communication errors may cause some of the objects in the database to continue to be related to an object in the VPN. Whenever you create or update an object, an error occurs when the loss of synchronization actually happens. The only way to fix the problem is to select **OK** on the error window. This launches the property sheet for the object in error. Only the name field on the property sheet will be filled in. Everything else is blank (or contains default values). Enter the attributes of the object, and select **OK**.

Similarly, when you attempt to delete the object, this error occurs because some links to objects in the VPN Policy Database are lost. To fix the problem, complete the *blank* property sheet that opens when you click **OK**.

14.2.16 A valid key policy is required

Symptom:

When you try to open the Properties for a Key Connection group, a message similar to the following example appears:

A valid key policy is required

Possible cause:

This happens when the key policy associated with the Key Connection Group has either been renamed or deleted since the last time the Key Connection Group was updated. After clicking OK on the error message, the property sheet opens with each of the attributes for the Key Connection Group filled in. By default, a Key Policy is selected, although it may not be the one you want. Go to the Associations page and either select or create a new Key Policy to associate with this group, and then select **OK** on the property sheet to save your changes.

14.2.17 Unable to update the object

Symptom:

When you select OK on the property sheet for a Dynamic Key Group, Manual Connection, Dynamic IP Connection Group, or an L2TP Connection, the following message appears:

Unable to update the object

Possible cause:

This error happens when an active connection is using the object you are trying to change. You cannot make changes to an object while it is associated with an active connection. To make changes to an object, go to the Active Connections window. Look for the appropriate active connections, right-click on it, and select **Stop** from the resulting context menu.

Note

If the Active Connections window is not started, you either need to select **Cancel** on the property sheet (which causes you to lose your changes). Or, you can go back to AS/400 Operations Navigator, start another VPN GUI, and start the Active Connections window from this second GUI. After stopping the connections, you can select the **OK** button on the property sheet again.

14.2.18 Connection is running after you stopped it

Symptom:

After you stopped a connection from the VPN main dialog, the Active Connections Monitor indicates that the connection is still running.

Possible cause:

This typically happens because the Active Connections window has not been refreshed yet. To fix this, select **View** from the Active Connections window main menu and then select **Refresh**.

14.2.19 Connection not displayed in the Active Connections window

Symptom:

After starting a connection from the VPN main dialog, the connection does not appear in the Active Connections window.

Possible cause:

This typically happens because the Active Connections window has not been refreshed yet. As such, the information in the monitor is outdated. To fix this, select **View** from the Active Connections window main menu, and then select **Refresh**.

14.2.20 Status for a connection in the Active Connection window is blank

Symptom:

When you view the Active Connections window in AS/400 Operations Navigator, your connection has no value in the Status column.

Possible cause:

The blank status value indicates that the connection is in the middle of starting. That is, it is not running yet, but it hasn't had an error yet either. When you refresh the window, the connection should either display a status of `Error` or `Running`.

14.2.21 Unexpected columns display in the Active Connections Monitor

Symptom:

You set up the columns you want to display in the Active Connections window. When you look at it at a later time, a different set of columns appears.

Possible cause:

The Active Connections window is a system-wide tool that is not specific to a particular user or PC. When someone else changes the columns on the window, the changes affect everyone who is viewing it.

14.2.22 Unable to retrieve connection information in the Active Connections window

Symptom:

When you start the Active Connections window, it shows no connections and the status bar says `Unable to retrieve the connection information`.

Possible cause:

This happens when the VPN Connection Manager is stopped. To fix the error, follow the path **AS/400 Operations Navigator->Network->IP Security**. Then, right-click **Virtual Private Networking**, and select **Start**.

14.2.23 Parameter PINBUF is not valid

Symptom:

When starting a connection, a message similar to the following example appears:

```
Parameter pinbuf is not valid
```

Possible cause:

This happens when your AS/400 system is set to use certain locales to which lower-case letters do not map correctly. To fix this error, either make sure that all objects use only upper-case letters, or change the locale of the AS/400 system.

14.2.24 Connection overlap with existing connection

Symptom:

When you try to start a connection, the following message appears:

```
Message ID TCP8604. VPN connection AS14HtoAS20H:L2 failed an audit.CONNECTION  
OVERLAP WITH EXISTING CONNECTION.
```

Possible cause:

Connection overlap with existing connection. There are two dynamic key connections under the same dynamic key group that cause an overlap condition. For an example of a situation causing the overlap condition, refer to 4.4.4, “Scenario 3: Allowing Telnet only in both directions” on page 144. To avoid this problem, configure two separate dynamic key groups and create a dynamic key connection under each one.

14.3 VPN key manager job messages and reason codes

The messages that the VPN key manager job, QTOKVPNIKE, reports in the job log are helpful in problem determination. This section lists some of the most common error messages in QTOKVPNIKE and associated return codes. As part of the problem determination process, you should always check the QTOKVPNIKE job log for errors and review the error information online.

14.3.1 TCP8705 error processing VPN Connection Manager command

The most common reason code type for the message TCP8705 is 82xx. The 82xx represents an error processing START command. A START command is a request for IKE to negotiate a phase 2 Security Association (SA). If there is a failure during this process, a return code of 82xx is logged. The most common 82xx return codes are listed here.

14.3.1.1 RC=8214: Failure occurred during phase 1 negotiations

Check the QTOKVPNIKE and QTOVMAN job log for additional messages.

14.3.1.2 RC=8220: No local pre-shared key found

IKE was unable to obtain the pre-shared key from the policy database. Verify that pre-shared keys exist. The pre-shared keys are located using the remote system’s identifier.

14.3.1.3 RC=8221: No remote phase 1 policy could be found

Refer to the remote system job log to verify what is being proposed and what is in the remote systems policy for phase 1. If possible, change the roles of the initiator and responder. This may create additional message logging for further problem determination.

14.3.1.4 RC=8222: No remote pre-shared key

The remote system was not able to determine the pre-shared key to use in phase 1 authentication. Verify the pre-shared keys that are configured on the remote system.

14.3.1.5 RC=8223: Phase 1 negotiations timed out

The most common reasons for a phase 1 time are:

- The remote IKE server is not running.

If the remote system is an AS/400 system verify that the QTOCVPNIKE job is running. If the remote system is not an AS/400 system, verify that the equivalent job or task is running. This can usually be verified with the NETSTAT command.

- Filtering rules on the local or remote system or possibly a firewall are blocking IKE traffic. IKE uses UDP port 500.

Verify that the filter rules allow UDP port 500 for inbound and outbound traffic. This needs to be done on the local and remote systems. Verify that filter rules on all firewalls allow UPD port 500 for inbound and outbound traffic along the Virtual Private Networking tunnel.

- The filtering rules that permit IKE (UDP port 500) are not defined prior to the first IPSEC filter rule.

The IPSEC filter rules are only defined for direction outbound. IPSEC automatically creates the associated inbound rule. If the IKE permits are after any of the IPSEC rules, the inbound may be automatically placed in front of the IKE permits blocking the IKE traffic.

Verify that IKE filter rules are placed *before* the IPSEC filter rules.

- The remote system is not an AS/400 system and does not have a policy that matches what the local system is proposing.

Verify that the remote system has a phase 1 policy that matches any of the proposals made by the local AS/400 system.

- The remote system is not an AS/400 system and does not have a pre-shared key for the local system or the pre-shared key is not the same as the locally configured pre-shared key.

Verify that the remote system has a pre-shared key for the local AS/400 system. The pre-shared keys are located using the remote system's identifier.

14.3.1.6 RC=24: IKE phase 1 authentication failed

Verify that the pre-shared key that is configured on the local system is the same as the pre-shared key on the remote system. Remember that pre-shared keys are *case sensitive*.

14.3.1.7 RC=8241: No remote phase 2 policy could be found

Refer to the remote system job log to verify what is being proposed and what is in the remote systems policy for phase 2. Verify that the filter rules on the remote system have been loaded. The phase 2 policy is not available on the remote system until filter rules with an action of IPSEC are started. Verify that the local definition for the connection is exact or is within the range of the remotely defined policy.

14.3.1.8 RC=8242: Phase 2 negotiation timed out

Phase 2 messages are retransmitted up to five times. If this AS/400 system does not receive a response from the remote system, a time-out occurs. Check the QTOCVPNIKE job log for additional messages.

It can cause a real problem if a connection is restarted with an outstanding phase 1 SA. If the AS/400 system attempts to start a connection in this case, phase 2 will time out with RC=8241. The only solution in this case is to stop and restart the VPN servers. This process will remove all the SAs on this AS/400 system.

14.3.1.9 RC=8243 or RC=8252: A network error has occurred

Verify that the local IP interface is active. If the interface is PPP, make sure that it has been started and a connection has been established.

14.3.1.10 RC=8257: Remote identifier mismatch

The remote identifier configured on the initiator is different than the identifier payload sent by the remote system. Verify that identifiers match on both systems. Possible identifiers are:

- Version 4 IP address
- User@FQDM
- Hostname
- Key Identifier

14.3.1.11 TCP8705 Complete list of reason codes

Table 83 includes the complete list of reason codes for message TCP8705.

Table 83. Error message TCP8705 - Complete list of reason codes

Complete list of reason codes	RC
INVALID_PAYLOAD_TYPE	= 1
DOI_NOT_SUPPORTED	= 2
SITUATION_NOT_SUPPORTED	= 3
INVALID_COOKIE	= 4
INVALID_MAJOR_VERSION	= 5
INVALID_MINOR_VERSION	= 6
INVALID_EXCHANGE_TYPE	= 7
INVALID_FLAGS	= 8
INVALID_MESSAGE_ID	= 9
INVALID_PROTOCOL_ID	= 10
INVALID_SPI	= 11
INVALID_TRANSFORM_ID	= 12
ATTRIBUTES_NOT_SUPPORTED	= 13
NO_PROPOSAL_CHOSEN	= 14
BAD_PROPOSAL_SYNTAX	= 15
PAYLOAD_MALFORMED	= 16
INVALID_KEY_INFORMATION	= 17
INVALID_ID_INFORMATION	= 18
INVALID_CERT_ENCODING	= 19

Complete list of reason codes	RC
INVALID_CERTIFICATE	= 20
CERT_TYPE_UNSUPPORTED	= 21
INVALID_CERT_AUTHORITY	= 22
INVALID_HASH_INFORMATION	= 23
AUTHENTICATION_FAILED	= 24
INVALID_SIGNATURE	= 25
ADDRESS_NOTIFICATION	= 26
NOTIFY_SA_LIFETIME	= 27
CERTIFICATE_UNAVAILABLE	= 28
UNSUPPORTED_EXCHANGE_TYPE	= 29
UNEQUAL_PAYLOAD_LENGTHS	= 30
INCOMPLETE_START_MSG	= 8200
INVALID_START_MSGLENGTH	= 8201
NULL_START_RESPONDERID_STRUCT	= 8202
INVALID_START_RESPONDERID_TYPE	= 8203
INVALID_START_RESPONDERID_LENGTH	= 8204
NULL_START_RESPONDERID_FIELD	= 8205
INVALID_START_LOCALCLIENTID_TYPE	= 8206
INVALID_START_LOCALCLIENTID_LENGTH	= 8207
NULL_START_LOCALCLIENTID_FIELD	= 8208
INVALID_START_REMOTECLIENTID_TYPE	= 8209
INVALID_START_REMOTECLIENTID_LENGTH	= 8210
NULL_START_REMOTECLIENTID_FIELD	= 8211
NULL_START_KEYSECPOLNAME	= 8212
NULL_START_SECPOLNAME	= 8213
STARTED_P1_FAILURE	= 8214
INCOMPLETE_P1RESPONSE_MSG	= 8215
INVALID_P1RESPONSE_MSGLENGTH	= 8216
INVALID_P1RESPONSE_RESULT	= 8217
STARTED_P1_SA KEP_ERROR	= 8218
NO_LOCAL_P1_POLICY	= 8219
NO_LOCAL_PREKEY	= 8220
NO_REMOTE_P1_POLICY	= 8221
NO_REMOTE_PREKEY	= 8222

Complete list of reason codes	RC
INVALID_PREKEY	= 8223
NO_LOCAL_ID	= 8224
NO_LOCAL_CERTIFICATE	= 8225
EXPIRED_LOCAL_CERTIFICATE	= 8226
INVALID_LOCAL_CERTIFICATE	= 8227
EXPIRED_REMOTE_CERTIFICATE	= 8228
INVALID_REMOTE_CERTIFICATE	= 8229
NO_CA_CERTIFICATE	= 8230
EXPIRED_CA_CERTIFICATE	= 8231
INVALID_CA_CERTIFICATE	= 8232
P1_TIMEOUT	= 8233
P2_FAILURE	= 8234
INCOMPLETE_P2RESPONSE_MSG	= 8235
INVALID_P2RESPONSE_MSGLENGTH	= 8236
INVALID_P2RESPONSE_RESULT	= 8237
INVALID_P2RESPONSE_P2SAPAIRCOUNT	= 8238
P2_SA_KEY_ERROR	= 8239
NO_LOCAL_P2_POLICY	= 8240
NO_REMOTE_P2_POLICY	= 8241
P2_TIMEOUT	= 8242
NETWORK_ERROR	= 8243
SOCKET_ERRNO_ENETDOWN	= 8244
SOCKET_ERRNO_ENETUNREACH	= 8245
SOCKET_ERRNO_EHOSTDOWN	= 8246
SOCKET_ERRNO_EPIPE	= 8247
SOCKET_ERRNO_ECONNREFUSED	= 8248
SOCKET_ERRNO_EHOSTUNREACH	= 8249
SOCKET_ERRNO_EINTR	= 8250
SOCKET_ERRNO_EIO	= 8251
SOCKET_ERRNO_EUNATCH	= 8252
CMREQ_DATA_NOT_FOUND	= 8253
POLICY_DB_ERROR	= 8254
P1_EXPIRED	= 8255
INVALID_REMOTE_IP	= 8256

Complete list of reason codes	RC
RID_MISMATCH	= 8257
INCOMPLETE_STOP_MSG	= 9001
INVALID_STOP_MSGLength	= 9002
INVALID_STOP_COLLECTIONHANDLE	= 9003
CMREQDATA_NOTFOUND	= 9004
MISSING_P1_PARAMETERS	= 9005
LOCALIP_INITIALIZATION_FAILED	= 9006
REMOTEIP_INITIALIZATION_FAILED	= 9007
FIND_SA_BY_COOKIES_FAILED	= 9008
FIND_P2SA_BY_MSGID_FAILED	= 9009
KEY_MANAGER_ERROR	= 16383
RC_OK	= 0

14.3.2 TCP870C proposal not accepted with remote system &1

The most common reason for message TCP870C is a configuration mismatch between the local AS/400 system and the remote key server. This message is almost always logged on the responder system. The most common reason codes are listed here.

14.3.2.1 RC=14: The local policy does not contain a match

The local policy does not contain a match for the remote system's proposal. Compare the remote proposal with the local policy and make corrections as appropriate. If the exchange is 32 and the local policy is *No Policy Found*, make sure that IP filter rules are loaded and correct.

In the case of phase 1 (key connection), the exchange being proposed does not match the exchange required on the responder, for example: identity protection proposed and aggressive mode required by responder. This appears in the responder's job log as *No local policy*.

14.3.2.2 Format of the Additional information field

The Additional information field of this message contains:

- **Exchange:** The IKE exchange of the proposal. Valid exchanges include:
 - Two for Identity protection (Main Mode)
 - Four for Aggressive Mode
 - 32 Quick Mode (phase 2)
- **Local role:** Either INITIATOR or RESPONDER. It almost always indicates responder.
- **Remote proposal:** Contains the entire SA proposals sent from the remote system in an attempt to negotiate an SA. The format of this proposal is described later in this section.

- **Local policy:** The policy that the local key manager has found in the VPN policy database in response to the proposal. This is of the same format as the Remote Proposal.

The syntax (format) of the Remote Proposal and Local Policy is:

- Proposals are separated by the “|” character. For example, an AH and ESP look like AH, MD5,... | ESP, 3DES, ...
- Protocols are separated by the “&” character. For example, a single proposal with both the AH and ESP protocols look like AH, MD5, ... & ESP, 3DES, ...
- Transforms are separated by the “:” character. For example, an AH with MD5 or SHA look like AH, MD5,...: AH, SHA,...

Tip

The additional information message TCP870C field is an invaluable tool in problem determination for mismatch in policy. If possible, make the AS/400 system the responder to generate this message.

14.3.3 TCP8709 VPN policy processing error. RC=5

The most frequent cause of a VPN policy processing error is that the particular item is not found. This is indicated with a Reason Code = 5. The most likely items that may appear as *not found* and the possible reasons are listed here:

- **REMOTE_ID_GROUP:** When responding to a request for phase 1, IKE first looks for a matching Key Connection Group based on the remote ID that has initiated a request for a phase 1 SA. When using identity protection, the remote ID is always the remote system’s IP address. When using aggressive mode, the ID may be something else, such as a key identifier or a User@FQDN.

Verify that a key connection group exists with the remote ID of the system that is initiating the connection.

- **P1_PREKEY:** IKE uses pre-shared keys for authentication. During a phase 1 negotiation, IKE looks up the pre-shared key to be used based on the remote servers ID. When using identity protection, the remote ID is always the remote system’s IP address. When using aggressive mode, the ID may be something else such as a key identifier or a User@FQDN name.

Verify that a pre-shared key exists in the database for the remote key manager (IKE).

- **CONNECTION_DEFINITION:** When responding to a request for a phase 2 SA, IKE looks for a connection definition based on the client identifiers sent from the initiating system. The client IDs must either be an exact match or within the locally defined connection. In addition, the local phase 2 policy is not valid until IP filter rules that specify an IPSEC action are loaded.

14.4 L2TP error messages

Table 84 shows the L2TP error messages, result codes (if applicable), and suggested recovery actions (if applicable).

Table 84. L2TP error messages, result code, and recovery action

Error message	Result code	Message text/suggested recovery action
TCP8500	N/A	<p>L2TP Server unable to start due to configuration errors.</p> <p>The server detected configuration errors during start up that will not allow the server to start.</p> <p>Use AS/400 Operations Navigator to correct the configuration errors and try starting the server again.</p> <p>See the QTPPPL2TP job log for previous error messages for more detail on the configuration error.</p>
TCP8501	N/A	<p>L2TP server unable to bind to UDP port 1701.</p> <p>The server was not able to get ownership of the specified port.</p> <p>Make the port and local IP address available for use, then try starting the server again.</p>
TCP8502	N/A	<p>L2TP server unable to bind to unix domain socket.</p> <p>The L2TP server was not able to get ownership of the UNIX domain socket located at /QIBM/UserData/OS400/TCPIP/PPP.</p> <p>Verify that path /QIBM/UserData/OS400/TCPIP/PPP exists and that the QTCP profile has *RWX authority to it. Then, try starting the server again.</p>
TCP8503	N/A	<p>L2TP Tunnel established.</p> <p>A L2TP Tunnel has been established for tunnel ID &1, remote host &2.</p>
TCP8504	N/A	<p>L2TP Tunnel ended.</p> <p>A L2TP Tunnel has been ended for tunnel ID &1, remote host &2.</p>

Error message	Result code	Message text/suggested recovery action
TCP8505	1 2 3	<p>L2TP Tunnel connection rejected. Reason code &1.</p> <p>A L2TP Tunnel connection was rejected for tunnel ID &2, remote host &3, Reason code &1.</p> <p>Authentication failed, remote host unknown.</p> <p>From Operations Navigator (Connections - Virtual line name - Authentication), verify that the host name and password are properly configured on both systems.</p> <p>Authentication challenge failed.</p> <p>From Operations Navigator (Connections - Virtual line name - Authentication), verify that the host name and password are properly configured on both systems.</p> <p>Exceed the maximum number of connections.</p>
TCP8506	1 2	<p>L2TP call connection rejected for reason code &1.</p> <p>The incoming call connection was rejected because of a program error, Reason code &1.</p> <p>Contact your IBM service representative to report the problem.</p> <p>The L2TP server was not able to construct a payload object.</p> <p>The L2TP server was not able to construct a call task.</p>
CPF9898 TCP8507	N/A	<p>Unable to retrieve host name for virtual line name &1.</p> <p>Verify that QUSRSYS/QTOCPTP *VLDL was not damaged or deleted.</p>
CPF9898 TCP8508	N/A	<p>L2TP server tunnel authentication is OFF for profile &1.</p> <p>Both ends of the L2TP tunnel must have authentication OFF or ON. The tunnel cannot be authenticated by one side only.</p>
CPF9898 TCP8509	N/A	<p>L2TP server unable to start profile &1 because profile &2 is using the same local IP address.</p> <p>Two L2TP Terminator profiles cannot listen on the same local IP address at the same time.</p>
CPF9898 TCP850A	N/A	<p>L2TP tunnel not established for profile: &1. Tunnel establishment timed out or was terminated.</p> <p>The remote L2TP host could have unexpectedly dropped the session or there could be network problems.</p>
CPF9898 TCP850B	N/A	<p>L2TP server unable to initialize mutex.</p> <p>Try restarting the L2TP server. If the problem persists, contact your IBM service representative to report the problem.</p>

Error message	Result code	Message text/suggested recovery action
CPF9898 TCP850C	N/A	L2TP server unable to lock mutex. RC = &1. Retry the operation. If the problem persists, contact your IBM service representative to report the problem.
CPF9898 TCP850D	N/A	L2TP server unable to unlock mutex. RC = &1. Retry the operation. If the problem persists, contact your IBM service representative to report the problem.
CPF9898 TCP850E	N/A	Interface error &1. L2TP profile &2 inactive. The interface that the L2TP server was listening on encountered an error. Verify that the interface is still active and that TCP/IP is still running. Then, try restarting the L2TP profile.
CPF9898 TCP850F	N/A	Interface error. L2TP server ending. The interface that the L2TP server was listening on encountered an error. Verify that the interface is still active and that TCP/IP is still running. Then, try restarting the L2TP profile.
CPF9898 TCP8510	N/A	L2TP server maximum number of connections exceeded for profile &1.
CPF9898 TCP8550	N/A	Error - VPN connection name: NULL. From Operations Navigator (Connection - Connection group name), verify that a valid connection group is specified.
CPF9898 TCP8551	N/A	Error - Requested connection type &1. Retry the operation. If the problem persists, contact your IBM service representative to report the problem.
CPF9898 TCP8552	ALL	VPN Error - Start connection return status: &1. See the QTOVMAN job in the QSYSWRK subsystem for more details.
CPF9898 TCP8553	ALL	VPN Error - End connection return status: &1. See the QTOVMAN job in the QSYSWRK subsystem for more details.

14.5 Known limitations in AS/400 VPN V4R4

You need to be aware of some known limitations in the first release of AS/400 VPN support to avoid interoperability problems with other platforms. They are:

- IPSEC specific notifications
- Phase 1 SA control
- Commit Bit and connected notification

14.5.1 IPSec specific notifications

RFC2407 *The Internet IP Security Domain of Interpretation for ISAKMP* defines several Domain of Interpretation (DOI) specific notification message types. These include:

- RESPONDER-LIFETIME
- REPLAY-STATUS
- INITIAL-CONTACT

The AS/400 V4R4 IKE implementation neither supports nor acknowledges any of these special notifications.

From our experience, the most frequently used notification of these is the RESPONDER-LIFETIME, which is used by a responder to inform the initiator the key lifetime or life-size that the responder will use. AS/400 V4R4 VPN support accepts this notification but ignores the message. The AS/400 system forces the responder to honor the proposed time by deleting the SA when the time expires.

14.5.2 Phase 1 SA control

The AS/400 V4R4 VPN solution completely isolates IKE phase 1 from the end user and administrator. As mentioned earlier, phase 1 SAs are created when needed and re-keyed when needed to support phase 2 SAs. In the simplest terms, the AS/400 IKE implementation is phase 2 driven.

The only time that this causes a problem is when another system stops using a phase 1 SA without reporting this condition with a *Delete* notification. The AS/400 system may continue to try and use the old phase 1, which the remote system has already stopped using.

Since there is no control to start or stop phase 1 SAs, the only way to correct this problem is to stop and start the *VPN server that causes all SAs and associated connections to stop.

14.5.3 Commit Bit and CONNECTED notification

Phase 2 (Quick Mode) negotiations consist of three messages between the initiator and responder. This has caused several problems requiring enhancements to the protocol to acknowledge the third message. These enhancements were introduced late in the protocol design and require compatibility with existing solutions that do not support it.

The solution is using the Commit Bit and Connected Notification. The responder informs the initiator that it will acknowledge the third message with a Connected Notification by setting the Commit Bit in the IKE message header when message 2 is sent. This tells the initiator to wait for the Connected Notification before considering the exchange complete.

AS/400 VPN on V4R4 solution tolerates the Commit Bit and Connected notification, but does not do anything special with this. When responding, AS/400 VPN does not set the Commit Bit or send the Connected Notification.

14.6 Internet Key Exchange (IKE) protocol overview

IKE, also referred to as Internet Security Association and Key Management (ISAKMP) with Oakley, is the protocol used by the AS/400 system to establish dynamic key VPN tunnels. This protocol is used to negotiate and generate Security Associations (SAs). The SA is a set of policy and keys used to protect information. This is accomplished with a two phase process. IKE defines the phases and Oakley defines the modes used in these phases.

IKE is defined in RFC2408 and RFC2409. Log on to <http://www.ietf.org> to access the full version of the RFCs. Refer to 1.8, "Key management objectives" on page 25, for a general overview of IKE. The information in this section is meant to help you analyze communication traces that include IKE negotiations.

14.6.1 IKE phases overview

IKE uses two distinct phases in its implementation. They are described in the following section:

14.6.1.1 IKE phase 1

During phase 1, the two IKE peers establish a secure authenticated channel over communication lines where security cannot otherwise be assumed. This is referred to as the IKE SA or Phase 1 SA. The ISAKMP SA can be created by one of two modes: Aggressive Mode or Main Mode.

14.6.1.2 IKE phase 2

During IKE phase 2, non-IKE SAs or phase 2 SAs are negotiated by IPSec-enabled hosts or gateways. Phase 2 SAs are created by using Quick Mode. Quick Mode can only be used in phase 2 since it must be protected by the IKE SA established in phase 1.

14.7 Oakley Mode overview

Oakley Modes define the exchanges used to establish SAs in both phases in the IKE framework. Each mode has a specific structure of exchanges and are used to create specific SAs.

14.7.1 Notation used to describe Oakley mode exchange

The following notation is used to describe the Oakley Mode message format and packet payloads used in all mode types:

HDR	The IKE header. The Exchange Type field in the header indicates the mode. The mode defines the message and payload ordering. When written as HDR*, it indicates payload encryption.
SA	The SA negotiation payload with one or more proposal and transform payloads. An initiator may provide multiple proposals, where a responder must reply with only one.
KE	The key exchange payload which contains the public information exchanged in a Diffie-Hellman exchange.
IDx	The identification payload for "x". The x can be "ii" or "ir" for the IKE initiator and responder respectively during phase 1 negotiation. The

x can be "ci" or "cr" if IKE is acting as a client negotiator (Gateway) during phase 2 negotiation.

- AUTH** The generic authentication mechanism, such as HASH in phase 1 pre-shared key negotiation.
- HASH** The hash payload. The contents of the hash are specific to the authentication method.
- NONCE** The nonce payload.
- PRF** The keyed pseudo-random function, often a keyed hash function. It is used to generate deterministic output that appears pseudo-random.
- SKEYID_a** The keying material used by the IKE SA to authenticate its messages.

14.7.2 The Main Mode model

The Main Mode also known as Identity Protection Mode is designed to first negotiate key exchange. This allows the Identity and authentication information to be sent as cipher text, based on an established pre-shared secret. This mode exchange requires six messages to establish the IKE SA as shown in Figure 763.

MAIN MODE EXCHANGE				
#	Initiator	Direction	Responder	NOTE
(1)	HDR; SA	=>		Begin ISAKMP-SA or Proxy negotiation
(2)		<=	HDR; SA	Basic SA agreed upon
(3)	HDR; KE; NONCE	=>		Key Generated (by Initiator and Responder)
(4)		<=	HDR; KE; NONCE	
(5)	HDR*; IDii; AUTH	=>		Initiator Identity Verified by Responder
(6)		<=	HDR*; IDir; AUTH	Responder Identity Verified by Initiator SA established

Figure 763. Main Mode Exchange

14.7.3 The Aggressive Mode model

The Aggressive Mode is designed to transmit the SA, Key exchange, identity, and authentication information together. This reduces the number of messages to the three required to establish the IKE SA. The identity is not afforded protection since the pre-shared secret is not established when identity information is transmitted as shown in Figure 764 on page 672.

AGGRESSIVE MODE EXCHANGE				
#	Initiator	Direction	Responder	NOTE
(1)	HDR; SA; KE; NONCE; IDi	=>		Begin ISAKMP-SA or Proxy negotiation and Key Exchange
(2)		<=	HDR; SA; KE; NONCE; IDr; AUTH	Initiator Identity Verified by Responder Key Generated Basic SA agreed upon
(3)	HDR; AUTH	=>		Responder Identity Verified by Initiator SA established

Figure 764. Aggressive Mode Exchange

14.7.4 The Quick Mode model

The Quick Mode is not a complete exchange itself. It requires an active IKE SA to be established. The Quick Mode assumes a secure communication path to the remote IPSec-enabled host or gateway. Quick Mode is used to derive keying material and negotiate shared policy for non-IKE SAs as shown in Figure 765.

QUICK MODE EXCHANGE				
#	Initiator	Direction	Responder	NOTE
(1)	HDR*; HASH(1); SA; NONCE [; KE] [; IDci IDcr]	=>		Begin non-ISAKMP SA negotiation
(2)		<=	HDR*; HASH(2); SA; NONCE [;KE] [;IDci IDcr]	Begin non-ISAKMP SA negotiation
(3)	HDR*; HASH(3)	=>		Both SAs established

HASH(1) = prf(SKEYID_a, M-ID SA NONCE [KE] [IDci IDcr])
HASH(2) = prf(SKEYID_a, M-ID Ni_b SA NONCE [KE] [IDci IDcr])
HASH(3) = prf(SKEYID_a, 0 M-ID Ni_b Nr_b)

Figure 765. Quick Mode exchange

Note

Some of the IKE traffic is encrypted, and, therefore, is not viewable in a communication trace. This includes all of phase 2 and the last two messages of Main Mode, phase 1 exchange.

14.8 AS/400 communication trace example

This section shows an example of a communication trace. It includes some information about how to read the trace.

```
.....1.....2.....3.....4.....5.....6.....7.....8.....9.....0.....1.....2.....
COMMUNICATIONS TRACE      Title: H2H - ESP w/Auth      03/15/99 19:03:42      Page:
Trace Description . . . . . : H2H - ESP w/Auth
Configuration object . . . . : TRNLINE
Type . . . . . : 1          1=Line, 2=Network Interface
                          3=Network server

Object protocol . . . . . : TRN
Start date/Time . . . . . : 03/15/99 19:02:40.181
End date/Time . . . . . : 03/15/99 19:03:37.039
Bytes collected . . . . . : 1039900
Buffer size . . . . . : 7          1=128K, 2=256K, 3=2M, 4=4M
                          5=6M, 6=8M, 7=16M, 8=32M
                          9=64M

Data direction . . . . . : 3          1=Sent, 2=Received, 3=Both
Stop on buffer full . . . . : N          Y=Yes, N=No
Number of bytes to trace
  Beginning bytes . . . . . : *MAX      Value, *CALC, *MAX
  Ending bytes . . . . . : *CALC      Value, *CALC
Select Trace Options:
-----
Remote Controller . . . . . :          Name, *ALL
Remote MAC Address . . . . . :          Value, *ALL
Remote SAP . . . . . :          Value, *ALL
Local SAP . . . . . :          Value, *ALL
IP Identifier . . . . . :          Value, *ALL
Remote IP Address . . . . . :          Value, *ALL
Format Options:
-----
Controller name . . . . . : *ALL      *ALL, name
Data representation . . . . : 3          1=ASCII, 2=EBCDIC, 3=*CALC
Format SNA data only . . . . : N          Y=Yes, N=No
Format RR, RNR commands . . . : N          Y=Yes, N=No
Format TCP/IP data only . . . : Y          Y=Yes, N=No
  IP address . . . . . : 10.50.21.1    *ALL, address
  IP address . . . . . : *ALL          *ALL, address
  IP port . . . . . : *ALL            *ALL, IP port
Format UI data only . . . . . : N          Y=Yes, N=No
Format IPX data only . . . . : N          Y=Yes, N=No
Format MAC or SMT data only : N          Y=Yes, N=No
Format Broadcast data . . . . : N          Y=Yes, N=No
                          RCHASM20 - V04R04M00 - 471125
Record Number . . . . . : Number of record in trace buffer (decimal)
S/R . . . . . : S=Sent R=Received M=Modem Change
Data Length . . . . . : Amount of data in record (decimal)
Record Status . . . . . : Status of record
Record Timer . . . . . : Time stamp. Based on communications hardware, the time
                          stamp will be either:
                          1. 10 microsecond resolution time of day
                              (HH:MM:SS.NNNNN) based on the system time when the
                              trace was stopped
                          2. 100 millisecond resolution relative timer with
                              decimal times ranging from 0 to 6553.5 seconds
Data Type . . . . . : EBCDIC data, ASCII data or Blank=Unknown
Controller name . . . . . : Name of controller associated with record
Command . . . . . : Command/Response information
Number sent . . . . . : Count of records sent
Number received . . . . . : Count of records received
Poll/Final . . . . . : ON=Poll for Commands, Final for Responses
Destination MAC Address . . . . : Physical address of destination
Source MAC Address . . . . . : Physical address of source
DSAP . . . . . : Destination Service Access Point
SSAP . . . . . : Source Service Access Point
Frame Format . . . . . : LLC (Logical Link Control) or MAC (Media
                          Access Control)
Commands/Responses:
-----
I . . . . . : Information
RR . . . . . : Receive Ready
RNR . . . . . : Receive Not Ready
REJ . . . . . : Reject
UI . . . . . : Unnumbered Information
UA . . . . . : Unnumbered Acknowledgment
DISC . . . . . : Disconnect/Request Disconnect
TEST . . . . . : Test
SIM . . . . . : Set Initialization Mode
FRMR . . . . . : Frame Reject
DM . . . . . : Disconnected Mode
```

XID Exchange ID
 SABME Set Asynchronous Balanced Mode Extended
 ***** Command/Response Not Valid

AS20 - V04R04M00 - 471125

COMMUNICATIONS TRACE Title: H2H - ESP w/Auth 03/15/99 15:29:43 Page: 3

Record Number	Data S/R	Record Length	Timer	Controller Name	Destination MAC Address	Source MAC Address	Frame Format	Command	Number Sent	Number Received	Poll/ Final	DSAP
---------------	----------	---------------	-------	-----------------	-------------------------	--------------------	--------------	---------	-------------	-----------------	-------------	------

***** The IKE negotiation is performed in aggressive mode. Three messages are used in phase 1.
 ***** The first two packets are Address Resolution Protocol (ARP) requests to resolve the MAC address for a given IP address

2676	S	33	19:03:19.12486		FFFFFFFFFFFF	800629B98CCA	LLC	UI			OFF	AA
			Routing Info	: 0270								
			Frame Type	: ARP		Src Addr: 10.50.21.1	Dest Addr: 10.50.41.1		Operation: REQUEST			
			ARP Header	: 0006080006040001000629B98CCA0A3215010000000000000000A322901								
2678	R	33	19:03:19.12496		000629B98CCA	C20000018188	LLC	UI			OFF	AA
			Routing Info	: 02F0								
			Frame Type	: ARP		Src Addr: 10.50.41.1	Dest Addr: 10.50.21.1		Operation: RESPONSE			
			ARP Header	: 00060800060400024200000181880A322901000629B98CCA0A321501								

*
 ***** record 2676 shows the first IKE packet flowing from AS20 (10.50.21.1) to AS25 (10.50.41.1). AS20 is the initiator of the VPN connection. The first message negotiates policy, exchange Diffie-Hellman public values and ancillary data necessary for the exchange, and identities.
 *

2679	S	237	19:03:19.12549		420000018188	800629B98CCA	LLC	UI			OFF	AA
			Routing Info	: 0270								
			Frame Type	: IP	TOS: NORMAL	Length: 232	Protocol: UDP	Datagram ID: EC				
				Src Addr: 10.50.21.1	Dest Addr: 10.50.41.1	Fragment Flags: MAY ,LAST						

Packet 1
 Phase 1

SNAP Header: 0000000800
 IP Header: 450000E8ECPD000040113AA20A3215010A322901
 IP Options: NONE
 UDP Src Port: 500, Unassigned Dest Port: 500, Unassigned Message Length: 212
 UDP Header: 01F401F400D40000
 Data: 9A52785EC1F3E3C4 0000000000000000 0110040000000000 000000CC04000034 **RX-****.....*
 0000000100000001 0000002801010001 0000002001010000 8001000580020002 *.....(.....*...*
 8003000180040001 800B0001800C0E10 0A0000644EC478F3 41517AA48F835420 **.....*.....DN*X*AQZ*

530D419AC68263D4 53C16D61AF7F36C3 9F361D8AEE561D41 BD9B06CFEAB98001 *S.A***S*MA*.6**6.**V.A**.*
 591E2CFAF1D5A0DB A0B0F571009E484 418E2A1DDB91A894 64B8527B679F0999 *Y.,*****.W.**A**.*...D*{
 5828C8D99685C2CE 12FC2D7BC723CC45 4954390305000000 F149B03211EE5D80 *X(*****.*-{*#*EIT*....*I*2
 0000000C01000000 0A321501 *.....2..

*
 ***** The second message negotiates policy, exchange Diffie-Hellman public values and ancillary data necessary for the exchange, and identities. In addition the second message authenticates the responder.
 *

2747	R	261	19:03:20.31764		000629B98CCA	C20000018188	LLC	UI			OFF	AA
			Routing Info	: 02F0								
			Frame Type	: IP	TOS: NORMAL	Length: 256	Protocol: UDP	Datagram ID: 95				
				Src Addr: 10.50.41.1	Dest Addr: 10.50.21.1	Fragment Flags: MAY ,LAST						

Packet 2
 Phase 1

SNAP Header: 0000000800
 IP Header: 45000100955B00004011922C0A3229010A321501
 IP Options: NONE
 UDP Src Port: 500, Unassigned Dest Port: 500, Unassigned Message Length: 236
 UDP Header: 01F401F400EC40A8
 Data: 9A52785EC1F3E3C4 E4509319158FFB4D 0110040000000000 000000E404000034 **RX-*****P**M.....*
 0000000100000001 0000002801010001 0000002001010000 8001000580020002 *.....(.....*...*
 8003000180040001 800B0001800C0E10 0A000064F355D922 DFDAD79636BA7B1C **.....*.....D*U**...*
 FA5951A20F6A835C 442833F57AB019DE 6F939E4928D62E74 5C9F9E3ABE01600E **YQ*.J*.D(3*Z*.O**I(*.T.**.
 1CAAC89093D69C1B 6F870779FD756F5D 1B73BEC11185C018 57A15BBC0B68A900 *.*****.O*.Y*UO!S**.*.W*ç*
 C231715DBA3FB2CD 893F78F1891B22F7 39313FC105000000 15237AC7E61C12A9 **1Q!?****?X**.*91?*.#Z*
 0800000C01000000 0A32290100000018 7088BF0F9ECA24AF C63AF451967EED30 *.....2).....P**.*\$**:*Q
 FFE7925F ****

*
 ***** The third message authenticates the initiator and provides a proof of participation in the exchange.
 *

AS20 - V04R04M00 - 471125

COMMUNICATIONS TRACE Title: H2H - ESP w/Auth 03/15/99 19:03:42 Page: 4

Record Number	Data S/R	Record Length	Timer	Controller Name	Destination MAC Address	Source MAC Address	Frame Format	Command	Number Sent	Number Received	Poll/ Final	DSAP
---------------	----------	---------------	-------	-----------------	-------------------------	--------------------	--------------	---------	-------------	-----------------	-------------	------

2751	S	85	19:03:20.44187		420000018188	800629B98CCA	LLC	UI			OFF	AA
			Routing Info	: 0270								
			Frame Type	: IP	TOS: NORMAL	Length: 80	Protocol: UDP	Datagram ID: EC				
				Src Addr: 10.50.21.1	Dest Addr: 10.50.41.1	Fragment Flags: MAY ,LAST						

```

Packet 3          SNAP Header: 0000000800
Phase 1          IP Header : 45000050ECFF000040113B380A3215010A322901
                  IP Options : NONE
                  UDP . . . : Src Port: 500,Unassigned   Dest Port: 500,Unassigned   Message Length: 60
                  UDP Header : 01F401F4003C0000
Data . . . . . : 9A52785EC1F3E3C4 E4509319158FFB4D 0810040000000000 0000003400000018 **RX-****P*..*M.....4
                  BCDC12EC45431C82 E74FCC7533155F9F 4A4E7BD4          ***.EC.**O*U3_.*JN}*

```

```

***** IKE Phase 2 starts *****
***** Packet 4 is the first packet for the phase 2 negotiation.

```

```

2783 S 173 19:03:21.18657          420000018188 800629B98CCA LLC UI OFF AA
Routing Info . : 0270
Frame Type : IP TOS: NORMAL Length: 168 Protocol: UDP Datagram ID: ED
Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST

```

```

Packet 4          SNAP Header: 0000000800
Phase 2          IP Header : 450000A8ED00000040113ADF0A3215010A322901
                  IP Options : NONE
                  UDP . . . : Src Port: 500,Unassigned   Dest Port: 500,Unassigned   Message Length: 148
                  UDP Header : 01F401F400940000
Data . . . . . : 9A52785EC1F3E3C4 E4509319158FFB4D 081020018F236A6A 0000008C79422629 **RX-****P*..*M.. .*#J...*
                  26E12778C9A38DE0 54800E7E6F69377A 441AE71883E8874E 80ADA45CAECD9336 *&*'X****T*.OI7ZD.*.***N***.
                  5BFABBC88499F963 3E4CABC8B829E8F1 96EC2749A864E507 340C4A1D3144D508 *C*****C>L***)****'I*D*.4.J.
                  BA17DD6B0723E805 6BCB7A095D62FF2B 482DC4B38AAD35DF BC9B17E48A7D778B **.K.#.*K*Z.!B*+H-****5***.
                  61529EC31B750740 830BEB40          *AR** .U.@*.*@

```

```

2808 R 173 19:03:21.79773          000629B98CCA C20000018188 LLC UI OFF AA
Routing Info . : 02F0
Frame Type : IP TOS: NORMAL Length: 168 Protocol: UDP Datagram ID: 95
Src Addr: 10.50.41.1 Dest Addr: 10.50.21.1 Fragment Flags: MAY ,LAST

```

```

Packet 5          SNAP Header: 0000000800
Phase 2          IP Header : 450000A895FE0000401191E10A3229010A321501
                  IP Options : NONE
                  UDP . . . : Src Port: 500,Unassigned   Dest Port: 500,Unassigned   Message Length: 148
                  UDP Header : 01F401F40094DBFD
Data . . . . . : 9A52785EC1F3E3C4 E4509319158FFB4D 081020018F236A6A 0000008C84DAFE7 **RX-****P*..*M.. .*#J...*
                  6B6BE38C253568DD E6CBF6FFD75A172F 142CA1B499DF8528 3A78AA4E982BD629 **K**%5H*****Z./,*****(:X*N
                  01EA49FBB10C007E 11C47A74DD7EE9A8 447EA35E023804F4 7E5DD6921E93616B *.I**...*ZT*.**D.*.8.*!**.
                  AD244D52A0B7A915 80D47ED30BA1BE15 DF75A7E8E4467193 B7D850746F249BA8 **$MR***.***.***.***U***FQ***PT
                  72FBC80B7CBF0A0D E6C3A82D          *R**..*..***-

```

```

2812 S 85 19:03:21.84172          420000018188 800629B98CCA LLC UI OFF AA
Routing Info . : 0270
Frame Type : IP TOS: NORMAL Length: 80 Protocol: UDP Datagram ID: ED
Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST

```

```

Packet 6          SNAP Header: 0000000800
Phase 2          IP Header : 45000050ED03000040113B340A3215010A322901
                  IP Options : NONE
                  UDP . . . : Src Port: 500,Unassigned   Dest Port: 500,Unassigned   Message Length: 60
                  UDP Header : 01F401F4003C0000
Data . . . . . : 9A52785EC1F3E3C4 E4509319158FFB4D 081020018F236A6A 00000034B564286C **RX-****P*..*M.. .*#J...4
                  302BEEB3BF3BD6B7 C814C6D846FF6619 4B8F8C88          *0+****,***.***F*P.K***

```

```

***** End of IKE negotiation. *****

```

```

***** User data following *****

```

```

3557 S 325 19:03:33.69112          420000018188 800629B98CCA LLC UI OFF AA
Routing Info . : 0270
Frame Type : IP TOS: NORMAL Length: 320 Protocol: ESP Datagram ID: ED
Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST

```

```

1. Ping request  SNAP Header: 0000000800
                  IP Header : 45000140ED2400003F323B020A3215010A322901
                  IP Options : NONE
                  ESP header : SPI: '4046763C'X SNF: 1
Data . . . . . : 3EACD99422BF2918 838914D4E508C375 F5290962B040C0BA C674114886FE36CC *>*****)..**.*U*).B@****.H
                  559480F32260C893 321BA278E90A39FE 2DCA5770F2AF1AE3 CF14E3F201E2D37D *U****).**2.*X*.9*-*WP**.*.***
                  962BBCC240526D09 53FCCB36A7CE19D5 15456E5B43FB8D83 0876DC14F30E207B *****@RM.S**6**.*.ENÇC***.V*.
                  80FEA67522050728 230B47223614D2CA 723E74091B14379F 2E4A4B608E90C841 ****U".(#.#'6.**R>T...7*.JK.
                  7EB78F0429B2A336 5E9E994ED83DEEF5 C702C770692F9E91 AFA4ECDCEBFB34D12 *(.)* **6-***N**=***.*PI/*****
                  042002EB00AE58FC B4F7C0D5A723E150 B61E0EBCE10964C6 80911DBB69830CE7 *.*.X*****#*P*..*..D****.
                  9AFC9B795B09DB45 441749F3311D8881 4EE1C57E7AD14A5C B6A6685DF457851A ****Yç.*ED.I*1.**N**.*Z*J.*#H!
                  D6C74A3B53EA5E67 9373F8EE2629AB4B CFA5ACA2484977F9 9FA2FA00E3A1243C ***J;S*V**S**&)*K****HIW****.

```

C01232905C432E47 E99DBFFB614EDAD6 3F1E464F57CC21F8 7FDA8F0E314C0C29 **.2*.C.G****AN**?.FOW*|*.*.
CE3E6BBS **>K*

3569 R 325 19:03:33.92233 000629B98CCA C2000018188 LLC UI OFF AA
Routing Info . : 02F0

Frame Type : IP TOS: NORMAL Length: 320 Protocol: ESP Datagram ID: 9C
Src Addr: 10.50.41.1 Dest Addr: 10.50.21.1 Fragment Flags: MAY ,LAST

1. Ping response

SNAP Header: 0000000800
IP Header : 450001409CD800003F328B4E0A3229010A321501
IP Options : NONE

ESP header : SPI: '751F128C'X SNF: 1

Data : 27807AD006BD636E 00C648C5AA43715A 415BB910392595CA 5C84B0321CCBE9BD **Z*.CN.*H**CQZA<*.9***.**2
3087ADD156C0C490 51716D0E9634BE62 76E8E061800A654E 510A97CA817E05F1 *0***V***QQM.*4*BV**A*.ENQ.**
1B326231779B017D ED89F4C9586FD9C6 B154D1CD2B88D139 7ED053C82D106B1E *.2B1W*.)***XO***T***9.*S*
D7A6201A5F817D65 14E9BAE4C68AD924 3423FE6DBBC7824B 2D1C7915EBC63C68 ***.}_E.*****\$4#M**K-.Y.
78C5835AC2361716 471D3804D563761E C76739EFE2A42EBF 876CAD7794905AF0 *X**Z*6..G.8.*CV.*G9***.**L*W
121720E6734579FE D475BB23D11F1633 D36BDB16BC0AC91E 66800A39289DBF11 *. *SEY**U*#*..3*K*.*.F*.9
ED4197CC041F465E 6E812BF1A38373EC 2A3FD85CA84A2C3B FD02F098FC5C0122 **A**..F~N+****S**?.*J,;.***
8DEA9E9F52074C07 B659E4B29DF24118 0EFFF515F97E9B16 57CC38BB3645BD90 *****R.L.Y****A..*Q_Y..*W*8*
59F85761C7379D3F BEAD33FDEA39397D 61BF3B9D28A0D047 44564B723215A23D *Y*WA*7*?*3*99)A*;* (**GDVVKR
9727933D **!*=

AS20 - V04R04M00 - 471125

COMMUNICATIONS TRACE Title: H2H - ESP w/Auth 03/15/99 19:03:42 Page: 6

Record Number	Data S/R	Record Length	Record Timer	Controller Name	Destination MAC Address	Source MAC Address	Frame Format	Command	Number Sent	Number Received	Poll/ Final	DSAP
---------------	----------	---------------	--------------	-----------------	-------------------------	--------------------	--------------	---------	-------------	-----------------	-------------	------

3572	S	325	19:03:33.92545		420000018188	800629B98CCA	LLC	UI			OFF	AA
------	---	-----	----------------	--	--------------	--------------	-----	----	--	--	-----	----

Routing Info . : 0270
Frame Type : IP TOS: NORMAL Length: 320 Protocol: ESP Datagram ID: ED
Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST

2. Ping request

SNAP Header: 0000000800
IP Header : 45000140ED2600003F323B000A3215010A322901
IP Options : NONE

ESP header : SPI: '4046763C'X SNF: 2

Data : AA11B2150A0D5077 8F77B2A0DC6F771 F52D25264E2DB0B9 0AA0DFD1A82A6EFC **. *..PW*W*****Q*~%&N-***.
8ECE97D2B9E19217 67EB3C4F33D1B496 47BA02B6C07682A0 17545B51E25BCBC7 *****.G<03***G*. *.V**..TQ
FFA5E15585E61C6A DAAF6D3CE8D9AB49 CFF57F79C81DD6C1 90E41B2C79899540 ***U**..J*M<***I**..Y*..***. ,
D81A56571B183E16 E2B3B688A36479DA E7EA72325D6E896D 55F73CEDB540BF9 **..VW..>..*****DY**R2!N*MU*<
2D6A0C6408928CF9 C21F45D2684E3440 C7A3AD138EA6A02F A2EA02D09A3FD212 *-J.D.***.E*HN4@***.***/**.*
18EF9111E44D9D66 A3BE10BF1CA93362 26A77A551EE4C5D1 12479CBDBDACD67C *. *..M*F**..*3B&*ZU.***.G**
419E56952A8EA1B7 91585B96D8761D52 70EBC45E2E313D78B BB5852A7223985D6 *A*V*****X&*V..RP**R*..**XR*
ODDAA96233157CF2 6B74C72969E05180 EA5064E6A49F7CAB 0C4FF6B466D61981 *.**B3..*KT*)I*Q**PD***..O**
1499E25FC92FC54 FDAEFA931A03AEFD 57E1238D60EB21F9 BCBD0D89F65300EB **I*%***T***..**W*#*..|***.*
BF797896 **YX*

3573 R 325 19:03:33.92798 000629B98CCA C2000018188 LLC UI OFF AA
Routing Info . : 02F0

Frame Type : IP TOS: NORMAL Length: 320 Protocol: ESP Datagram ID: 9C
Src Addr: 10.50.41.1 Dest Addr: 10.50.21.1 Fragment Flags: MAY ,LAST

2. Ping response

SNAP Header: 0000000800
IP Header : 450001409CD900003F328B4D0A3229010A321501
IP Options : NONE

ESP header : SPI: '751F128C'X SNF: 2

Data : 27807AD006BD636E AA52A32039AD9E9F AE40F13184802419 AA3D1833091B2DEC **Z*.*CN*R* 9****@*1**\$.*=.3
377202BD2408C101 713C6D707E655EA0 D8E8F4AE4AFD512A DE2C99A64ACA4AF4 *7R.*\$. *.Q*MP.E-*****J*Q**,**
5CE380A6CE5A8928 2A4FE441E5D01C6B 34E83C320FD2F024 5D5482136FA0770E *.***Z*(*O*A**..K4*<2.**\$!T*.
397A691C08C8D573 3424297CEP34187F A752B316FF1827A3 64C6B63F11D883D4 *9ZI..**S4\$).*4..*R*.*.1*?D**?
78BF891D09723AFA 524ACBE99F89E2B7 9973AFD8E0E5B007 B0A4E605559D4322 *X**..R:R*J*****S*****.***.
E76404775882BA06 C87E79ACC8D9E9A9 AEA72CA35B82B413 89DE7E027944615A **D.WX**.*.Y*****.φ**.*..
686F879D07973A54 A73B4D9DA0F6E5C AE991D58593C38A9 6204395FD9A155D8 *HO**.*.T*;M**..N.**.XY*8*B..9_
B01C8471809E41D1 F97E0C7EBF910A22 958080B41D39CCA0 D962BAF283AD07CF **. *Q*A*A*..**."****.9***B**
6D18F94F4D6EF4C5 3355C98304673E85 EE96E5D38F00B1ED E1B736D8E9FBF823 *M.*OMN**3U*.G>*****.****6*
9D80EC27 ****:

AS20 - V04R04M00 - 471125

*** END OF COMPUTER PRINTOUT ***

14.9 AS/400 communication trace example with details

This section includes the same trace that is shown in 14.8, “AS/400 communication trace example” on page 673. However, this trace example offers more details on how to read the messages exchanged in phase 1 and phase 2.

***** The header of the trace is removed.

 ***** ***** The IKE negotiation is performed in aggressive mode. Three messages are used for phase 1.
 ***** Aggressive mode with a pre-shared key is described as follows:

	Initiator		Responder
*****	-----		-----
*****	Packet 1	HDR, SA, KE, Ni, IDii -->	
*****	Packet 2	<--	HDR, SA, KE, Nr, IDir, HASH_R
*****	Packet 3	HDR, HASH_I -->	

***** HDR is an IKE header whose exchange type is the mode.
 ***** SA is an SA negotiation payload with one or more proposals. An initiator MAY provide multiple proposals for negotiation, a responder MUST reply with only one.
 ***** KE is the key exchange payload which contains the public information exchanged in a Diffie-Hellman exchange. There is no particular encoding (e.g. a TLV) used for the data of a KE payload.
 ***** Nx is the nonce payload; x can be: i or r for the IKE initiator and responder respectively.
 ***** IDx is the identification payload for "x". x can be: "ii" or "ir" for the IKE initiator and responder respectively during phase one negotiation; or "ui" or "ur" for the user initiator and responder respectively during phase two.
 ***** Nx is the nonce payload; x can be: i or r for the IKE initiator and responder respectively.
 ***** HASH (and any derivative such as HASH(R) or HASH_I) is the hash payload. The contents of the hash are specific to the authentication method.

Record Number	Data S/R	Record Length	Record Timer	Controller Name	Destination MAC Address	Source MAC Address	Frame Format	Command	Number Sent	Number Received	Poll/ Final	DSAP
---------------	----------	---------------	--------------	-----------------	-------------------------	--------------------	--------------	---------	-------------	-----------------	-------------	------

***** The first two packets are Address Resolution Protocol (ARP) requests to resolve the MAC address for a given IP address

2676	S	33	19:03:19.12486		FFFFFFFFFFFF	800629B98CCA	LLC	UI			OFF	AA
			Routing Info	. : 0270								
				Frame Type : ARP	Src Addr: 10.50.21.1	Dest Addr: 10.50.41.1					Operation: REQUEST	
				ARP Header : 0006080006040001000629B98CCA0A32150100000000000A322901								
2678	R	33	19:03:19.12496		000629B98CCA	C20000018188	LLC	UI			OFF	AA
			Routing Info	. : 02F0								
				Frame Type : ARP	Src Addr: 10.50.41.1	Dest Addr: 10.50.21.1					Operation: RESPONSE	
				ARP Header : 00060800060400024200000181880A322901000629B98CCA0A321501								

*
 ***** record 2676 shows the first IKE packet flowing from AS20 (10.50.21.1) to AS25 (10.50.41.1). AS20 is the initiator of the VPN connection. The first message negotiate policy, exchange Diffie-Hellman public values and ancillary data necessary for the exchange, and identities.
 *

2679	S	237	19:03:19.12549		420000018188	800629B98CCA	LLC	UI			OFF	AA
			Routing Info	. : 0270								
Packet 1				Frame Type : IP	TOS: NORMAL	Length: 232	Protocol: UDP				Datagram ID: EC	
Phase 1												

---> UDP protocol is used
 For IKE negotiation
 Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST
 SNAP Header: 0000000800
 IP Header : 450000E8ECPD000040113AA20A3215010A322901

 ! !--> IP destination address
 !--> IP source address
 IP Options : NONE
 UDP . . . : Src Port: 500,Unassigned Dest Port: 500,Unassigned Message Length: 212

 ! !--> Total UDP datagram
 ! !--> The destination port is UDP port 500 of the remote QTOKVPNIKE job.
 !
 !--> VPN server job QTOKVPNIKE is sending phase 1 messages through UDP port 500.
 UDP Header : 01F401F400D40000

```

Data . . . . . : 9A52785EC1F3E3C4 0000000000000000 01 1 0 04 00 00000000 000000CC 04 00 0034 **RX-****.....*
-----
!<----- IKE Header ----->!<---SA---
!           !           ! ! ! ! !           !           ! !           !-> Payload Length (2 octets)
!           !           ! ! ! ! !           !           ! !           of the current payload
!           !           ! ! ! ! !           !           ! !           incl. the generic header
!           !           ! ! ! ! !           !           ! !           !
!           !           ! ! ! ! !           !           ! !           !-> reserved
!           !           ! ! ! ! !           !           ! !           !
!           !           ! ! ! ! !           !           !           !-> Next Payload (1 octet)
!           !           ! ! ! ! !           !           !           04=Key Exchange (KE)
!           !           ! ! ! ! !           !           !           !
!           !           ! ! ! ! !           !           !           !-> Length (4 octets) Length of total
!           !           ! ! ! ! !           !           !           message (header + payload)
!           !           ! ! ! ! !           !           !           204 bytes (Message Length - UDP Header)
!           !           ! ! ! ! !           !           !           !
!           !           ! ! ! ! !           !           !           !-> Message ID (4 octets) during phase 1 always 0
!           !           ! ! ! ! !           !           !           !
!           !           ! ! ! ! !           !           !           !-> Flags (1 octet)
!           !           ! ! ! !           !           !           !
!           !           ! ! ! !-> Exchange Type (1 octet) 04=Agressive mode
!           !           ! ! !           !           !           !
!           !           ! ! !-> Minor Version (4 bits) indicates the minor version
!           !           ! !           of the IKE protocol in use.
!           !           ! !           !
!           !           ! !-> Major version (4 bits) indicates the major version of
!           !           !           the IKE protocol in use.
!           !           !           !
!           !           !-> Next Payload (1 octet) indicates the type of the first
!           !           !           payload in the message. 01=Security Association (SA)
!           !           !           !
!           !           !-> Responder Cookie (8 octets) - Cookie of entity that is responding
!           !           !           to an SA establishment request (Set to 0 in first message).
!           !           !           !
!-> Initiator Cookie (8 octets) - Cookie of entity that initiated SA establishment.

```



```

00 00 000C 01 00 0000 0A321501                                     *.....2..
-----
!<--Identification Payload-->!
! ! ! ! ! ! ! !
! ! ! ! ! ! ! !-> Identification data (variable length). Value as indicated
! ! ! ! ! ! ! !      by the Identification type (initiator IP address 10.50.21.1)
! ! ! ! ! ! ! !
! ! ! ! ! ! ! !-> Port (2 octets) - during phase 1 must be set to 0 or UDP port 500. Any other
! ! ! ! ! ! ! !      will be treated as an error.
! ! ! ! ! ! ! !
! ! ! ! ! ! ! !-> Protocol ID (1 octet) - Value specifying an associated IP protocol ID (e.g. UDB/TCP).
! ! ! ! ! ! ! !      A value of 0 means that the Protocol ID should be ignored.
! ! ! ! ! ! ! !
! ! ! ! ! ! ! !-> Identification type (1 octet) - Value describing the identity information found in the
! ! ! ! ! ! ! !      Identification Data field. 01=ID_IPV4_ADDR
! ! ! !
! ! !-> Payload length (2 octets) - Length of the identification data, including the generic header
! !
! !-> reserver (1 octet)
!
End of packet 1      !-> Next payload (1 octet). If the current payload is the last in the message, this field is 00.

***** The second messages negotiate policy, exchange Diffie-Hellman public values and ancillary data necessary for the
***** exchange, and identities. In addition the second message authenticates the responder.
*
 2747  R      261  19:03:20.31764          000629B98CCA  C20000018188  LLC  UI          OFF  AA
      Routing Info . : 02F0
Packet 2      Frame Type : IP          TOS: NORMAL          Length: 256  Protocol: UDP          Datagram ID: 95
Phase 1      Src Addr: 10.50.41.1      Dest Addr: 10.50.21.1      Fragment Flags: MAY ,LAST
      SNAP Header: 0000000800
      IP Header : 45000100955B00004011922COA3229010A321501
      IP Options : NONE
      UDP . . . : Src Port: 500,Unassigned  Dest Port: 500,Unassigned  Message Length: 236
      UDP Header : 01F401F400EC40A8

      !<----- IKE Header ----->!<--SA --
Data . . . . . : 9A52785EC1F3E3C4 E4509319158FFB4D 0110040000000000 000000E404000034 *RX~****P~**M.....*
      !
      !-> Responder Cookie (8 octets) - Cookie of entity that is responding
      to an SA establishment request (Is set in second message).

      ----- SA -----
      !<----- Proposal -----
      !<----- Transform -----
0000000100000001 0000002801010001 0000002001010000 8001000580020002 *.....(.....)*...

      ----- SA ----->!
      ----- Proposal ----->!
      ----- Transform ----->! !<----- Key Exchange (KE) ----
8003000180040001 800B0001800C0E10 0A000064F355D922 DFDAD79636BA7B1C **.....*.....D*U*****
      ----- KE -----
FA5951A20F6A835C 442833F57AB019DE 6F939E4928D62E74 5C9F9E3ABE01600E **YQ*.J*.D(3*Z*.*O**I(*.T.**:

      ----- KE -----
1CAAC89093D69C1B 6F870779FD756F5D 1B73BEC11185C018 57A15BBC0B68A900 *.*****.O*.Y*UO!.S***.W*φ*

      ----- KE ----->!<----- Nonce ----->!
C231715DBA3FB2CD 893F78F1891B22F7 39313FC10500000C 15237AC7E61C12A9 **1Q!??***?X**."*91?.....#Z*

!<--- Identification -->!<----- HASH Responder -----
0800000C01000000 0A32290100000018 7088BF0F9ECA24AF C63AF451967EED30 *.....2).....P**.**$**:*Q

-----
!
! !> Hash Data (variable length) Data that results from
! applying the hash routine to the IKE message.
! !-> Responder ID (10.50.41.1)

End of Packet 2      ----->!
      FFE7925F

```

****_

*
***** The third message authenticates the initiator and provides a proof of participation in the exchange.
*

AS20 - V04R04M00 - 471125
COMMUNICATIONS TRACE Title: H2H - ESP w/Auth 03/15/99 19:03:42 Page: 4
Record Data Record Controller Destination Source Frame Number Number Poll/
Number S/R Length Timer Name MAC Address MAC Address Format Command Sent Received Final DSAP

2751 S 85 19:03:20.44187 420000018188 800629B98CCA LLC UI OFF AA
Routing Info . : 0270
Frame Type : IP TOS: NORMAL Length: 80 Protocol: UDP Datagram ID: EC
Packet 3 Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST
Phase 1 SNAP Header: 0000000800
IP Header : 45000050ECFF000040113B380A3215010A322901
IP Options : NONE
UDP . . . : Src Port: 500,Unassigned Dest Port: 500,Unassigned Message Length: 60
UDP Header : 01F401F4003C0000

!<----- IKE Header ----->!<-----
Data : 9A52785EC1F3E3C4 E4509319158FFB4D 0810040000000000 0000003400000018 **RX-****P*..*M.....4
! ! !
! ! !<- Payload Length
! ! !
! ! !<- Next Payload 00=Last payload
! ! !
! ! !<- Length (4 octets) Length of total
! ! ! message (header + payload)
! ! !
! !<- Exchange Type 04=Agressive Mode
! !
!<- Next Payload 08=Hash

----- Hash Initiator ----->!
BCDC12EC45431C82 E74FCC7533155F9F 4A4E7DB4 ***.EC.**U3._*JN}*

End of Packet 3 !<- Hash Data (variable length) Data that results from
applying the hash routine to the IKE message.

*
***** IKE Phase 2 starts *****
***** Phase 2 is performed in Quick mode. Following is a description about the quick mode. For more information refer to
***** RFC2409 "The Internet Key Exchange (IKE)"

***** Quick Mode is not a complete exchange itself (in that it is bound to a phase 1 exchange), but is used as part of the SA
***** negotiation process (phase 2) to derive keying material and negotiate shared policy for non-IKE SAs. The information
***** exchanged along with Quick Mode MUST be protected by the IKE SA-- i.e. all payloads except the IKE header are encrypted. *****
In Quick Mode, a HASH payload MUST immediately follow the IKE header and a SA payload MUST immediately follow the HASH.
***** This HASH authenticates the message and also provides liveness proofs.
***** Quick Mode is defined as follows:
***** Initiator Responder
***** -----
***** Packet 4 HDR*, HASH(1), SA, Ni
***** [, KE] [, IDci, IDcr] -->
***** Packet 5 <-- HDR*, HASH(2), SA, Nr
***** [, KE] [, IDci, IDcr]
***** Packet 6 HDR*, HASH(3) -->

2783 S 173 19:03:21.18657 420000018188 800629B98CCA LLC UI OFF AA
Routing Info . : 0270
Frame Type : IP TOS: NORMAL Length: 168 Protocol: UDP Datagram ID: ED
Packet 4 Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST
Phase 2 SNAP Header: 0000000800
IP Header : 450000A8ED00000040113ADF0A3215010A322901
IP Options : NONE
UDP . . . : Src Port: 500,Unassigned Dest Port: 500,Unassigned Message Length: 148
UDP Header : 01F401F400940000

!<----- IKE Header -----<!
Data : 9A52785EC1F3E3C4 E4509319158FFB4D 081020018F236A6A 0000008C79422629 **RX-****P*..*M.. .#JJ...*
! !
! !<- Message ID (4 octets) The message ID in the IKE
! ! header identifies a Quick Mode in progress for a

```

!           particular IKE SA which itself is identified by
!           the cookies in the IKE header.
!
!<- Next Payload 08=Hash

```

```

26E12778C9A38DE0 54800E7E6F69377A 441AE71883E8874E 80ADA45CAECD9336 *&'X***T*..OI7ZD*.*N***.
5BFABBC88499F963 3E4CABC8B829E8F1 96EC2749A864E507 340C4A1D3144D508 *C*****C>L***)*I*D*.4.J.
BA17DD6B0723E805 6BCB7A095D62FF2B 482DC4B38AAD35DF BC9B17E48A7D778B **.K.#.K*Z.!B*+H-****5***.*
61529EC31B750740 830BEB40 *AR** .U.@*.*@

```

**** Note that the Hash is following immediately after the IKE header, and all the SA exchange data are encrypted.

```

2808 R 173 19:03:21.79773 000629B98CCA C20000018188 LLC UI OFF AA
Routing Info . : 02F0
Packet 5 Frame Type : IP TOS: NORMAL Length: 168 Protocol: UDP Datagram ID: 95
Phase 2 Src Addr: 10.50.41.1 Dest Addr: 10.50.21.1 Fragment Flags: MAY ,LAST
SNAP Header: 0000000800
IP Header : 450000A895FE0000401191E10A3229010A321501
IP Options : NONE
UDP . . . : Src Port: 500,Unassigned Dest Port: 500,Unassigned Message Length: 148
UDP Header : 01F401F40094DBFD
!<----- IKE Header ----->!
Data . . . . : 9A52785EC1F3E3C4 E4509319158FFB4D 081020018F236A6A 0000008C84CDAFE7 **RX-****P*..*M..*#JJ...
6B6BE38C253568DD E6CBF6FFD75A172F 142CA1B499DF8528 3A78AA4E982BD629 *KK**%5H*****Z./.,*****(:X*N
01EA49FBB10C007E 11C47A74DD7EE9A8 447EA35E023804F4 7E5DD6921E93616B *.I*...*ZT*.*D.*.8.*!**
AD244D52A0B7A915 80D47ED30BA1BE15 DF75A7E8E4467193 E7D850746F249BA8 **$MR***.*.*.*.*U***FQ***PT
72FBC80B7CBFOA0D E6C3A82D *R**..*.*.*.*

```

```

2812 S 85 19:03:21.84172 420000018188 800629B98CCA LLC UI OFF AA
Routing Info . : 0270
Packet 6 Frame Type : IP TOS: NORMAL Length: 80 Protocol: UDP Datagram ID: ED
Phase 2 Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST
SNAP Header: 0000000800
IP Header : 45000050ED03000040113B340A3215010A322901
IP Options : NONE
UDP . . . : Src Port: 500,Unassigned Dest Port: 500,Unassigned Message Length: 60
UDP Header : 01F401F4003C0000
!<----- IKE Header ----->!
Data . . . . : 9A52785EC1F3E3C4 E4509319158FFB4D 081020018F236A6A 00000034B564286C **RX-****P*..*M..*#JJ...
302BEBE3BF3BD6B7 C814C6D846FF6619 4B8F8C88 *0+****;***.***F*F.K***
***** IKE Phase 2 end *****

```

```

3557 S 325 19:03:33.69112 420000018188 800629B98CCA LLC UI OFF AA
Routing Info . : 0270
Frame Type : IP TOS: NORMAL Length: 320 Protocol: ESP Datagram ID: ED
---
!<- ESP protocol (Prot No. 50)
Note that this is not anymore
An UDP datagram.

```

```

1. Ping request Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST
SNAP Header: 0000000800
IP Header : 45000140ED2400003F323B020A3215010A322901
IP Options : NONE
ESP header : SPI: '4046763C'X SNF: 1
-----
!           !           !
!           !           !<- The Sequence Number Field (SNF) is used for Replay Protection.
!           !           The sequence number is initialized to 0 on the sender and
!           !           receiver side when a SA is established.
!           !           !
!           !           !<- The SPI is an arbitrary 32-bit value that, in combination with the destination IP
!           !           address and security protocol (ESP), uniquely identifies the Security Association
!           !           for this datagram. Note that the SPI is uni-directional, that means the SPI for
!           !           data sent from 10.50.21.1 is different from the SPI for data sent from 10.50.41.1.
!           !           !
!<- Note that the ESP protocol has its own header.

```

***** All data following the ESP header are encrypted *****

Data : 3EACD99422BF2918 838914D4E508C375 F5290962B040C0BA C674114886FE36CC *>*****)**.***.U*).B*@***T.H
559480F32260C893 321BA278E90A39FE 2DCA5770F2AF1AE3 CF14E3F201E2D37D
*U****.***2.*X*.9*~*WP***.***
962BBCC240526D09 53FCCB36A7CE19D5 15456E5B43FB8D83 0876DC14F30E207B
@*RM.S**6**.*.ENC.V*.
80FEA67522050728 230B47223614D2CA 723E74091B14379F 2E4A4B608E90C841
****U".(.#.#"6.**R>T...7*.JK.
7EB78F0429B2A336 5E9E994ED83DEEF5 C702C770692F9E91 AFA4ECCBFB34D12
..)**6~**N*=***.PI/*****
042002EB00AE58FC B4F7C0D5A723E150 B61E0EBCE10964C6 80911DBB69830CE7
...*X*****#*P*...D**.*.
9AFC9B795B09DB45 441749F3311D8881 4EE1C57E7AD14A5C B6A6685DF457851A
****Yç.*ED.I*1.**N**.*Z*J.**H!
D6C74A3B53EA56E7 9373F8EE2629AB4B CFA5ACA2484977F9 9FA2FA00E3A1243C
J;S*V**S**&)*K*HIW****.
C01232905C432E47 E99DBFFB614EDAD6 3F1E464F57CC21P8 7FDA8F0E314C0C29
.*2*.C.G**AN**?.FOW*|*..
CE3E6BB5 **>K*

3569 R 325 19:03:33.92233 000629B98CCA C2000018188 LLC UI OFF AA

Routing Info . : 02F0
Frame Type : IP TOS: NORMAL Length: 320 Protocol: ESP Datagram ID: 9C
Src Addr: 10.50.41.1 Dest Addr: 10.50.21.1 Fragment Flags: MAY ,LAST

1. Ping response

SNAP Header: 0000000800
IP Header : 450001409CD800003F328B4E0A3229010A321501
IP Options : NONE
ESP header : SPI: '751F128C'X SNF: 1

Data : 27807AD006BD636E 00C648C5AA43715A 415B910392595CA 5C84B0321CCBE9BD
.*Z*.*CN.H**CQZAç*.9%***.**2
3087ADD156C0C490 51716D0E9634BE62 76E8E061800A654E 510A97CA817E05F1
*0***V***QQM.*4*BV**A*.ENQ.**
1B326231779B017D ED89F4C9586FD9C6 B154D1CD2B88D139 7ED053C82D106B1B
*.*2B1W*.)***XO***T**.*9.*S*
7A6201A5F817D65 14E9BAE4C68AD924 3423FE6DBBC7824B 2D1C7915EBC63C68
.*.}*E.**\$4#*M***K-.Y.
D7C5835AC2361716 471D3804D563761E C76739EFE2A42EBF 876CAD7794905AF0
*X**Z*6.*G.8.*CV.*G9***.**L*W
121720E6734579FE D475BB23D11F1633 D36BDB16BC0AC91E 66800A39289DBF11
*..*SEY**U*#*..3*K*.*.*F*.9
ED4197CC041F465E 6E812BF1A38373EC 2A3FD85CA84A2C3B FD02F098FC5C0122
A..F-N*.....S**?*J;,*.*
8DEA9E9F52074C07 B659E4B29DF24118 0EFF515F597E9B16 57CC38BB3645BD90
****R.L.*Y****A.*Q_Y.*.W*8*
59F85761C7379D3F BEAD33FDEA39397D 61BF3B9D28A0D047 44564B723215A23D
*Y*WA*7**?*3**99}A*;* (**GDVVKR
9727933D **!*=

3572 S 325 19:03:33.92545 42000018188 800629B98CCA LLC UI OFF AA

Routing Info . : 0270
Frame Type : IP TOS: NORMAL Length: 320 Protocol: ESP Datagram ID: ED
Src Addr: 10.50.21.1 Dest Addr: 10.50.41.1 Fragment Flags: MAY ,LAST

2. Ping request

SNAP Header: 0000000800
IP Header : 45000140ED2600003F323B000A3215010A322901
IP Options : NONE
ESP header : SPI: '4046763C'X SNF: 2

Data : AA11B2150A0D5077 8F77B2A0DC6F6771 F52D25264E2B0B09 0AA0DFD1A82A6EFC
.*...PW*W***Q*~%&N-***.***
8ECE97D2B9E19217 67EB3C4F33D1B496 47BA02B60C7682A0 17545B51E25BCBC7
*****.G*ç03***G*.*.V**.*TçQ
FFA5E15585E61C6A DAAF6D3CE8D9AB49 CFF57F79C81DD6C1 90E41B2C79899540
U**.*J**MI**.*Y*.****.
D81A56571B183E16 E2B3B688A36479DA E7EA72325D6E896D 55F73CED6B540BF9
.*VW..>.**D*Y**R2!N*MU*ç<
2D6A0C6408928CF9 C21F45D2684E3440 C7A3AD138EA6A02F A2EA02D09A3FD212
*-J.D.***.E*HN4@***.***/*.*
18EF9111E44D9D66 A3BE10BF1CA93362 26A77A551EE4C5D1 12479CBDBDACD67C
...*M*F**.*.3B&*ZU.***.G**
419E56952A8EA1B7 9158B96D8761D52 70EBC452E313D78B BB5852A7223985D6
*A*V*****Xç*V.RP**R*.*.*XR*
0DDAA96233157CF2 6B74C72969E05180 EA5064E6A49F7CAB 0C4FF6B466D61981
*.*B3..*KT*)I*Q**PD***.*O**
C1499E25FC92FC54 FDAEFA391A03AEFD 57E1238D60EB21F9 BCBDD089F65300EB
I*%*T***..**W*#*.*|***.***
BF797896 **YX*

3573 R 325 19:03:33.92798 000629B98CCA C2000018188 LLC UI OFF AA

Routing Info . : 02F0
Frame Type : IP TOS: NORMAL Length: 320 Protocol: ESP Datagram ID: 9C
Src Addr: 10.50.41.1 Dest Addr: 10.50.21.1 Fragment Flags: MAY ,LAST

2. Ping response

SNAP Header: 0000000800
IP Header : 450001409CD900003F328B4D0A3229010A321501
IP Options : NONE
ESP header : SPI: '751F128C'X SNF: 2

Data : 27807AD006BD636E AA52A32039AD9E9F AE40F13184802419 AA3D1833091B2DEC
.*Z*.*CN*R* 9*@*1**\$.*=.*3
377202BD2408C101 713C6D707E655EA0 D8E8F4AE4AFD512A DE2C99A64ACA4AF4
7R.\$.*.Q<MP.E~*****J*Q**.*
5CE380A6CE5A8928 2A4FE441E5D01C6B 34E83C320FD2F024 5D5482136FA0770E
*..***Z*(*O*A**.*K4*ç2.***\$!T*.
397A691C08C8D573 3424297CEF34187F A752B316FF1827A3 64C6B63F11D883D4
*9ZI..**S4\$).*4..*R*.*.*D**?
78BF891D09723AFA 524ACBE99F89E2B7 9973AFD8E0E5B007 B0A4E605559D4322
*X**..R:*R*J*****S*****.***
E76404775882BA06 C87E79ACC8D9E9A9A EAE72CA35B82B413 89DE7E027944615A
D.WX*.*.Y***.*ç**.*..
686F879D07973A54 A73B4D9DA40F6E5C AE991D5859C338A9 6204395FD9A155D8
*HO**.*.T*;M**.*N.**.XY*8*B.9_
B01C8471809E41D1 F97E0C7EBF910A22 958080B41D39CCA0 D962BAF283AD07CF
.*QA**..**.******.9***B**
6D18E94F4D6EF4C5 3355C98304673E85 EE96E5D38F00B1ED E1B736D8E9F8F823
*M.*OMN**3U**.*G.>*****.***6*
9D80EC27 ****!

AS20 - V04R04M00 - 471125

*** * END OF COMPUTER PRINTOUT * * * * *

Part 3. VPN interoperability scenarios

It is likely that your VPN network includes several different platforms. Since VPN implementations are recent, you may find differences in the way platforms name configuration values.

Even more important, differences between VPN implementations from different vendors may lead to serious interoperability problems. Until VPN implementations become more mature, you should be cautious when designing solutions that involve multiple vendors and platforms. It is always a good idea to run a pilot or proof of concepts scenarios.

This part reviews the concepts presented in previous chapters, but focuses on configurations involving multiple IBM platforms that implement Virtual Private Networks.

Chapter 15. Host-to-gateway VPN: AS/400 to 2212 router

This chapter describes a VPN host-to-gateway configuration between an AS/400 system and a 2212 router.

A machine that acts as a gateway usually connects systems in two separate networks at both sides of the gateway. The gateway system is not the data endpoint of the connection. Tunnel mode is used when at least one of the two systems participating in an IPsec tunnel is a gateway. For information on how the IP datagrams are processed in tunnel mode, refer to 1.5.2, “AH transport and tunnel modes” on page 16, and 1.6.2, “ESP transport and tunnel modes” on page 20.

A machine acting as a host is the VPN server and the data endpoint of the connection.

15.1 Branch office VPN connection (AS/400 host to 2212 router gateway)

In this scenario, we present a data center at the company’s head office and a remote branch office. The AS/400 system is located at the data center. Users located at the branch office need to secure access to the AS/400 system over the Internet. The branch office PCs are only allowed to access the AS/400 system at the data center. Figure 766 represents this scenario.

15.1.1 Scenario characteristics

Both the data center and the branch office networks belong to the same company. However, the branch office PCs are only allowed to access the AS/400 system and no other LAN resources (file servers, LAN printers, and so on) in the data center network. The subnet in the branch office network is the data endpoint on the router end of the VPN tunnel. The AS/400 system at the data center is both the data endpoint and the VPN server on the AS/400 end of the VPN tunnel.

The data center network is connected to the Internet through a firewall. The filters in the data center firewall must be opened to allow IKE negotiation and IPsec protocols between the AS/400 system and the remote branch office’s 2212 router VPN partner.

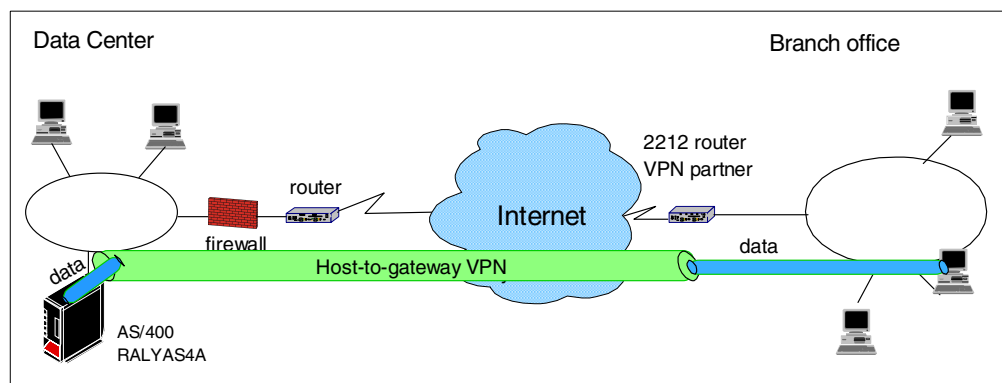


Figure 766. Branch office VPN - Host-to-gateway AS/400 system to 2212 router

15.1.2 Scenario objectives

The objectives of this scenario are:

- All traffic between RALYAS4A and the branch office must be protected by IPSec.
- The branch office PCs can only access the data center AS/400 system, and no other hosts, in the data center network.
- The data traffic can flow in the clear in the branch office network behind the VPN network. The data center and the branch office belong to the same company.

15.1.3 Scenario network configuration

Figure 767 shows our simple network configuration for the host to gateway AS/400 system to 2212 router.

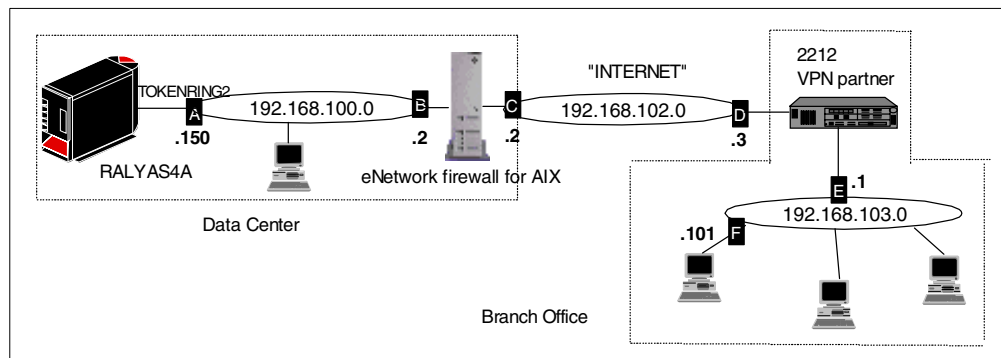


Figure 767. AS/400 host to 2212 router gateway scenario network configuration

Note

The AIX firewall filter rules were configured to route IKE (UDP port 500), AH, and ESP traffic between the VPN partner nodes.

15.1.4 2212 router software

Access Integration Services Version 3.3 is required on the 2212 router to support dynamic VPN connections.

15.1.5 Implementation tasks: Summary

The following list summarizes the tasks used to implement this VPN host-to-gateway environment:

1. Verify connectivity. Before you start configuring VPN and filters, you must be sure that the underlying TCP/IP network is properly configured and working.
2. Complete the planning worksheet for the 2212 router.
3. Configure a VPN in the 2212 router.
4. Complete the planning worksheet for the AS/400 system.

5. Configure a host-to-gateway VPN in the AS/400 system using the VPN configuration wizard.
6. Modify the VPN configuration created by the wizard to match the 2212 router VPN configuration.
7. Configure filters in the AS/400 system.
8. Start the VPN connection.
9. Perform verification tests.

15.1.6 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the AS/400 system and the branch office network are correct:

1. From the AS/400 system, run the following PING command to a host in the branch office network:

```
PING RMTSYS ('192.168.103.101')
```

2. Repeat the PING in the reverse direction from the branch office PC:

```
PING 192.168.100.150
```

Note

To test basic TCP/IP routing before activating the VPN connection, it is useful to temporarily enable PING through the firewall. The AIX firewall filter rules were changed to route the relevant ICMP messages before the test was run and were reverted to block PING when the test completed.

15.2 2212 router configuration

The following sections explain how to configure the VPN in the 2212 router to establish a secure tunnel with the AS/400 system RALYAS4A. It is beyond the scope of this redbook to provide detailed information about the 2212 router configuration. Refer to *A Comprehensive Guide to Virtual Private Networks, Vol III: IBM Cross-Platform and Key Management Solutions*, SG24-5309, for more information about the routers configuration.

15.2.1 Completing the planning worksheets for the 2212 router

Complete the 2212 router planning worksheets as shown in Table 85 through Table 93 on the following pages. The planning worksheets allow you to gather all the configuration data before the actual implementation. We completed these planning worksheets from the perspective of 2212 router in this scenario.

Table 85. IBM 2212 router configuration - Remote user definitions

Information you need to create your VPN	Scenario answers
How to identify the remote IKE peer (user): <ul style="list-style-type: none"> – IP address – Fully qualified domain name – User fully qualified domain name – Key ID 	Select IP address with AS/400
IP address that distinguishes this user?	192.168.100.150

Information you need to create your VPN	Scenario answers
Authenticate user with: – Pre-shared key – Public certificate?	Select pre-shared key with AS/400
Mode in which you will enter the pre-shared key: – ASCII – HEX	Select ASCII with AS/400
Pre-shared key (even number of characters):	123456

Table 86. IBM 2212 router configuration - Policy definitions

Information you need to create your VPN	Scenario answers
Policy name:	ike-pre-103-to-h100
Priority of this policy in case of multiple policies:	5

Table 87. IBM 2212 router configuration - Policy profile

Information you need to create your VPN	Scenario answers
Profile name:	103-to-h100
Source address format: – NetMask – Range – Single address	NetMask
Source address:	192.168.103.0
Destination address format: – NetMask – Range – Single address	Single address
Destination address:	192.168.100.150
Select the protocol to filter on: – TCP – UDP – All protocols – Specify range	All protocols
Starting value for the source port: 0 for all protocols	0
Ending value for the source port: 65535 for all protocols	65535
Starting value for the destination port: 0 for all protocols	0
Ending value for the destination port: 65535 for all protocols	65535
Enter the mask to be applied to the Received-DS-byte	0

Information you need to create your VPN	Scenario answers
Enter the value to match against after the mask has been applied to the Receive-DS-byte:	0
Do you want to configure local and remote IDs for ISAKMP?	Yes
Select the identification type of the local ID to be sent to the remote IKE peer: – Local tunnel endpoint address – Fully qualified domain name – User fully qualified domain name – Key ID (any string)	Select local tunnel endpoint address with AS/400
Do you want to limit this profile to specific remote users?	No
Do you want to limit this profile to specific interfaces?	No

Table 88. IBM 2212 router configuration - Policy validity profile

Information you need to create your VPN	Scenario answers
Validity profile name:	Always
Enter the lifetime of this policy: – yyyymmddhhmmss – * denotes forever	*
During which months should this profile be valid? ALL to signify all year round	ALL
During which days should this profile be valid? ALL to signify all week	ALL
During which hours should this profile be valid? * denotes all day	*

Table 89. IBM 2212 router configuration - IPSec action profile

Information you need to create your VPN	Scenario answers
IPSec action profile name:	tun-30
Select the IPSec security action type: – Block – Permit	Permit
Should the traffic flow into a secure tunnel or in the clear? – Clear – Secure tunnel	Secure tunnel
What is the tunnel start-point IP address?	192.168.102.3
What is the tunnel end-point IP address?	192.168.100.150
Does this IPSec tunnel flow within another IPSec tunnel?	No
Percentage of SA lifesize or lifetime to use as the acceptable minimum? The default is 75%.	75%

Information you need to create your VPN	Scenario answers
Security association refresh threshold in percent: The default is 85%.	85%
Select the option for the DF bit in the outer header: – Copy – Set – Clear	Copy
Do you want to enable replay prevention?	No
Do you want to negotiate the security association at system initialization (autostart)?	No

Table 90. IBM 2212 IPSec proposal

Information you need to create your VPN	Scenario answers
What name do you want to give this IPSec proposal?	esp-prop3
Does this proposal require Diffie-Hellman Perfect Forward Secrecy?	No
Do you wish to enter any AH transforms for this proposal?	No
Do you wish to enter any ESP transforms for this proposal?	Yes

Table 91. IBM 2212 router configuration - IPSec ESP transform

Information your need to create your VPN	Scenario answers
IPSec ESP transform name:	esp-trans3
Select the protocol ID: – IPSec AH – IPSec ESP	IPSec ESP
Select the encapsulation mode: – Tunnel – Transport	Tunnel
Select the ESP authentication algorithm: – HMAC_MD5 – HMAC_SHA	HMAC_MD5
Select the ESP cipher algorithm: – ESP DES – ESP 3DEC – ESP CDMF – ESP NULL	ESP DES
What is the SA lifesize (in kilobytes)? The default is 50000 kilobytes.	50000
What is the SA lifetime? The default is 3600 sec.	3600

Table 92. IBM 2212 router configuration - ISAKMP action

Information you need to create your VPN	Scenario answers
ISAKMP action name:	ike-3
Select the ISAKMP exchange mode: – Main – Aggressive	Aggressive
Percentage of SA lifesize/lifetime to use as the acceptable minimum: The default is 75%.	75%
What is the ISAKMP connection lifesize, in kilobytes? The default is 5000 kilobytes.	5000
What is the ISAKMP connection lifetime in seconds? The default is 30000 sec.	30000
Do you want to negotiate the SA at system initialization (autostart)?	No

Table 93. IBM 2212 router configuration - ISAKMP proposal

Information you need to create your VPN	Scenario answers
ISAKMP proposal name:	ike-prop3
Select the authentication method: – Pre-shared key – Digital certificate	Pre-shared key
Select the hashing algorithm: – MD5 – SHA	MD5
Select the cipher algorithm: – DES – 3DES	DES
What is the SA lifesize, in kilobytes? Default is 1000 kilobytes	999999
What is the SA lifetime? Default is 15000 sec.	86400
Select the Diffie-Hellman Group ID: – Diffie-Hellman Group 1 – Diffie-Hellman Group 2	Diffie-Hellman Group 1
Do you wish to map a DiffServ Action to this policy?	No
What will be the status of the policy? – Enabled – Disabled	Enabled

15.2.2 Configuring the VPN in the 2212 Router: Configuration summary

This section summarizes the 2212 router VPN configuration for this scenario. For detailed information about the routers configuration, refer to *A Comprehensive*

The user represents the remote VPN partner which is the AS/400 system. For security reasons, when displaying the *user*, the associated pre-shared key is not displayed. Figure 768 on page 694 shows the *user* configuration in the 2212 router.

```
Branch *TALK 6

Branch Config>FEATURE Policy
IP Network Policy configuration
Branch Policy config>LIST USER BY-NAME
List of Users:
  num: User Info                               :Group Name
      1: 192.168.100.150                         :
Enter the number of user [1]? 1
Name      = 192.168.100.150
Type      = IPV4 Addr
Group     =
Auth Mode =Pre-Shared Key
```

Figure 768. Listing the user information in the 2212 router

2212 router console command List Policy Complete allows you to list a policy with all its related objects. The policy configuration summary is shown in Figure 769 on page 695.

```

Branch *TALK 5
Branch +FEATURE Policy
IP Network Policy console
Branch Policy console>LIST POLICY COMPLETE
1: (Enabled,Valid)      ike-pre-103-to-h100
Number of Policy to display (0 for All) [0]? 1
Policy name:                ike-pre-103-to-h100
Policy Loaded from:        Local Configuration
Policy state:              Enabled and Valid
Policy Priority:           5

Profile Name = 103-to-h100
sAddr:Mask= 192.168.103.0 : 255.255.255.0  sPort= 0 : 65535
dAddr      =192.168.100.150 : dPort= 0 : 65535
proto      = 0 : 255
TOS        = x00 : x00
Remote Grp=All Users

Validity Name = always
Duration = Forever
Months   = ALL
Days     = ALL
Hours    = All Day

IPSECAction Name = tun-30
Tunnel Start:End      = 192.168.102.3 : 192.168.100.150
Tunnel In Tunnel      = No
Min Percent of SA Life = 75
Refresh Threshold     = 85%
Autostart             = No
DF Bit                = COPY
Replay Prevention     = Disabled
IPSEC Proposals:
-----
1:Name = esp-prop3
Pfs = N
ESP Transforms:
-----
1:Name = esp-trans3
Mode      = Tunnel
LifeSize  = 50000
LifeTime  = 3600
Authent   = MD5          Encr =DES

ISAKMP Name = ike-3
Mode      = Main
Min Percent of SA Life = 75
Conn LifeSize:LifeTime = 5000 : 30000
Autostart = No
ISAKMP Proposals:
-----
1:Name = ike-prop3
AuthMethod = Pre-Shared Key
LifeSize   = 999999
LifeTime   = 86400
DHGroupID  = 1
Hash Algo  = MD5
Encr Algo  = DES CBC

```

Figure 769. Listing the policy information in the 2212 router configuration

Based on information entered when creating a policy, the necessary filtering rules are generated implicitly. Figure 770 shows the filters rules generated in the 2212 router in this scenario.

```
Branch Policy console>LIST POLICY GENERATED
1: (Enabled,Valid)      ike-pre-103-to-h100
Number of Policy to display [0]? 1
Rules generated for policy ike-pre-103-to-h100:
Rule 1.  ike-pre-103-to-h100.p2in
Rule 2.  ike-pre-103-to-h100.p1in
Rule 3.  ike-pre-103-to-h100.p1out
Rule 4.  ike-pre-103-to-h100.traffic
Rule 5.  ike-pre-103-to-h100.inBoundTunnel
```

Figure 770. Listing the filter rules in the 2212 router configuration

Rule 1. Phase 2 inbound (p2in)

This rule allows incoming phase 2 negotiation traffic. This traffic is the result of the remote VPN partner initiating a phase 2 negotiation or a phase 2 refresh. The source and destination IP addresses are the tunnel endpoints. The source and destination port is 500. The protocol is UDP.

Rule 2. Phase 1 inbound (p1in)

This rule allows incoming phase 1 negotiation traffic. The source and destination IP addresses are the tunnel endpoints. The source and destination port is 500. The protocol is UDP.

Rule 3. Phase 1 outbound (p1out)

This rule allows outgoing phase 1 negotiation traffic. The source and destination IP addresses are the tunnel endpoints. The source and destination port is 500. The protocol is UDP.

Rule 4. Traffic into the secure tunnel (traffic)

This rule causes the outbound traffic, based on the source and destination IP address, to be channeled through the VPN and processed by IPSec.

Rule 5. Traffic from the secure tunnel (inbBoundTunnel)

15.3 AS/400 host-to-gateway VPN configuration

The following sections explain how to configure the host-to-gateway connection on the AS/400 system RALYAS4A to establish a VPN with the 2212 router in this scenario.

15.3.1 Completing the planning worksheets for the AS/400 system

Complete the AS/400 system planning worksheets as shown in Table 94 on page 697 and Table 95 on page 697. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 94. RALYAS4A New Connection Wizard planning worksheet

This is the information needed to create VPN with the New Connection Wizard	Scenario answers
What is the type of connection to be created? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Host – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Gateway
What is the name of the connection group?	HtoG4AtoR
What type of security and system performance is required to protect the keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How is the local VPN server identified?	IP address
What is the IP address of the local VPN server?	192.168.100.150
How is the remote VPN server identified?	IP address
What is the IP address of the remote VPN server?	192.168.102.3
What is the pre-shared key?	123456
What type of security and system performance is required to protect the data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

Table 95 shows the information you need to configure IP filters to complete the VPN implementation.

Table 95. Planning worksheets - IP filter rules RALYAS4A

This is the information needed to create the IP filters to support the VPN connection	Scenario answers
Is the local VPN server acting as a <i>host</i> or <i>gateway</i> ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, the VPN server acts as a host. If no, the VPN server acts as a gateway.	Host
Is the remote VPN server acting as a <i>host</i> or <i>gateway</i> ?	Gateway
What is the name used to group together the set of filters that will be created?	VPNIFC
If the local VPN server is acting as a gateway... – What is the IP address of the local ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	Not applicable

This is the information needed to create the IP filters to support the VPN connection	Scenario answers
If the remote VPN server is acting as a gateway... <ul style="list-style-type: none"> – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>destination address</i> on the IPSEC filter. 	192.168.103.0 255.255.255.0 RTRsubnets
What is the IP address of the local VPN server? <ul style="list-style-type: none"> – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host. 	192.168.100.150
What is the IP address of the remote VPN server? <ul style="list-style-type: none"> – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host. 	192.168.102.3
What is the name of the interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TOKENRING2
What other IP addresses, protocols, and ports are permitted on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> ! Add filter rules to permit internal traffic. Internal traffic IP address and mask If the Internal traffic IP address and mask value is a subnet, use the defined address name.	192.168.100.0 255.255.255.0 DataCtr
Protocols and ports permitted	All

The filter rules allow IPSec traffic between the local AS/400 system and any 192.168.103.* address on the remote network. To configure the filter rules, the remote subnet (192.168.102.0 with mask 255.255.255.0) must have a name assigned to it (RTRsubnets in this example). This name is used in the Defined Address definition in the filter configuration.

The internal data center traffic is allowed in the clear over the TOKENRING2 line. The Define Address DataCtr defines the internal subnet.

VPNIFC is the filter set name that groups all the related rules together and is applied to a physical interface. The interface is TOKENRING2. This is the Token-Ring line description.

15.3.2 Configuring a host-to-gateway VPN on RALYAS4A

Perform the following steps to configure a host-to-gateway VPN on RALYAS4A:

1. Start Operations Navigator from the desktop.
2. Expand the AS/400 system (in this case, **RALYAS4A**). Sign on when prompted.
3. Expand **Network** (Figure 771 on page 699).

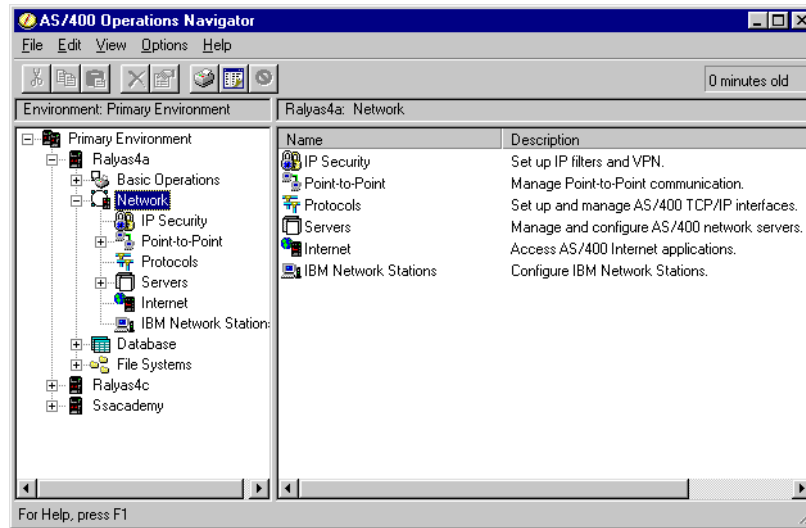


Figure 771. IP security

- Double-click **IP Security** to reveal two server names in the right window: IP Packet Security and Virtual Private Networking. Although both functions must be configured, start with Virtual Private Networking.

Note

At this stage, Virtual Private Networking may already have a status of *Started* since the default is for the server to automatically start when TCP/IP starts. The server can be either started or stopped during the following steps.

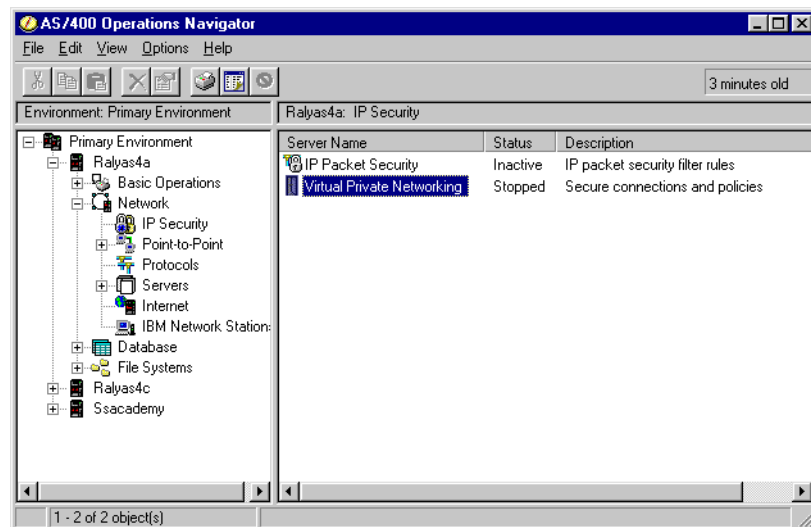


Figure 772. Operations Navigator: Virtual Private Networking

- Double-click **Virtual Private Networking** to start the Virtual Private Networking GUI (Figure 772). The window shown in Figure 773 on page 700 appears.

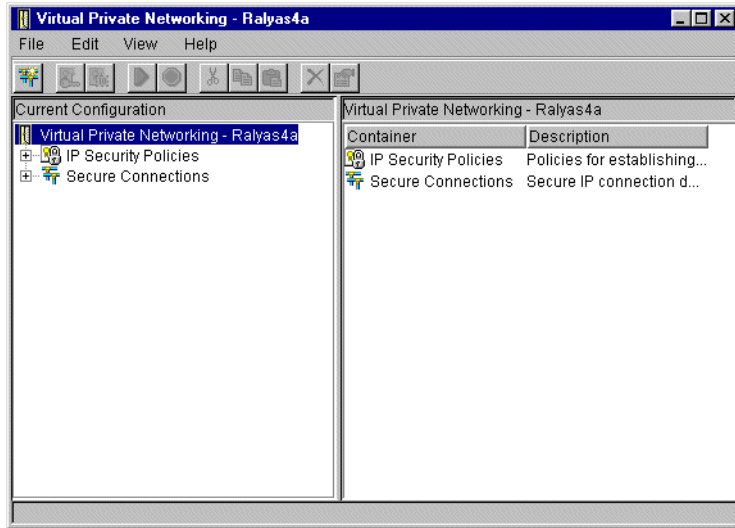


Figure 773. Virtual Private Networking GUI configuration interface

6. Select **File** from the menu bar, and then select **New Connection**.

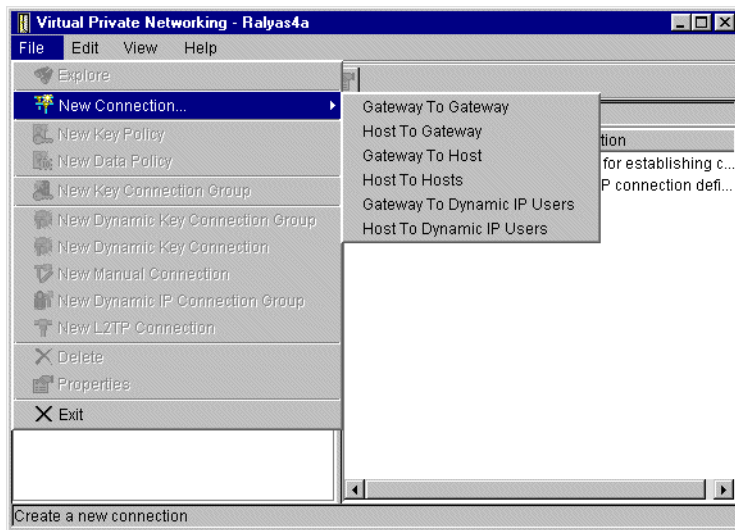


Figure 774. New Connection -> Gateway to Gateway

7. Select **Host To Gateway** from the drop down list (Figure 774). This starts the New Connection Wizard for a host-to-gateway connection (Figure 775 on page 701).

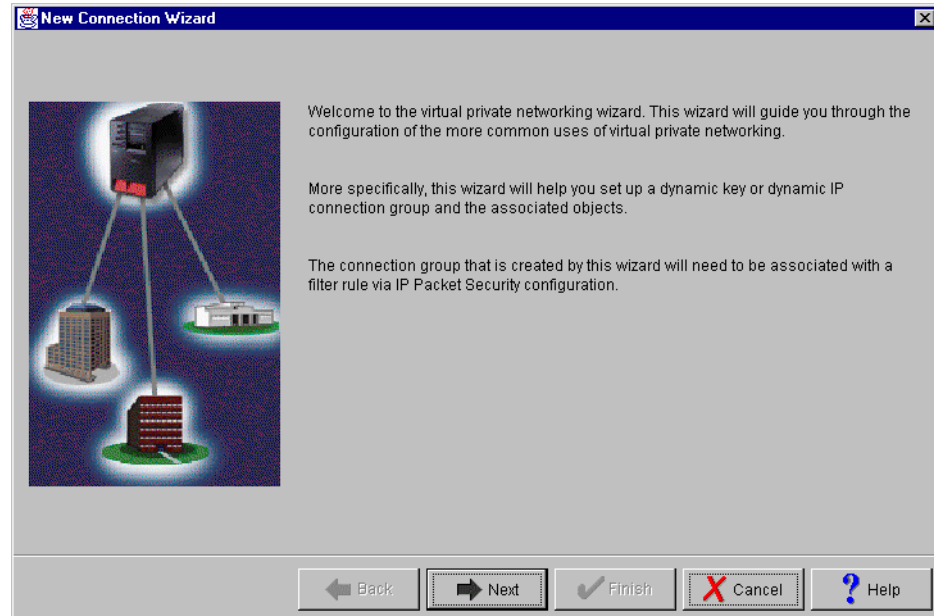


Figure 775. New Connection Wizard welcome window

8. Click **Next** after reading the Welcome window.
9. Enter the name, `HtoG4AtoR`, for the connection group. Recall that `HtoG4AtoR` is the name from the worksheet in Table 94 on page 697. The name specified here is the name for all objects that the wizard creates for this particular connection. It is case sensitive. Enter a description for this configuration (Figure 776).

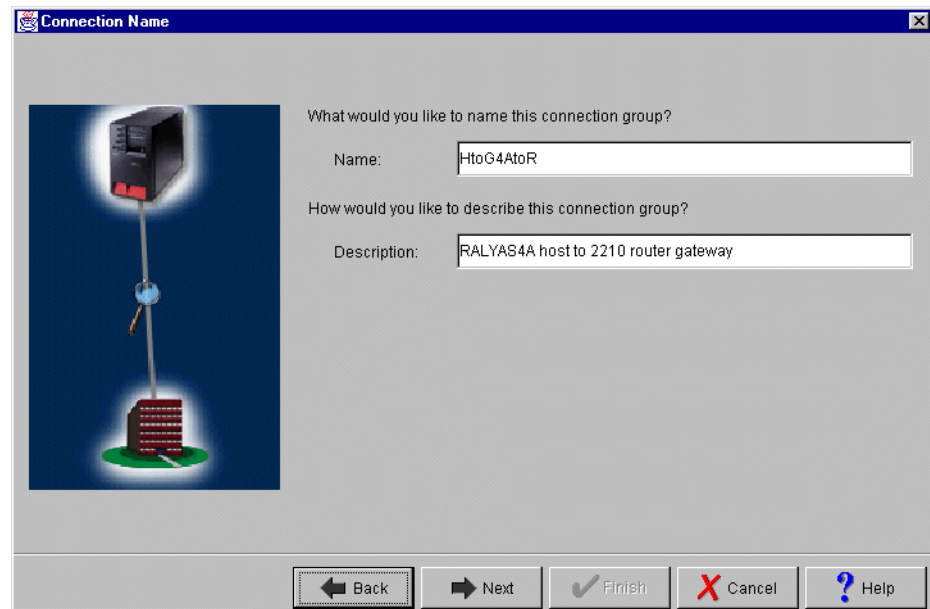


Figure 776. Connection Name window

10. Click **Next**.
11. In the Key policy window (Figure 777 on page 702), specify the level of authentication or encryption protection IKE uses during phase 1 negotiations.

Phase 1 establishes the keys that protect the messages that flow during subsequent phase 2 negotiations. Phase 2 protects the data itself. For the purposes of this example, select **Balance security and performance** as specified on the worksheets. The wizard chooses the appropriate encryption and authentication algorithms based on the selection made here.

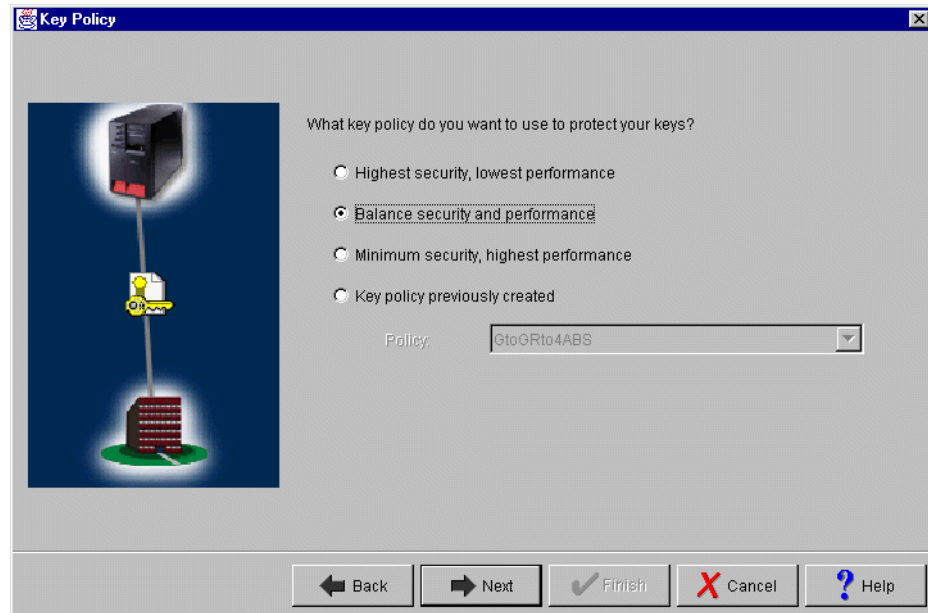


Figure 777. Key Policy window

12. Click **Next** when complete.
13. On the Local Identifier window, specify the identity of the local key server. In other words, specify the local AS/400 that acts as the VPN gateway, which, in this case, is RALYAS4A. Leave Identifier type as the default value, **Version 4 IP address**. For the IP Address parameter, use the pull-down menu to select the IP address of the interface that is connecting to the remote gateway 2212 router. Refer back to the planning worksheets and to the network configuration in Figure 778 on page 703. For RALYAS4A, this is **192.168.100.150**.

Note: Figure 778 shows various IP addresses, including 9.24.104.21, 9.24.106.18, and so on, that we do not reference anywhere in this scenario. These interfaces are configured on RALYAS4A, but they are used for other scenarios and projects and should be ignored here.

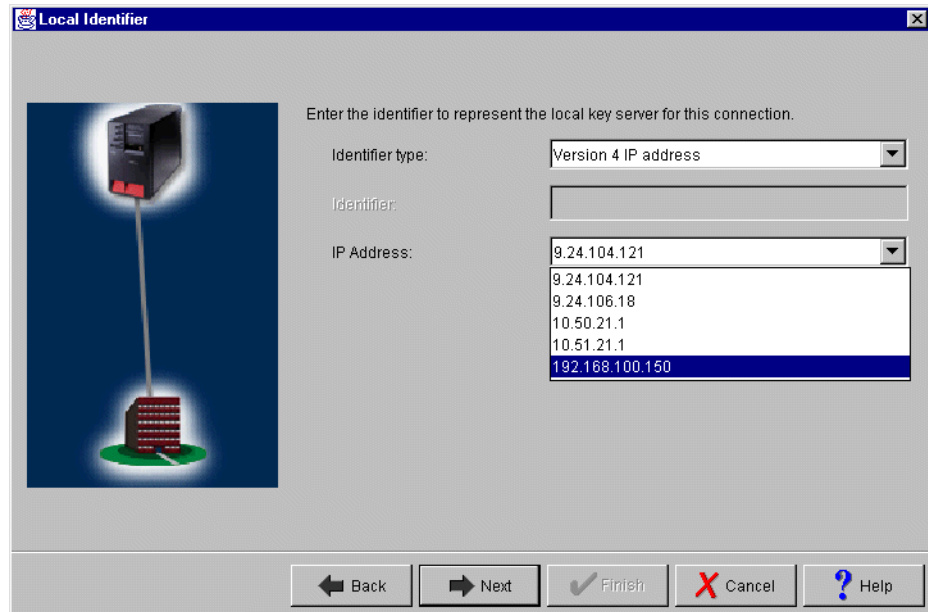


Figure 778. Local identifier window pull down

14. Click **Next**.

15. Use the Remote key server identifier window (Figure 779) to enter details about the remote key server, as well as the pre-shared key. The pre-shared key is the shared "secret" that IKE uses to generate the actual keys for phase 1. The remote key server is the 2212 router with IP address 192.168.102.3. Specify 123456 in the Pre-shared key parameter. Remember, the same pre-shared key must be entered when configuring the VPN on the remote 2212 router.

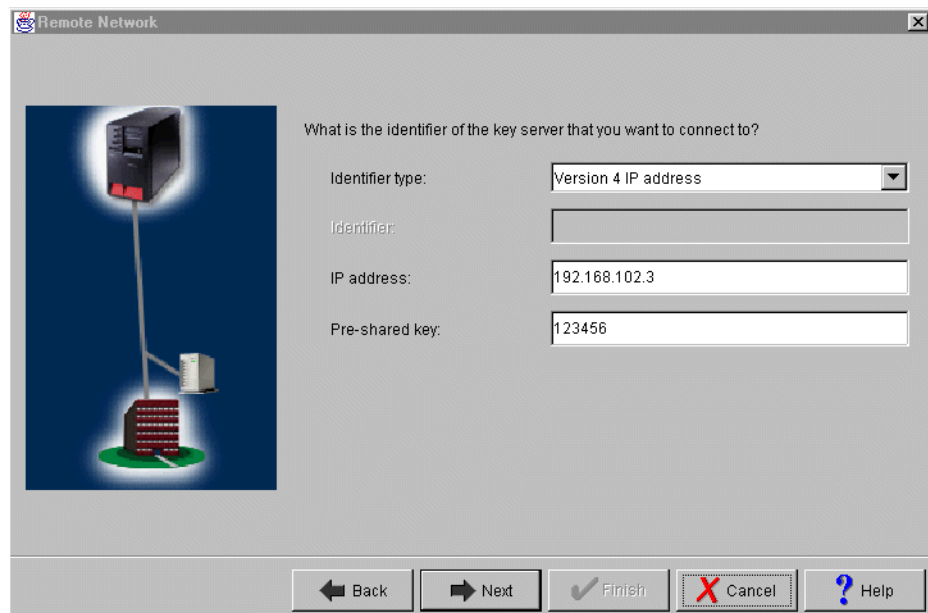


Figure 779. Remote key server identifier window

16. Click **Next**.

17. Use the Data policy window to specify the level of authentication or encryption that IKE uses to protect data flowing through the host-to-gateway tunnel during phase 2 negotiations. For this example, select **Balance security and performance** (Figure 780) as specified on the worksheets.

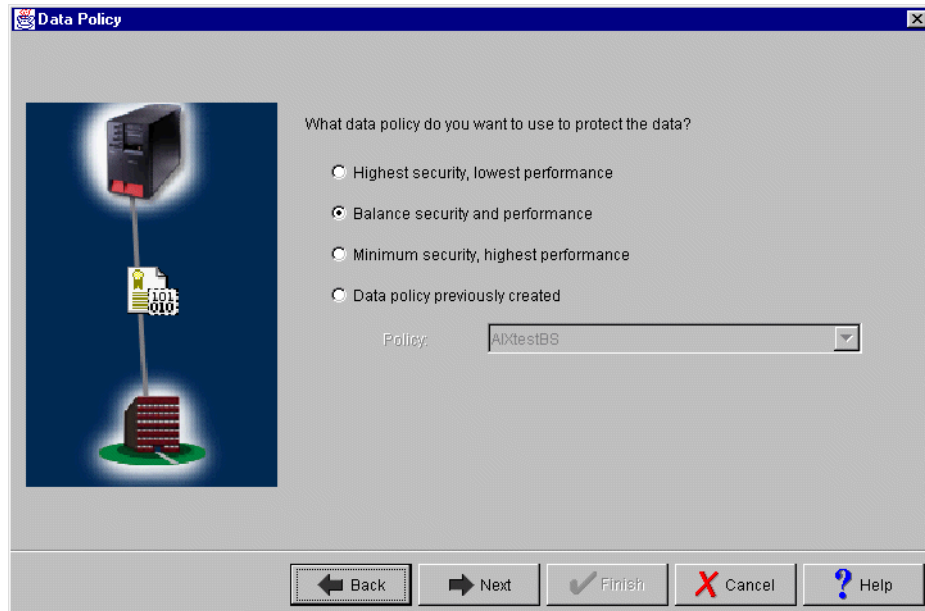


Figure 780. Data policy window

18. Click **Next**.

19. The final window (Figure 781) summarizes the configuration values entered. Scroll down to see a list of the configuration objects that the wizard creates when you click Finish. Check the configuration values against the worksheets. If changes need to be made, click **Back**.

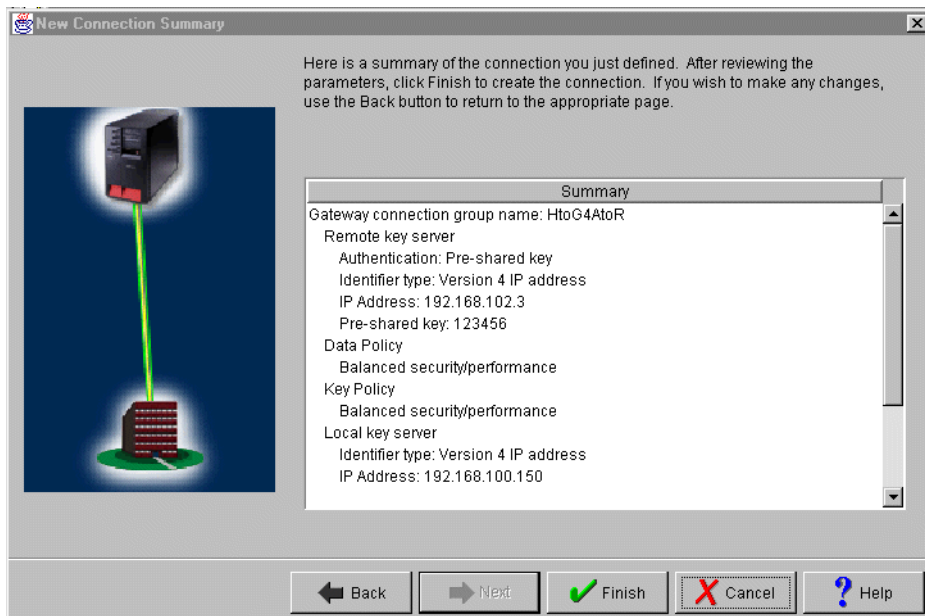


Figure 781. New Connection Summary window RALYAS4A

20. When you are satisfied with the values, click **Finish**.

The wizard creates the various objects that were configured for this VPN connection. After a short delay (and assuming there are no errors), the initial Virtual Private Networking GUI Configuration window is shown (Figure 782).

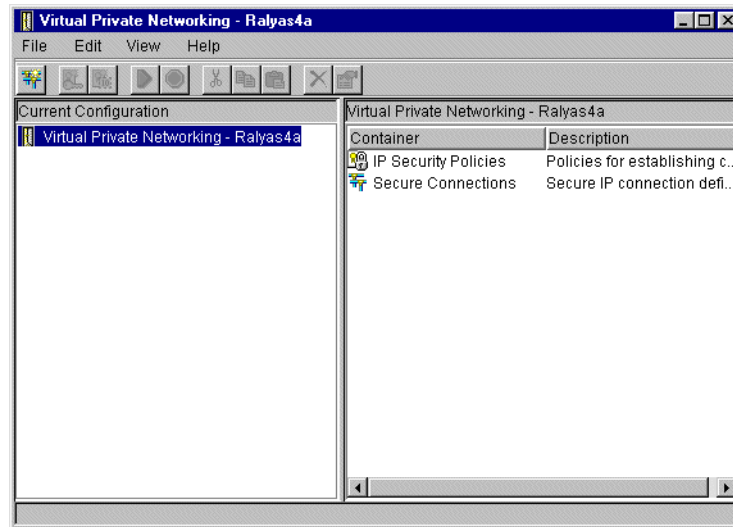


Figure 782. VPN GUI configuration interface

15.3.3 Matching the 2212 router VPN configuration

In this example scenario, use the Virtual Private Networking Configuration GUI to customize the key refresh policies for:

- Key protection
- Data protection

The key refresh policies on the AS/400 system must be consistent with the policy of the router. The Virtual Private Networking New Connection Wizard does not provide the option to allow you to customize the key refresh policies. Refer to 3.6.7, “Key policy (IKE phase 1) and data policy (IKE phase 2) lifetime and size limits” on page 65, for information on how the AS/400 system negotiates key life values.

You can change the VPN GUI default values before the wizard configuration as explained in 3.7.6, “Changing the Virtual Private Networking GUI default values” on page 76. Or, you can customize the appropriate parameters later as shown in the following steps.

To customize the key refresh policies, follow these steps:

1. Expand all the subfolders on the VPN Configuration GUI (Figure 783 on page 706).

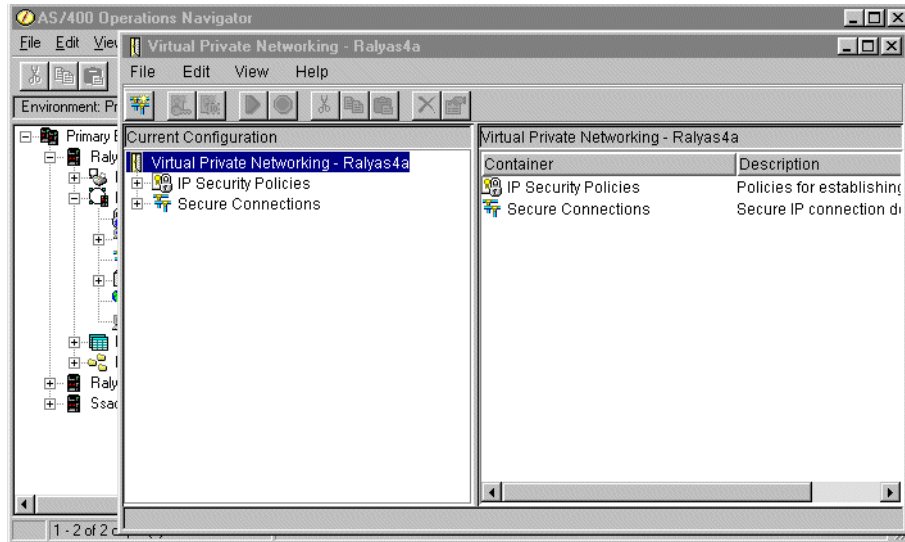


Figure 783. VPN configuration GUI

2. Click **Key Policies** to display a list of key policies configured on your system (Figure 784). The key policy name is the connection group name that you entered on the VPN configuration wizard, followed by a two-letter suffix. In this example, the suffix is *BS* because *Balanced security and performance* was selected for the key policy. When *Highest security, lowest performance* is selected for the key policy, the suffix is *HS*. Similarly, when *Minimum security, highest performance* is selected, the suffix is *HP*. This is the naming convention that the wizard follows.
3. Double-click **HtoG4AtoR** to view the key policy for this connection (Figure 784).

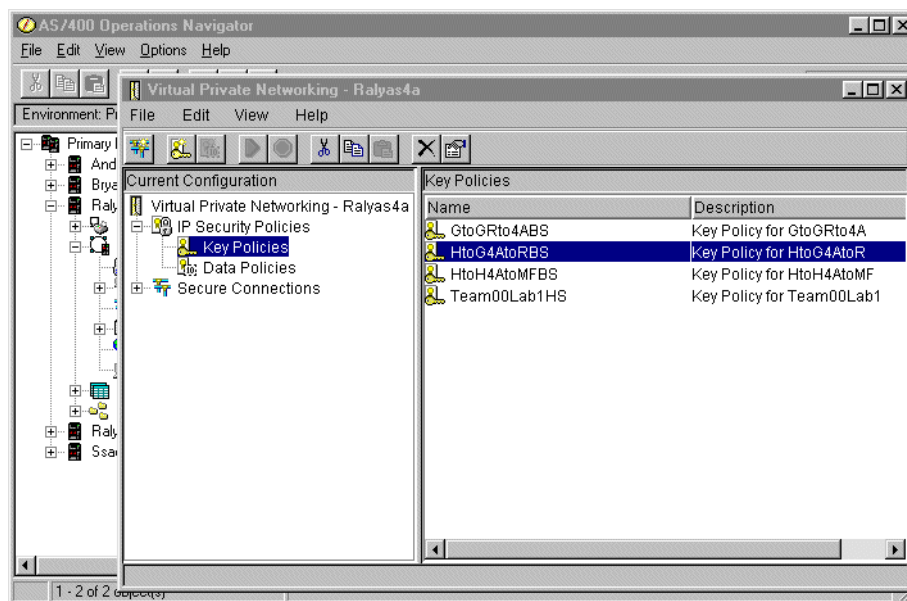


Figure 784. VPN Key Policies

4. At the key policy Properties window, select the **Transforms** tab. Select the key protection transform, and click **Edit** (Figure 785 on page 707).

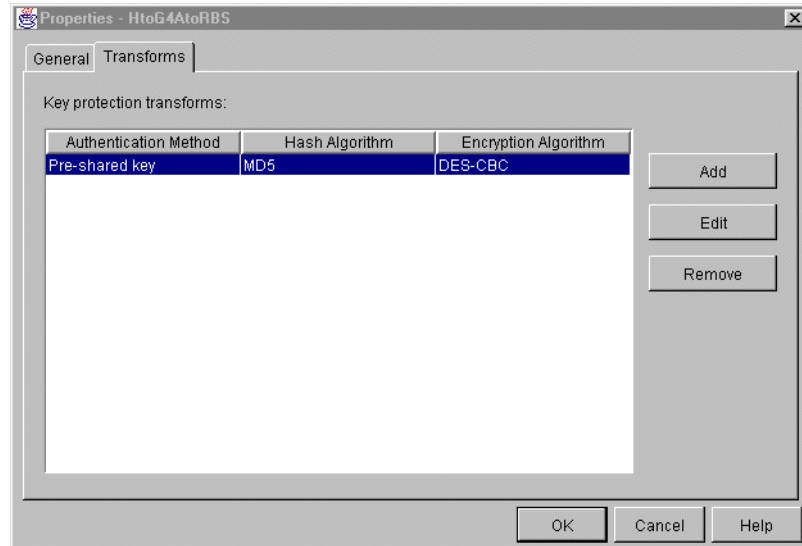


Figure 785. Key protection transforms

- Set the Maximum key lifetime parameter value to 1440. You must define a Maximum size limit value since it is required by the router configuration. Otherwise, there will be no match (Figure 786).

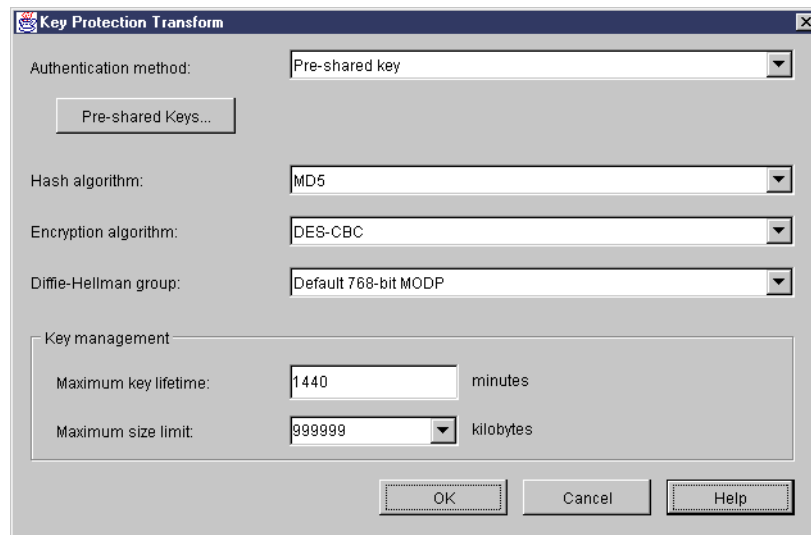


Figure 786. Key Protection Transform window

- Click **OK**.
- Back at the key protection transforms (Figure 785), click **OK**.
- Click **Data Policies** to display a list of data policies.
- Double-click **HtoGRto4ABS** to view the data policy for this connection (Figure 787 on page 708).

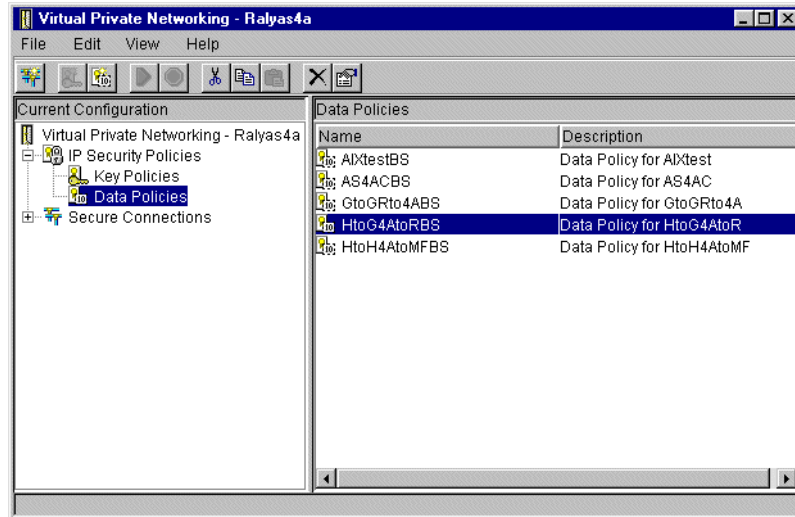


Figure 787. VPN Data Policies

- At the data policy Properties window, select the **Proposals** tab (Figure 788). Select the data protection proposal that you want to change, and click **Edit**.

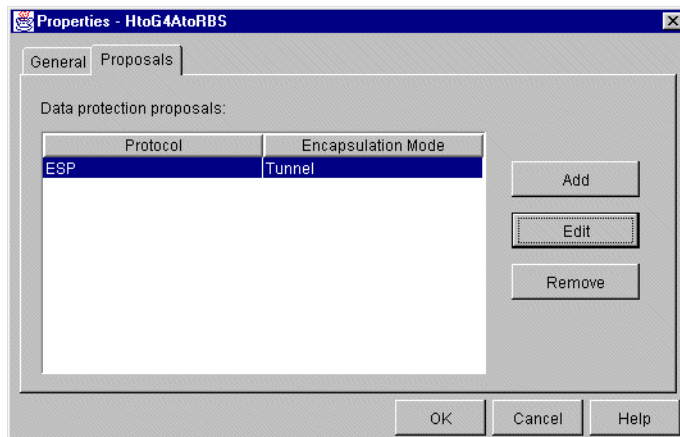


Figure 788. Data policy properties window

- At the Data Protection Proposal window, select the **Key Expiration** tab (Figure 789 on page 709). Set the Expire after parameter value to 60 and change the Expire at size limit parameter value to 50000.

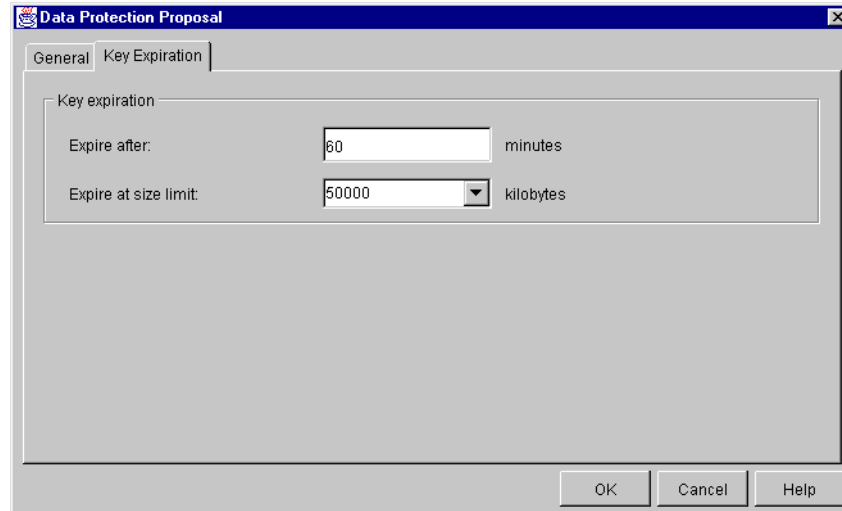


Figure 789. Data Protection Proposal window

12. Click **OK**.

13. Back at the data policy properties window (Figure 788), click **OK**.

You have now completed the VPN configuration for RALYAS4A. You configure AS/400 IP filtering in the next task.

15.3.4 Configuring IP filtering on the AS/400 system (RALYAS4A)

The Virtual Private Networking New Connection wizard does *not* configure IP filters. You must configure filter rules to allow IKE negotiation traffic. You must also configure a filter rule with action IPsec and associate it with the connection group created by the wizard. Use IP Packet Security in Operations Navigator to configure filters. Follow these steps:

1. Configure a defined address to allow the general traffic from the internal data center network to flow in the clear. The AS/400 system RALYAS4A is connected to the internal network and to the firewall that connects it to the Internet, over the same physical interface (TOKENRING2). Enabling the filters required by the VPN configuration stops all the internal traffic, unless you explicitly permit it. In our example, the address name is DataCtr with subnet 192.168.100.0 and subnet mask 255.255.255.0. See Figure 790 on page 710.

Tip

The type TRUSTED is not used in the defined address filter rule. It is used for audits or verifications when the address statement is used in a NAT rule.

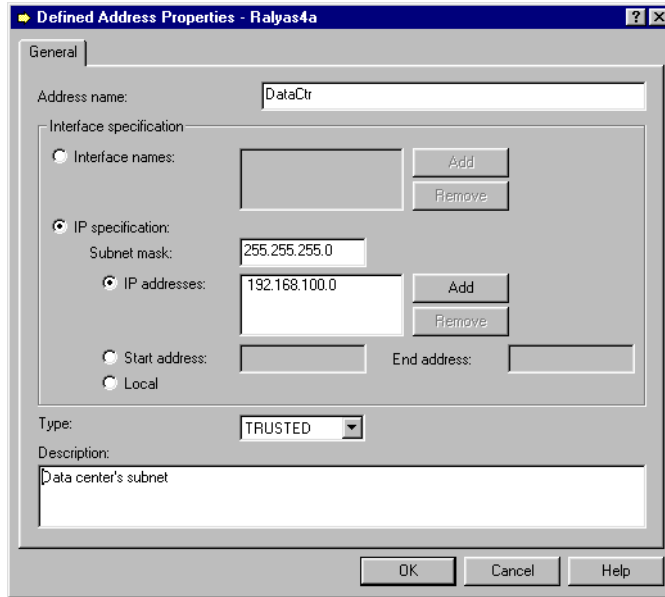


Figure 790. Defining the trusted subnet for the internal network

2. Configure a filter rule with action PERMIT to allow general traffic with source and destination IP address in the trusted subnet (DataCtr in our example). Notice that the direction field is has a wildcard (*) to indicate both inbound and outbound. See Figure 791.

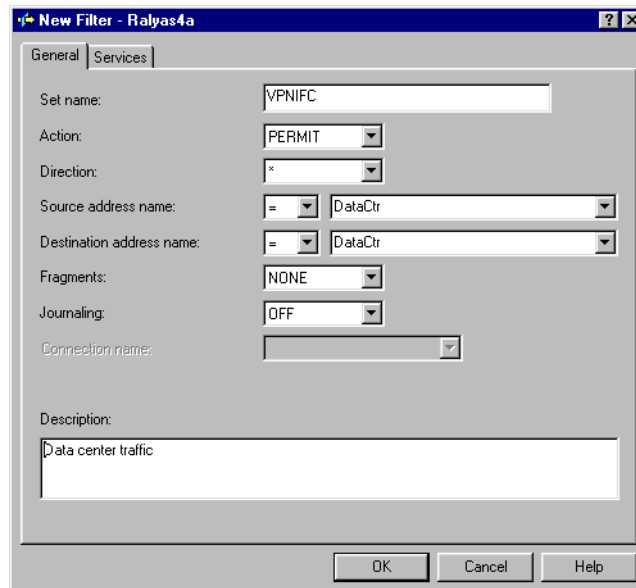


Figure 791. Filter rule to permit general traffic in the internal network

Tip

A more restricted way to represent this filter rule is to configure two rules:

- Inbound filter rule with a destination of RALYAS4A (192.168.100.150) and a source DataCtr defined address.
- Outbound filter rule with a source of RALYAS4A and a destination DataCtr defined address.

3. Click the **Services** tab to configure the services allowed by this filter rule. All traffic is allowed in the internal network. Therefore, enter a wildcard (*) in the Protocol, Source port, and Destination port fields (Figure 792).

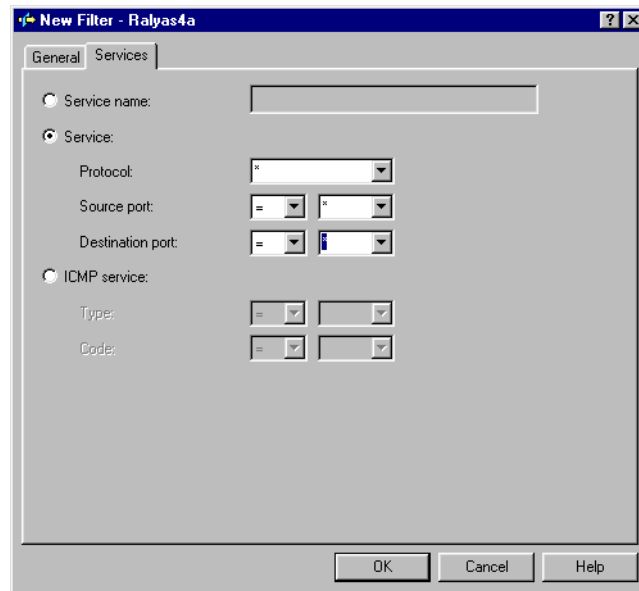


Figure 792. Configuring services in the internal network

4. Configure a defined address for the subnet behind the remote VPN gateway that is allowed to use the VPN tunnel (Figure 793 on page 712). In our example, the address name is `RTRsubnets`, with subnet `192.168.103.0` and subnet mask `255.255.255.0`. In this host-to-gateway scenario, the remote network at the branch office is part of the same organization as the data center and has full access to the local AS/400 system and its applications.

Tip

The type UNTRUSTED is not used in the defined address filter rule. It is used for audits or verifications when the address statement is used in a NAT rule.

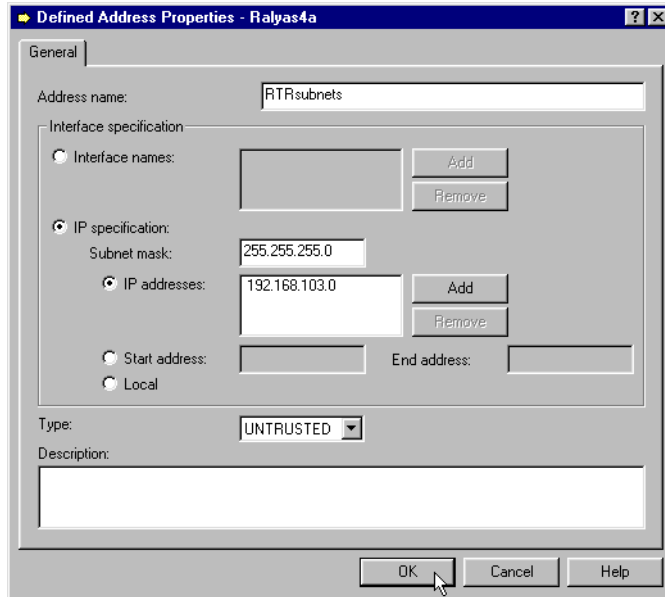


Figure 793. Defined addresses RTRsubnets

5. Create two filter rules to allow IKE traffic to flow into and out of the AS/400 system. All associated filter rules (for example, all rules for one interface) in the filter file should have the same *Set name*. In this example, we use `VPNIFC` as the Set Name.
 - a. For the first filter rule, specify `VPNIFC` for the Set Name parameter. Select **PERMIT** for the Action parameter and **OUTBOUND** for the Direction parameter. The local AS/400 system address, `192.168.100.150`, is the value in the Source address name field, and the remote 2212 router address is `192.168.101.2` in the Destination address name field.
 On the **Services** page, select **Service** and **UDP** for the Protocol parameter. Specify `500` for the Source port and Destination port parameters (Figure 794 and Figure 795 on page 713).

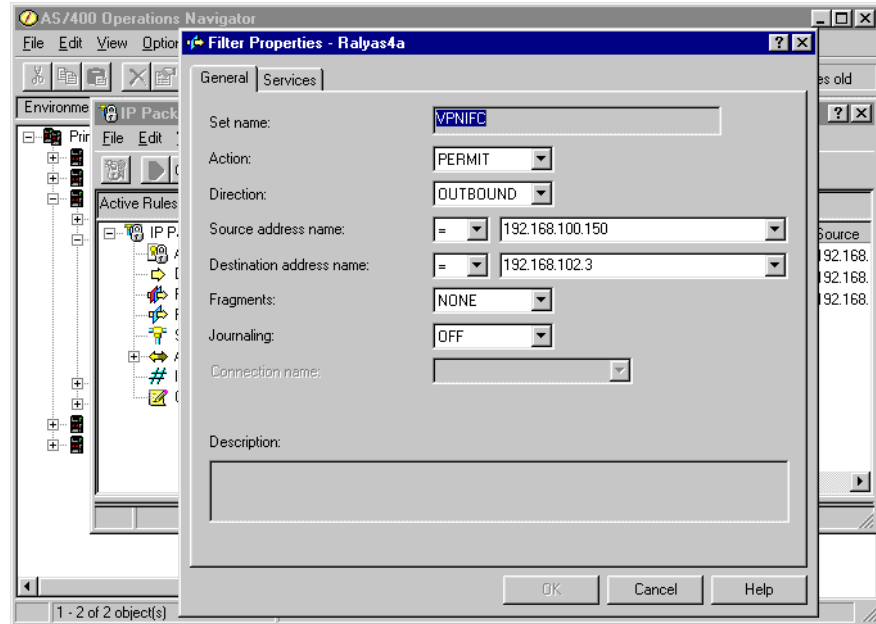


Figure 794. Outbound IKE filter rule

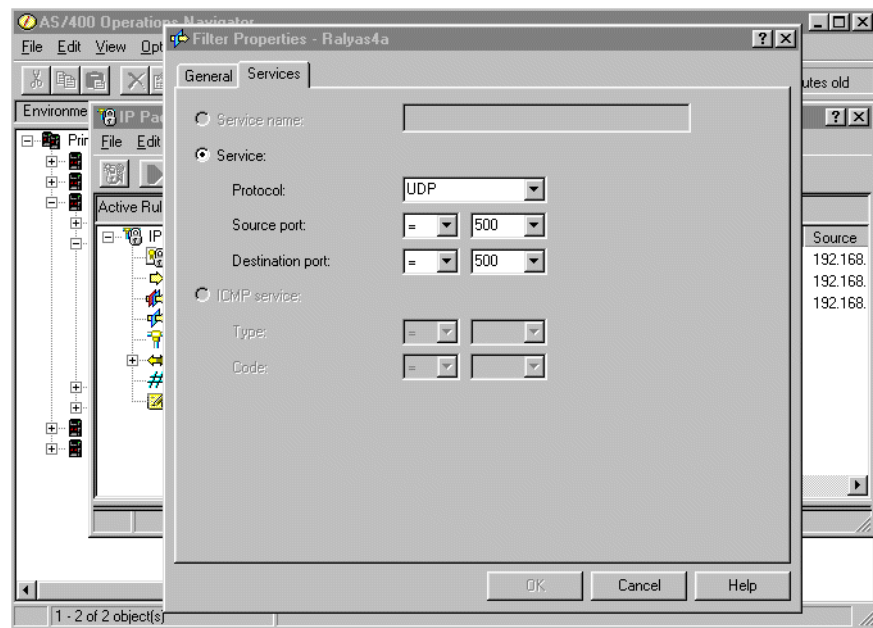


Figure 795. IKE filter rule services

- b. For the second filter rule, specify `VPNIFC` for the Set Name parameter. Select **PERMIT** for the Action parameter and **INBOUND** for the Direction parameter. The remote 2212 router address, `192.168.101.2`, is the value in the Source address name field, and the local AS/400 system address is `192.168.100.150` in the Destination address name field.

On the **Services** page, select **Service** and **UDP** for the Protocol parameter. Specify `500` for the Source port and Destination port parameters. See Figure 796 and Figure 797 on page 714.

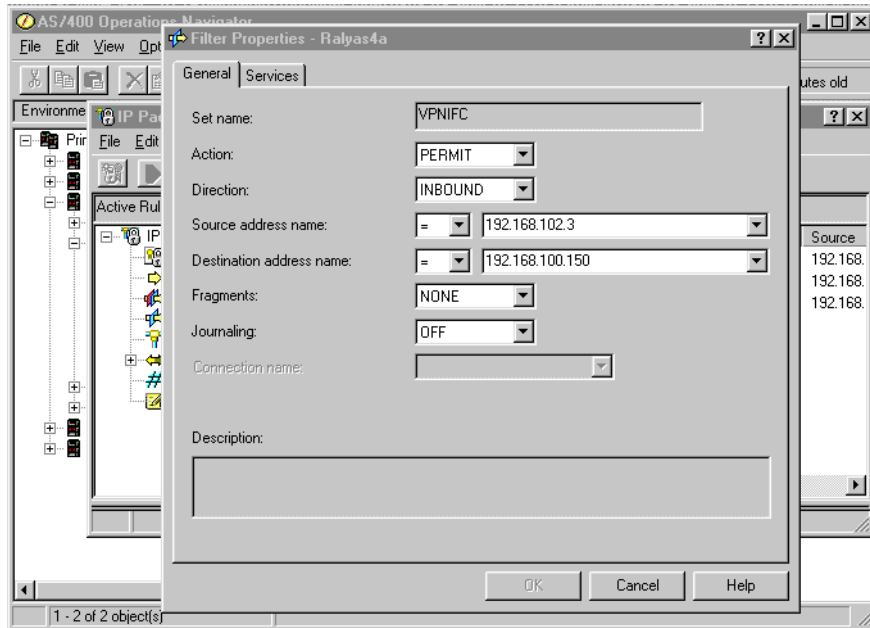


Figure 796. Inbound IKE filter rule

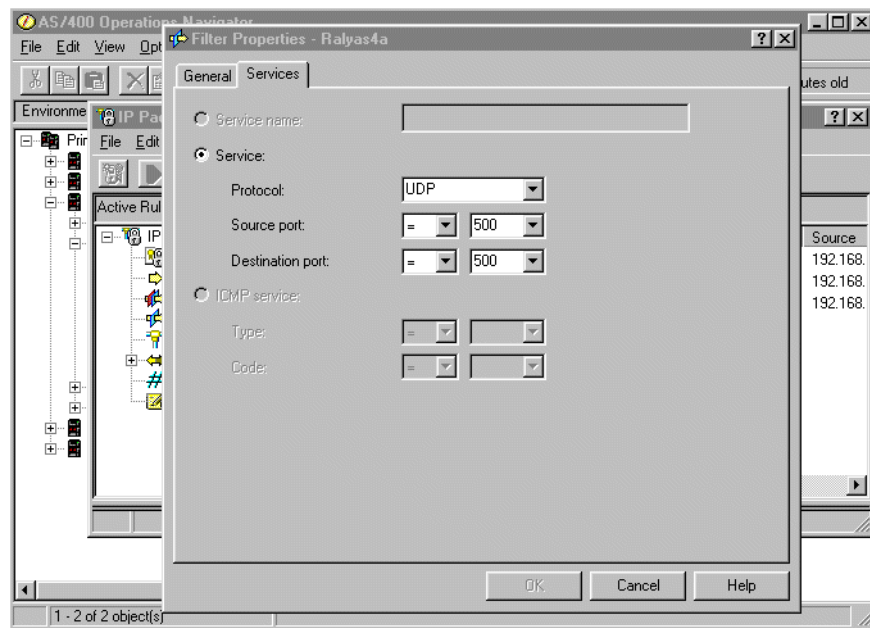


Figure 797. IKE filter rule services

6. Create a filter rule by setting Action to **IPSEC** to define the data endpoints that use the secure tunnel.

Use the same filter, set the name `VPNIFC`. The action is `IPSec`. Direction is always set to `OUTBOUND` and grayed out. The corresponding `INBOUND` `IPSEC` rule is created implicitly. Specify `192.168.100.150` for the Source address name parameter. Set the Destination address name to **RTRsubnets**, which is the defined address name that you created earlier. The Connection name is the name of the dynamic key connection that you created in 15.3.2, “Configuring a host-to-gateway VPN on RALYAS4A” on page 698. Use the

pull-down menu to list all the connections configured in your system and select one of them. In this scenario, select **HtoG4AtoR** (Figure 798).

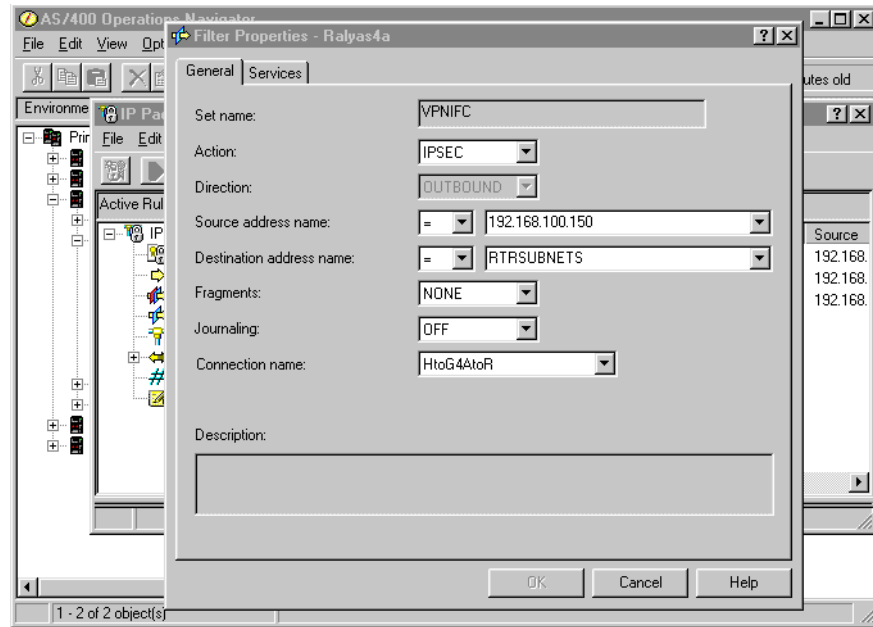


Figure 798. IPSEC filter rule

7. Click the **Services** tab to specify the protocols and ports allowed in the tunnel. In this scenario, select wildcard (*) for the Protocol, Source port, and Destination port fields. This allows any protocol using any port through the secure tunnel. See Figure 799.

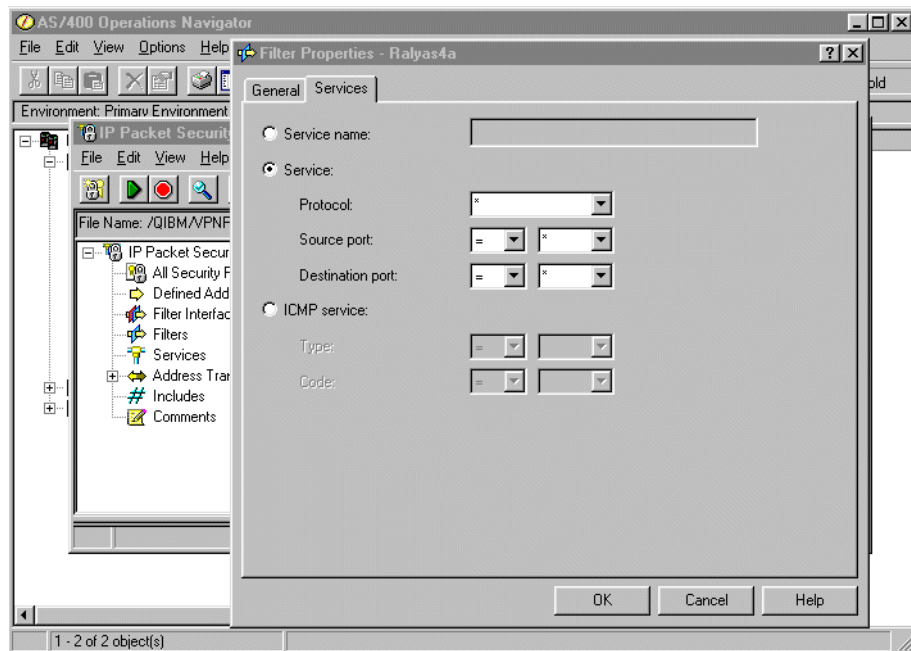


Figure 799. IPSEC filter rule service

Tip

Always configure the IPSEC filter rules below all the filter rules that permit IKE negotiations in the filter rules file.

8. Create a filter interface to tie the filter rules grouped by the VPNIFC set to the appropriate interface. The line description that connects the AS/400 system to the remote 2212 router VPN gateway is TOKENRING2. Associate the VPNIFC set to the TOKENRING2 line as shown in Figure 800.

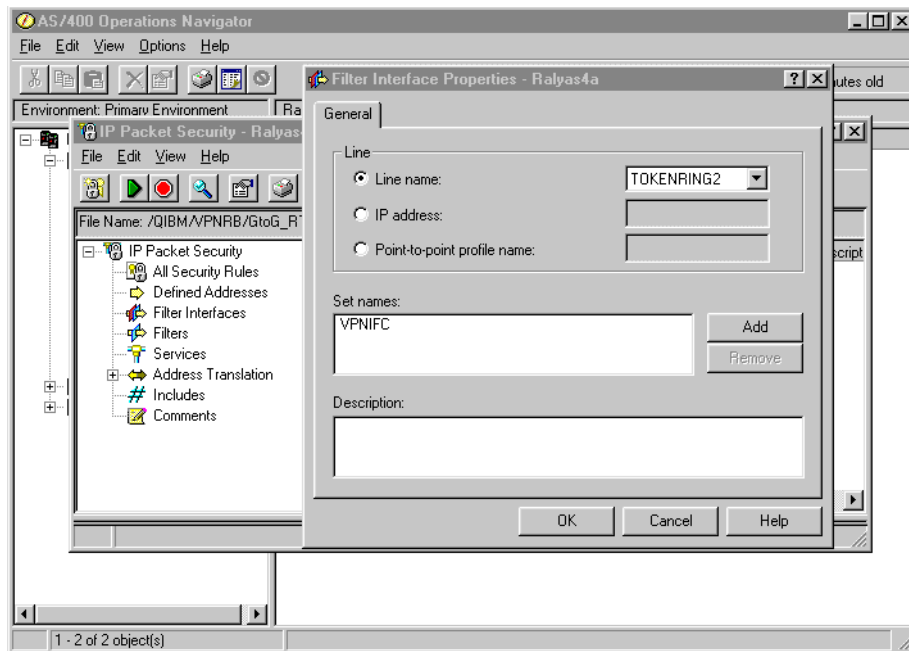


Figure 800. Filter Interface Properties window

9. Save the filter file in the IFS. In this scenario, create a subdirectory, VPNRB, under the directory QIBM. Save the filter file in /QIBM/VPNRB/HtoG_AStoRTR.i3p.

Figure 801 shows a summary of the filter rules configured in this scenario.

```
IP Packet Security: Filters
ADDRESS DataCtr IP = 192.168.100.0 MASK = 255.255.255.0 TYPE = TRUSTED
ADDRESS RTRsubnets IP = 192.168.103.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = * SRCADDR = DataCtr DSTADDR = DataCtr
PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 192.168.100.150
DSTADDR = 192.168.102.3 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 192.168.102.3
DSTADDR = 192.168.100.150 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
FRAGMENTS = NONE JRN = OFF
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 192.168.100.150
DSTADDR = RTRsubnets PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = HtoG4AtoR
FILTER_INTERFACE LINE = TOKENRING2 SET = VPNIFC
```

Figure 801. RALYAS4A - Filter rules summary

15.4 VPN configuration cross-reference table: AS/400 to 2212 router

Table 96 summarizes the AS/400 system and 2212 router configuration and provides a cross-reference list.

Table 96. AS/400 and 2212 router VPN configuration cross-reference table

AS/400	ROUTER
Key Policy	ISAKMP-Action
Name = HtoG4AtoRBS	Mode = Aggressive
Initiator Negotiation = Aggressive Mode (1)	Autostart = N (1)(2)
Responder Negotiation = Aggressive Mode only (2)	
Key Protection Transforms	ISAKMP-Proposal
Authentication Method = Pre-shared key (3)	AuthMethod = Pre-shared key
Pre-shared key value = 123456 (4)	LifeSize = 999999 (9)
Hash Algorithm = MD5 (5)	LifeTime = 86400 (8)
Encryption Algorithm = DES-CBC (6)	DHGroupID = 1 (7)
Diffie-Hellman Group = Default 768-bit MODP (7)	Hash Algorithm = MD5 (5)
Key Management	Encryption Algorithm = DES (6)
Maximum key lifetime (minutes) = 1440 (8)	
Maximum size limit (kilobytes) = 999999 (9)	IPSEC Action
	Tunnel Start = 192.168.102.3 (18)
Data Policy	Tunnel End = 192.168.100.150 (20)
Name = HtoG4AtoRBS	Tunnel-in-Tunnel = N
Use Diffie-Hellman Perfect Forward Secrecy = No (10)	Autostart = N
Diffie-Hellman Group = Not Applicable	Replay Prevention = N (29)
Data Protection Proposals	IPSEC Proposal
Encapsulation mode = Tunnel (11)	Diffie-Hellman Perfect Forward Secrecy = N
Protocol = ESP (12)	
Algorithms	IPSEC Transform
Authentication Algorithm = (13)	Type = IPSecESP
HMAC-MD5	Mode = Tunnel (11)
Encryption Algorithm = DES-CBC (14)	LifeSize = 50000
Key Expiration	LifeTime = 3600 (16)
Expire after (minutes) = 60 (15)	Authentication Algorithm = HMAC-MD5 (13)
Expire at size limit (kilobytes) = 50000 (16)	Cipher Algorithm = ESP DES (14)
Key Connection Group	Validity Period
Name = HtoG4AtoR	Life Time = Always
Remote Key Server	User
Identifier Type = Version 4 IP address (17)	Name = 192.168.100.150
IP address = 192.168.102.3 (18)	Type = IPv4 address
Local Key Server	Authentication Mode = Pre-shared key (19)
Identifier Type = Version 4 IP address (19)	Key Mode = ASCII (3)
IP address = 192.168.100.150 (20)	Pre-shared key = 123456
Key Policy = HtoG4AtoRBS (4)	Policy Profile
	Source Address Format = NetMask
Dynamic Key Group	Source Address = 192.168.103.0 (23)(25)
Name = HtoG4AtoR	Source Mask = 255.255.255.0 (22)(25)
System Role = Local system is a host, and the remote system is a gateway	Destination Address Format = NetMask
Initiation = Either systems can initiate the connection	Destination Address = 192.168.100.150 (24)
Data Management Security Policy = HtoG4AtoRBS	Destination Mask = 255.255.255.255
Connection Lifetime = Never Expires (21)	Protocol to filter = All Protocols (26)
Local addresses = Filter rule	Source Ports = 0 - 65535 (28)
Local ports = Filter rule	Destination Ports = 0 - 65535 (27)
Remote addresses = Filter rule	Local Identifier Type = IPv4 address (17)
Remote ports = Filter rule	
Protocol = Filter rule	
Dynamic Key Connection	
Name = HtoG4AtoR:L1	
Key Connection Group = HtoG4AtoRBS	
Start when TCP/IP is started? = No	
IP Filters	
Name = HtoG_AStoRTR13P	
Defined Addresses = RTRsubnets	
Subnet mask = 255.255.255.0 (22)	
IP addresses = 192.168.103.0 (23)	
IPSEC rule	
Source address name = 192.168.100.150 (24)	
Destination address name = RTRsubnets (25)	
Connection Name = HtoG4AtoR	
Services	
Protocol = * (26)	
Source port = * (27)	
Destination port = * (28)	

15.5 Starting the VPN connections and final verification

This section describes how to start the connection at both ends of the tunnel and perform the final verification test.

15.5.1 Starting the VPN connection on the AS/400 system

To start the VPN connection on the AS/400 system, perform the following steps:

1. Start filters.
2. Start Virtual Private Networking.
3. Open Virtual Private Networking.
4. Right click the **HtoGRto4A:L1** connection in the right panel, and select **Start** to initiate a VPN connection to the 2212 router (Figure 802).

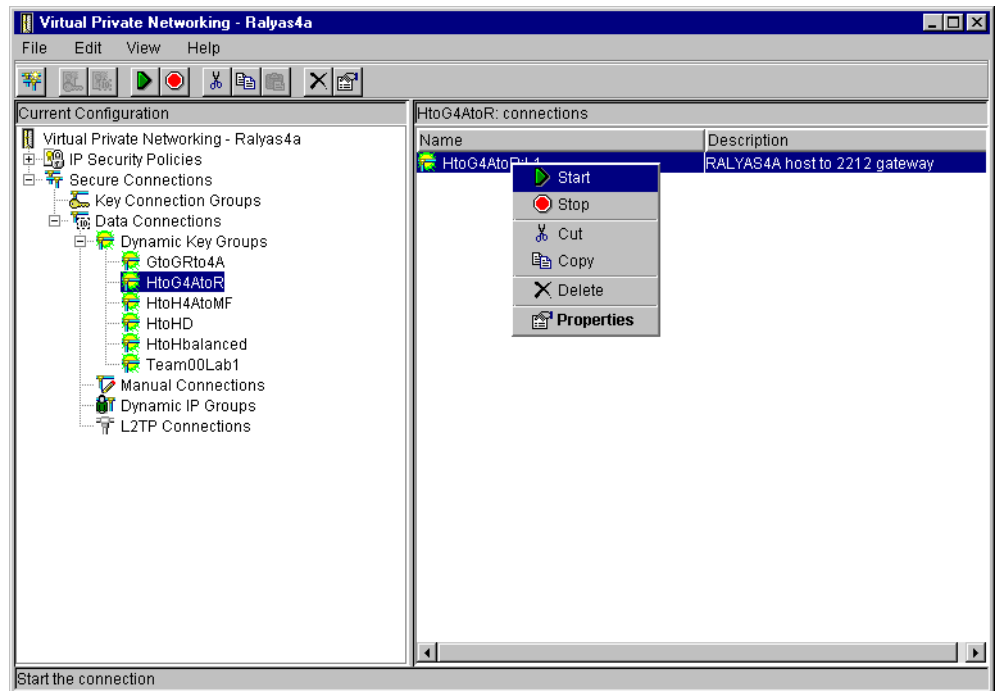


Figure 802. Starting the host-to-gateway connection - HtoG4AtoR

5. Display the connection to verify that it is active. At the Virtual Private Networking window, select **View->Active Connections** as shown in Figure 803.

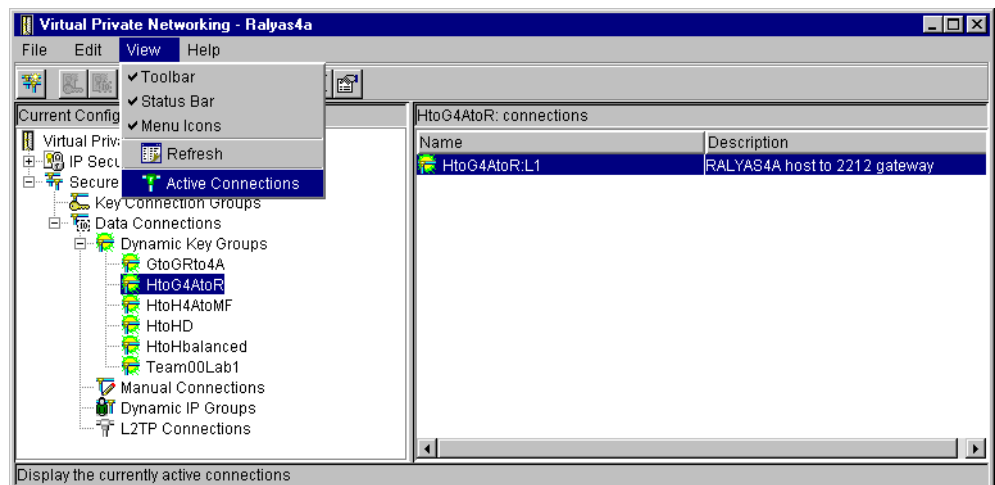


Figure 803. Starting the Active Connections window

The Active Connections window is shown in Figure 804.

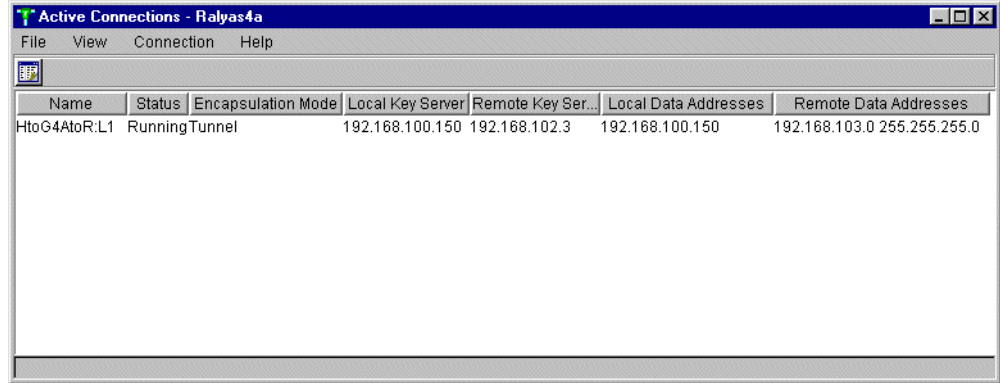


Figure 804. Active Connections window

- Use the 2212 router console to verify that the VPN connection is successfully established. Figure 805 shows the IPSEC section in the 2212 router.

```
Branch* TALK 5
Branch* FEATURE IPSEC
Branch IPV4-IPsec>LIST ALL

IPsec is ENABLED

IPsec Path MTU Aging Timer is 220 minutes

Defined Tunnels for IPv4:
-----
  ID      Type      Local IP Addr  Remote IP Addr  Mode  State
-----
   1     ISAKMP    192.168.102.3  192.168.100.150  TUNN  Enabled

Defined Manual Tunnels for IPv6:
-----

Tunnel Cache for IPv4:
-----
-
  ID      Local IP Addr  Remote IP Addr  Mode  Policy  Tunnel Expiration
-----
   1     192.168.102.3  192.168.100.150  TUNN  ESP      none

Tunnel Cache for IPv6:
-----
-
Branch IPV4-IPsec>
```

Figure 805. Verifying the VPN connection status on the 2212 router

- Use the 2212 router console `STATS` command to display the VPN tunnel traffic statistics.

```

Branch IPv4-IPsec>STATS
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

Global IPsec Statistics

Received:
total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
-----
           16           0           16         8032         4016         4016

Sent:
total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
-----
           25           0           25         2104           0         2104

Receive Packet Errors:
total errs  AH errors  AH bad seq  ESP errors  ESP bad seq
-----
           0           0           0           0           0

Send Packet Errors:
total errs  AH errors  ESP errors  Exceed MTU
-----
           0           0           0           0

```

Figure 806. Displaying the VPN tunnel traffic statistics on the 2212 router

8. Use the IBM 2212 router event logging system (ELS) to trace the phase 1 and phase 2 key and data policy negotiation. Figure 807 shows how to start ELS in the 2212 router console.

```

Branch *TALK 5
Branch +
Branch +EVENT
Event Logging System user console
Branch ELS >NODISPLAY SUBSYSTEM all all
Branch ELS >DISPLAY SUBSYSTEM ike all
Branch ELS >CTRL-P
Branch *TALK 2

```

Figure 807. Starting the 2212 router event logging system (ELS)

Figure 808 on page 721 shows the output of the event logging system. To terminate event logging, press **CTRL+P**.


```

00:29:46 IKE.001: Trace IKE packet from 192.168.100.150
00:29:46 IKE.013: From Peer: 192.168.100.150 AG HDR SA KE NONCE ID
00:29:46 IKE.009: Begin Aggressive mode - Responder
00:29:49 IKE.014: Oakley proposal is acceptable. Peer: 192.168.100.150
00:29:49 IKE.003: Processing ISA_KE
00:29:52 IKE.003: Processing NONCE
00:29:52 IKE.013: To Peer: 192.168.100.150 AG HDR SA KE NONCE ID HASH
00:29:52 IKE.001: Trace IKE packet to 192.168.100.150
00:29:52 IKE.001: Trace IKE packet from 192.168.100.150
00:29:52 IKE.011: isakmp_input: drop incoming retransmitted message
00:29:52 IKE.001: Trace IKE packet from 192.168.100.150
00:29:52 IKE.014: Received unencr packet when crypto act, Peer: 192.168.100.150
00:29:52 IKE.013: From Peer: 192.168.100.150 AG HDR* HASH
00:29:52 IKE.010: Finished Aggressive mode -responder
00:29:53 IKE.001: Trace IKE packet from 192.168.100.150
00:29:53 IKE.009: Begin Quick mode - Responder
00:29:53 IKE.002: Trace IKE payload after decryption from Peer: 192.168.100.150
00:29:53 IKE.013: From Peer: 192.168.100.150 QM HDR* HASH SA NONCE ID ID
00:29:53 IKE.003: Processing Quick Mode ID
00:29:53 IKE.003: Processing Quick Mode ID
00:29:53 IKE.015: Acceptable phase 2 proposal # 1
00:29:53 IKE.003: Processing NONCE
00:29:53 IKE.013: To Peer: 192.168.100.150 QM HDR* HASH SA NONCE ID ID
00:29:53 IKE.002: Trace IKE payload before encryption to Peer: 192.168.100.150
00:29:53 IKE.001: Trace IKE packet to 192.168.100.150
00:29:53 IKE.001: Trace IKE packet from 192.168.100.150
00:29:53 IKE.002: Trace IKE payload after decryption from Peer: 192.168.100.150
00:29:53 IKE.013: From Peer: 192.168.100.150 QM HDR* HASH
00:29:53 IKE.008: Load Out SA: Alg=18 Prot=3 Sec=86400 KB=50000 SPI=3153885377
00:29:53 IKE.008: Load In SA: Alg=18 Prot=3 Sec=86400 KB=50000 SPI=1272503440

```

Figure 808. Event logging system screen

15.5.2 Verification tests

Table 97 presents a summary of the verification tests run after the host-to-gateway VPN was configured and the connection started. The tests verify the scenario objectives stated in 15.1.2, “Scenario objectives” on page 688.

Table 97. Verification test - OS/400 to 2212 router host-to-gateway scenario

	TELNET	FTP	PING
From RALYAS4A to RTRsubnet hosts	Yes	Yes	Yes
From RTRsubnet hosts to RALYAS4A	Yes	Yes	Yes
From RTRsubnet hosts to DataCtr hosts	No	No	No
From DataCtr hosts to RTRsubnet hosts	No	No	No
Note: RTRsubnet represents the network behind the router at the branch office. DataCtr hosts represents the network at the data center behind the firewall.			

Note

After the VPN is started, the AIX firewall filter rules do not need to be changed to route the ICMP messages. This is because the ICMP messages now flow through the VPN tunnel.

Chapter 16. Gateway-to-gateway VPN: AS/400 to 2210 router

This chapter describes a VPN gateway-to-gateway configuration between an AS/400 system and a 2210 router.

16.1 Branch office VPN connection (AS/400 gateway to 2210 gateway)

In this scenario, we present a data center at the company's corporate office and a remote branch office. The AS/400 system is located at the data center. Users at both networks are allowed to access all systems and applications on the remote network. Figure 809 represents this scenario.

16.1.1 Scenario characteristics

The characteristics of this scenario are:

- Both networks belong to the same company, so the data is trusted on the remote network and can flow in the clear on the secure side of the VPN gateway.
- The secure tunnel is between the branch office's 2210 router and the data center's AS/400 system.
- Both networks are connected to the Internet through routers and firewalls. The filters in the data center firewall must be opened to allow IKE negotiation and IPsec protocols between the data center AS/400 system and the branch office's router VPN partners.
- There are two separate physical lines attached to the gateway AS/400 system:
 - TOKENRING2 connects the gateway to the "Internet" and represents the non-secure interface.
 - TOKENRING1 connects the gateway to the internal data center network and represents the secure interface. See Figure 810 on page 724.

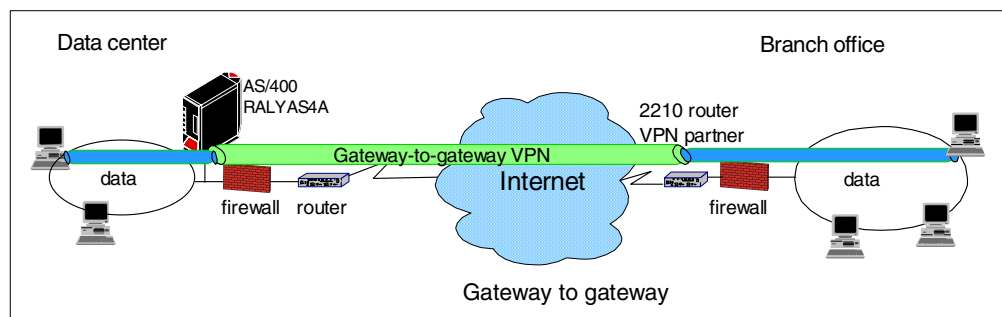


Figure 809. Branch office VPN - Gateway-to-gateway AS/400 system to 2210 router

Note

For a higher level of security, the 2210 VPN partner should be placed on the secure side of the firewall at the branch office.

16.1.2 Scenario objectives

The objectives of this scenario are:

- All traffic between the branch office and the data center must be protected by IPSec.
- All the users in the branch office can access all resources in the data center's network and vice versa.
- The data traffic can flow in the clear in both internal networks behind the VPN gateways. The data center and the branch office belong to the same company.

16.1.3 Scenario network configuration

Figure 810 shows our simple network configuration for the gateway-to-gateway AS/400 system to 2210 router.

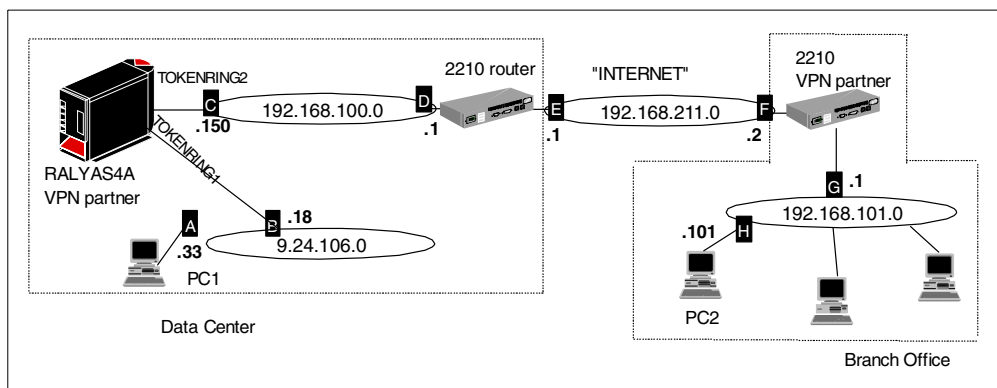


Figure 810. Gateway to gateway - AS/400 to 2210 router

16.1.4 2210 router software

Multiprotocol Routing Services Version 3.3 is required on the 2210 router to support dynamic VPN connections.

16.1.5 Implementation tasks: Summary

The following procedure summarizes the tasks you need to perform to implement this VPN gateway to gateway environment:

1. Verify connectivity. Before you start configuring VPN and filters, you must be sure that the underlying TCP/IP network is properly configured and working.
2. Complete the planning worksheets for the 2210 router.
3. Configure a VPN in the 2210 router.
4. Complete the planning worksheet for the AS/400 system.
5. Configure a host-to-gateway VPN in the AS/400 system.
6. Configure filters in the AS/400 system.
7. Start the VPN connection.
8. Perform verification tests.

16.1.6 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the data center and the branch office network is correct:

1. From PC1 in the data center network, PING PC2 at the branch office. Enter the following PING command:

```
PING 192.168.101.101
```

2. Repeat the PING in the reverse direction from PC2 at the branch office to PC1 at the data center:

```
PING 9.24.106.33
```

Both tests must succeed before you continue. In a real Internet environment, there may be routers on the way that disallow the PING command.

16.2 2210 router configuration

The following sections explain how to configure the VPN in the 2210 router to establish a secure tunnel with the AS/400 system RALYAS4A. It is beyond the scope of this redbook to provide detailed information about the 2210 router configuration. Refer to *A Comprehensive Guide to Virtual Private Networks, Vol III: IBM Cross-Platform and Key Management Solutions*, SG24-5309, for more information about the routers configuration.

16.2.1 Completing the planning worksheets for the 2210 router

Complete the 2210 router planning worksheets as shown in Table 98 through Table 106. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 98. IBM 2210 router configuration - Remote user definitions

Information you need to create your VPN	Scenario answers
How to identify the remote IKE peer (user): <ul style="list-style-type: none">– IP address– Fully qualified domain name– User fully qualified domain name– Key ID	Select IP address with AS/400
IP address that distinguishes this user?	192.168.100.150
Authenticate user with: <ul style="list-style-type: none">– Pre-shared key– Public certificate?	Select pre-shared key with AS/400
Mode in which you will enter the pre-shared key: <ul style="list-style-type: none">– ASCII– HEX	Select ASCII with AS/400
Pre-shared key (even number of characters):	87654321

Table 99. IBM 2210 router configuration - Policy definitions

Information you need to create your VPN	Scenario answers
Policy name:	ike-pre-101-to-106
Priority of this policy in case of multiple policies:	5

Table 100. IBM 2210 router configuration - Policy profile

Information you need to create your VPN	Scenario answers
Profile name:	101-to-106
Source address format: – NetMask – Range – Single address	NetMask
Source address	192.168.101.0
Destination address format: – NetMask – Range – Single address	NetMask
Destination address	9.24.106.0
Select the protocol to filter on: – TCP – UDP – All protocols – Specify range	All protocols
Starting value for the source port: 0 for all protocols	0
Ending value for the source port: 65535 for all protocols	65535
Starting value for the destination port: 0 for all protocols	0
Ending value for the destination port: 65535 for all protocols	65535
Enter the mask to be applied to the Received-DS-byte:	0
Enter the value to match against after the mask has been applied to the Receive-DS-byte:	0
Do you want to configure local and remote IDs for ISAKMP?	Yes
Select the identification type of the local ID to be sent to the remote IKE peer: – Local tunnel endpoint address – Fully qualified domain name – User fully qualified domain name – Key ID (any string)	Select local tunnel endpoint address with AS/400
Do you want to limit this profile to specific remote users?	Yes
Do you want to limit this profile to specific interfaces?	No

Table 101. IBM 2210 router configuration - Policy validity profile

Information you need to create your VPN	Scenario answers
Validity profile name:	Always
Enter the lifetime of this policy: – yyymmddhhmmss – * denotes forever	*
During which months should this profile be valid? All to signify all year round	All
During which days should this profile be valid? All to signify all week	All
During which hours should this profile be valid? * denotes all day	*

Table 102. IBM 2210 router configuration - IPSec action profile

Information you need to create your VPN	Scenario answers
IPSec action profile name:	tun-16
Select the IPSec security action type: – Block – Permit	Permit
Should the traffic flow into a secure tunnel or in the clear? – Clear – Secure tunnel	Secure tunnel
What is the tunnel startpoint IP address?	192.168.211.2
What is the tunnel endpoint IP address?	192.168.100.150
Does this IPSec tunnel flow within another IPSec tunnel?	No
Percentage of SA lifesize or lifetime to use as the acceptable minimum? The default is 75%.	75 %
Security association refresh threshold in percent The default is 85%.	85 %
Select the option for the DF bit in the outer header: – Copy – Set – Clear	Copy
Do you want to enable replay prevention?	Disable
Do you want to negotiate the security association at system initialization (autostart)?	No

Table 103. IBM 2210 IPSec proposal

Information you need to create your VPN	Scenario answers
What name do you want to give this IPSec proposal?	esp-prop6
Does this proposal require Diffie-Hellman Perfect Forward Secrecy?	No
Do you wish to enter any AH transforms for this proposal?	No
Do you wish to enter any ESP transforms for this proposal?	Yes

Table 104. IBM 2210 router configuration - IPSec ESP transform

Information you need to create your VPN	Scenario answers
IPSec ESP transform name:	esp-trans6
Select the protocol ID: – IPSec AH – IPSec ESP	IPSec ESP
Select the encapsulation mode: – Tunnel – Transport	Tunnel
Select the ESP authentication algorithm: – HMAC_MD5 – HMAC_SHA	HMAC_MD5
Select the ESP cipher algorithm: – ESP DES – ESP 3DEC – ESP CDMF – ESP NULL	ESP DES
What is the SA lifesize, in kilobytes? The default is 50000 kilobytes.	50000
What is the SA lifetime? The default is 3600 seconds.	3600

Table 105. IBM 2210 router configuration - ISAKMP action

Information you need to create your VPN	Scenario answers
ISAKMP action name:	ike-6
Select the ISAKMP exchange mode: – Main – Aggressive	Aggressive
Percentage of SA lifesize or lifetime to use as the acceptable minimum: The default is 75%.	75 %

Information you need to create your VPN	Scenario answers
What is the ISAKMP connection lifeseize, in kilobytes? The default is 5000 kilobytes.	5000
What is the ISAKMP connection lifetime in seconds? The default is 30000 seconds.	30000
Do you want to negotiate the SA at system initialization (autostart)?	No

Table 106. IBM 2210 router configuration - ISAKMP proposal

Information you need to create your VPN	Scenario answers
ISAKMP proposal name:	ike-prop6
Select the authentication method – Pre-shared key – Digital certificate	Pre-shared key
Select the hashing algorithm – MD5 – SHA	MD5
Select the cipher algorithm – DES – 3DES	DES
What is the SA lifeseize, in kilobytes? Default is 1000 kilobytes	999999
What is the SA lifetime? Default is 15000 sec	86400
Select the Diffie Hellman Group ID – Diffie Hellman Group 1 – Diffie Hellman Group 2	Group 1
Do you wish to map a DiffServ Action to this policy?	No
What will be the status of the policy? – Enabled – Disabled	Enabled

16.2.2 Configuring the VPN in the 2210 router: Configuration summary

This section summarizes the 2210 router VPN configuration for this scenario. For detailed information about the routers configuration, refer to *A Comprehensive Guide to Virtual Private Networks, Vol III: IBM Cross-Platform and Key Management Solutions*, SG24-5309.

An IBM 2210 router was used as the branch office VPN partner in our example scenario. To configure the 2210 router, follow these steps:

1. For the 2210 router, the encryption package is part of the running image. However, the IBM 2210 router needs to load the encryption package. Use `RELOAD` (not `restart`) for the router to load the encryption package (Figure 811).

```

Config>LOAD ADD PACKAGE encryption
encryption package configured successfully
This change requires a reload.
Config>RELOAD y

```

Figure 811. Reloading the 2210 router

- For this scenario, we used an IBM 2210 model 24T router. Figure 812 shows the configuration setup of the V.24 and the Token-Ring interface.

```

*
talk 6
Config>SET HOSTNAME Branch
Host name updated successfully
Branch Config>NETWORK 1
Point-to-Point user configuration
Branch PPP 1 Config>SET HDLC CABLE V24 DTE
Branch PPP 1 Config>SET HDLC CLOCKING EXTERNAL
Must also set the line speed to a valid value
Line speed (2400 to 6312000) [0]? 64000
Branch PPP 1 Config>EXIT
Config>NETWORK 0
Token-Ring interface configuration
Branch TKR Config [0]>SPEED 16
Branch TKR Config [5]>EXIT

```

Figure 812. Interface configuration

- Configure the IP addresses and routes as shown in Figure 813.

```

Config>PROTOCOL IP
Internet protocol user configuration
Branch IP config>ADD ADDRESS 1 192.168.211.2 255.255.255.0
Branch IP config>ADD ADDRESS 0 192.168.101.1 255.255.255.0
Branch IP config>ADD route 0.0.0.0 0.0.0.0 192.168.211.1
Branch IP config>EXIT

```

Figure 813. IP address and route configuration

Tip

Add a default route to the router configuration. The router checks the routing table first and then checks the policy database. Although the destination is mapped into the policy traffic profile, the router drops the packet and does not check the policy database unless there is a route for that destination. A default route satisfies the routing table lookup requirement.

After a successful routing table lookup, the router checks the policy database. If the destination matches the policy database, then the traffic passes through the tunnel and does not follow the path as defined by the routing table.

4. Enable IPsec to use the router for secure tunnel with pre-shared keys (Figure 814).

```
Branch *TALK 6
Branch Config>FEATURE IPsec
IP Security feature user configuration
Branch IPsec config>IPV4
Branch IPV4-IPsec config>ENABLE IPSEC
It is necessary to restart the router for IPsec to be active.
Branch IPV4-IPsec config>EXIT
Branch IPsec config>CTRL-P
Branch *RESTART y
```

Figure 814. Enabling IPSEC

5. Create the user for pre-shared key. Figure 815 shows how to add a *user* that represents the remote VPN partner and the pre-shared key. The IP address must be the same as the tunnel endpoint. The pre-shared key is not displayed for security reasons. The pre-shared key is shown in Figure 815 for documentation purposes.

```
Branch Config>FEATURE Policy
IP Network Policy configuration
Branch Policy config>ADD USER
Choose from the following ways to identify a user:
  1: IP Address
  2: Fully Qualified Domain Name
  3: User Fully Qualified Domain Name
  4: Key ID (Any string)
Enter your choice(1-4) [1]?
Enter the IP Address that distinguishes this user
  [0.0.0.0]? 192.168.100.150
Group to include this user in []?
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars): 87654321
Enter the Pre-Shared Key again (8 characters) in ascii: 87654321

Here is the User Information you specified...

Name      = 192.168.100.150
Type      = IPV4 Addr
Group     =
Auth Mode =Pre-Shared Key
Is this correct? [Yes]:
Branch Policy config>
```

Figure 815. Adding a user

Tip

For dynamic connections, the pre-shared key is configured in the AS/400 system in ASCII characters.

6. Add a policy to the 2210 router configuration.

A policy is the framework for describing how traffic entering or leaving the router should be handled. If a policy creates a security tunnel, only the

packets matching the profile will be encrypted and forwarded. Other packets, *not matching the profile*, are passed in the clear unless explicitly dropped by another policy. When more than one policy exists on a router, the policies are evaluated according to priority number.

The components of a policy are shown in Figure 816.

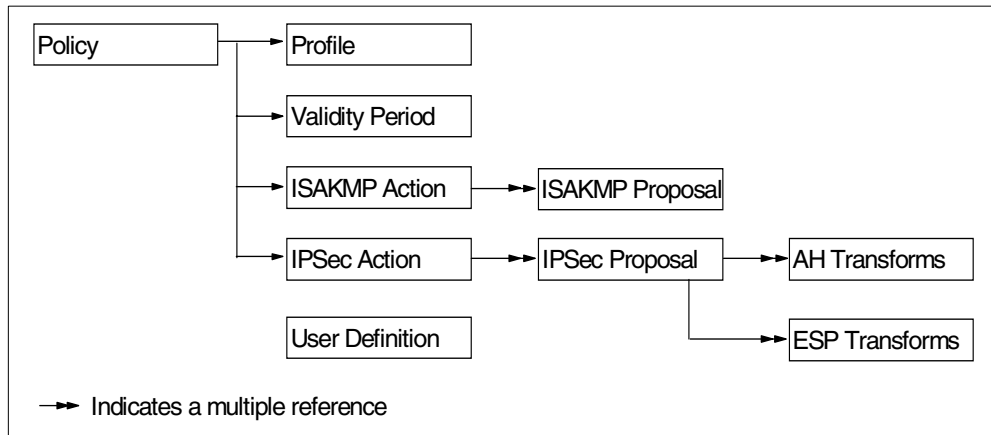


Figure 816. Policy component relationship

The ADD POLICY command (Figure 817) prompts you through all of the configuration steps. In this scenario, the overall policy name is `ike-pre-101-to-106`.

```

Branch Config>FEATURE Policy
IP Network Policy configuration
Branch Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ike-pre-101-to-106
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
    0: New Profile
  
```

Figure 817. Adding a policy

7. Add a profile to the policy previously configured.

After adding the policy, you must create a profile associated with the policy (Figure 818 on page 733). In this scenario, the profile name is `101-to-106` to describe the criteria used to determine if a packet should be processed by the policy. This criteria includes a source and destination address, protocol, port type, and Differentiated Services (DS) byte, also known as Type of Service (TOS) byte.

```
List of Profiles:
    0: New Profile

Enter number of the profile for this policy [0]?
Profile Configuration questions. Note for Security Policies, the Source
Address and Port Configuration parameters refer to the Local Client Proxy
and the Destination Address and Port Configuration parameters refer to the
Remote Client Proxy
Enter a Name (1-29 characters) for this Profile []? 101-to-106
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPv4 Source Address [0.0.0.0]? 192.168.101.0
Enter IPv4 Source Mask [255.255.255.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPv4 Destination Address [0.0.0.0]? 9.24.106.0
Enter IPv4 Destination Mask [255.255.255.0]?

Protocol IDs:
    1) TCP
    2) UDP
    3) All Protocols
    4) Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
```

Figure 818. Adding a profile

8. Configure the ISAKMP local and remote IDs (Figure 819). This configuration must match the remote VPN partner configuration.

```
Configure local and remote ID's for ISAKMP? [No]: yes
Enter local identification to send to remote
    1) Local Tunnel Endpoint Address
    2) Fully Qualified Domain Name
    3) User Fully Qualified Domain Name
    4) Key ID (any string)

Select the Identification type (1-4) [1]?
Any user within profile definition allowed access? [Yes]:
Limit this profile to specific interface(s)? [No]:
```

Figure 819. Configuring IDs for ISAKMP

9. Confirm the policy profile as shown in Figure 820 on page 734. Enter option 1 to select the 101-to-106 profile.

```
Here is the Profile you specified...

Profile Name      = 101-to-106
sAddr:Mask= 192.168.101.0 : 255.255.255.0   sPort= 0 : 65535
dAddr:Mask= 9. 24.106.0 : 255.255.255.0   dPort= 0 : 65535
  proto          =          0 : 255
  TOS            =          x00 : x00
  Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
  0: New Profile
  1: 101-to-106

Enter number of the profile for this policy [1]?
```

Figure 820. Confirming the policy profile

10. Add the validity period to the policy.

The validity period defines the time period during which the policy is valid. You may specify a time duration, or the months of the year, days of the week, and hours of the day that the policy is valid.

We configured the validity period to be valid all the time (Figure 821 on page 735).

```

List of Validity Periods:
    0: New Validity Period

Enter number of the validity period for this policy [0]?
Enter a Name (1-29 characters) for this Policy Valid Profile []? always
Enter the lifetime of this policy. Please input the
information in the following format:
        yyyyymmddhhmmss:yyyyymmddhhmmss OR '*' denotes forever.
[*]?
During which months should policies containing this profile
be valid. Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
[ALL]?
During which days should policies containing this profile
be valid. Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
[ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
[*]?

Here is the Policy Validity Profile you specified...

Validity Name   = always
Duration       = Forever
Months         = ALL
Days           = ALL
Hours          = All Day
Is this correct? [Yes]:
List of Validity Periods:
    0: New Validity Period
    1: always

Enter number of the validity period for this policy [1]?

```

Figure 821. Policy validity period

11. Add the IPSec Action to the policy.

In addition to a profile and a validity period, a policy must also be associated with an IPSec action. In this step, we configure an IPSec action.

An IPSec action may specify either a drop, pass, or secure action. If the action is drop, all packets matching the profile used by this policy are dropped. If the action is pass with no security, then all packets are passed in the clear. If the action is pass with security, all packets are secured by means of the Security Association (SA) specified by this action. The IPSec action also contains the IP addresses of the tunnel endpoints for the IPSec tunnel and IKE SAs.

We specified that the policy should enforce an IPSEC action to create a tunnel, tun-16, to the AS/400 system (Figure 822 on page 736).

```

Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
    0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
Enter a Name (1-29 characters) for this IPsec Action []? tun-16
List of IPsec Security Action types:
    1) Block (block connection)
    2) Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
    1) Clear
    2) Secure Tunnel
[2]?
Enter Tunnel Start Point IPV4 Address
[192.168.211.2]?
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
[0.0.0.0]? 192.168.100.150
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifetime/lifetime to use as the acceptable minimum [75]?
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
    1) Copy
    2) Set
    3) Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:

```

Figure 822. Creating a new IPSEC action

12. Add an IPSec Proposal to the policy

The IPSec proposal contains information about which ESP or AH (or both), transforms to propose or check against during phase 2 ISAKMP negotiations.

Figure 823 walks through the creation of an IPSec proposal. We created a proposal called `esp-prop6`, which selects ESP transforms. Each proposal requires at least one transform.

```

You must choose the proposals to be sent/checked against during phase 2
negotiations. Proposals should be entered in order of priority.
List of IPSEC Proposals:
    0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
Enter a Name (1-29 characters) for this IPsec Proposal []? esp-prop6
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: yes

```

Figure 823. Creating an IPSec proposal

13. Add an IPSec ESP Transform to the IPSec proposal.

The attributes of the IPSec transform contain information about the IPSec encryption and authentication parameters and also specify how often the keys are refreshed. The transform is either AH (authentication only) or ESP

(encryption, authentication, or both) and may be configured to operate in either tunnel or transport mode.

Figure 824 shows the creation of the transform esp-trans6. Transform esp-trans6 is an ESP Security Association (SA) in tunnel mode, with HMAC_MD5 authentication and DES encryption. You are prompted for the SA lifetime or lifesize of the phase 2 tunnel. When the SA lifetime expires, IKE performs another phase 2 calculation to refresh the keys.

```
List of ESP Transforms:
  0: New Transform

Enter the Number of the ESP transform [0]?
Enter a Name (1-29 characters) for this IPsec Transform []? esp-trans6
List of Protocol IDs:
  1) IPSEC AH
  2) IPSEC ESP

Select the Protocol ID (1-2) [1]? 2
List of Encapsulation Modes:
  1) Tunnel
  2) Transport

Select the Encapsulation Mode(1-2) [1]?
List of IPsec Authentication Algorithms:
  0) None
  1) HMAC-MD5
  2) HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [1]?
List of ESP Cipher Algorithms:
  1) ESP DES
  2) ESP 3DES
  3) ESP CDMF
  4) ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]?
Security Association Lifesize, in kilobytes (1024-2147483647) [50000]?
Security Association Lifetime, in seconds (120-2147483647) [3600]? 3600

Here is the IPsec transform you specified...

Transform Name = esp-trans6
  Type =ESP   Mode =Tunnel   LifeSize= 50000 LifeTime= 3600
  Auth =MD5  Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
  0: New Transform
  1: esp-trans6

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [No]:
```

Figure 824. Adding an IPsec ESP Transform

14. Confirm the IPsec proposal.

After adding the IPsec transform, confirm the IPsec proposal (Figure 825 on page 738).

```

Here is the IPsec proposal you specified...

Name = esp-prop6
Pfs = N
ESP Transforms:
    esp-trans6
Is this correct? [Yes]:
List of IPSEC Proposals:
    0: New Proposal
    1: esp-prop6

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:

```

Figure 825. Confirming the IPsec proposal

15. Confirm the IPsec action.

After creating the IPsec transform and proposal, finish the IPsec action. Select the action to be associated with the policy (Figure 826).

```

Here is the IPsec Action you specified...

IPSECAction Name = tun-16
Tunnel Start:End = 192.168.211.2 : 192.168.100.150
Tunnel In Tunnel = No
Min Percent of SA Life = 75
Refresh Threshold = 85 %
Autostart = No
DF Bit = COPY
Replay Prevention = Disabled
IPSEC Proposals:
    esp-prop6
Is this correct? [Yes]:
IPSEC Actions:
    0: New IPSEC Action
    1: tun-16

Enter the Number of the IPSEC Action [1]?

```

Figure 826. Confirming the IPsec action

16. Add the ISAKMP action.

Since a secure IPsec action was specified, you are automatically prompted to create an ISAKMP action (Figure 827 on page 739).

The ISAKMP action specifies the key management information for phase 1. It specifies whether the phase 1 negotiations are to start in main mode (provides identity protection) or in aggressive mode. It also specifies whether the phase 1 security association is to be negotiated at device start-up or on demand. The ISAKMP action also must reference one or more ISAKMP proposals.

Since no ISAKMP action exists, you must create one called `ike-6` in aggressive mode.

```
ISAKMP Actions:
    0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
Enter a Name (1-29 characters) for this ISAKMP Action []? ike-6

List of ISAKMP Exchange Modes:
    1) Main
    2) Aggressive

Enter Exchange Mode (1-2) [2]?
Percentage of SA lifese/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifeseize, in kilobytes (100-2147483647) [5000]?
ISAKMP Connection Lifetime, in seconds (120-2147483647) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [YES] :no
```

Figure 827. Adding an ISAKMP action

17. Add an ISAKMP proposal.

The ISAKMP proposal specifies the encryption and authentication attributes of the phase 1 security association. It also specifies which Diffie-Hellman group to use to generate the keys, and the life of the phase 1 security.

Since no ISAKMP proposal exists, you must create one called `Ike-prop6` (Figure 828 on page 740). Specify pre-shared keys, with authentication using MD5, encryption by DES, and an SA lifetime.

```

You must choose the proposals to be sent/checked against during phase 1
negotiations. Proposals should be entered in order of priority.
List of ISAKMP Proposals:
    0: New Proposal

Enter the Number of the ISAKMP Proposal [0]?
Enter a Name (1-29 characters) for this ISAKMP Proposal []? ike-prop6

List of Authentication Methods:
    1) Pre-Shared Key
    2) Certificate (RSA SIG)

Select the authentication method (1-2) [1]?

List of Hashing Algorithms:
    1) MD5
    2) SHA

Select the hashing algorithm(1-2) [1]?

List of Cipher Algorithms:
    1) DES
    2) 3DES

Select the Cipher Algorithm (1-2) [1]?
Security Association Lifesize, in kilobytes (100-2147483647)
[1000]?999999
Security Association Lifetime, in seconds (120-2147483647) [15000]? 86400

List of Diffie Hellman Groups:
    1) Diffie Hellman Group 1
    2) Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?

```

Figure 828. Adding an ISAKMP proposal

18. Confirm the ike-prop6 ISAKMP proposal called.

```

Here is the ISAKMP Proposal you specified...

Name = ike-prop6
AuthMethod = Pre-Shared Key
LifeSize = 1000
LifeTime = 3600
DHGroupID = 1
Hash Algo = MD5
Encr Algo = DES CBC

Is this correct? [Yes]:
List of ISAKMP Proposals:
    0: New Proposal
    1: ike-prop6

Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:

```

Figure 829. Confirming the ISAKMP proposal

19. Confirm the ISAKMP action.

The ISAKMP action ike-6 is presented for confirmation (Figure 830). This concludes the creation of the ISAKMP action.

```
Here is the ISAKMP Action you specified...

ISAKMP Name      = ike-6
  Mode           =           Main
  Min Percent of SA Life =       75
  Conn LifeSize:LifeTime =    5000 : 30000
  Autostart      =           Yes
  ISAKMP Proposals:
    ike-prop6
Is this correct? [Yes]:
ISAKMP Actions:
  0: New ISAKMP Action
  1: ike-6

Enter the Number of the ISAKMP Action [1]?
```

Figure 830. Confirming the ISAKMP action

20. Confirm the policy as shown in Figure 831.

After confirming the ISAKMP action and proposal, you are asked if you wish to configure a DiffServ Action. The DiffServ action describes the quality of service that is to be provided to packets that match a policy that specifies a DiffServ action. We did not select this option.

After creating all of the objects necessary for a secure tunnel policy, a summary of the policy is presented for confirmation.

We defined a policy named ike-pre-101-to-106, with a default priority of 5, which sets up a secure tunnel between the 192.168.211.2 and the 192.168.100.150 endpoint IP addresses. The IPsec action specifies a secure tunnel, which is always in effect as specified by the validity period. The packets allowed to enter the tunnel are determined by the profile that describes the two subnets. The authentication and encryption methods are specified in the ISAKMP action and ISAKMP proposal.

```
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name      =ike-pre-101-to-106
  State:Priority  =Enabled      : 5
  Profile        =101-to-106
  Valid Period   =always
  IPSEC Action   =tun-16
  ISAKMP Action  =ike-6
Is this correct? [Yes]:
Branch Policy config>
```

Figure 831. Confirming the policy

We have now created a policy that will evaluate all packets entering the router and forward those packets matching the profile to IPsec for encryption. If we do

not create any further policies, then all packets not matching the profile will be routed in the clear to the appropriate interface.

16.3 AS/400 gateway-to-gateway VPN configuration

The following sections explain how to configure the gateway-to-gateway connection on the AS/400 system RALYAS4A to establish a VPN with the 2210 router in this scenario.

16.3.1 Completing the planning worksheets for the AS/400 system

Complete the AS/400 system planning worksheets as shown in Table 107 and Table 108 on page 743. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 107. RALYAS4A New Connection Wizard planning worksheet

This information needed to create VPN with the New Connection Wizard	Scenario answers
What is the type of connection to be created? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to hosts – Gateway to Dynamic IP User – Host to Dynamic IP User	Gateway to Gateway
What is the name of the connection group?	GtoGRto4A
What type of security and system performance is required to protect the keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How is the local VPN server identified?	IP address
What is the IP address of the local VPN server?	192.168.100.150
How is the remote VPN server identified?	IP address
What is the IP address of the remote server?	192.168.211.2
What is the pre-shared key?	87654321
What type of security and system performance is required to protect the data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

We completed this planning worksheet (Table 107) from the perspective of RALYAS4A. The wizard will balance security and performance for protecting both key and data information. The main configuration object, the *connection group*, is named *GtoGRto4A*. The pre-shared key is a "random" string of characters, *87654321*.

Table 108. Planning worksheet - IP filter rules RALYAS4A

This is the information needed to create the IP filters to support the VPN connection	Scenario answers
Is the local VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication/encryption endpoint? If yes, the VPN server acts as a host. If no, the VPN server acts as a gateway.	gateway
Is the <i>remote</i> VPN server acting as a host or gateway ?	gateway
What is the name used to group together the set of filters that will be created?	VPNIFC
If the <i>local</i> VPN server is acting as a gateway ... – What is the IP address of the local ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	9.24.106.0 255.255.255.0 AS4Asubnets
If the <i>remote</i> VPN server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	192.168.101.0 255.255.255.0 RTRsubnets
What is the IP address of the local VPN server? - Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. - Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	192.168.100.150
What is the IP address of the remote VPN server? - Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. - Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	192.168.211.2
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TOKENRING2
What other IP addresses, protocols, and ports are permitted on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	

We also completed the IP filter rules planning worksheet (Table 108) from the perspective of RALYAS4A. The filter rules allowed traffic between any 9.24.106.* address on the local network and any 192.168.101.* address on the remote network.

To configure the filter rules, the local and remote subnets must have a name assigned to them. In this example, the local subnet name is AS4Asubnets and the remote subnet is RTRsubnets. These names are used in the Defined Address definition in the filter configuration.

VPNIFC is the filter set name that groups all the related rules together and is applied to a physical interface. The interface is TOKENRING2. This is the Token-Ring line description that connects the gateway AS/400 system RALYAS4A to the Internet.

Only the secure tunnel traffic is allowed to flow in the TOKENRING2 interface. When the filter rules are active, they only allow the VPN gateway-to-gateway tunnel through TOKENRING2.

The internal network traffic flows through the TOKENRING1 line without any restrictions. There is no need to create filter rules to allow the general traffic to and from the internal network since no filter rules are active on TOKENRING1.

16.3.2 Configuring a gateway-to-gateway VPN on RALYAS4A

Perform the following steps to configure a gateway-to-gateway VPN on RALYAS4A:

1. Start Operations Navigator from the desktop.
2. Expand the AS/400 system (in this case, **RALYAS4A**). Sign on when prompted.
3. Expand **Network** (Figure 832).

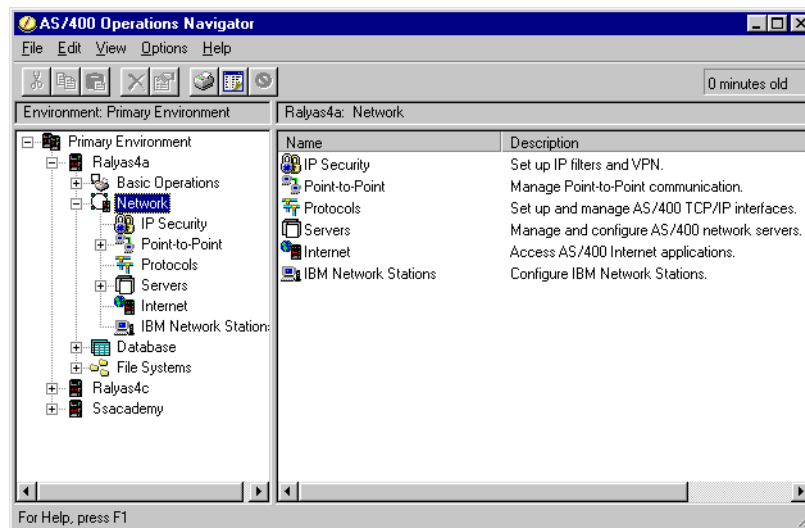


Figure 832. IP security

4. Double-click **IP Security** to reveal two server names in the right window: IP Packet Security and Virtual Private Networking (Figure 833 on page 745). Both functions must be configured, but Virtual Private Networking must be configured first.

Note

At this stage, Virtual Private Networking may already have a status of started since the default is for the server to automatically start when TCP/IP starts. The server can be either started or stopped during the following steps.

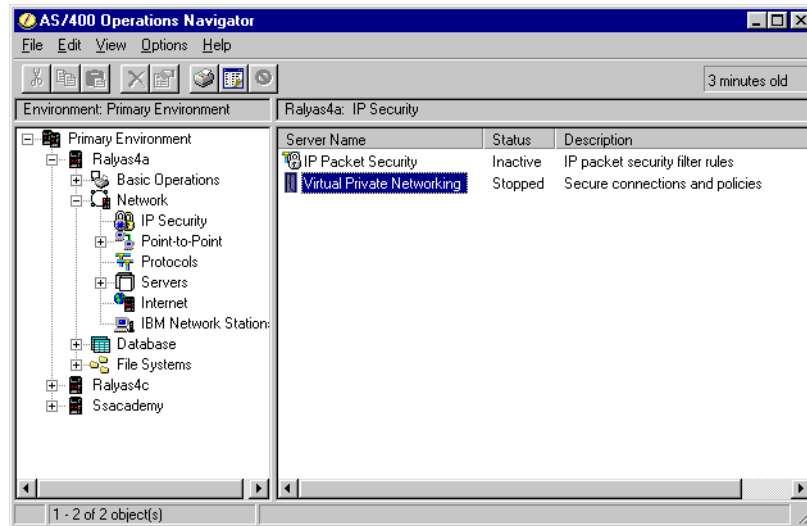


Figure 833. Operations Navigator - Virtual Private Networking

5. Double-click **Virtual Private Networking** to start the Virtual Private Networking GUI (Figure 834).

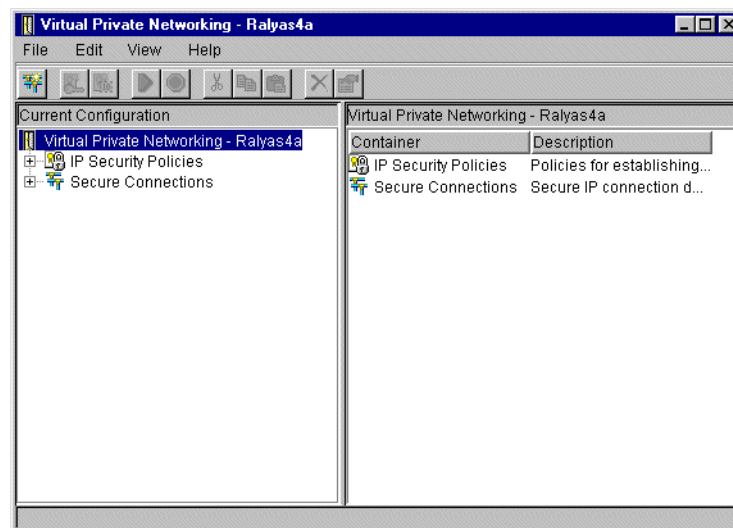


Figure 834. Virtual Private Networking GUI configuration interface

6. Select **File->New Connection->Gateway To Gateway** (Figure 835 on page 746). This starts the New Connection Wizard for a gateway-to-gateway connection.

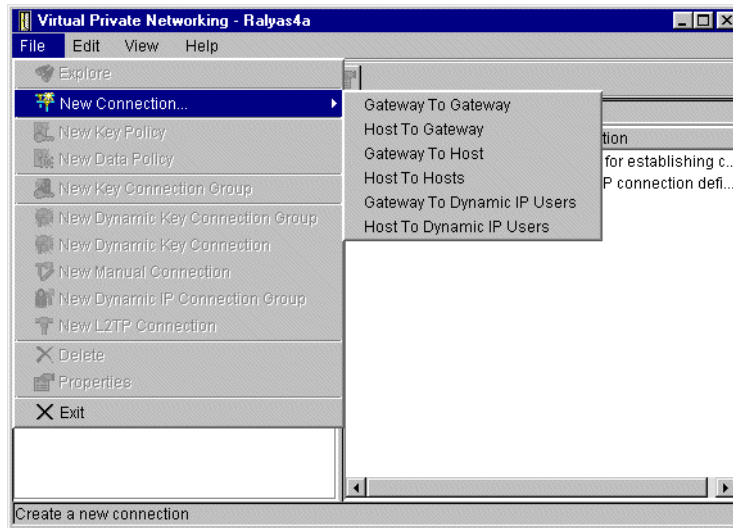


Figure 835. New Connection -> Gateway to Gateway

The VPN New Connection Wizard welcome window is displayed as shown in Figure 836.

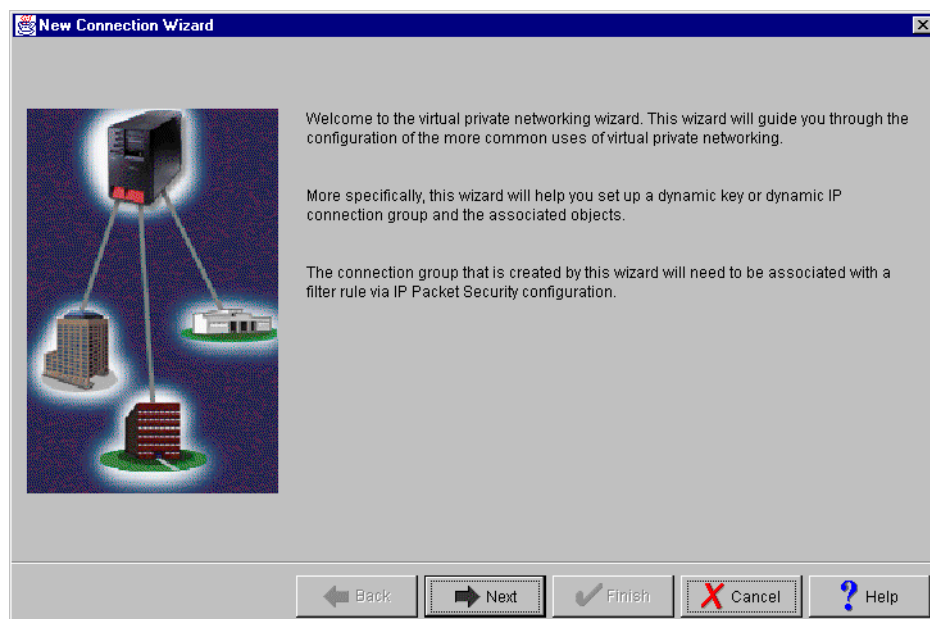


Figure 836. New Connection Wizard welcome window

7. Click **Next** after reading the Welcome window.
8. At the Connection Name window (Figure 837 on page 747), enter the name `GtoGRto4A` for the connection group. `GtoGRto4A` is the name from the worksheet in Table 107 on page 742. The name specified here is the name for all objects that the wizard creates for this particular connection. It is case sensitive. Also enter a description of the configuration.

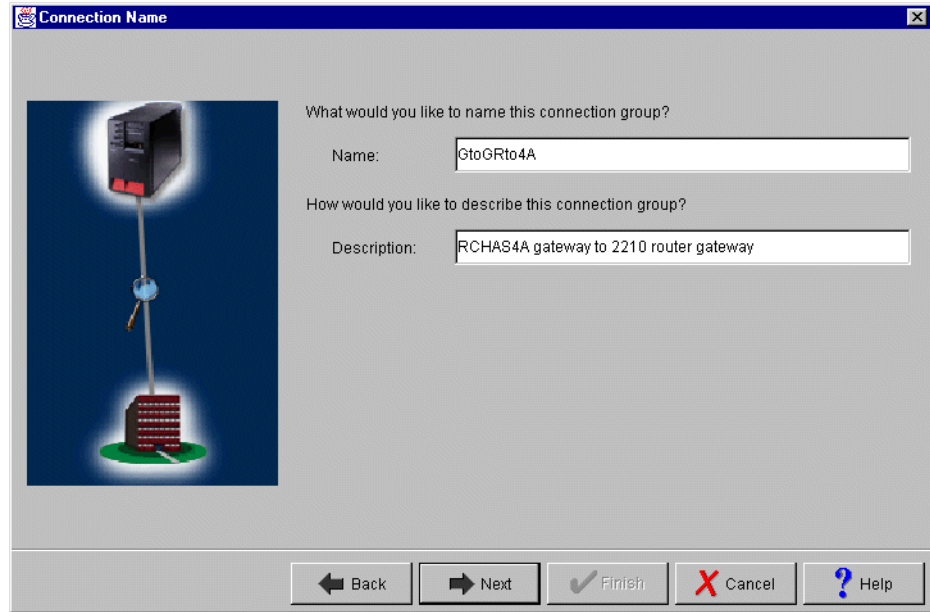


Figure 837. Connection Name window

9. Click **Next**.

10. At the Key Policy window (Figure 838), specify the level of authentication or encryption protection that IKE uses during phase 1 negotiations. Phase 1 establishes the keys that protect the messages that flow during subsequent phase 2 negotiations. Phase 2 protects the data itself. For the purposes of this example, select **Balance security and performance** as specified on the worksheet. The wizard chooses the appropriate encryption and authentication algorithms based on the selection made here.

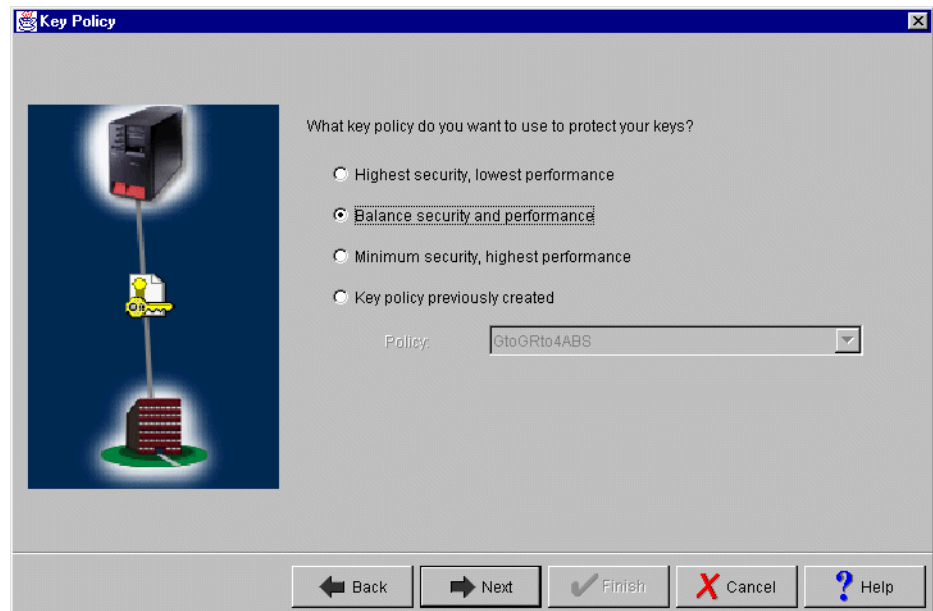


Figure 838. Key Policy window

11. Click **Next**.

12. In the Local Identifier window, specify the identity of the local key server. In other words, specify the local AS/400 system that acts as the VPN gateway, which, in this case, is RALYAS4A. Leave Identifier type as the default value, **Version 4 IP address**. For the IP Address parameter, use the pull-down list to select the IP address of the interface which is connecting to the remote gateway 2210 router. Refer back to the planning worksheet (Table 107 on page 742) and to the network configuration in Figure 810 on page 724. For RALYAS4A this is **192.168.100.150** (interface **C**).

Note: Figure 839 shows various IP addresses, 9.24.104.21, 9.24.106.18, and so on, that we do not reference anywhere in this scenario. These interfaces are configured on RALYAS4A, but are used for other scenarios and projects. They should be ignored here.

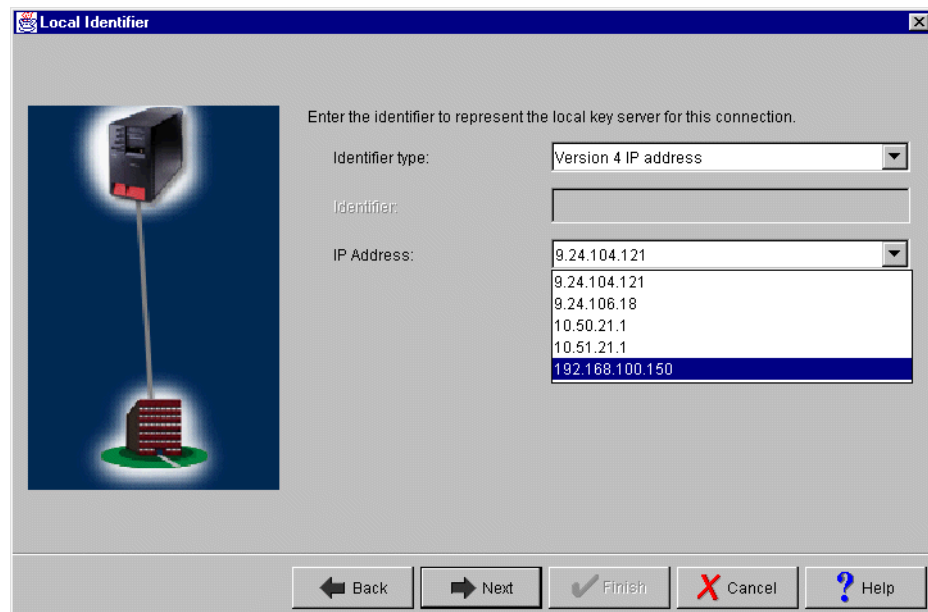


Figure 839. Local identifier window pull-down list

13. Click **Next**.

14. Use the Remote Network window (Figure 840 on page 749) to enter details about the remote key server, as well as the pre-shared key. The pre-shared key is the shared "secret" IKE uses to generate the actual keys for phase 1. The remote key server is the 2210 router with IP Address 192.168.211.2. This is interface **F** in Figure 810 on page 724. Refer also to the planning worksheet in Table 107 on page 742. Specify 87654321 in the Pre-shared key parameter. Remember, the same pre-shared key must be entered when configuring VPN on the remote 2210 router.

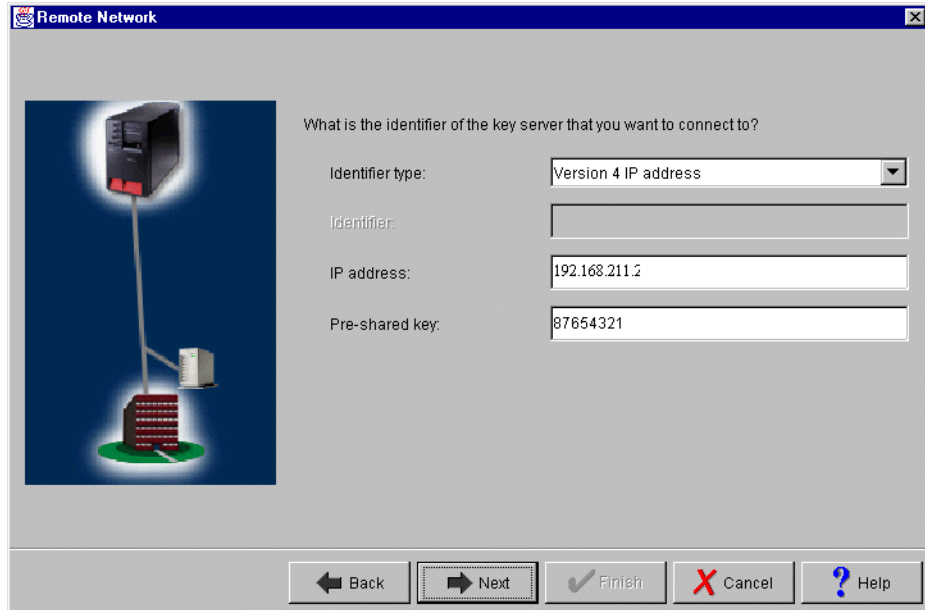


Figure 840. Remote key server identifier window

15. Use the Data Policy window (Figure 841) to specify the level of authentication or encryption that IKE uses to protect data flowing through the gateway-to-gateway tunnel during phase 2 negotiations. For this example, select **Balance security and performance** as specified on the worksheet.

16. Click **Next**.

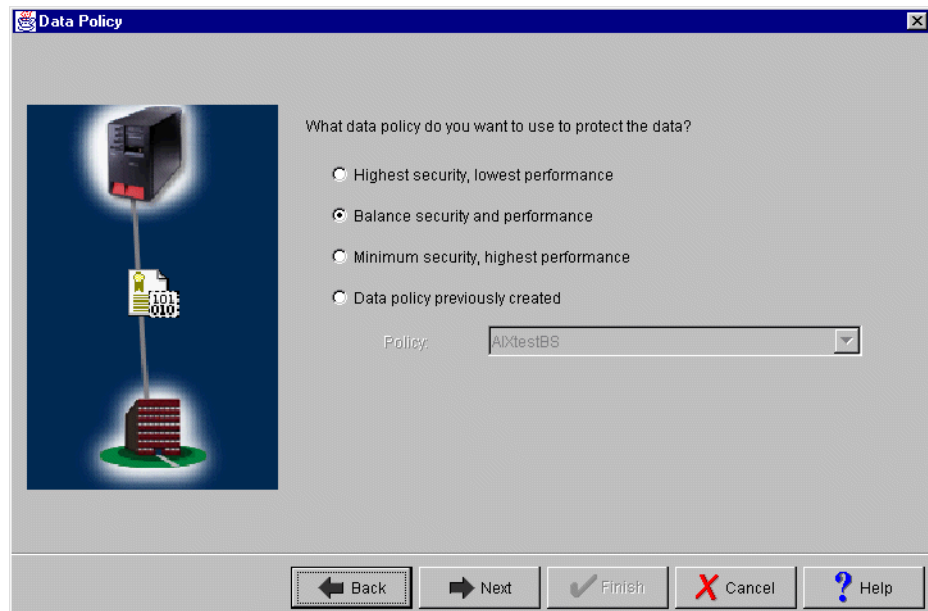


Figure 841. Data Policy window

17. Click **Next**.

18. The final window (Figure 842 on page 750) summarizes the configuration values entered. Scroll down to see a list of the configuration objects that the

wizard will create when you click **Finish**. Check the configuration values against the worksheet. If changes need to be made, click **Back**.

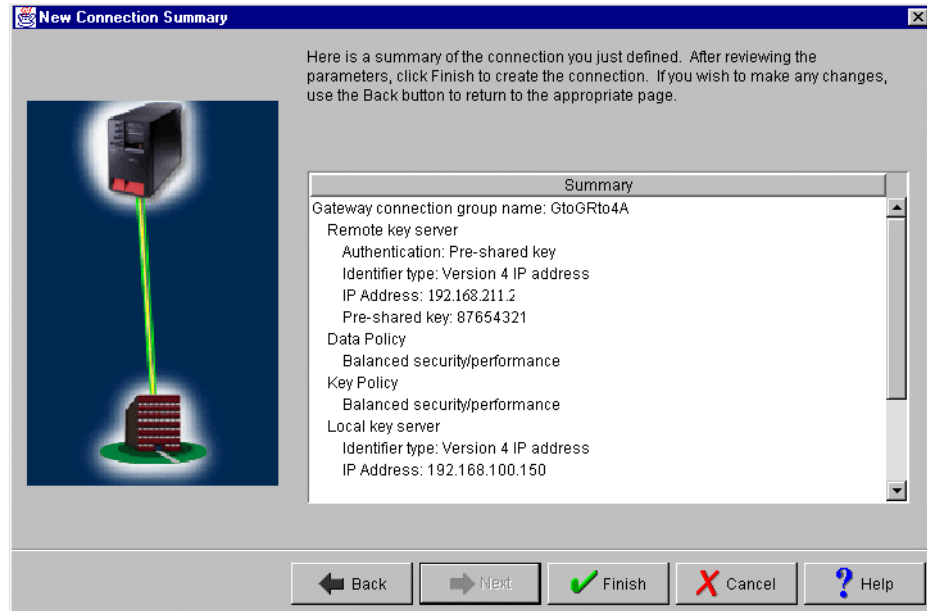


Figure 842. New Connection Summary window RALYAS4A

19. When you are satisfied with the values, click **Finish**.

The wizard creates the various objects that were configured for this VPN connection. After a short delay (and assuming there are no errors), the initial Virtual Private Networking GUI Configuration window (Figure 843) is shown.

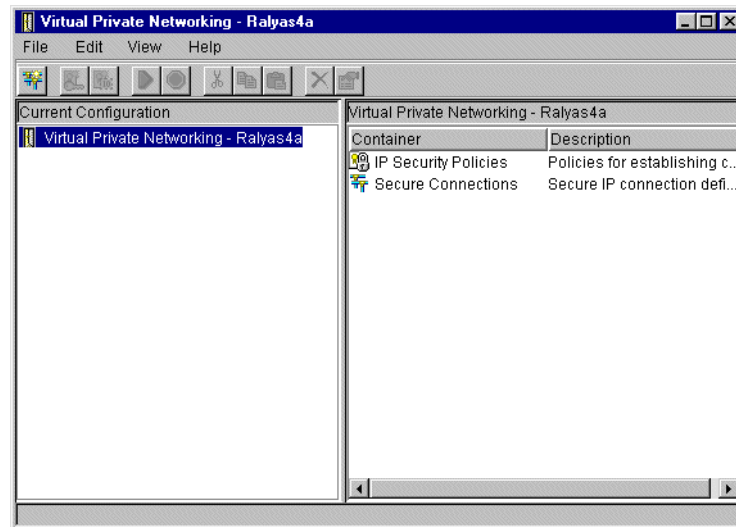


Figure 843. VPN GUI configuration interface

16.3.3 Matching the 2210 router VPN configuration

In this example scenario, use the Virtual Private Networking Configuration GUI to customize the key refresh policies for:

- Key protection
- Data protection

The key refresh policies on the AS/400 system must be consistent with the policy of the router. The Virtual Private Networking New Connection Wizard does not provide the option to allow you to customize the key refresh policies. Refer to 3.6.7, “Key policy (IKE phase 1) and data policy (IKE phase 2) lifetime and size limits” on page 65, for information on how the AS/400 system negotiates key life values.

You can change the VPN GUI default values before the wizard configuration, as explained in 3.7.6, “Changing the Virtual Private Networking GUI default values” on page 76. Or, you can customize the appropriate parameters later as shown in the following steps.

To customize the key refresh policies, follow these steps:

1. Expand all the subfolders on the VPN Configuration GUI interface (Figure 844).

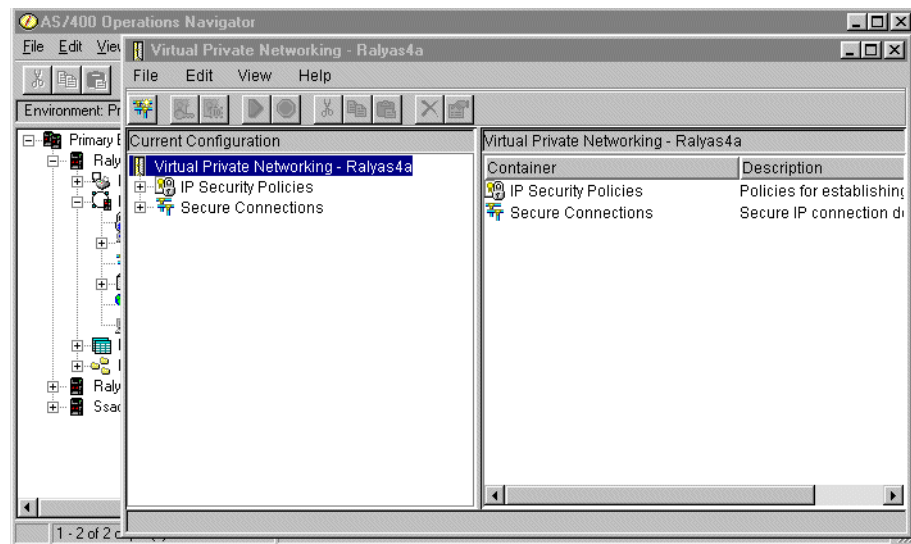


Figure 844. VPN GUI configuration interface

2. Click **Key Policies** to display a list of key policies configured on your system (Figure 845 on page 752). The key policy name is the connection group name that was entered on the wizard, followed by a two-letter suffix. In this example, the suffix is *BS* because *Balanced security and performance* was selected for the key policy. When *Highest security, lowest performance* is selected for the key policy, the suffix is *HS*. Similarly, when *Minimum security, highest performance* is selected, the suffix is *HP*. This is the naming convention that the wizard follows.

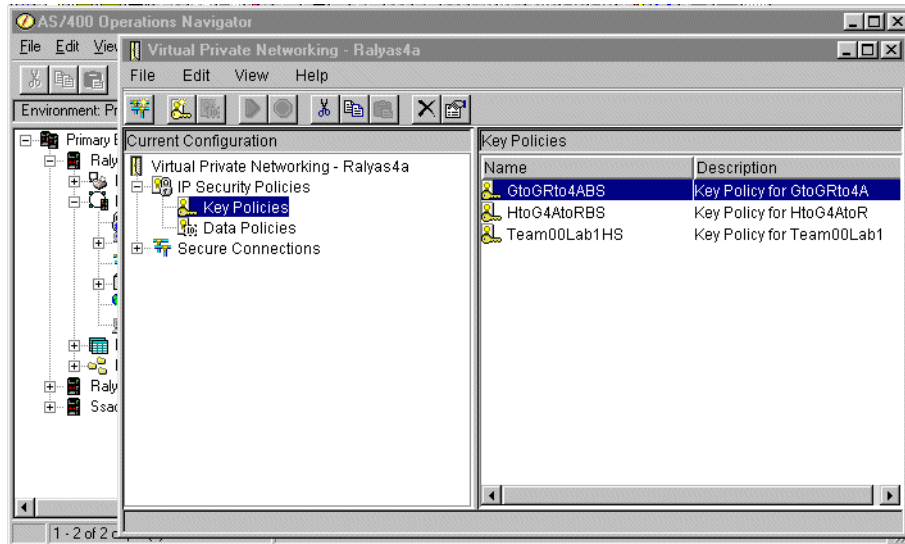


Figure 845. VPN Key Policies

3. Double-click **GtoGRto4ABS** to view the key policy for this connection.
4. At the key policy Properties window, select the **Transforms** tab. Select the key protection transform, and click **Edit** (Figure 846).

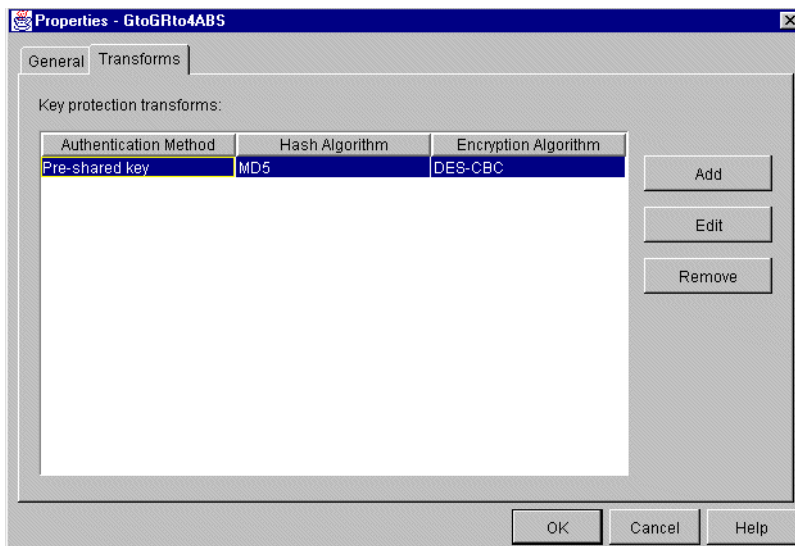


Figure 846. Key policy customization window

5. Set the Maximum key lifetime parameter value to 1440. You must define a Maximum size limit value since it is required by the router configuration. Otherwise, there will be no match. Refer to Figure 847 on page 753.

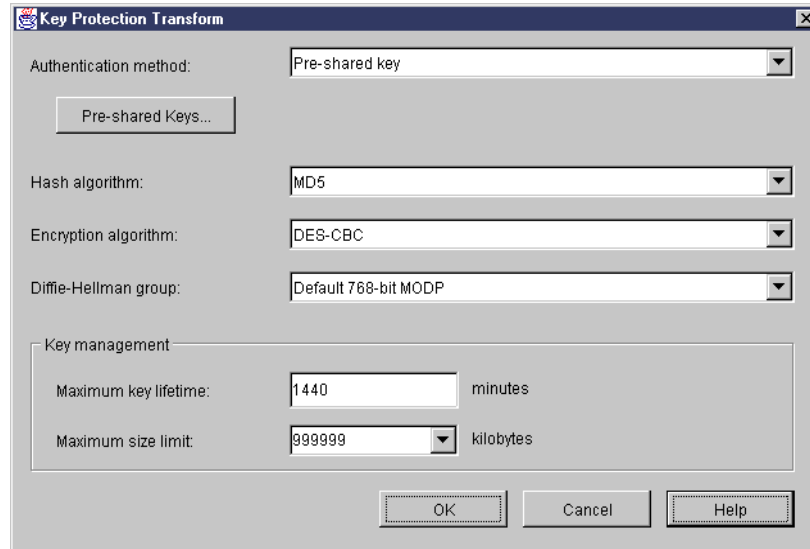


Figure 847. Key Protection Transform window

6. Click **OK**.
7. Back at the key policy customization window (Figure 846 on page 752), click **OK**.
8. Click **Data Policies** to display a list of data policies.
9. Double-click **GtoGRto4ABS** to view the data policy for this connection (Figure 848).

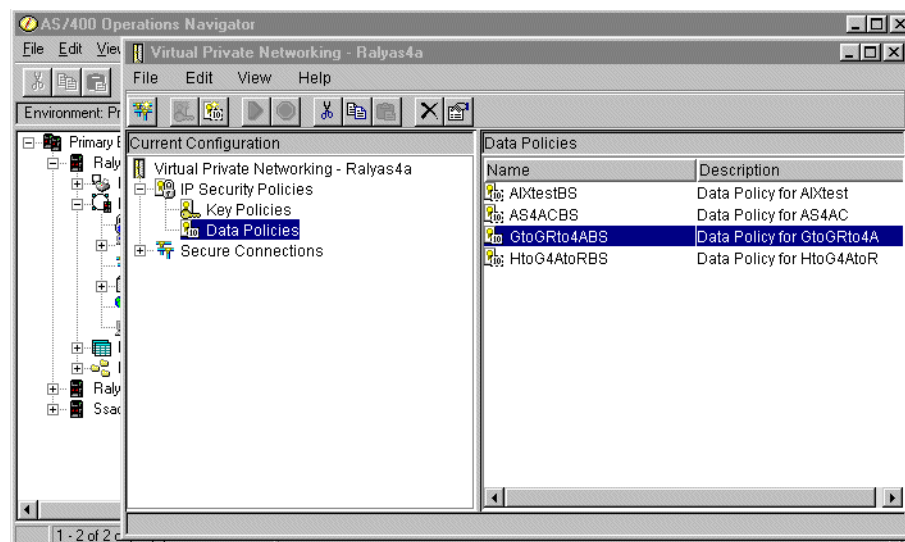


Figure 848. VPN data policies

10. At the data policy Properties window, select the **Proposals** tab (Figure 849 on page 754). Select the data protection proposal that you want to change, and click **Edit**.

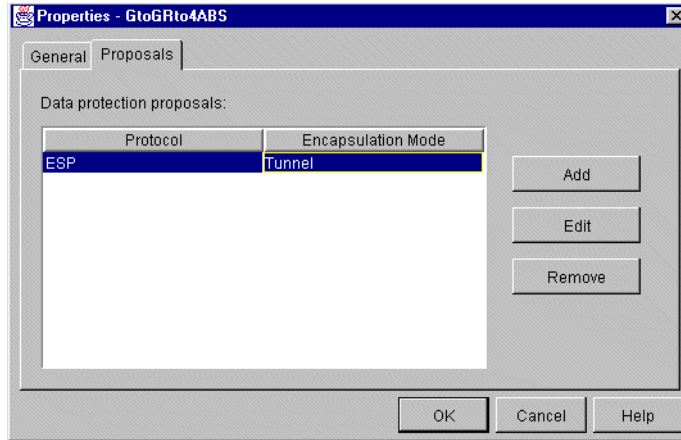


Figure 849. Data policy customization window

- At the Data Protection Proposal window (Figure 850), select the **Key Expiration** tab. Set the Expire after parameter value to 60, and change the Expire at size limit parameter value to 50000.

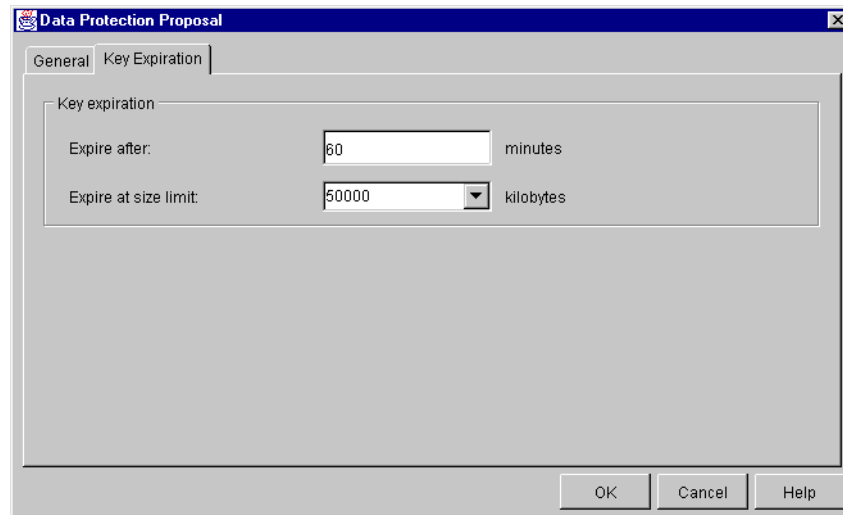


Figure 850. Data protection proposal window

- Click **OK**.
- Back at the data policy properties window (Figure 849), click **OK**.

You have now completed the VPN configuration for RALYAS4A. You configure AS/400 IP filtering in the next task.

16.3.4 Configuring IP filtering on the AS/400 system (RALYAS4A)

The Virtual Private Networking New Connection wizard does *not* configure IP filters. You must configure filter rules to allow IKE negotiation traffic. You must also configure a filter rule with action IPSec and associate it with the connection group created by the wizard. Use IP Packet Security in Operations Navigator to configure filters.

- Configure a defined address for the local subnet that is allowed to use the VPN. The TRUSTED subnet behind the AS/400 gateway is 9.24.106.0, with

subnet mask 255.255.255.0. Refer to the planning worksheet for RALYAS4A in Table 108 on page 743 and to Figure 810 on page 724. Figure 851 shows the defined address for the data center subnet AS4subnets.

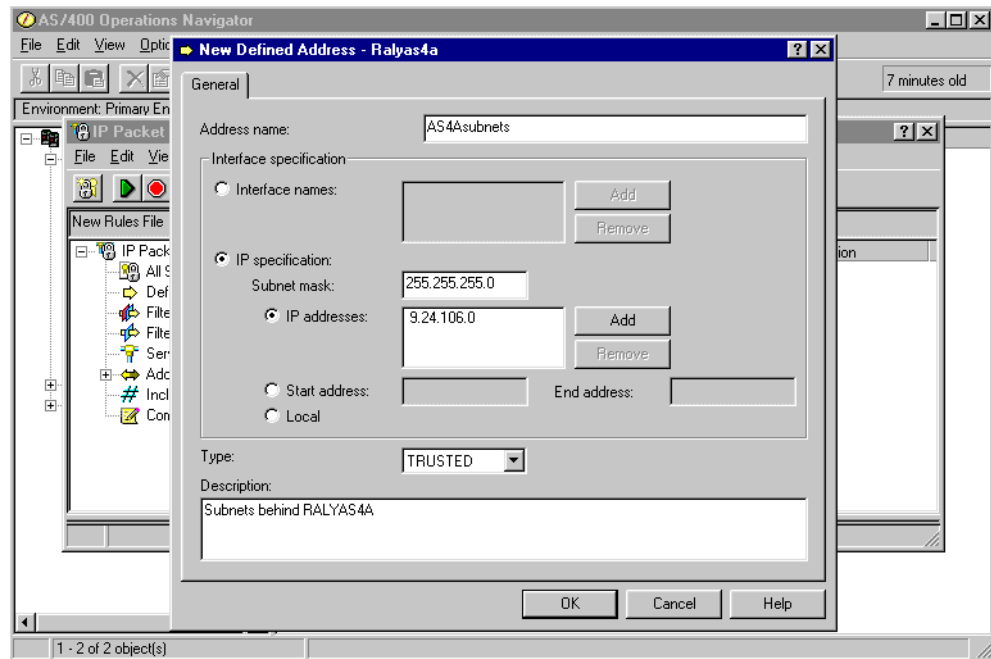


Figure 851. Defined addresses AS4subnets

2. Configure a defined address for the remote subnet that is allowed to use the VPN. The UNTRUSTED subnet behind the 2210 router gateway is 192.168.101.0, with subnet mask 255.255.255.0. Refer to the planning worksheet for RALYAS4A in Table 108 on page 743 and to Figure 810 on page 724. Figure 852 on page 756 shows the defined address for the branch office subnet RTRsubnets.

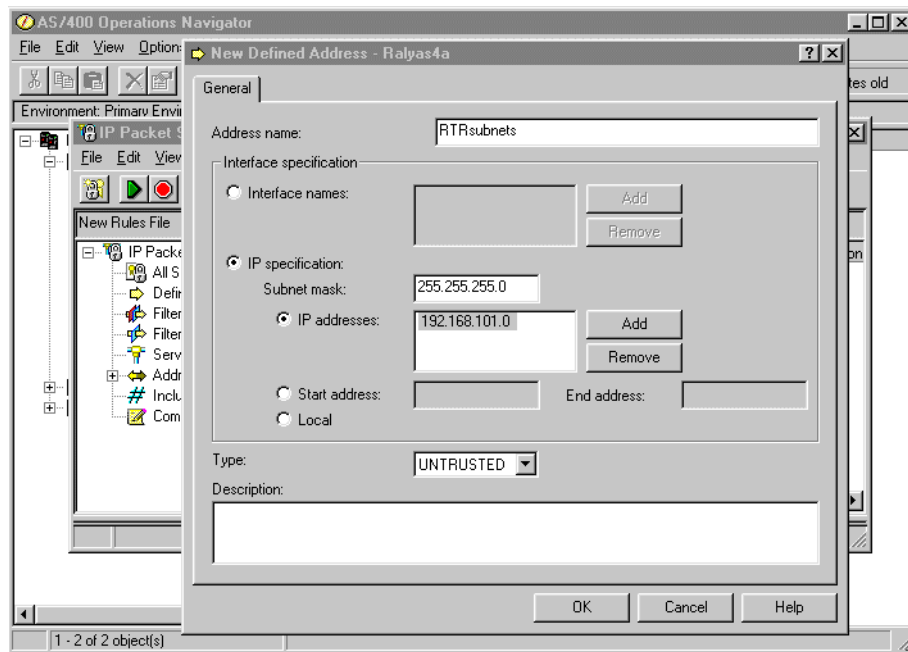


Figure 852. Defined addresses RTRsubnets

3. Create two filters rules to allow IKE traffic to flow into and out of the AS/400 system. All associated filter rules (for example, all rules for one interface) in the filter file should have the same *Set name*. In this example, we use `VPNIFC` as the Set Name.
 - a. For the first filter rule, specify `VPNIFC` for the Set Name parameter. Select **PERMIT** for the Action parameter and **OUTBOUND** for the Direction parameter. The local AS/400 system address, `192.168.100.150`, is the value in the Source address name field. The remote 2210 router address is `192.168.211.2` in the Destination address name field.

Click on the **Services** tab. Select **Service** and **UDP** for the Protocol parameter. Specify `500` for the Source port and Destination port parameters (see Figure 853 and Figure 854 on page 757).

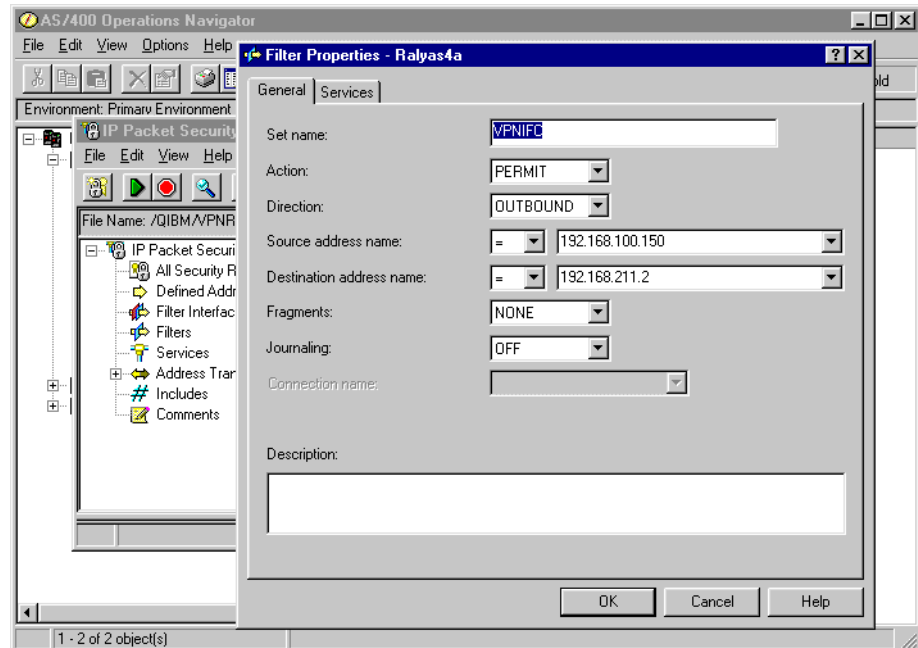


Figure 853. Outbound IKE filter rule

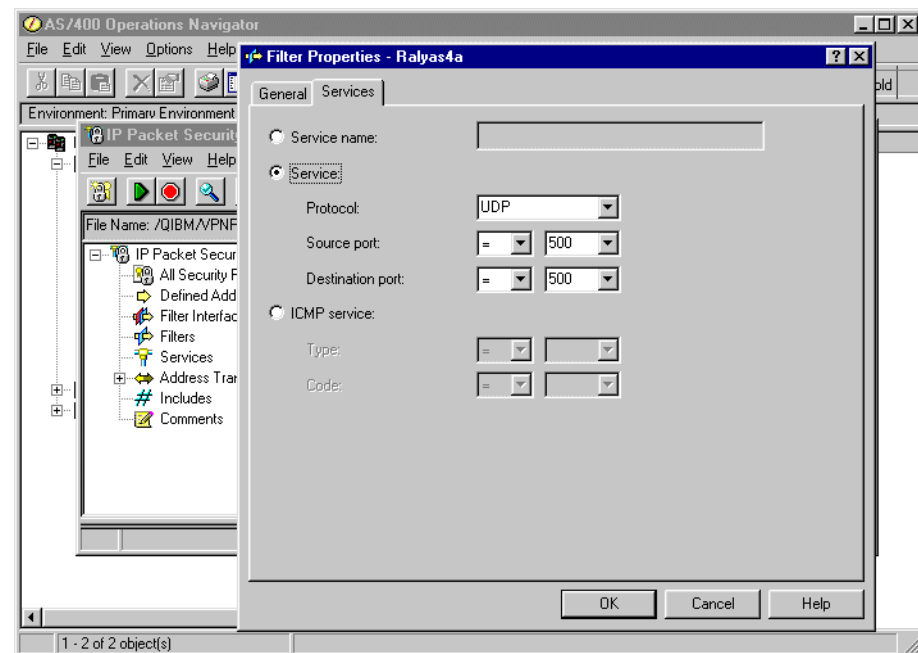


Figure 854. IKE filter rule services

- b. For the second filter rule, specify `VPNIFC` for the Set Name parameter. Select **PERMIT** for the Action parameter and **INBOUND** for the Direction parameter. The remote 2210 router address, `192.168.211.2`, is the value in the Source address name field. The local AS/400 system address is `192.168.100.150` in the Destination address name field.

On the **Services** page, select **Service** and **UDP** for the Protocol parameter. Specify 500 for the Source port and Destination port parameters (Figure 855 and Figure 856).

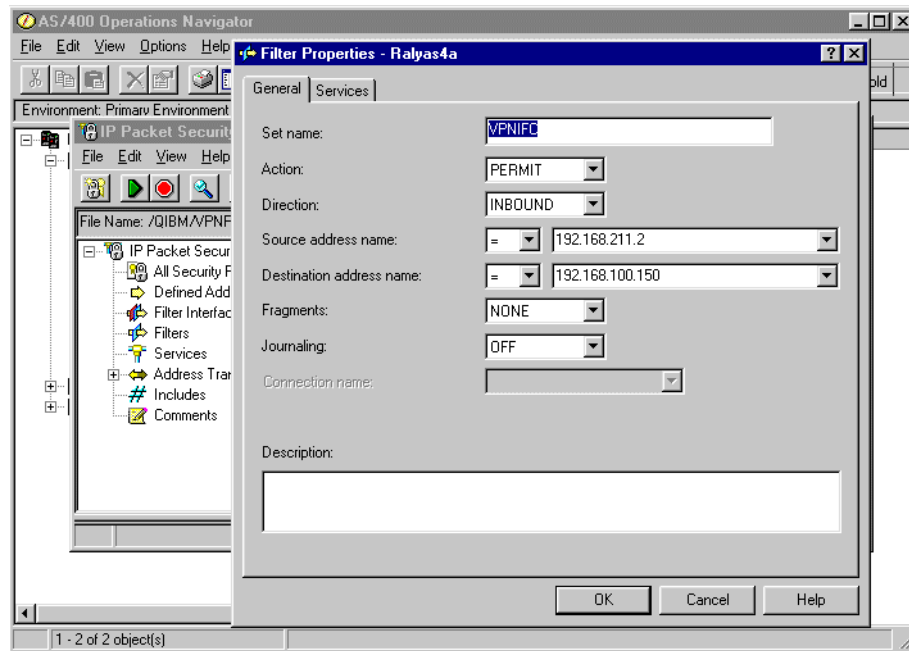


Figure 855. Inbound IKE filter rule

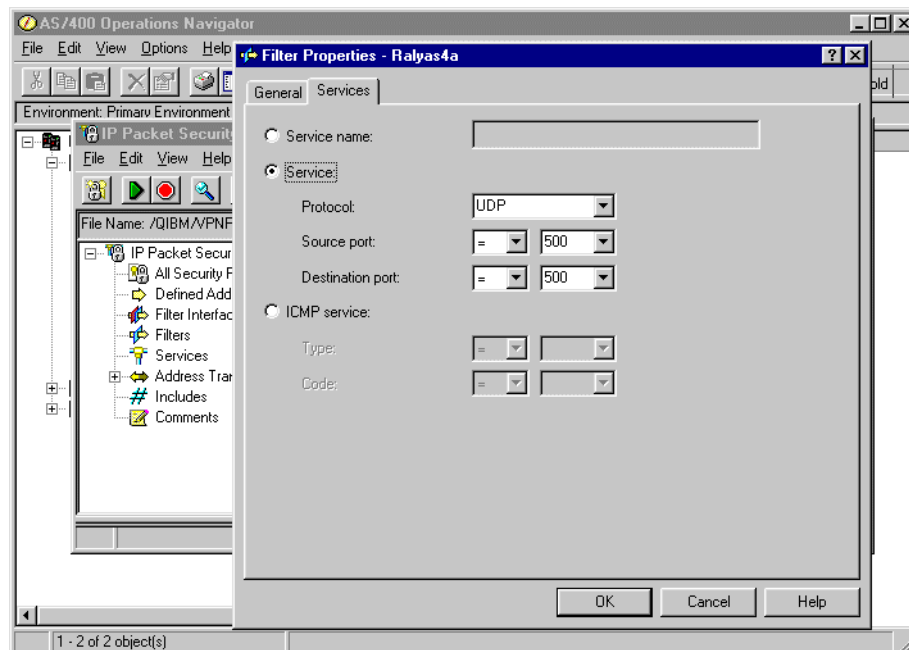


Figure 856. IKE filter rule services

4. Create a filter rule with action IPSEC to define the data endpoints that use the secure tunnel.

Use the same filter set name, which is `VPNIFC`. Action is IPsec. Direction is always set to OUTBOUND and grayed out. The corresponding INBOUND

IPSEC rule is created implicitly. Specify **AS4subnets** for the Source address name parameter. The Destination address name is **RTRsubnets**. Both names correspond to the defined addresses created earlier in this section. The Connection name is, in fact, the data connection, which, in this case, is a dynamic key connection group. Use the pull-down list to see all the data connections configured in your system and select one of them. In this scenario, select **GtoG4AtoR** (Figure 857).

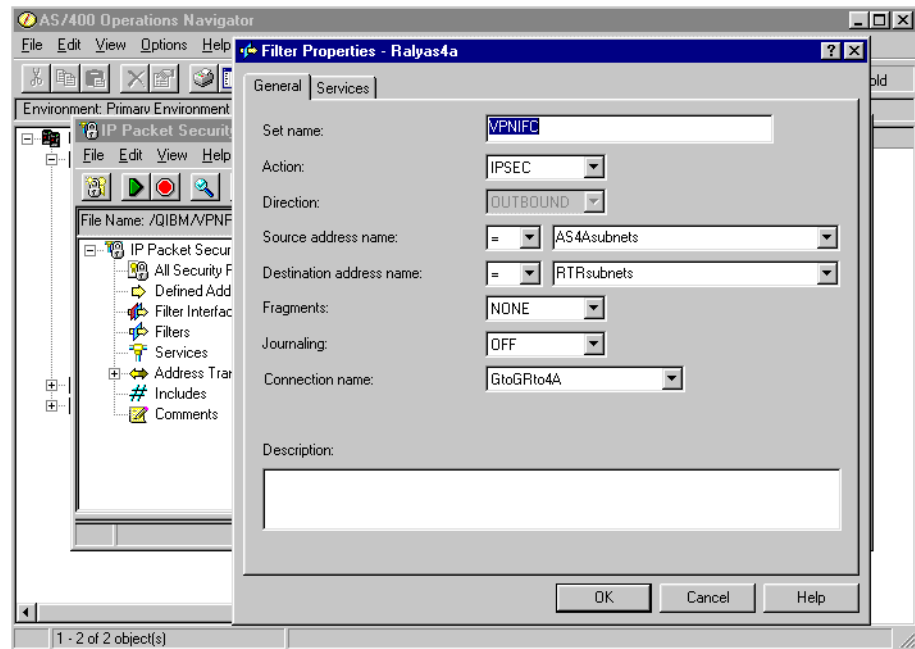


Figure 857. IPSEC filter rule

5. Select the **Services** tab to specify the protocols and ports allowed in the tunnel. In this scenario, select wildcard (*) for the Protocol, Source port and Destination port fields. This allows any protocol using any port through the secure tunnel. See Figure 858 on page 760.

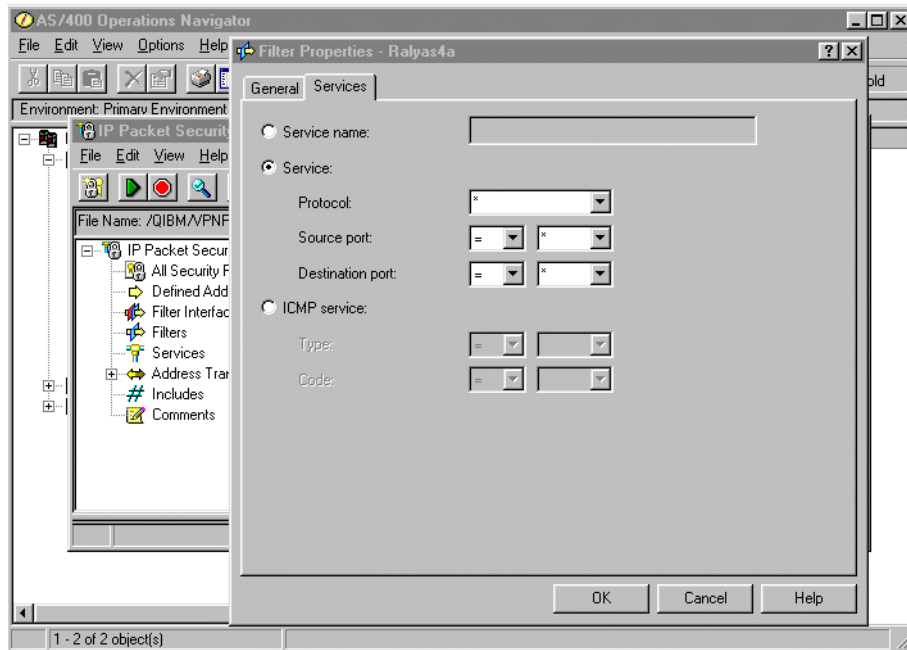


Figure 858. IPSEC filter rule service

6. Create a Filter Interface to tie the filter rules grouped by the VPNIFC set to the appropriate interface. The line description that connects the AS/400 system to the remote 2210 router VPN gateway is TOKENRING2. Associate the VPNIFC set to the TOKENRING2 line as shown in Figure 859.

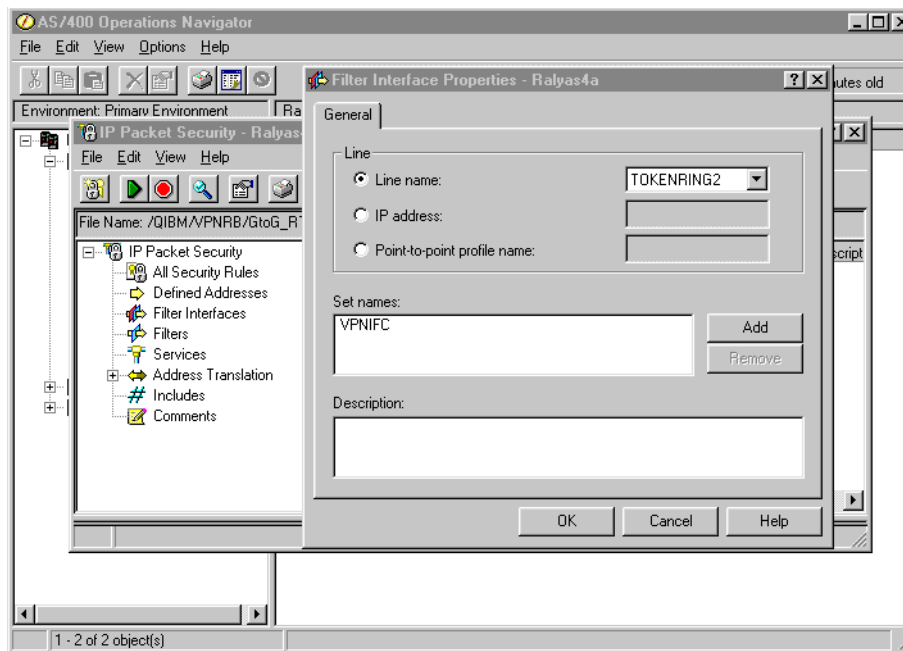


Figure 859. Filter interface rule

7. Save the filter file in the IFS. In our scenario, we created a subdirectory, VPNRB, under the directory QIBM. We saved the filter file in /QIBM/VPNRB/GtoG_AStoRTR.i3p.

Figure 860 shows the summary of the IP filters configured for this scenario.

```
#Internal subnet
ADDRESS AS4Asubnets IP = 9.24.106.0 MASK = 255.255.255.0 TYPE = TRUSTED
#Remote subnet
ADDRESS RTRsubnets IP = 192.168.101.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
#IKE negotiation
FILTER SET VPNIFC ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 192.168.100.150
DSTADDR = 192.168.211.2 PROTOCOL = UDP
DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF

FILTER SET VPNIFC ACTION = PERMIT DIRECTION = INBOUND
SRCADDR = 192.168.211.2 DSTADDR = 192.168.100.150 PROTOCOL = UDP
DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC rule
FILTER SET VPNIFC ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS4Asubnets
DSTADDR = RTRsubnets PROTOCOL = * DSTPORT = * SRCPORT = *
FRAGMENTS = NONE JRN = OFF CONNECTION_DEFINITION = GtoGRto4A
#Filter interface
FILTER_INTERFACE LINE = TOKENRING2 SET = VPNIFC
```

Figure 860. RALYAS4A IP filter summary

16.4 VPN configuration cross-reference table: AS/400 to 2210 router

Table 109 summarizes the AS/400 system and 2210 router configuration and provides a cross-reference list.

Table 109. AS/400 and 2210 router VPN configuration cross reference table

<u>AS/400</u>	<u>ROUTER</u>
Key Policy	
Name = GtoGRto4ABS	(1) (2) ISAKMP-Action
Initiator Negotiation = Aggressive Mode	(3) Mode = Aggressive
Responder Negotiation = Aggressive Mode only	Autostart = N
Key Protection Transforms	
Authentication Method = Pre-shared key	(3) ISAKMP-Proposal
Pre-shared key value = 87654321	(9) AuthMethod = Pre-shared key
Hash Algorithm = MD5	(8) LifeSize = Nomax
Encryption Algorithm = DES-CBC	(7) LifeTime = 86400
Diffie-Hellman Group = Default 768-bit MODP	(5) DHGroupID = 1
Key Management	(6) Hash Algorithm = MD5
Maximum key lifetime (minutes) = 1440	(6) Encryption Algorithm = DES
Maximum size limit (kilobytes) = No size limit	
	(18) IPSEC Action
	(20) Tunnel Start = 192.168.211.2
	Tunnel End = 192.168.100.150
	Tunnel-in-Tunnel = N
	Autostart = N
	Replay Prevention = N
Data Policy	
Name = GtoGRto4ABS	
Use Diffie-Hellman Perfect Forward Secrecy = No	(31) IPSEC Proposal
Diffie-Hellman Group = Not Applicable	Diffie-Hellman Perfect Forward Secrecy = N
Data Protection Proposals	
Encapsulation mode = Tunnel	(11) IPSEC Transform
Protocol = ESP	(12) Type = IPsecESP
Algorithms	(11) Mode = Tunnel
Authentication Algorithm =	(16) LifeSize = 50000
HMAC-MD5	(15) LifeTime = 3600
Encryption Algorithm = DES-CBC	(13) Authentication Algorithm = HMAC-MD5
Key Expiration	(14) Cipher Algorithm = ESP DES
Expire after (minutes) = 60	
Expire at size limit (kilobytes) = 50000	
	(21) Validity Period
	Life Time = Always
Key Connection Group	
Name = GtoGRto4A	
Remote Key Server	
Identifier Type = Version 4 IP address	(17) User
IP address = 192.168.211.2	(20) Name = 192.168.100.150
Local Key Server	(19) Type = IPV4 address
Identifier Type = Version 4 IP address	(3) Authentication Mode = Pre-shared key
IP address = 192.168.100.150	Key Mode = ASCII
Key Policy = GtoGRto4ABS	(4) Pre-shared key = 87654321
Dynamic Key Group	
Name = GtoGRto4A	
System Role = Both systems are gateways	(23)(27) Policy Profile
Initiation = Either systems can initiate the connection	(22)(27) Source Address = 192.168.101.0
Policy	Source Mask = 255.255.255.0
Data Management Security Policy =	Destination Address Format = NetMask
GtoGRto4ABS	(25)(26) Destination Address = 9.24.106.0
Connection Lifetime = Never Expires	(24)(26) Destination Mask = 255.255.255.0
Local addresses = Filter rule	(28) Protocol to filter = All Protocols
Local ports = Filter rule	(30) Source Ports = 0 - 65535
Remote addresses = Filter rule	(29) Destination Ports = 0 - 65535
Remote ports = Filter rule	(17) Local Identifier Type = IPV4 address
Protocol = Filter rule	
Dynamic Key Connection	
Name = GtoGRto4A:L1	
Key Connection Group = GtoGRto4ABS	
Start when TCP/IP is started? = No	
IP Filters	
Name = GtoG_RTtoAS.I3P	
Defined Addresses = RTsubnets	
Subnet mask = 255.255.255.0	(22)
IP addresses = 192.168.101.0	(23)
Defined Addresses = AS4subnets	
Subnet mask = 255.255.255.0	(24)
IP addresses = 9.24.106.0	(25)
IPSEC rule	
Source address name = AS4subnets	(26)
Destination address name = RTsubnets	(27)
Connection Name = GtoGRto4A	
Services	
Protocol = *	(28)
Source port = *	(29)
Destination port = *	(30)

16.5 Starting the VPN connections and final verification

This section describes how to start the connection at both ends of the tunnel and perform the final verification test. For detailed information about starting the VPN connection refer to Chapter 4, "AS/400 IP filtering overview" on page 103.

16.5.1 Starting the VPN connection on the AS/400 system

To start the VPN connection on the AS/400 system, perform the following steps:

1. Start filters.
2. Start Virtual Private Networking.
3. Open **Virtual Private Networking**.
4. Right-click the **GtoGRto4A:L1** connection in the right panel, and select **Start** to initiate a VPN connection to the 2210 route (Figure 861).

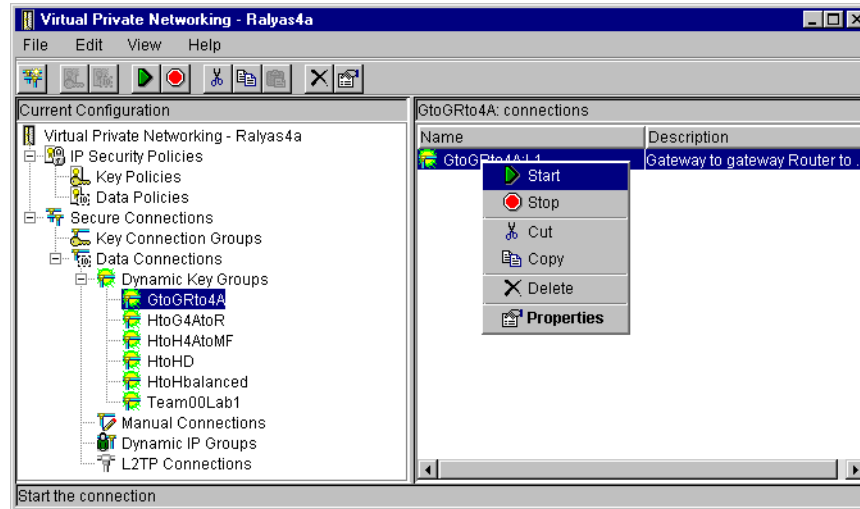


Figure 861. Starting the host-to-gateway connection - GtoGRto4A

5. Display the connection to verify that it is active. At the Virtual Private Networking window, select **View->Active Connections** as shown in Figure 862.

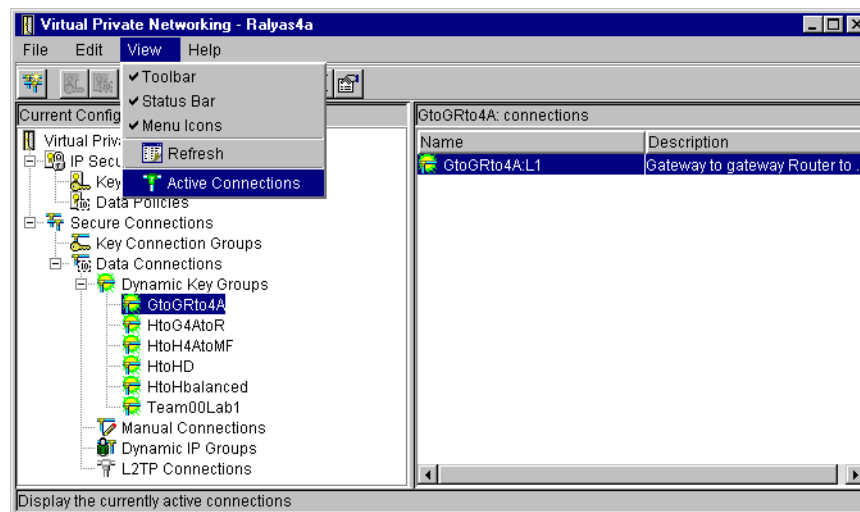


Figure 862. Starting the Active Connections window

The active connections window is shown in Figure 863 on page 764.

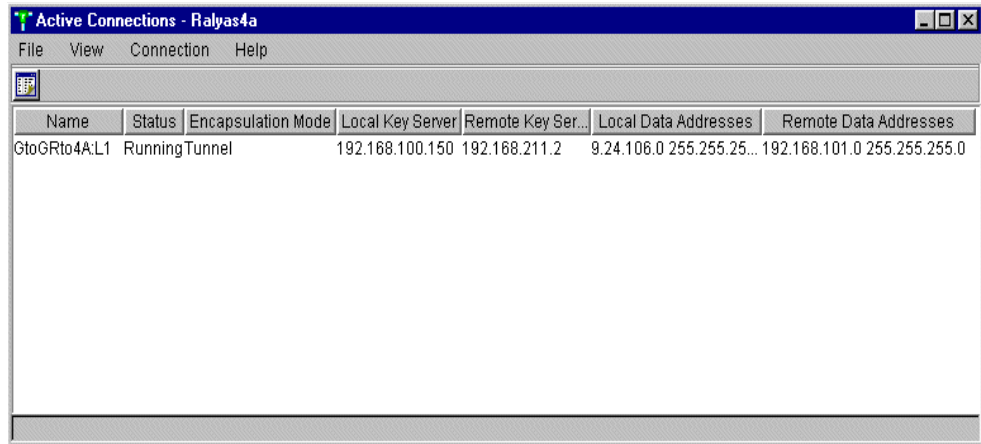


Figure 863. Active Connections window

- Use the 2210 router console to verify that the VPN connection is successfully established. Figure 864 shows the IPSEC section in the 2210 router.

```
Branch +FEATURE IPsec
Branch IPSP>IPV4
Branch IPV4-IPsec>LIST ALL

IPsec is ENABLED

IPsec Path MTU Aging Timer is 0 minutes

Defined Tunnels for IPv4:
-----
  ID      Type      Local IP Addr  Remote IP Addr  Mode   State
-----
   1     ISAKMP    192.168.211.2  192.168.100.150 TUNN   Enabled

Tunnel Cache for IPv4:
-----
  ID      Local IP Addr  Remote IP Addr  Mode   Policy  Tunnel Expiration
-----
   1     192.168.211.2  192.168.100.150 TUNN   ESP     none
```

Figure 864. Verifying the VPN connection status on the 2210 router

- Use the 2210 router console `STATS` command to display the VPN tunnel traffic statistics (Figure 865 on page 765).

```

Branch IPV4-IPsec>STATS all

Global IPsec Statistics

Received:
total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
-----
          12           0           12         4736       2386       2386

Sent:
total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
-----
          19           0           19         1632         0         1632

Receive Packet Errors:
total errs  AH errors  AH bad seq  ESP errors  ESP bad seq
-----
          0           0           0           0           0

Send Packet Errors:
total errs  AH errors  ESP errors  Exceed MTU
-----
          0           0           0           0

```

Figure 865. Displaying the VPN tunnel traffic statistics on the 2210 router

- Switch to the IKE section of the IBM 2210 console (Figure 866). Verify the security association established through IKE. The information provided includes the type of authentication using pre-shared keys, mode, peer IP address, and the current state.

```

Branch IPSP>IKE
Branch IKE>LIST ALL

Phase 1 ISAKMP Tunnels for IPv4:
-----
Peer Address  I/R  Mode  Auto  State      Auth
-----
192.168.100.150  R  Aggr  Y   QM_IDLE    pre-shared

```

Figure 866. Checking the IKE status on the 2210 router

- Use the `STATS all` command to view the number of bytes and packets that are involved in the IKE negotiation.

```

Branch IKE>STATS all
Peer address [192.168.100.150?

Peer IP address.....: 192.168.100.150
Active time (secs)...: 2043

In      Out
---    ---
Octets.....: 468      408
Packets.....: 4        2
Drop pkts.....: 0        0
Notifys.....: 0        0
Deletes.....: 0        0
Phase 2 Proposals....: 1        1
Invalid Proposals....: 0        0
Rejected Proposals...: 0        0

```

Figure 867. Checking the IKE statistics on the 2210 router

10. Use the `LIST STATS` command, as shown in Figure 868, to display a set of filter rules created implicitly as part of the policy when you configure the IPSEC action.

```

Branch +FEATURE Policy
IP Network Policy console
Branch Policy console>LIST STATS
+-----+
|Name                                     |Hits  |
+-----+
|ike-pre-101-to-106.plin                 | 2    |
|   ike-6                               (ISAKMP) | 2    |
+-----+
|ike-pre-101-to-106.p2in                 | 1    |
|                                     tun-16 (IPSEC) | 39   |
+-----+
|ike-pre-101-to-106.traffic              | 19   |
|                                     tun-16 (IPSEC) | 39   |
+-----+
|ike-pre-101-to-106.inBoundTunnel        | 12   |
|               ipsecPermitIfInboundTunnel (IPSEC) | 12   |
+-----+

```

Figure 868. Checking the policy statistics on the 2210 router

11. The event logging system (ELS) displays the dynamic key negotiation steps. First, we set the event filters. With `TALK 2`, we start the event logging. The event logging can be stopped by using `CTRL+P`.

```

Branch *TALK 5
Branch +
Branch +EVENT
Event Logging System user console
Branch ELS >NODISPLAY SUBSYSTEM all all
Branch ELS >DISPLAY SUBSYSTEM ike all
Branch ELS >CTRL-P
Branch *TALK 2

```

Figure 869. Setting the event filters on the 2210 router

Figure 870 shows the output of the event logging system. To terminate event logging, press **CTRL+P**.

```
00:29:46 IKE.001: Trace IKE packet from 192.168.100.150
00:29:46 IKE.013: From Peer: 192.168.100.150 AG HDR SA KE NONCE ID
00:29:46 IKE.009: Begin Aggressive mode - Responder
00:29:49 IKE.014: Oakley proposal is acceptable. Peer: 192.168.100.150
00:29:49 IKE.003: Processing ISA_KE
00:29:52 IKE.003: Processing NONCE
00:29:52 IKE.013: To Peer: 192.168.100.150 AG HDR SA KE NONCE ID HASH
00:29:52 IKE.001: Trace IKE packet to 192.168.100.150
00:29:52 IKE.001: Trace IKE packet from 192.168.100.150
00:29:52 IKE.011: isakmp_input: drop incoming retransmitted message
00:29:52 IKE.001: Trace IKE packet from 192.168.100.150
00:29:52 IKE.014: Received unencr packet when crypto act, Peer: 192.168.100.150
00:29:52 IKE.013: From Peer: 192.168.100.150 AG HDR* HASH
00:29:52 IKE.010: Finished Aggressive mode -responder
00:29:53 IKE.001: Trace IKE packet from 192.168.100.150
00:29:53 IKE.009: Begin Quick mode - Responder
00:29:53 IKE.002: Trace IKE payload after decryption from Peer: 192.168.100.150
00:29:53 IKE.013: From Peer: 192.168.100.150 QM HDR* HASH SA NONCE ID ID
00:29:53 IKE.003: Processing Quick Mode ID
00:29:53 IKE.003: Processing Quick Mode ID
00:29:53 IKE.015: Acceptable phase 2 proposal # 1
00:29:53 IKE.003: Processing NONCE
00:29:53 IKE.013: To Peer: 192.168.100.150 QM HDR* HASH SA NONCE ID ID
00:29:53 IKE.002: Trace IKE payload before encryption to Peer: 192.168.100.150
00:29:53 IKE.001: Trace IKE packet to 192.168.100.150
00:29:53 IKE.001: Trace IKE packet from 192.168.100.150
00:29:53 IKE.002: Trace IKE payload after decryption from Peer: 192.168.100.150
00:29:53 IKE.013: From Peer: 192.168.100.150 QM HDR* HASH
00:29:53 IKE.008: Load Out SA: Alg=18 Prot=3 Sec=86400 KB=50000 SPI=3153885377
00:29:53 IKE.008: Load In SA: Alg=18 Prot=3 Sec=86400 KB=50000 SPI=1272503440
```

Figure 870. Event logging system screen

16.5.1.1 2210 router tips

This section offers several helpful tips for working with the 2210 router:

- IP filtering conflicts

A 2210 router policy must be enabled to be used for VPN connections. The 2210 router policy definitions include IP filters. These IP filters are activated when the policy is enabled. This is regardless of whether the policy is in use for a VPN connection. The policy should be disabled if it is not used. This will avoid potential problems caused by the policy's IP filters.

- Main or aggressive mode negotiation

The 2210 IKE negotiation mode (main or aggressive) is defined within the ISAKMP action. The 2210 IKE negotiation mode is used regardless of whether the 2210 router is a connection initiator or a connection responder. The 2210 router negotiation mode has to match the equivalent parameter defined at the remote VPN partner. As a responder, the 2210 router is not able to negotiate the mode as compared with the AS/400 system.

- 2210 router as a connection initiator

The 2210 router can only be a connection initiator if it is configured to autostart the VPN connection at system initialization. The 2210 router system initialization means restarting the configuration or reloading the router code. If

the router is not configured to autostart the VPN connection at system initialization, it acts as a VPN connection responder. There is no manual method available to make the router a VPN connection initiator other than to configure the router to autostart the VPN connection at system initialization.

16.5.2 Verification tests

Table 110 presents a summary of the verification tests run after the gateway-to-gateway VPN was configured and the connection started. The tests verify the scenario objectives stated in 16.1.2, “Scenario objectives” on page 724.

Table 110. Verification test - OS/400 to 2210 router gateway-to-gateway scenario

	TELNET	FTP	PING
From AS4Asubnets to RTRsubnet hosts	Yes	Yes	Yes
From RTRsubnet hosts to RALYAS4A	Yes	Yes	Yes

Note: AS4subnets represents hosts in the data center network behind the AS/400 system. RTRsubnet represents hosts in the branch office network behind the router.

Chapter 17. Host-to-host VPN: AS/400 to AIX server

This chapter describes a VPN host-to-host configuration between an AS/400 system and an AIX server.

17.1 Business partners VPN connection (host-to-host AS/400 to AIX)

In this scenario, we present two business partners that need to access each other's servers over the Internet. Not only do they want the data to flow securely over the public network, but they do not fully trust each other's private networks. Therefore, they want to ensure the connection is protected by IPSec protocols to the hosts that they want to connect. Figure 871 represents this scenario.

17.1.1 Scenario characteristics

The characteristics of this scenario are:

- Both the distributor and the manufacturer networks belong to different companies. Therefore, the secure tunnel must start and end at the data endpoints.
- Both networks are connected to the Internet through routers and firewalls.

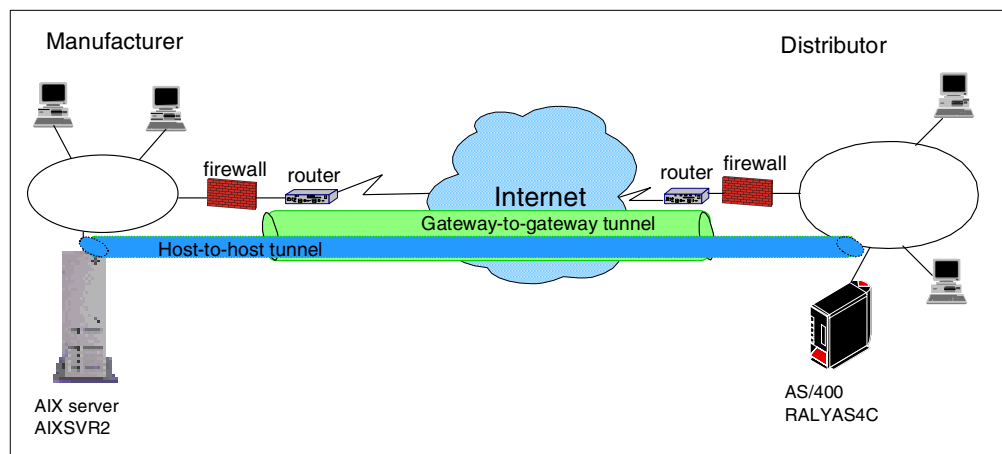


Figure 871. Business partners VPN - Host-to-host AS/400 system to AIX server

Note

Unlike the branch office scenarios, where we can assume that a consistent addressing plan is implemented across the company's intranets, in a business-to-business scenario, you need to consider addressing issues. Business partners implement an addressing scheme independently of one another. In this case, it is possible that both companies use private (globally ambiguous) IP addresses in their networks, and that some of those addresses overlap. In this case, conventional routing protocols will not be able to resolve these ambiguities.

In the host-to-host scenarios that apply to intercompany VPNs, we assume that one or more of the following techniques is used to resolve addressing problems:

- The systems have been assigned unique globally routable IP addresses. Even if the systems are assigned globally routable addresses, they most likely will not have connectivity since their networks may be protected by firewalls. In this case, a tunnel solution, similar to the one described in Figure 871 on page 769 solves the problem.
- If the systems are assigned private IP addresses, they don't overlap.
- If the systems are assigned private IP addresses, a tunneling protocol is used between the gateways that connect both companies' networks to the intervening network (for example, the Internet). In this context, the gateways are firewalls, routers, or any other appliance. Some possible mechanisms include Frame Relay, MPLS, IPSec, L2TP, L2F, PPTP. It is important to note that the gateway-to-gateway tunnel between the firewalls or routers is totally transparent to the host-to-host configuration, such as the one shown in this chapter.

The AS/400 VPN implementation includes an AS/400-unique solution to the addressing issues, called *VPNAT*. Refer to Chapter 13, "VPN Network Address Translation (VPN NAT)" on page 551, for more information.

17.1.2 Scenario objectives

The objectives of this scenario are:

- All traffic between RALYAS4C and AIXSVR2 must be protected by IPSec.
- Only AIXSVR2 in the manufacturer's network can access RALYAS4C in the distributor's network and vice versa.
- Only Telnet from the distributor (RALYAS4C) to the manufacturer (AIXSVR2) is allowed over the VPN.
- Only the distributor (RALYAS4C) is allowed to initiate the VPN connection.

17.1.3 Scenario network configuration

Figure 872 on page 771 shows our simple network configuration for the host-to-host AS/400 system to AIX server.

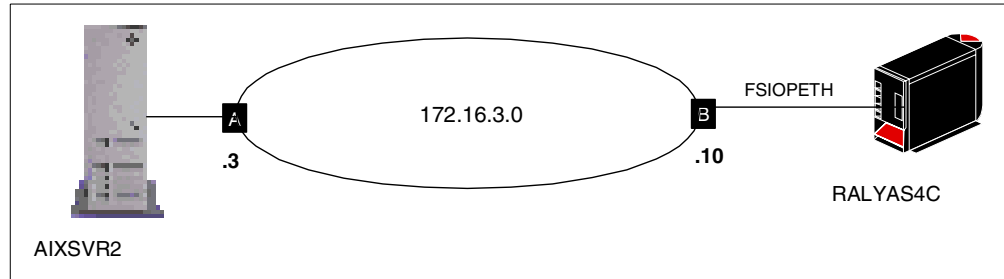


Figure 872. Host-to-host AS/400 to AIX - Scenario network configuration

17.1.4 AIX software

VPN support is included in AIX V4.3.2 (5765-C34) with the latest available PTFs.

17.1.5 Implementation tasks: Summary

The following process summarizes the tasks used to implement this VPN gateway-to-gateway environment:

1. Verify connectivity. Before you start configuring VPN and filters, you must be sure that the underlying TCP/IP network is properly configured and working.
2. Complete planning worksheet for the AIX server.
3. Configure a host-to-host VPN in the AIX server.
4. Complete the planning worksheet for the AS/400 system.
5. Configure a host-to-host VPN in the AS/400 system.
6. Configure filters in the AS/400 system.
7. Start the VPN connection.
8. Perform verification tests.

17.1.6 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the two hosts is correct. A simple PING command accomplishes this task:

```
PING RMTSYS('172.16.3.3') LCLINTNETA('171.16.3.10')
```

17.2 AIX VPN configuration

The following sections explain how to configure the tunnel in the AIX server to establish a VPN with the AS/400 system RALYAS4C. It is beyond the scope of this redbook to provide detailed information about AIX server configuration. Refer to *A Comprehensive Guide to Virtual Private Networks, Vol III: IBM Cross-Platform and Key Management Solutions*, SG24-5309, for more information about AIX VPN configuration.

17.2.1 Completing the AIX server planning worksheet

Complete the AIX planning worksheet as shown in Table 111 on page 772. The planning worksheet allows you to gather all the configuration data before the

actual implementation. In this scenario, we completed this planning worksheet from the perspective of AIXSVR2.

Table 111. AIX planning worksheet - Internet Key Exchange (IKE) tunnels configuration

Information you need to configure VPN in the AIX server		Scenario answers
Key server host name		AIXSVR2
IP address		172.16.3.3
Role		Responder
Key Management Tunnel (Phase 1)		
Mode		Main
Encryption		DES
Authentication algorithm		MD5
Key exchange group		1
Key lifetime		28800 sec (default)
Negotiation ID		IP address
Pre-shared key		3132333435363738 (HEX of 12345678)
Data Management Tunnel (Phase 2)		
Security Protocols		
<input type="checkbox"/>	AH (Authentication)	
<input checked="" type="checkbox"/>	ESP (Encryption)	DES
<input checked="" type="checkbox"/>	ESP (Authentication)	MD5
Encapsulation mode		Transport
Perfect Forward Secrecy (PFS)		No
Tunnel lifetime		30 min

17.2.2 Configuring a host-to-host VPN in the AIX server

Perform the following steps to configure a host-to-host VPN on AIXSRV2 using the Web System Management tool:

1. Start the Web System Management tool.
2. Double-click the **Network** icon.
3. Right-click **Internet Key Exchange (IKE) Tunnels**, and select **Start IP Security** from the pull-down menu to enable IPSec.
4. Double-click **Internet Key Exchange (IKE) Tunnels** on the Network panel (Figure 873 on page 773) to open the Internet Key Management (IKE) Tunnel configuration panel.

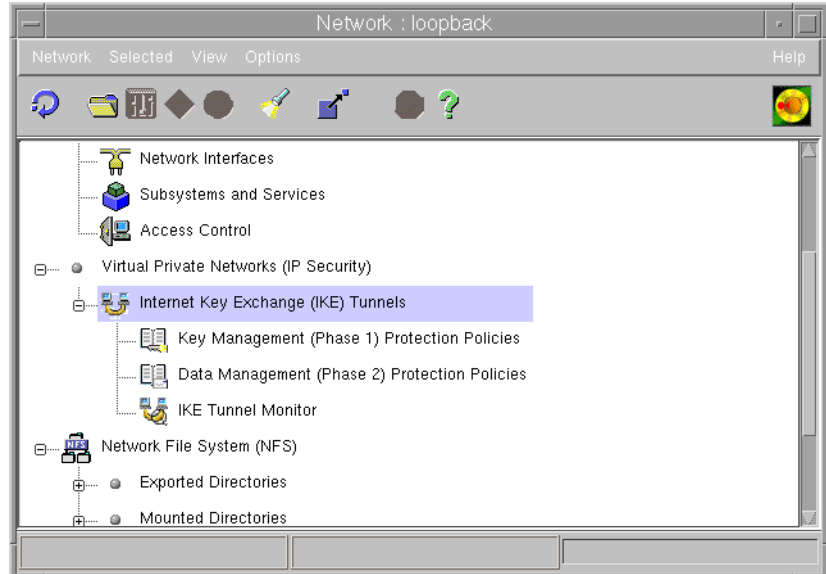


Figure 873. Network panel - VPN menu

The Internet Key Exchange (IKE) Tunnels configuration panel is displayed (Figure 874).

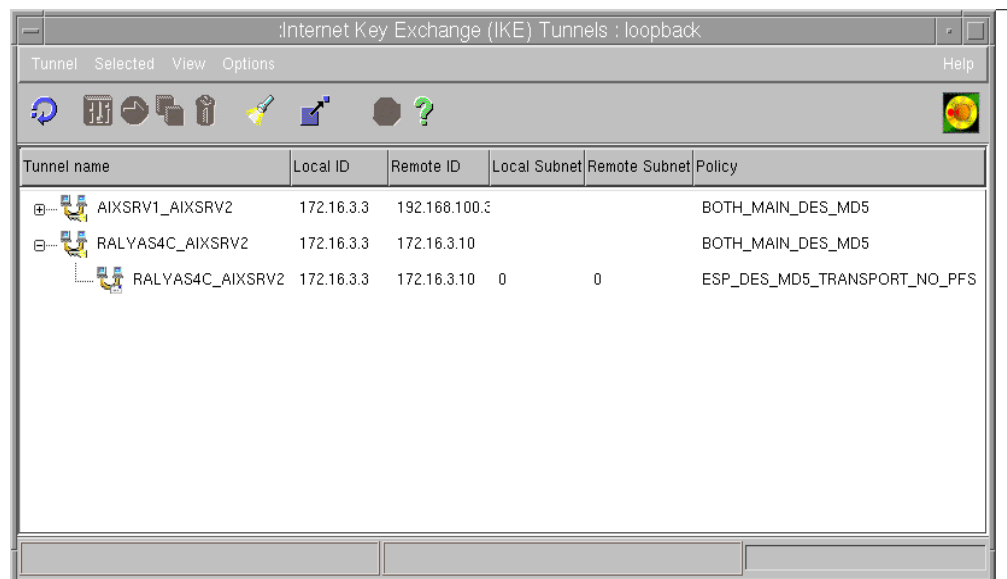


Figure 874. Internet Key Exchange (IKE) Tunnel configuration panel

5. Select **Tunnel->New Key Mgmt. Tunnel** to open the Key Management (Phase 1) Tunnel Properties window (Figure 875 on page 774).

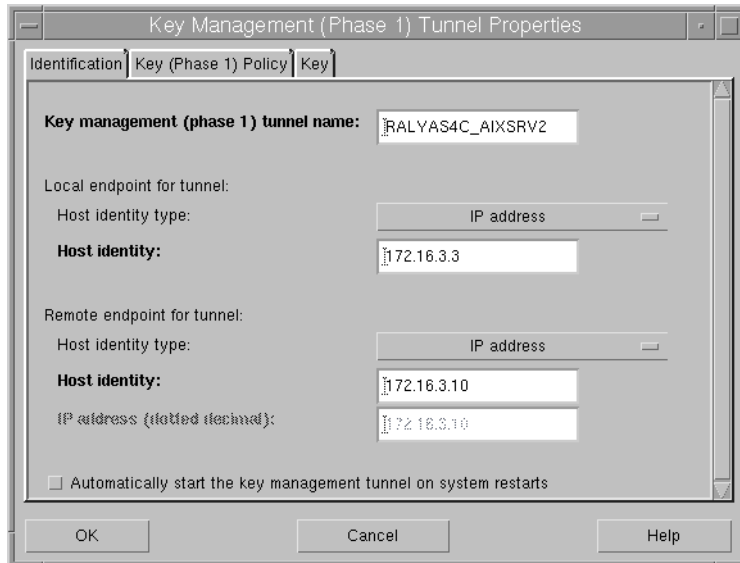


Figure 875. Key Management (Phase 1) Tunnel Properties - Identification

6. On the Identification panel, enter the key management tunnel name. In this scenario, enter `RALYAS4C_AIXSRV2`.
7. Select **IP address** as Host Identity type for local and remote endpoint for tunnel. Enter the IP addresses of the local and remote hosts.
8. Select the **Key (Phase 1) Policy** window. The Key Management (Phase 1) Tunnel Properties panel (Figure 876) is displayed.

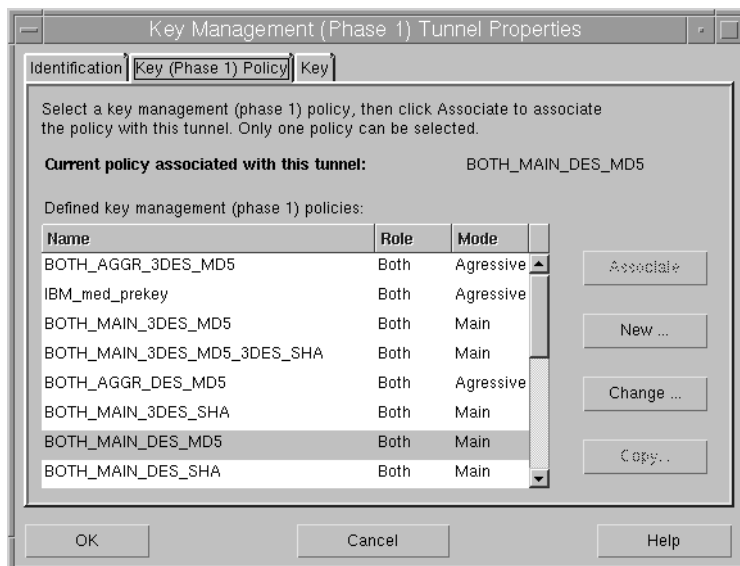


Figure 876. Key Management (Phase 1) Tunnel Properties - Key (Phase 1) policy

9. Select **BOTH_MAIN_DES_MD5** policy from Defined key management (phase 1) policies, and click **Associate**.
10. Select **Key**. The Key Management (Phase 1) Tunnel Properties window is displayed (Figure 877 on page 775).

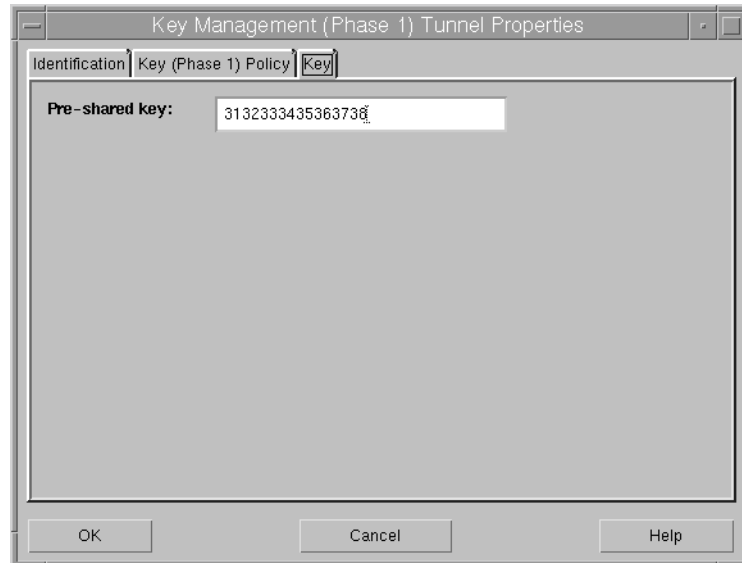


Figure 877. Key Management (Phase 1) Tunnel Properties - Key

11. Enter the pre-shared key. Use the hexadecimal notation. For example, Hex "31", "32" is equivalent to the ASCII decimal value 1, 2....entered on the AS/400 configuration.

12. Click **OK**.

You have now completed the key management tunnel configuration. Next, configure the data management tunnel associated with the key management tunnel.

13. Select **Tunnel->New Data Mgmt. Tunnel** on the Internet Key Exchange (IKE) Tunnels configuration panel (Figure 874 on page 773) to open the Data Management (Phase 2) Tunnel Properties window (Figure 878).

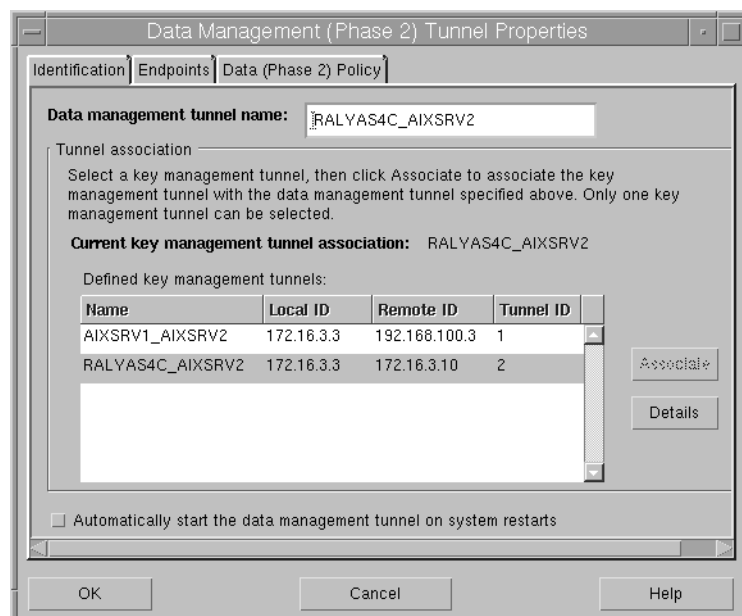


Figure 878. Data Management (Phase 2) Tunnel Properties - Identification

14. On the Identification panel, enter the data management tunnel name. In this scenario, enter `RALYAS4C_AIXSRV2`.
15. Select the key management tunnel that should be associated with this data management tunnel, which, in this scenario, is **RALYAS4C_AIXSRV2**. Click **Associate**.

Note

Do not check *Automatic data management tunnel* if your side is the responder or you do not want to establish a data management tunnel at system restart.

16. Click **Endpoints**. The Data Management (Phase 2) Tunnel Properties window (Figure 879) is displayed.

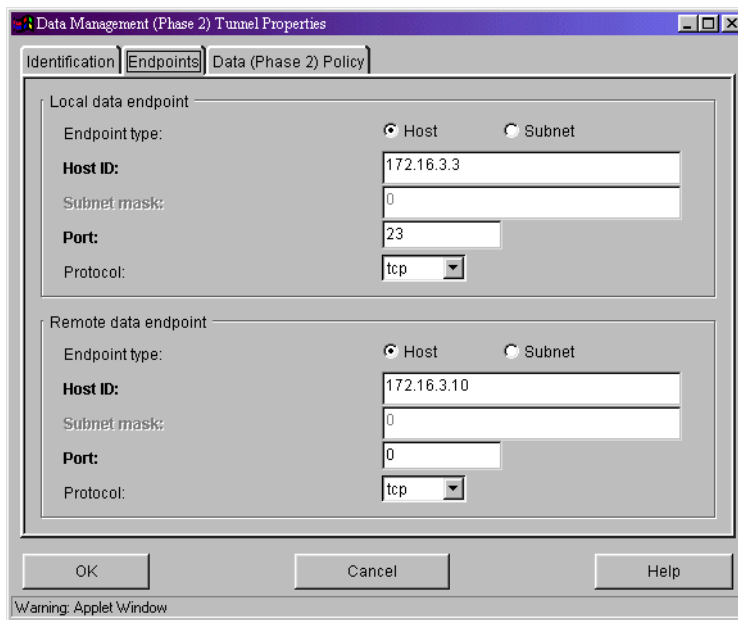


Figure 879. Data Management (Phase 2) Tunnel Properties - Endpoints

17. For Local data endpoint, enter:
 - **Endpoint type:** Host (this is a host to host scenario)
 - **Host ID:** 172.16.3.3
 - **Port:** 23 (only Telnet from RALYAS4C to AIXSVR2 is allowed)
 - **Protocol:** TCP (only Telnet from RALYAS4C to AIXSVR2 is allowed)
18. For Remote data endpoint, enter:
 - **Endpoint type:** Host (this is a host to host scenario)
 - **Host ID:** 172.16.3.10
 - **Port:** 0 (Telnet client in RALYAS4C coming from ephemeral port)
 - **Protocol:** TCP (only Telnet from RALYAS4C to AIXSVR2 is allowed)
19. Click **Data (Phase 2) Policy**. The Data Management (Phase 2) Tunnel Properties panel (Figure 880 on page 777) is displayed.

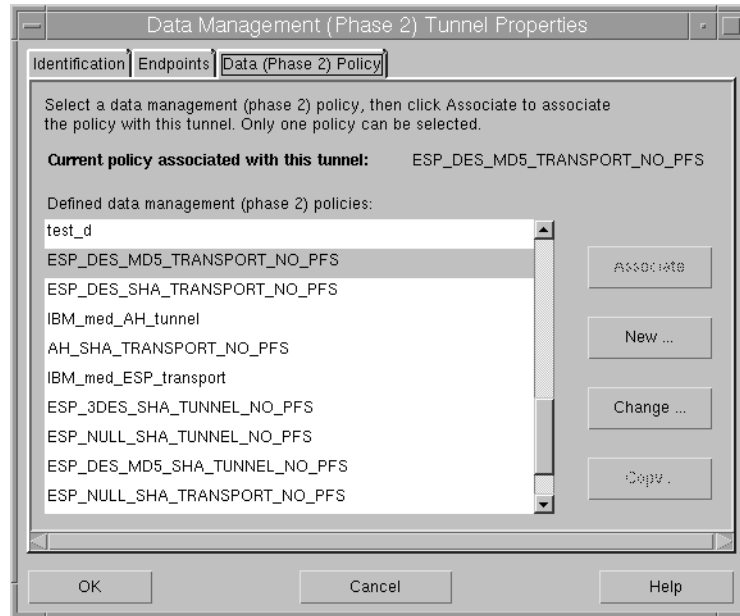


Figure 880. Data Management (Phase 2) Tunnel Properties - Data (Phase 2) Policy

20. Select **ESP_DES_MD5_TRANSPORT_NO_PFS** policy from Defined data management (phase 2) policies. Click **Associate**.

21. Click **OK**.

Now the data management tunnel is configured. Wait for the tunnel creation request from the AS/400 system.

The IKE Tunnel Monitor is used to check the status of IKE tunnels. Double-click **IKE Tunnel Monitor** under Virtual Private Networks (IP Security) Network panel (see Figure 873 on page 773). The status of the phase 1 and phase 2 tunnels is displayed as shown in Figure 881.

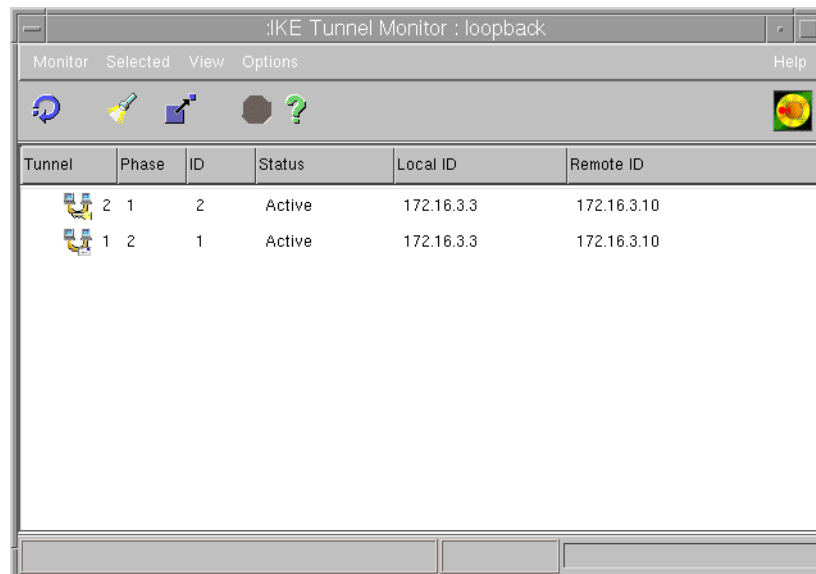


Figure 881. IKE Tunnel Monitor

17.3 AS/400 host-to-host VPN configuration

The following sections explain how to configure the host-to-host dynamic connection on the AS/400 system RALYAS4A to establish a VPN with the AIX server.

17.3.1 Completing the AS/400 system planning worksheet

Complete the AS/400 system planning worksheet as shown in Table 112. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 112. RALYAS4C New Connection Wizard AS/400 planning worksheet

This is the information you need to create your VPN with the New Connection Wizard	Scenario answers
What type of connection are you creating? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Hosts – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Hosts
What will you name the connection group?	HtoH4CtoAIX
What type of security and system performance do you require to protect your keys? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Balanced
How will you identify your local server?	IP address
What is the IP address of your local server?	172.16.3.10
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	172.16.3.3
What is the pre-shared key?	12345678
What type of security and system performance do you require to protect your data? – Highest security, lowest performance – Balance security and performance – Minimum security and highest performance	Balanced

We completed this planning worksheet (Table 112) from the perspective of RALYAS4C. The wizard selects the IPSec protocols to balance security and performance for protecting both key and data information. The main configuration object, the connection group, is named *HtoH4CtoAIX*, and the pre-shared key is a "random" string of characters, *12345678*.

Tip

When configuring a Dynamic key connection, as is the case in this scenario, you must provide the pre-shared key in ASCII format to the AS/400 GUI. Notice that the AIX GUI requires a hexadecimal format.

Table 113 shows the planning worksheet that we used to configure the AS/400 IP filters in this scenario.

Table 113. Planning worksheet - IP filter rules RALYAS4A

This is the information you need to create your IP filters to support your VPN	Scenario answers
<p>Is <i>your</i> VPN server acting as a host or gateway? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.</p>	Host
<p>Is the <i>remote</i> VPN server acting as a host or gateway?</p>	Host
<p>What name do you want to use to group together the set of filters that will be created?</p>	AIXSet
<p>If <i>your</i> server is acting as a gateway... – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.</p>	<p>n/a n/a n/a</p>
<p>If the <i>remote</i> server is acting as a gateway... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.</p>	<p>n/a n/a n/a</p>
<p>If you will <i>limit services</i> allowed through the VPN, use the information from the following list in the IPSEC filter rule Services options ... – What protocol will be allowed? – What source port will be allowed? – What destination port will be allowed?</p>	<p>TCP Any (*) 23</p>
<p>What is the IP address of your VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host.</p>	172.16.3.10
<p>What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host.</p>	172.16.3.3
<p>What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?</p>	FSIOPETH

This is the information you need to create your IP filters to support your VPN	Scenario answers
<p>What other IP addresses, protocols, and ports do you wish to permit on this interface?</p> <p>Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i>.</p>	

We also completed the IP filter rules planning worksheets (Table 113) from the perspective of RALYAS4C. Because we are configuring a host-to-host connection, the VPN servers and the data endpoint have the same IP addresses.

Note: If the AS/400 system has only one physical interface (line) that also connects it to the internal network, you must configure a pair of filter rules to allow inbound and outbound general internal traffic. This general traffic filter rule is not shown in the example.

17.3.2 Configuring a host-to-host VPN in the AS/400 system

Perform the following steps to configure a host-to-host VPN on RALYAS4C:

1. Start Operations Navigator from your desktop.
2. Expand your AS/400 system, which, in this case, is **RALYAS4C**. Sign on when prompted.
3. Expand **Network**.
4. Double-click **IP Security**
5. Double-click **Virtual Private Networking**.
6. Click **File->New Connection**, and select **Host to Hosts** from the pull-down menu (Figure 882 on page 781). This starts a new connection wizard for a host-to-hosts connection.

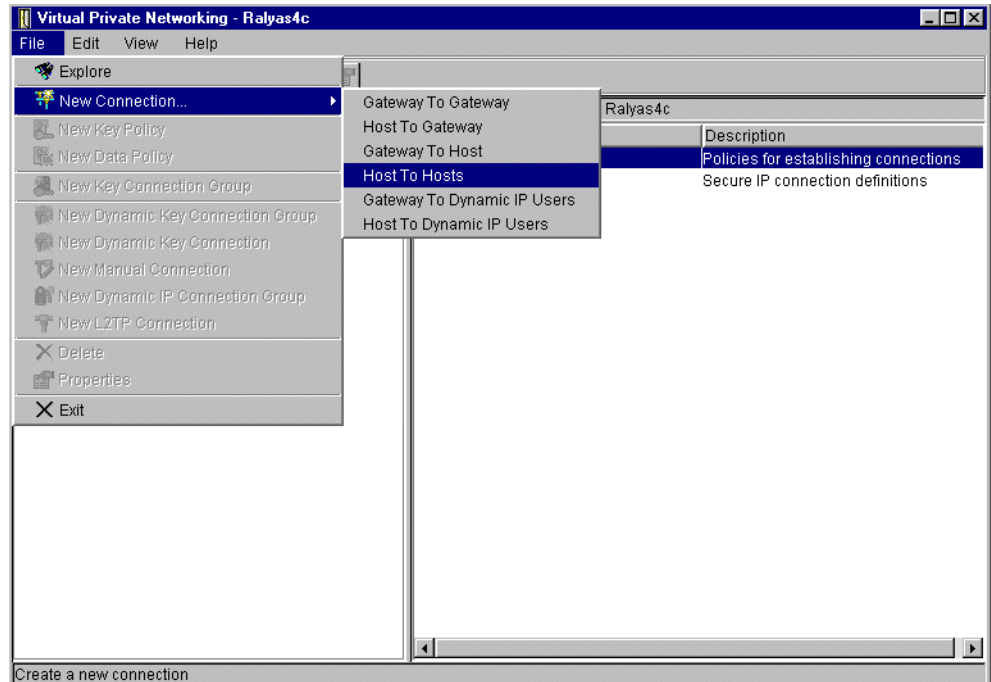


Figure 882. New Connection->Host to Hosts - AS/400 system to AIX server

The wizard welcome window is displayed (Figure 883).

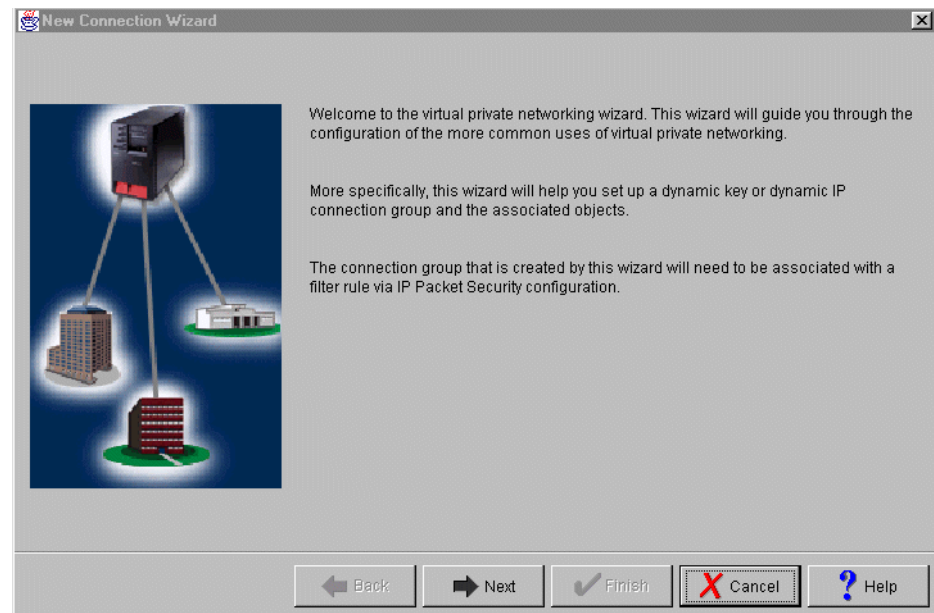


Figure 883. New connection->Host to Hosts - AS/400 system to AIX server

7. Click **Next** after reading the Welcome window.
8. Enter the Name, HtoH4CtoAIX, for the connection group. Recall that HtoH4CAIX is the name from the planning worksheet in Table 112 on page 778. The name you specify here is the name for all objects that the wizard creates for this particular connection. It is case sensitive. Also enter a description of the configuration that you are creating as shown in Figure 884 on page 782.

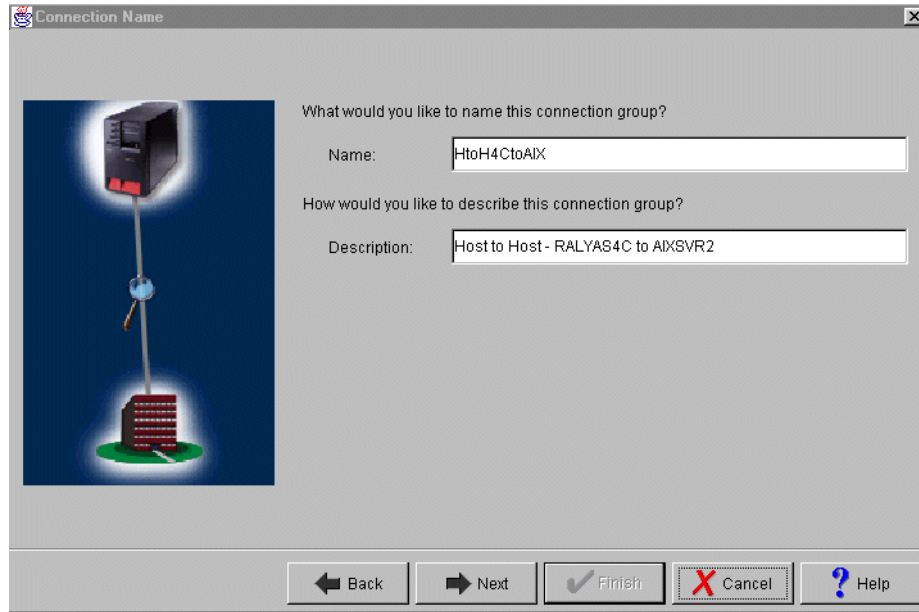


Figure 884. Connection Name window - AS/400 system to AIX server

9. Click **Next**.

10. On the Key Policy window, specify the level of authentication or encryption protection that IKE uses during phase 1 negotiations. Phase 1 establishes the keys that protect the messages that flow during subsequent phase 2 negotiations. Phase 2 protects the data itself. For the purposes of this example, select **Balance security and performance** (Figure 885) as specified on the worksheet. The wizard chooses the appropriate encryption and authentication algorithms based on the selection you make here.

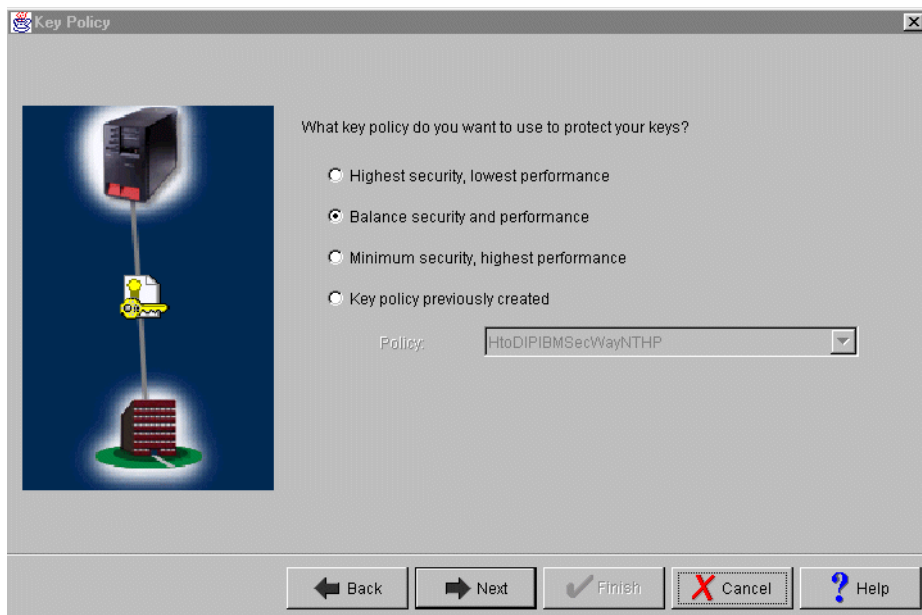


Figure 885. Key Policy window - AS/400 system to AIX server

11. Click **Next** when complete.

12. On the Local Identifier window (Figure 886), specify the identity of the local key server. In other words, specify the local AS/400 system IP address. In this host-to-host scenario, the AS/400 system RALYAS4C is the key server and data endpoint for the connection. Leave Identifier type as the default value, Version 4 IP address. For the IP Address, use the pull-down list to select the IP address of the interface which is connecting to the remote VPN server. Refer back to the planning worksheet in Table 112 on page 778 and to the network configuration in Figure 872 on page 771. For RALYAS4C, this is 172.16.3.10 (interface **B** in Figure 872 on page 771).

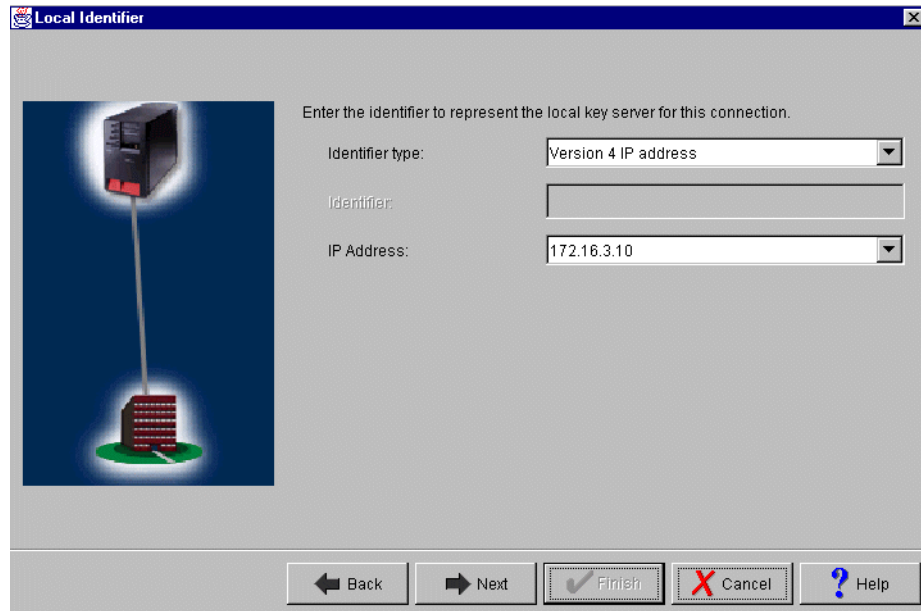


Figure 886. Local Identifier window pull-down list - AS/400 system to AIX server

13. Click **Next**.

14. Use the Remote Identifier window (Figure 887 on page 784) to enter details about the remote key server, as well as the pre-shared key. The pre-shared key is the shared "secret" IKE uses to generate the actual keys for phase 1. Our remote key server is the AIX server with IP address 172.16.3.3 (interface **A** in Figure 872 on page 771). Specify 12345678 in the Pre-shared key field. Remember, the same pre-shared key must be entered when configuring VPN on the remote AIX server. When entering this value in the AIX configuration, it must be in the hexadecimal format (3132333435363738).

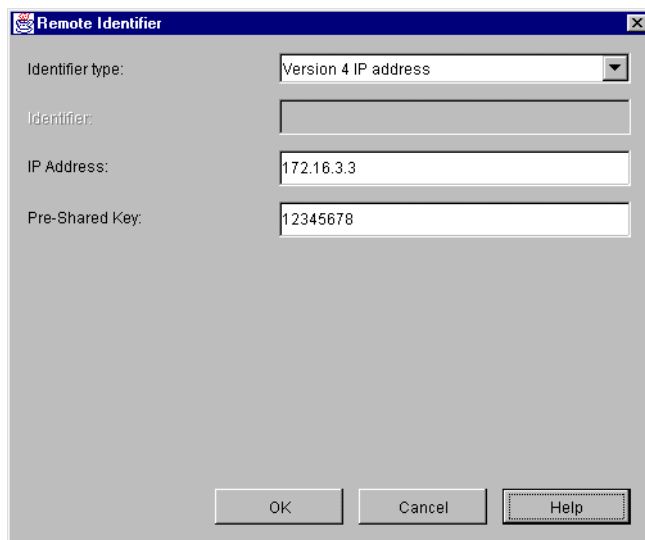


Figure 887. Remote key server identifier window - AS/400 system to AIX server

15. Click **Next**.

16. Use the Data Policy window (Figure 888) to specify the level of authentication or encryption that IKE uses to protect data flowing through the host-to-host tunnel during phase 2 negotiations. For this example, select **Balance security and performance** as specified on the planning worksheet (Table 112 on page 778).

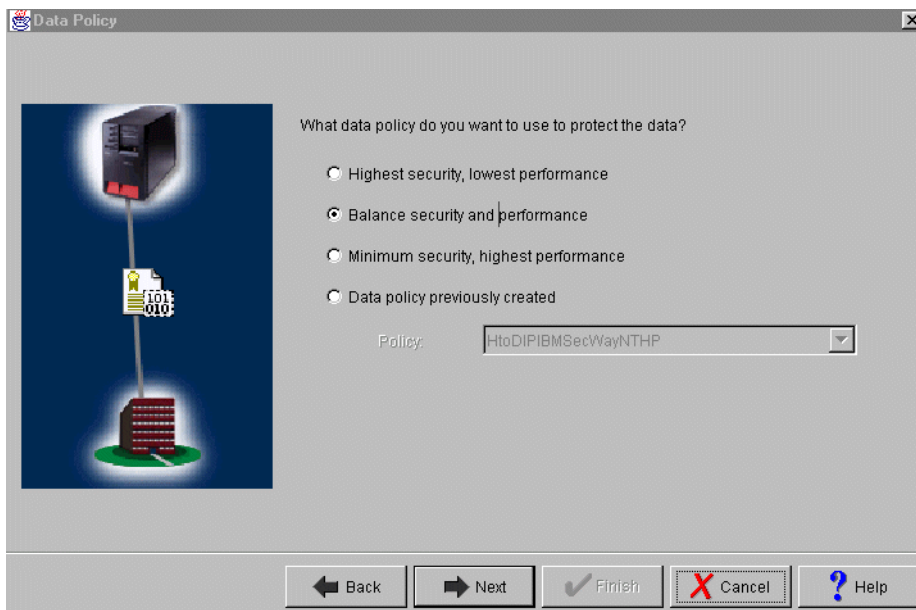


Figure 888. Data Policy window - AS/400 system to AIX server

17. Click **Next**.

18. The final window summarizes the configuration values you entered (Figure 889 on page 785).

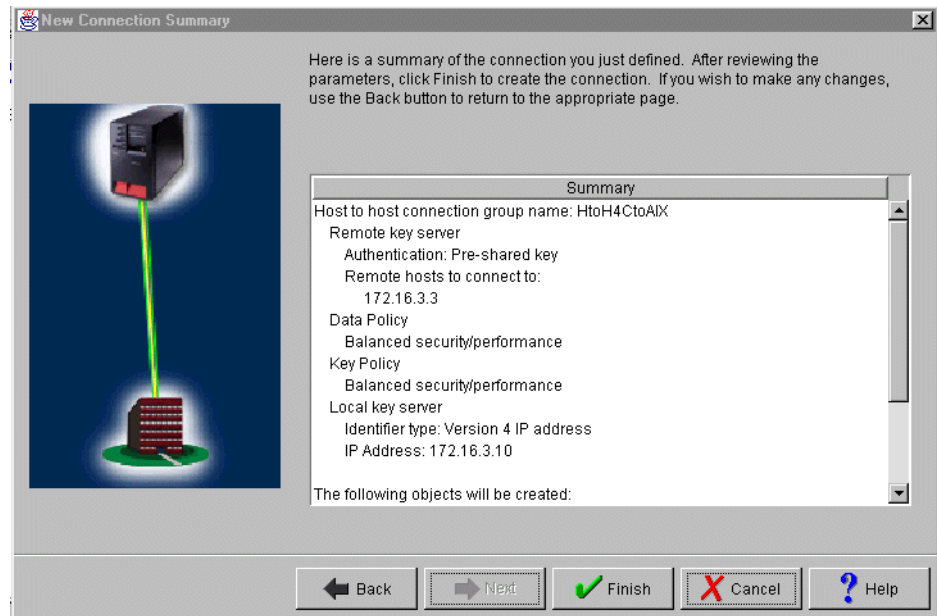


Figure 889. New Connection Summary window Host to Host - AS/400 system to AIX server

If you scroll down, you can also see a list of the configuration objects that the wizard will create when you click Finish (Figure 890). Check the configuration values against your worksheet. If changes need to be made, click **Back**.

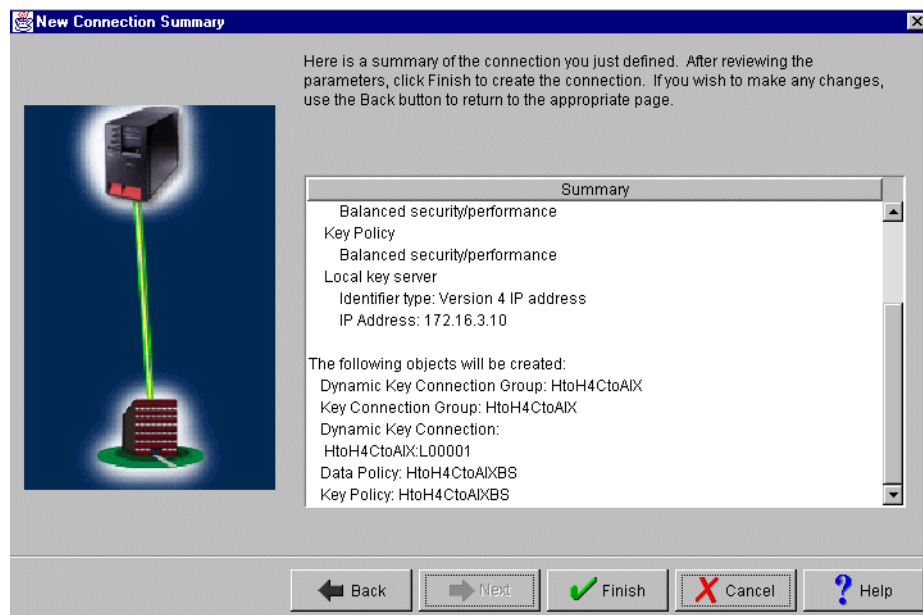


Figure 890. New Connection Summary window Host to Host - AS/400 system to AIX server

19. Click **Finish**.

The wizard now creates the various objects you configured for this VPN connection. After a short delay (and assuming there are no errors), you return to the initial VPN GUI Configuration window.

17.3.2.1 Matching the AIX server VPN configuration

The simplest way to configure VPN on the AS/400 system is through the VPN configuration wizard, as shown in the steps presented in the previous section. However, the wizard configures default values that you may need to change to match the VPN partner's configuration. Refer to 3.7.6, "Changing the Virtual Private Networking GUI default values" on page 76, for a discussion on how to change the default values configured by the wizard.

Since phase 1 mode, Perfect Forward Secrecy (PFS), phase 1 key lifetime and lifesize, phase 2 key lifetime and lifesize, and connection lifetime were not properly setup in the VPN default values prior to running the wizard, these values must be ensured after the wizard creates the configuration objects.

In this scenario, we change the following parameters to match the VPN partner AIX server configuration:

- Phase 1 mode: `main`
- Phase 1 key lifetime: `480 min`
- Phase 2 key lifetime: `30 min`

Perform the following steps to change some parameters configured by the wizard to match the AIX server configuration:

1. At the Virtual Private Networking window, expand Key Policies.
2. Double-click **HtoH4CtoAIXBS** (this scenario's key policy) to update phase 1 mode.
3. At the Properties - HtoH4CtoAIXBS window, select **Identity protection** for Initiator negotiation and **Require identity protection** for Responder negotiation (Figure 891).

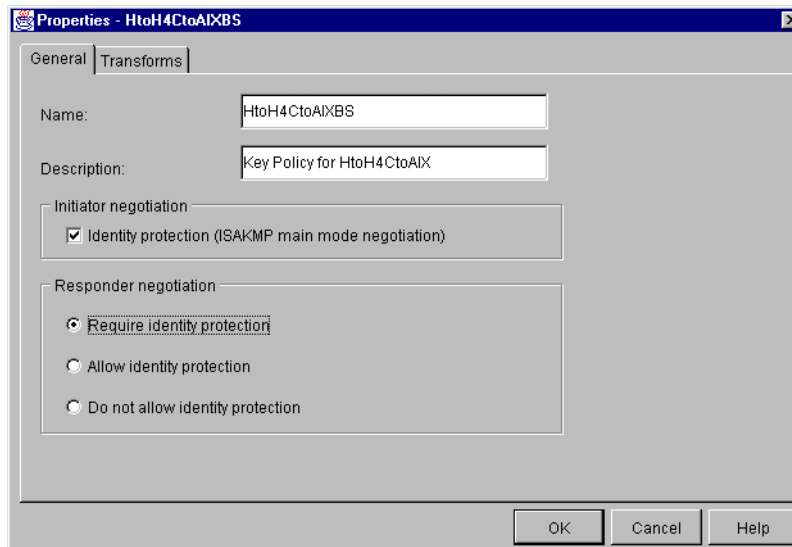


Figure 891. Changing phase 1 mode to main mode - Key policy Properties window

4. To change phase 1 key lifetime, from the Key Policies - Properties window, select the **Transforms** tab.
5. Select the transform that you want to change (Figure 892 on page 787).

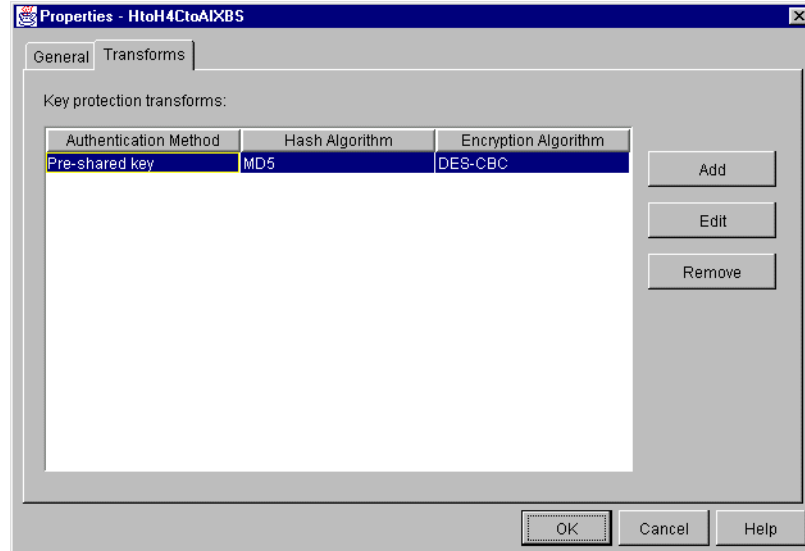


Figure 892. Key policies Properties window - Updating the phase 1 transforms

6. Click **Edit**.
7. Change the Maximum key lifetime to 480 minutes (Figure 893).

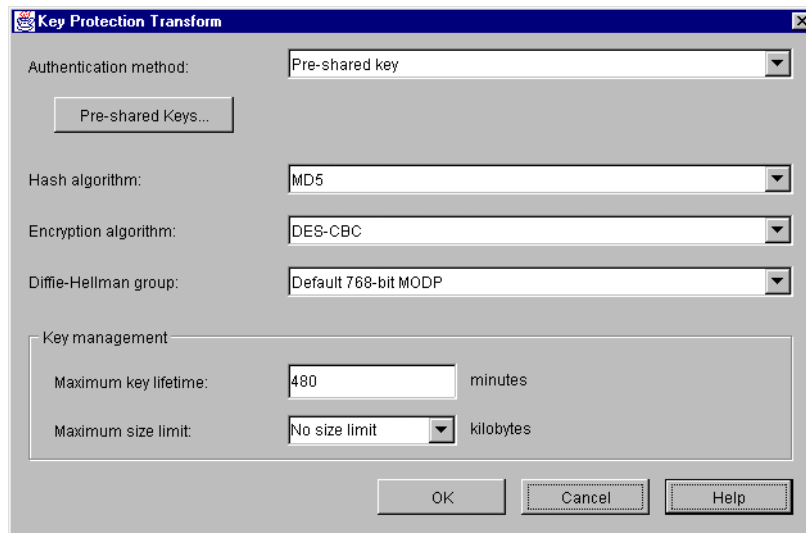


Figure 893. Key Protection Transform window - Changing phase 1 key lifetime

8. Click **OK**.
9. To change phase 2 key lifetime, double-click **Data Policies**.
10. Double-click **HtoH4CtoAIXBS**.
11. At the Properties - HtoH4CtoAIXBS windows, click the **Proposals** tab.
12. Select the proposal you want to update, and click **Edit**.
13. At the Data Protection Proposal window, click the **Key Expiration** tab.
14. Change the Key expiration to 30 minutes as shown in Figure 894 on page 788.

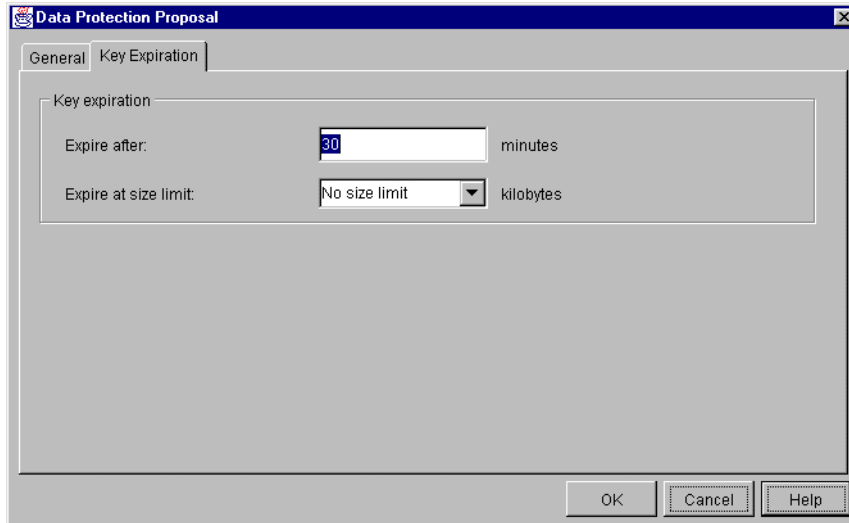


Figure 894. Data Protection Proposal - Changing phase 2 key lifetime

15. Click **OK**.

To enforce the requirement, stated in 17.1.2, "Scenario objectives" on page 770, that only the distributor's system RALYAS4C can initiate the connection, continue with the following steps.

16. At the Virtual Private Networking window, right-click the **HtoH4CtoAIX** dynamic key group, and select **Properties** from the pull-down menu (Figure 895).

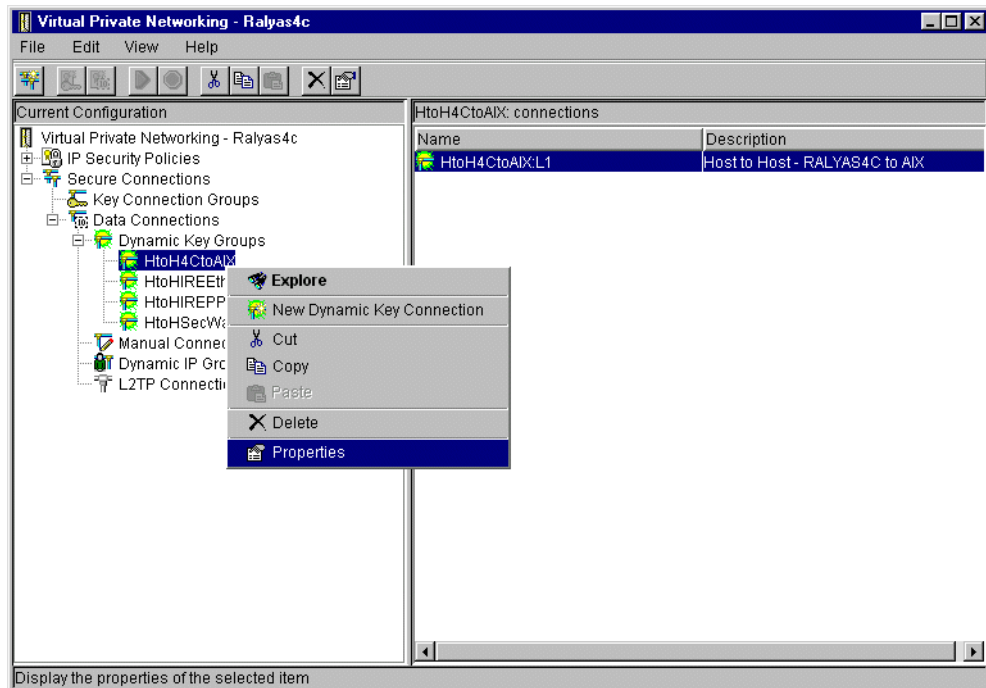


Figure 895. Changing connection initiation to only local system

17. At the Properties window, select **Only the local system can initiate the connection** (Figure 896 on page 789).

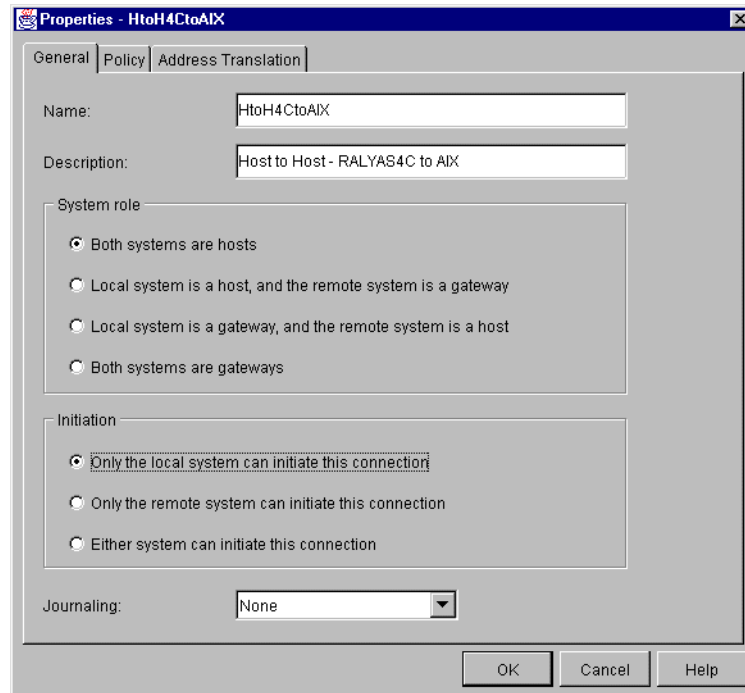


Figure 896. Limiting the initiation of the connection to only the local system

Table 114 on page 790 summarizes the OS/400 and AIX VPN configuration and provides a cross-reference list.

17.4 VPN configuration cross-reference table: AS/400 to AIX server

Table 114 provides a cross-reference list of the VPN configuration parameters for the AS/400 system and the AIX server.

Table 114. AS/400 and AIX VPN configuration cross-reference table

<u>AS/400</u>	<u>AIX Server</u>
Key Policy	Key management (phase 1) tunnel
Name = HtoH4CtoAIXBS	
Initiator Negotiation = Identity Protection (Main Mode)	(1) (1) Policy role & Identity Protection = BOTH(I,R) & MAIN
Responder Negotiation = Require	(1) Transform Property
Key Protection Transforms	(2) (2) Authentication Method = Pre-Shared Keys(PSK)
Authentication Method = Pre-shared key	Preshared key=3132333435363738
Pre-shared key value = 12345678	(3) (3) Hash Algorithm =HMAC- MD5
Hash Algorithm = MD5	(3) (4) Encryption Algorithm = DES
Encryption Algorithm = DES-CB	(4) (5) Diffie-Hellmann Group = Group 1
Diffie-Hellman Group = Default 768-bit MODP	(5) (6) Key lifetime
Key Management	(6) Time(minutes) = 480
Maximum key lifetime (minutes) = 480	Size(kilobytes)=0
Maximum size limit (kilobytes) = No size limit	(14) (14) Policy Role=Allow responder negotiations only
Data Policy	Data management (phase2) tunnel
Name = HtoH4CtoAIXBS	
Use Diffie-Hellman Perfect Forward Secrecy =No	(7) (7) PFS (Perfect Forward Secrecy) = No
Data Protection Proposals	
Encapsulation mode = Transport	(8) (8) Encapsulation Mode = Transport
Protocol = ESP	(9) (9) Protocol=ESP
Algorithms	
Authentication Algorithm =HMAC-MD5	(9) (9) AH authentication algorithm = N/A
Encryption Algorithm = DES-CBC	(9) (9) ESP Authentication Algorithm =MD5
Key Expiration	ESP Encryption Algorithm = DES
Expire after (minutes) = 30	(10) (10) Key Lifetime
Expire at size limit (kilobytes) =	Time (minutes) = 30
No size limit	Size (Kilobytes) = 0
	(13) (13) EndPoints->Endpoint type=Host
	(16) (16) Port = 23
	(15) (15) Protocol = TCP
Key Connection Group	Key management (phase 1) tunnel
Name = HtoH4CtoAIX	
Remote Key Server	
Identifier Type = Version 4 IP address	(11) Remote endpoint for tunnel
IP address = 172.163.3.3	(11) (12) Host identity type = IP address
Local Key Server	(12) (12) Host identity = 172.163.3.10
Identifier Type = Version 4 IP address	(12) Local endpoint for tunnel
IP address = 172.163.3.10	(11) (11) Host identity type = IP address
Key Policy = HtoH4CtoAIXBS	(11) (11) Host identity = 172.163.3.3 Ssaa
Dynamic Key Group	
Name = HtoH4CtoAIX	
System Role = Both systems are hosts	(13) (13) System Role = Both systems are hosts
Initiation = Only the local system can initiate the connection	(14) (14) Initiation = Only the local system can initiate the connection
Policy	
Data Management Security Policy =	
HtoH4CtoAIXBS	
Connection Lifetime = Never expires	
Local addresses = Filter rule	
Local ports = Filter rule	
Remote addresses = Filter rule	
Remote ports = Filter rule	
Protocol = Filter rule	
Dynamic Key Connection	
Name = HtoH4CtoAIX.L1	
Key Connection Group = HtoH4CtoAIXBS	
Start when TCP/IP is started? = No	
IP Filters	
Name =HtoH4CtoAIX.3ip	
IPSEC rule	
Source address name = 172.163.3.10	
Destination address name = 172.163.3.3	
Connection name = HtoH4CtoAIXBS	
Services	
Protocol =TCP	(15) (15) Protocol =TCP
Source port = *	
Destination port = 23	(16) (16) Destination port = 23

You have now completed the VPN configuration for RALYAS4C. You configure AS/400 IP filtering in the next task.

17.4.1 Configuring IP filters on the AS/400 system (RALYAS4C)

The wizard does *not* configure IP filtering. You must complete this task manually by using Operations Navigator. If IP filtering is already configured and active, then any new filters must be integrated with those already in existence.

Refer to Chapter 4, “AS/400 IP filtering overview” on page 103, on how this is done. Only the windows specific to this scenario are shown here. The following filter rules, which are not shown in this section, must be configured:

- Filter interface
- Defined address for the subnet in the internal network to which the AS/400 system is connected
- Filter rules to permit inbound and outbound traffic to and from the internal network

To complete the VPN configuration on the AS/400 system, the following IP filters must be configured:

1. Configure the outbound filter to allow IKE negotiation between the key servers as shown in Figure 897 and Figure 898 on page 792.

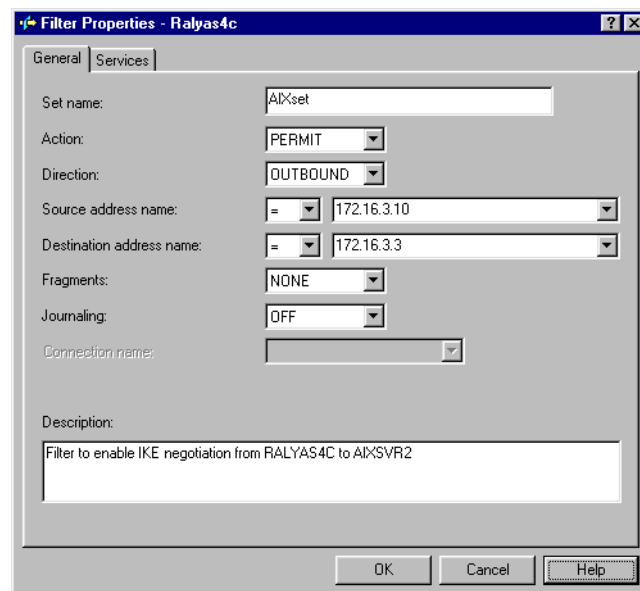


Figure 897. IP filter for outbound IKE messages - RALYAS4C to AIXSVR2

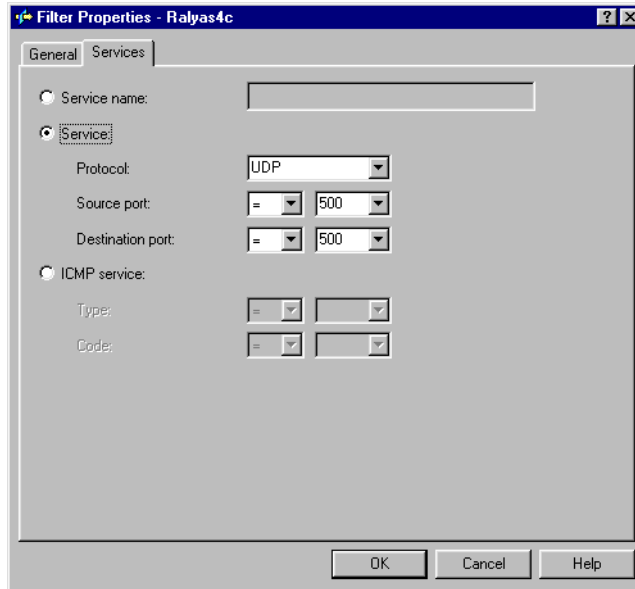


Figure 898. Services for IKE negotiation

2. Configure the inbound filter to allow IKE negotiation between the key servers as shown in Figure 899 and Figure 900 on page 793.

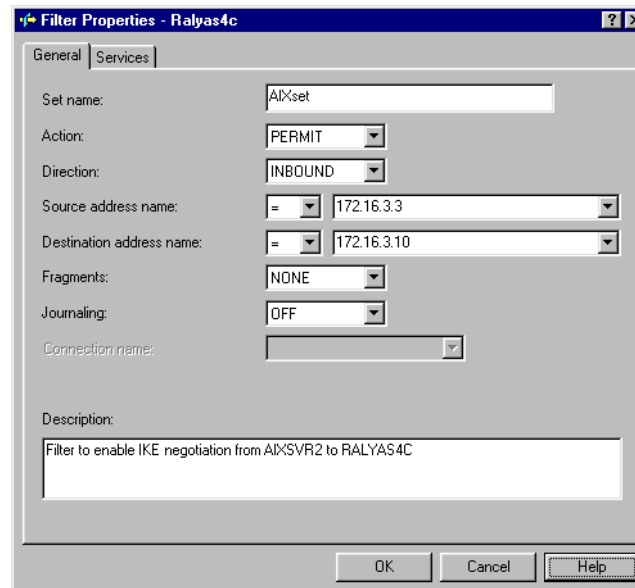


Figure 899. IP filter for inbound IKE messages - AIXSVR2 to RALYAS4C

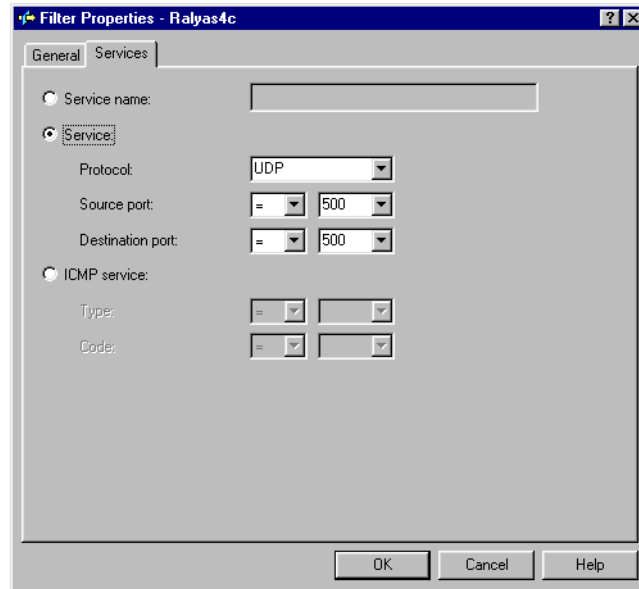


Figure 900. Services for IKE negotiation

- Use the same filter Set name, **AIXset**, but specify **IPSEC** in the Action field. With an IPSEC filter rule, Direction is always set to **OUTBOUND** and grayed out. In the Source and Destination address name fields, enter the host's IP addresses for **RALYAS4C** and **AIXSVR2**.

The Connection name is the data connection, which, in this case, is a dynamic key connection *group*. Use the pull-down list to view all the data connection names that have been configured on this system, and select the one required. In this example, you select **HtoH4CtoAIX** (Figure 901).

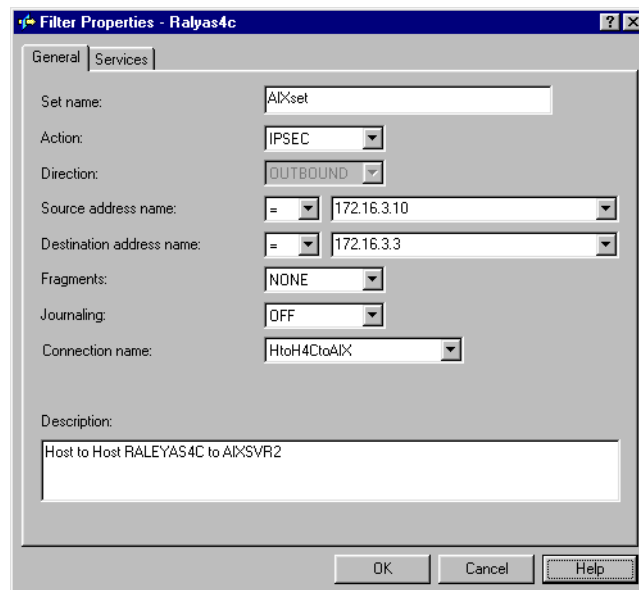


Figure 901. Host-to-host connection - IPSEC filter rule

- When you complete the required fields, click on the **Services** tab.

5. Enter `TCP` in the *Protocol*, wildcard (*) in the Source port and `23` (Telnet) in the Destination port fields. This allows only Telnet using port 23 to use this filter rule, and, therefore, the VPN tunnel. See Figure 902.

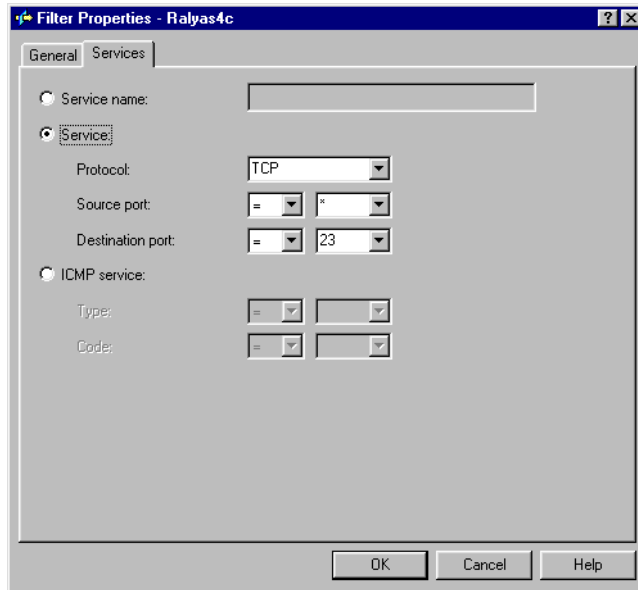


Figure 902. IPSEC filter rule service - Limiting the services to Telnet

Tip

In this scenario, we decided to limit the services allowed through the VPN by configuring the values in the Services page in the IPsec filter configuration as shown in Figure 902 on page 794. In this case, in the corresponding dynamic key group policy, the values that define the traffic for active connections must come from the filter rule (see Figure 903 on page 795). Refer to Chapter 4, "AS/400 IP filtering overview" on page 103, for further information on how to limit services in a VPN.

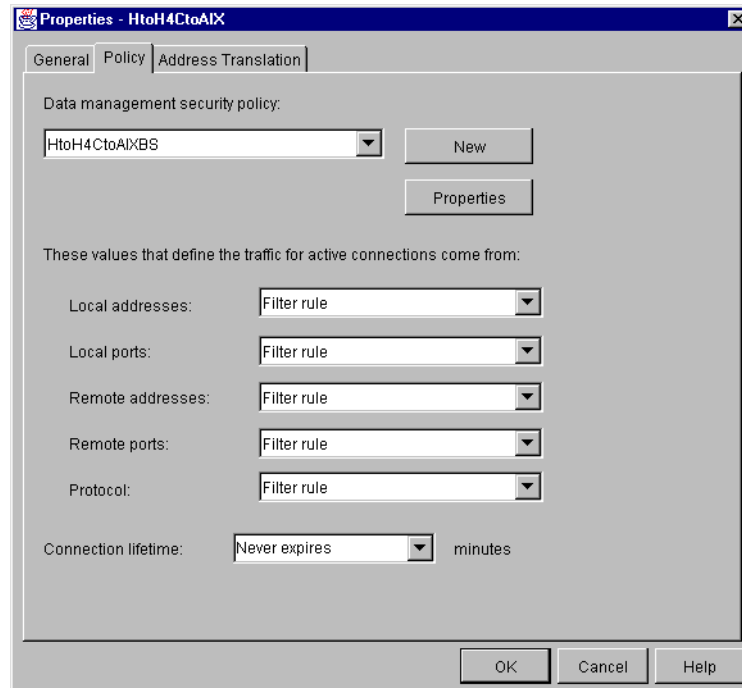


Figure 903. Dynamic key group - Values that define traffic for active connections

Figure 904 shows the summary of the IP filters configured for this scenario.

```
#IKE Negotiation
FILTER SET AIXset ACTION = PERMIT DIRECTION = INBOUND
SRCADDR = 172.16.3.3 DSTADDR = 172.16.3.10 PROTOCOL = UDP
DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
FILTER SET AIXset ACTION = PERMIT DIRECTION = OUTBOUND
SRCADDR = 172.16.3.10 DSTADDR = 172.16.3.3 PROTOCOL = UDP
DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#IPSEC rule
FILTER SET AIXset ACTION = IPSEC DIRECTION = OUTBOUND
SRCADDR = 172.16.3.10 DSTADDR = 172.16.3.3 PROTOCOL = TCP
DSTPORT = 23 SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = HtoH4CtoAIX
#Filter interface
FILTER_INTERFACE LINE = FSIOPETH SET = AIXset
```

Figure 904. RALYAS4C - Filter rules summary

17.4.2 Starting the VPN connection

This section explains how to start the VPN connection configured in the previous sections. For information about starting a VPN connection, refer to Chapter 4, “AS/400 IP filtering overview” on page 103.

Perform the following steps:

1. Activate IP filters.
2. Start the VPN server jobs by starting Virtual Private Networking.
3. Open **Virtual Private Networking**.

- Right-click the **HtoH4CtoAIX** connection, and click **Start** from the pull-down menu (Figure 905).

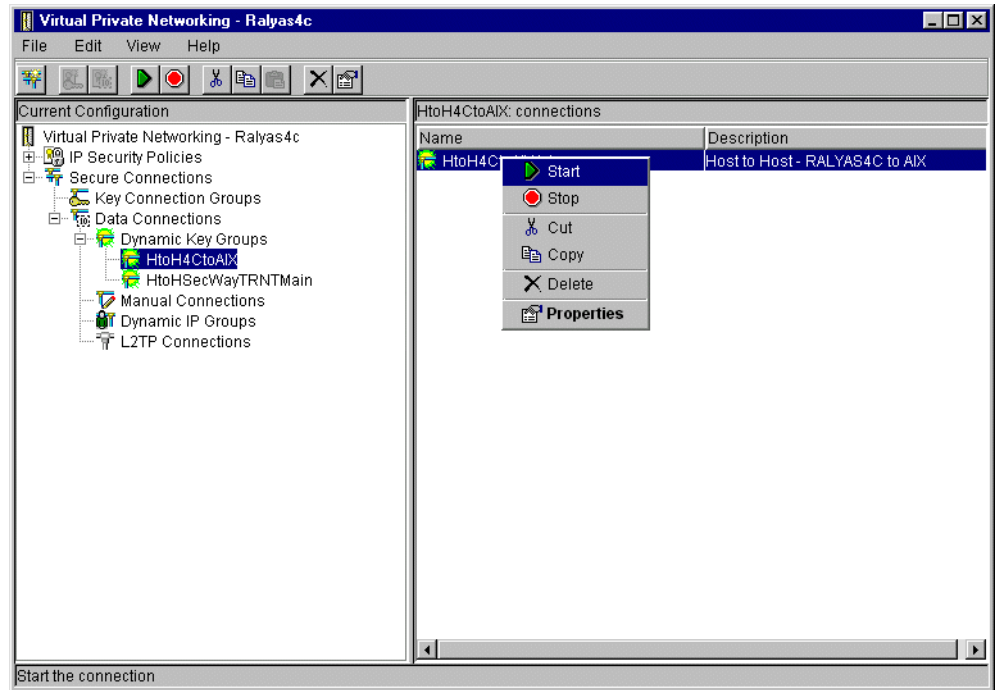


Figure 905. Starting the host to host connection - HtoH4CtoAIX

Note: Only RALYAS4C is allowed to initiate the connection, as configured in 17.3.2.1, “Matching the AIX server VPN configuration” on page 786.

- Display the connections to verify it is active. At the Virtual Private Networking window, select **View->Active Connections** as shown in Figure 906 on page 797.

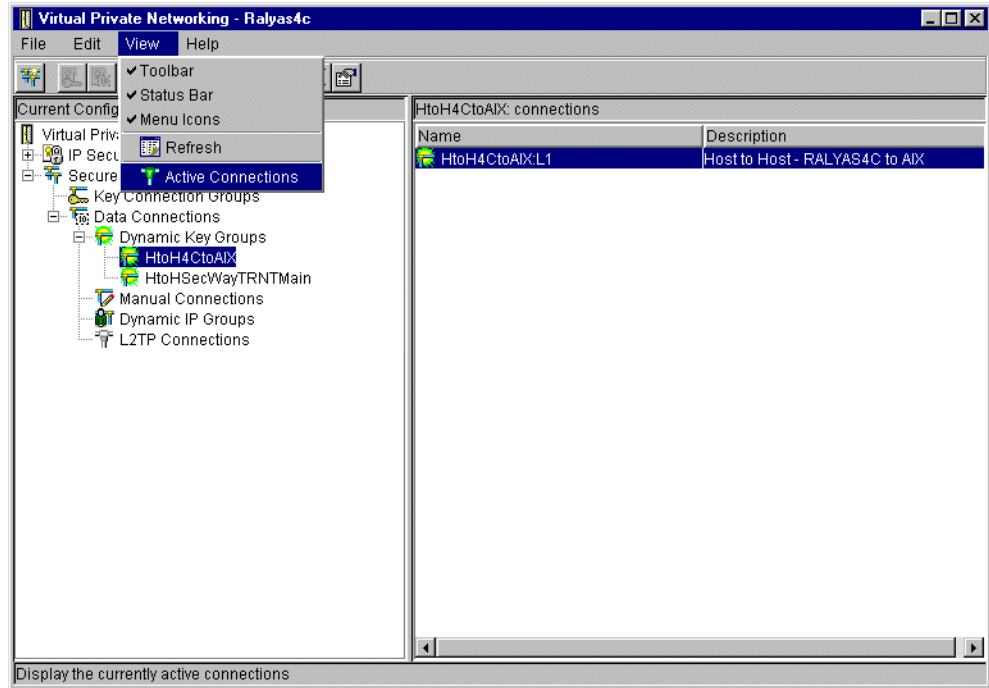


Figure 906. Viewing active connections

The Active Connections window is displayed as shown in Figure 907.

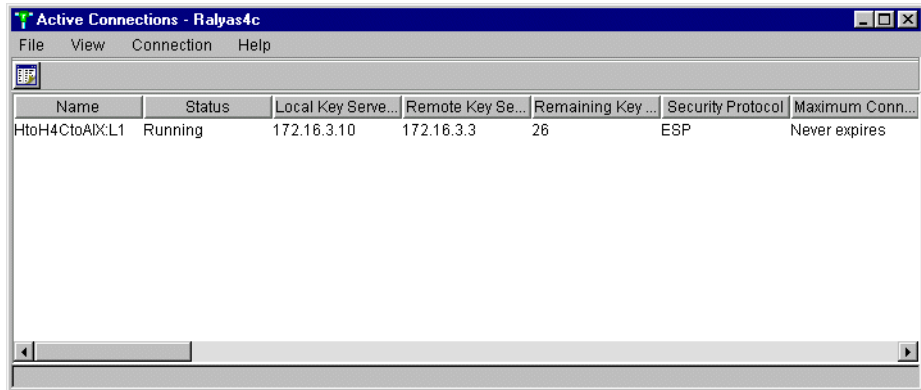


Figure 907. Active Connections window

17.4.3 Verification tests

Table 115 presents a summary of the verification tests run after the host-to-host VPN was configured. The tests verify the scenario objectives stated in 17.1.2, “Scenario objectives” on page 770.

Table 115. Verification test - OS/400 to AIX server host-to-host scenario

	Start connection	TELNET	FTP	PING
From RALYAS4C to AIXSVR2	Yes	Yes	No	No
From AIXSVR2 to RALYAS4C	No	No	No	No

Chapter 18. Host-to-host VPN: AS/400 to S/390

This chapter describes a VPN host-to-host configuration between the AS/400 system and the S/390 system.

18.1 Business partner VPN connection (host to host AS/400 to S/390)

In this scenario, we present two business partners that need to access each other's servers over the Internet. They want the data to flow securely over the public network, but they do not fully trust each other's private networks. Therefore, they want to ensure the connection is protected by IPSec protocols to the hosts that they want to connect. Figure 908 shows this scenario.

18.1.1 Scenario characteristics

The characteristics of this scenario are:

- Both the distributor and the manufacturer networks belong to different companies. Therefore, the secure tunnel must start and end at the data endpoints.
- Both networks are connected to the Internet through routers and firewalls. The filters in the firewalls must be opened to allow IKE negotiation and IPsec protocols between the host's VPN partners.
- The firewalls are configured to establish an AH tunnel-in-tunnel mode.
- The host-to-host VPN tunnel between the S/390 and the AS/400 system is ESP in transport mode.
- Both tunnels (AH tunnel between firewalls and ESP tunnel between hosts) are combined as described in 1.7.2, "Iterated tunnels" on page 23.

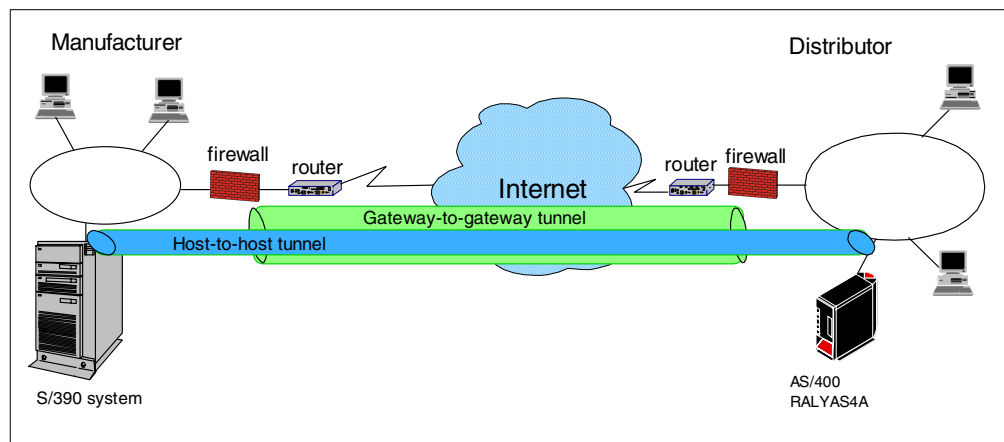


Figure 908. Business partners VPN - Host-to-host AS/400 system to OS/390 server

Note

Unlike the Branch Office scenarios, where we can assume that a consistent addressing plan is implemented across the company's intranets, in a Business-to-business scenario, you need to consider addressing issues. Business partners implement an addressing scheme independently of one another. In this case, it is possible that both companies use private (globally ambiguous) IP addresses in their networks, and that some of those addresses overlap. In this case, conventional routing protocols are not able to resolve these ambiguities.

In the host-to-host scenarios that apply to intercompany VPNs, we make the assumption that one or more of the following techniques is used to resolve addressing problems:

- The systems have been assigned unique globally routable IP addresses. Even if the systems are assigned globally routable addresses, they still most likely will not have connectivity since their networks will probably be protected by firewalls. In this case, a tunnel solution similar to the one described in Figure 908 on page 799 solves the problem.
- If the systems are assigned private IP addresses, they don't overlap.
- If the systems are assigned private IP addresses, a *tunneling protocol* is used between the gateways that connect both company networks to the intervening network (for example, the Internet). In this context, the gateways are firewalls, routers, or any other appliance. Some possible mechanisms include Frame Relay, MPLS, IPSec, L2TP, L2F, PPTP. It is important to note that the gateway-to-gateway tunnel between the firewalls or routers is totally transparent to the host-to-host configuration, such as the one shown in this chapter.

The AS/400 VPN implementation includes an AS/400-unique solution to the addressing issues, called VPNAT. Refer to Chapter 13, "VPN Network Address Translation (VPN NAT)" on page 551, for more information.

18.1.2 Scenario objectives

The objectives of this scenario are:

- All traffic between RALYAS4A and the S/390 system must be protected by IPSec.
- Only the S/390 system in the manufacturer's network can access RALYAS4A in the distributor's network and vice versa.
- Both the S/390 system and the AS/400 system (RALYAS4A) are allowed to initiate the VPN connection.

18.1.3 Scenario network configuration

Figure 909 on page 801 shows our simple network configuration for the host to host AS/400 system to S/390 system.

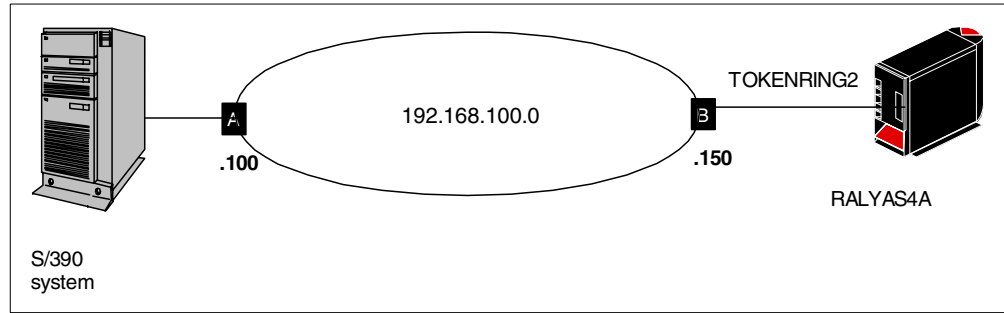


Figure 909. Host-to-host AS/400 to S/390 - Scenario test network

18.2 S/390 software

The scenario in this chapter only provides a cross-reference example of a VPN configuration between an S/390 system and the AS/400 system. This chapter is *not* meant to replace S/390 documentation. Refer to the following manuals for important information on this subject:

- *Security in OS/390-based TCP/IP Networks*, SG24-5383
- *SecureWay CS for OS/390 V2R8 TCP/IP: Guide to Enhancements*, SG24-5631
- *OS/390 Firewall Technologies Guide and Reference*, SC24-5835

The OS/390 Firewall Technologies Guide provides the support to configure a Virtual Private Network. IKE support was introduced in OS/390 V2R8. Prior to V2R8, OS/390 supported manual tunnels since V2R5.

To implement dynamic VPN connections on the S/390, the following IBM products are required:

- OS/390 V2R8
- OS/390 Firewall Technologies
- OS/390 V2R8 eNetwork Communications Server (IP security feature)
- OS/390 V2R8 Security Server (for firewall commands and servers)
- OS/390 V2R8 Security Server or other External Security Manager on OS/390 (for security management)
- OS/390 V2R8 Open Cryptographic Services Facilities (OCSF) (only required for ISAKMP)
- Security Server including RACF or equivalent OEM product.

18.2.1 Implementation tasks: Summary

The following is a summary of the tasks that you need to perform to implement this VPN host-to-host environment:

1. Verify connectivity. Before you start configuring VPN and filters, you must be sure that the underlying TCP/IP network is properly configured and working.
2. Complete the planning worksheet for the S/390 system
3. Configure a host to host VPN on the S/390 system.

4. Complete the planning worksheet for the AS/400 system.
5. Configure a host to host VPN on the AS/400 system.
6. Configure IP packet filtering on the AS/400 system.
7. Start the VPN connection.
8. Perform verification tests.

18.3 Verifying IP connectivity

Before starting the VPN configuration, verify that connectivity and routing between the two hosts are correct. Run the following command to verify that the IP connectivity from the RALYAS4A AS/400 system to the S/390 system is working:

```
PING '192.168.100.100'
```

The PING should succeed.

Repeat the ping test in the reverse direction to confirm that IP connectivity also works from the S/390 system to the RALYAS4A AS/400 system. Run the following command on the S/390 system:

```
PING 192.168.100.150
```

The PING should succeed.

Note

In a real Internet environment, many components (routers, firewalls, host filtering, etc.) may filter out ICMP messages. Unfortunately, this makes the verification of the route before starting the VPN tunnel more difficult. In any case, you need to understand the network and filters, and select, for testing purposes, an application that will allow you to verify connectivity.

18.4 S/390 VPN configuration

The following sections explain how to configure the tunnel in the S/390 to establish a VPN with the AS/400 system RALYAS4A. It is beyond the scope of this redbook to provide detailed information about S/390 server configuration. Refer to *SecureWay CS for OS/390 V2R8 TCP/IP: Guide to Enhancements*, SG24-5631, for more information about S/390 VPN configuration.

18.4.1 Completing the S/390 system planning worksheet

Table 116 shows the planning worksheet with the information required to configure the S/390 VPN in this scenario.

Table 116. S/390 system planning worksheet

VPN parameter	Value
Key Policy, Proposal, Transform:	
Initiator Negotiation	Main

VPN parameter	Value
Responder Negotiation	Main
Authentication Method	Pre-shared keys
Hash Algorithm	MD5
Encryption Algorithm	DES_CBC_8
Diffie-Hellmann Group	Group 1
Maximum Key Lifetime	1440 min
Maximum Size Limit	1000 KB
Key Lifetime Range	60 to 1440 minutes
Size Limit Range	1 to 1000 KB
Data Policy, Proposal, AH and ESP Transform:	
PFS (Perfect Forward Secrecy)	Group1
AH Encapsulation Mode	Not applicable
AH Authentication Algorithm	Not applicable
AH Maximum Data Lifetime	Not applicable
AH Maximum Size Limit	Not applicable
AH Data Lifetime Range	Not applicable
AH Size Limit Range	Not applicable
ESP Encapsulation Mode	Transport
ESP Authentication Algorithm	HMAC_MD5
ESP Encryption Algorithm	DES_CBC_8
ESP Maximum Data Lifetime	60 min
ESP Maximum Size Limit	50000 KB
ESP Data Lifetime Range	60 to 480 minutes
ESP Size Limit Range	1 to 50000 KB
Dynamic Tunnel Policy:	
Initiation	Either
Connection Lifetime	0
Authentication Information:	
Remote Key Server	192.168.100.150
Authentication Method	Pre-Shared Keys
Shared Key	61626364 see Note
Certificate Authority	Not applicable
Radcert Label	Not applicable

VPN parameter	Value
Key Ring:	
User ID	Not applicable
Key Ring Name	Not applicable
Dynamic Connection:	
Source	192.168.100.100
Destination	192.168.100.150
Source Port	0
Destination Port	0
Automatic Activation	No
Protocol	All
Remote Key Server	192.168.100.150
Key Servers:	
Local Key Server ID Type	IPV4
Local Key Server ID	192.168.100.100
Remote Key Server ID Type	IPV4
Remote Key Server ID	192.168.100.150

Note

The Shared Key value *61626364* is the hexadecimal representation of *abcd*. The S/390 requires the pre-shared key in a hexadecimal value, although it must be in ASCII on the AS/400 system.

18.4.2 Configuring a host-to-host VPN on the S/390 system

Perform the following steps to configure a host-to-host VPN connection on the S/390 system using the OS/390 Firewall Technologies Configuration Client GUI:

1. Start the OS/390 Firewall Technologies Configuration Client GUI.
2. Expand the folders as shown in Figure 910 on page 805.

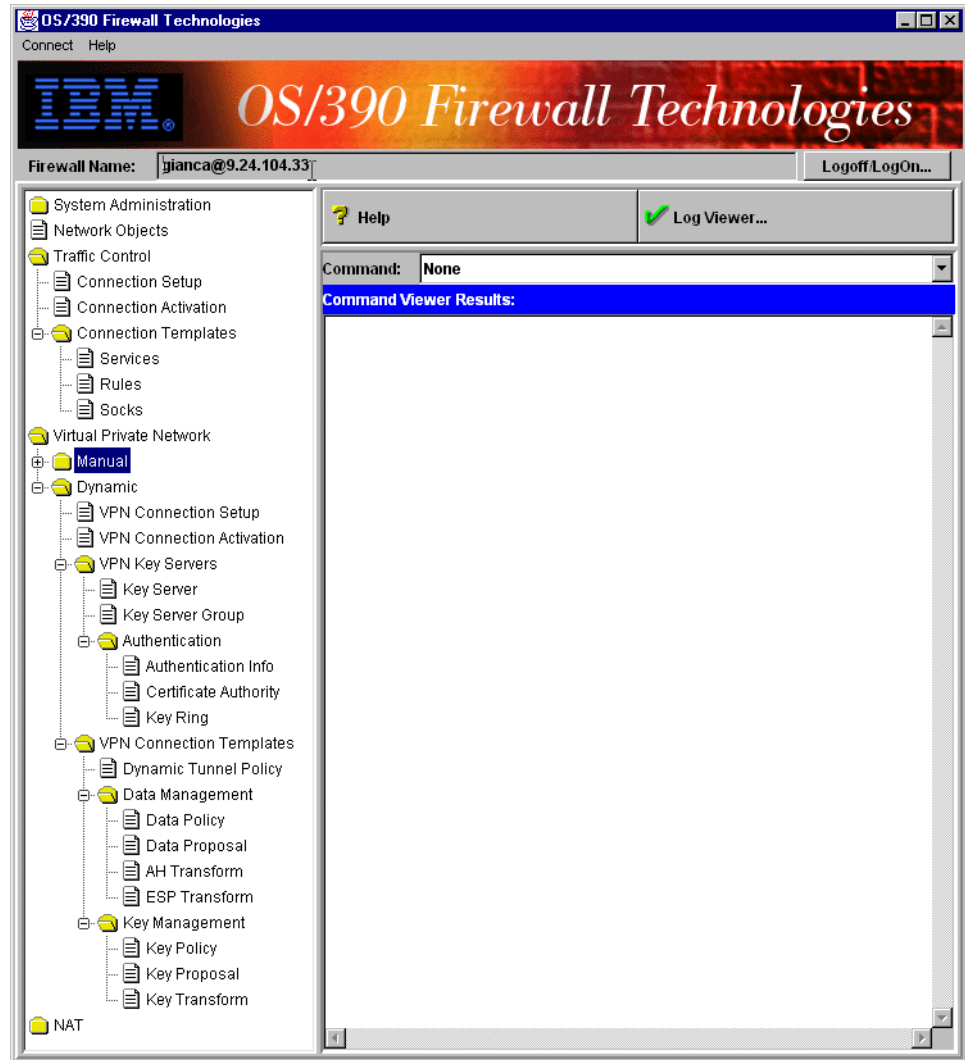


Figure 910. OS/390 Firewall Technologies client GUI

Note

The following windows were displayed after the configuration was completed. That is why *Modify* appears at the window title instead of *Add*. The *Name* parameters appear grayed out for the same reason.

3. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910), select **Key Transform** to display the Key Transform Administration panel.
4. Double-click **New**. The Add Key Transform window appears. Complete the parameters as shown in Figure 911 on page 806.

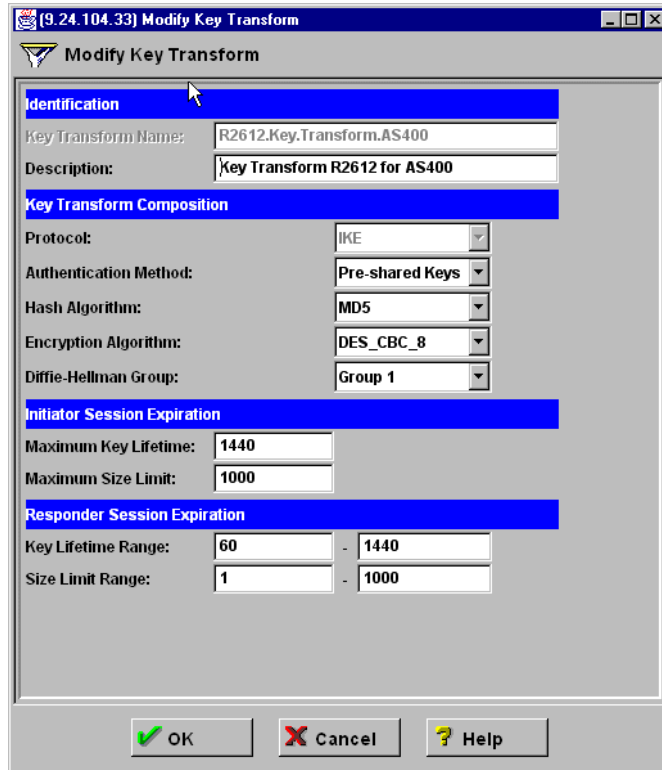


Figure 911. Adding a key transform

5. Click **OK**.
6. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Key Proposal** to display the Key Proposal Administration panel.
7. Double-click **New**. The Add Key Proposal window appears. Complete the parameters as shown in Figure 912. For the Key Transforms Objects parameter, click **Select** to select the Key Transform that was created in Figure 911.

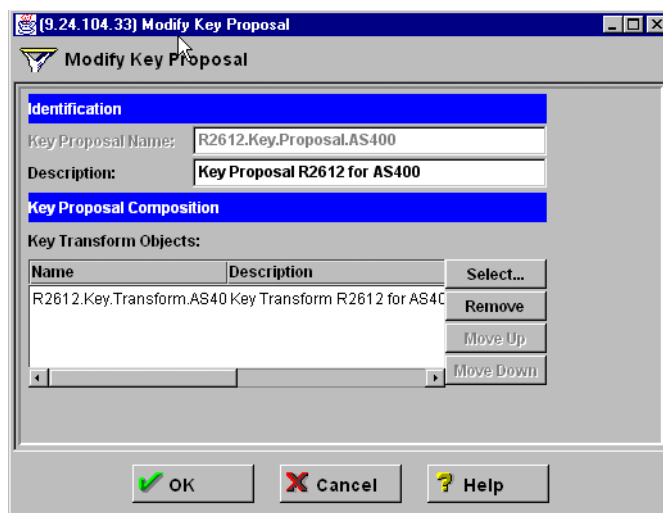


Figure 912. Adding a key proposal

8. Click **OK**.
9. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910), select **Key Policy** to display the Key Policy Administration panel.
10. Double-click **New**. The Add Key Policy window appears. Complete the parameters as shown in Figure 913. For the Key Proposal parameter, click **Select** to select the Key Proposal that was created in Figure 912.

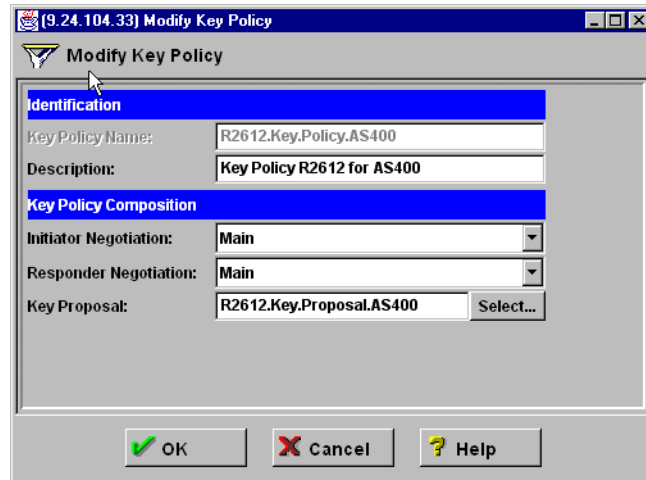


Figure 913. Adding a key policy

11. Click **OK**.
12. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **ESP Transform** to display the ESP Transform Administration panel.
13. Double-click **New**. The Add ESP Transform window appears. Complete the parameters as shown in Figure 914 on page 808.

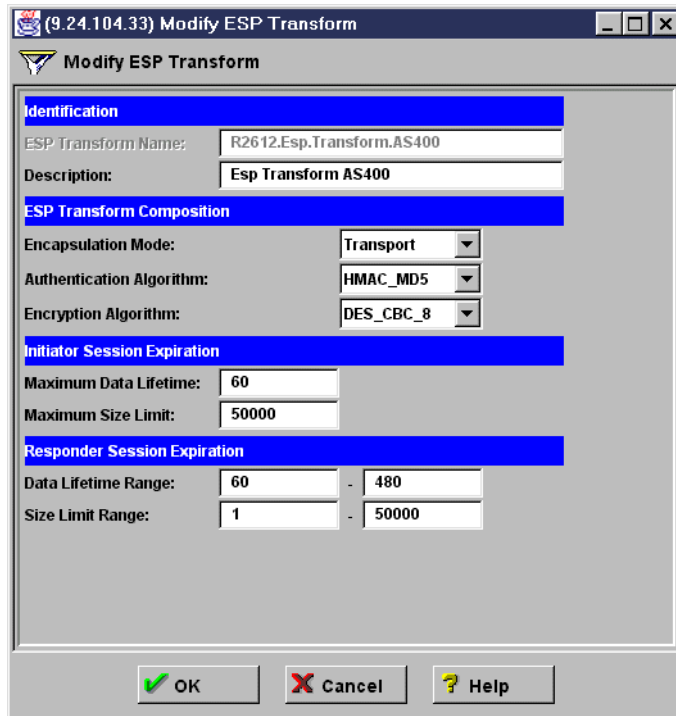


Figure 914. Adding an ESP transform

14. Click **OK**.
15. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Data Proposal** to display the Data Proposal Administration panel.
16. Double-click **New**. The Add Data Proposal window appears. Complete the parameters as shown in Figure 915 on page 809. For the ESP Transform Objects parameter, click **Select** to select the ESP transform that was created in Figure 914.

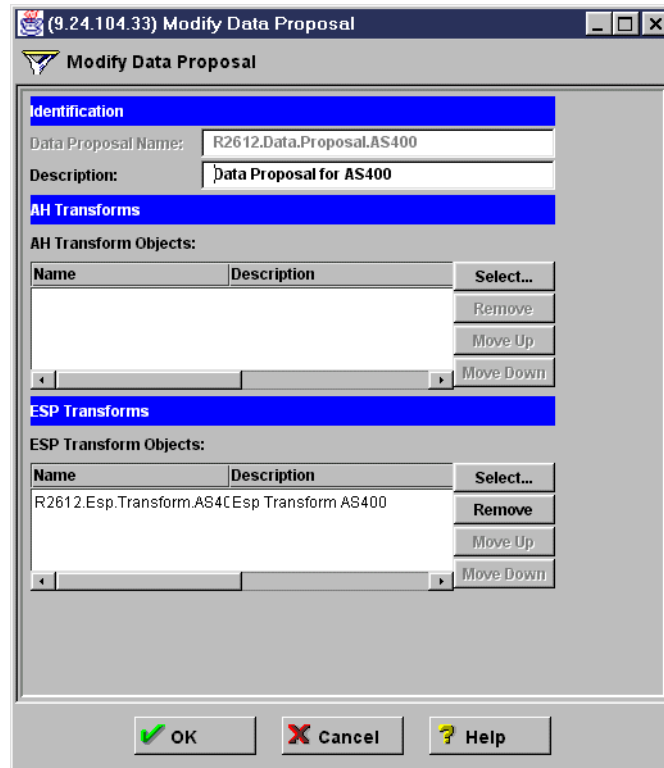


Figure 915. Adding a data proposal

17. Click **OK**.
18. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Data Policy** to display the Data Policy Administration panel.
19. Double-click **New**. The Add Data Policy window appears. Complete the parameters as shown in Figure 916 on page 810. For the Data Proposal Objects parameter, click **Select** to select the data proposal that was created in Figure 915.

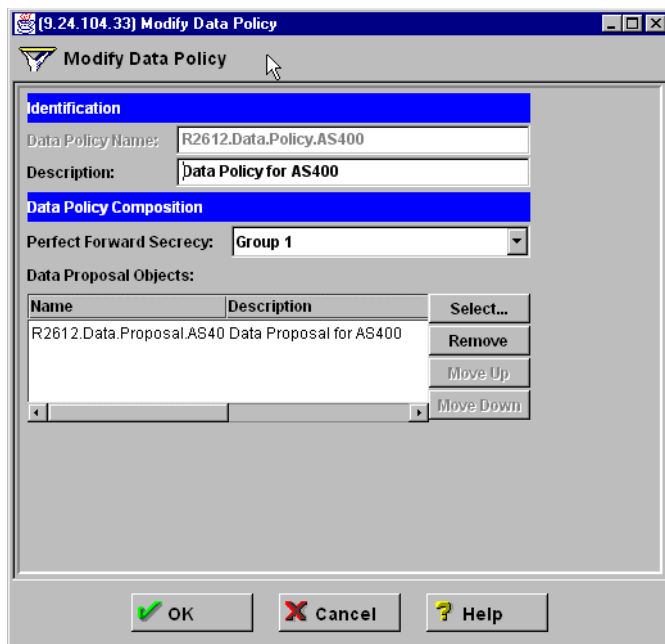


Figure 916. Adding a data policy

20. Click **OK**.

21. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Dynamic Tunnel Policy** to display the Dynamic Tunnel Policy Administration panel.

22. Double-click **New**. The Add Dynamic Tunnel Policy window appears. Complete the parameters as shown in Figure 917. For the Data Policy parameter, click **Select** to select the data policy that was created in Figure 916.

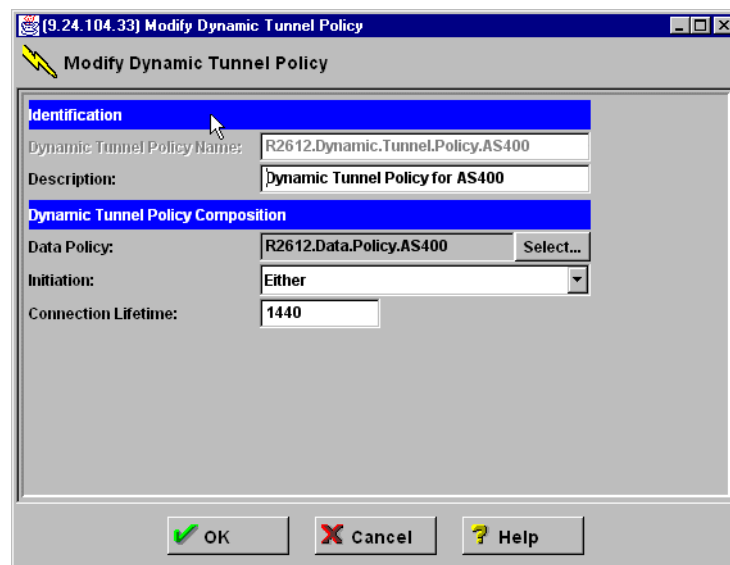


Figure 917. Adding a dynamic tunnel policy

23. Click **OK**.

24. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Key Server** to display the Key Server Administration panel.
25. Double-click **New**. The Add Key Server window appears. Complete the parameters for the OS/390 key server as shown in Figure 918.

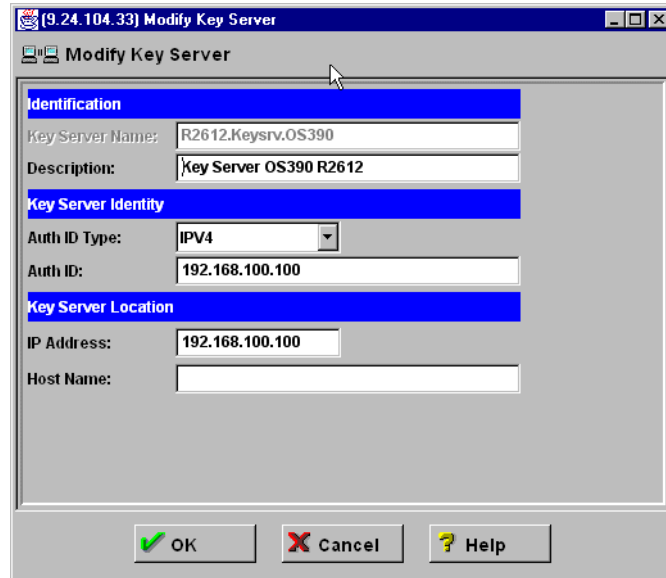


Figure 918. Adding a local key server - S/390

26. Click **OK**.
27. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Key Server** again to display the Key Server Administration panel.
28. Double-click **New**. The Add Key Server window appears. This time, complete the parameters for the AS/400 system as shown in Figure 919.

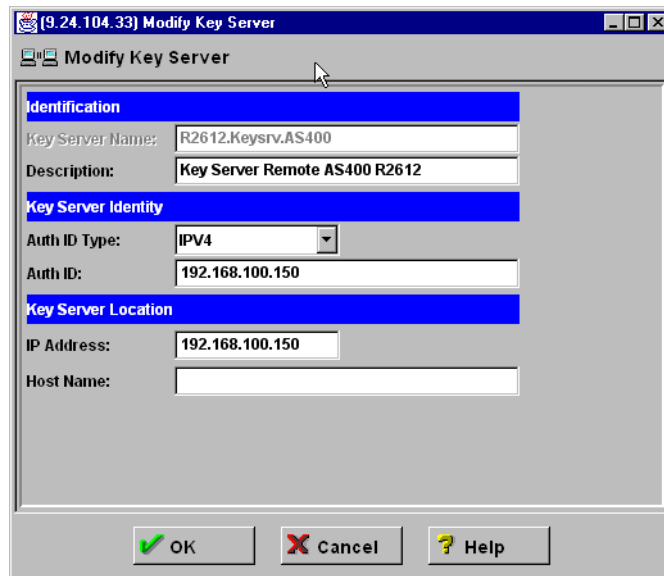


Figure 919. Adding a remote key server - RALYAS4A

29. Click **OK**.
30. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Authentication Info** to display the Authentication Information Administration panel.
31. Double-click **New**. The Add Authentication Information window appears. Complete the parameters as shown in Figure 920. For the Remote Key Server parameter, click **Select** to select the AS/400 key server as shown in Figure 919. Enter the Shared Key parameter value as 61626364, which is the hexadecimal representation of *abcd*.

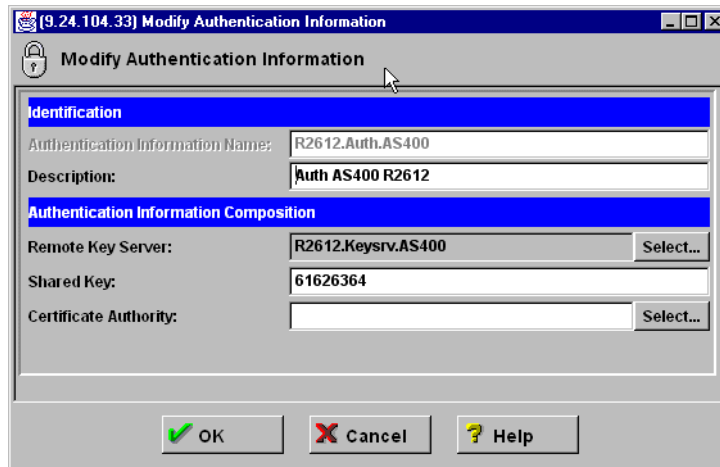


Figure 920. Adding authentication information

32. Click **OK**.
33. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Key Server Group** to display the Key Server Group Administration panel.
34. Double-click **New**. The Add Key Server Group window appears. Complete the parameters as shown in Figure 921 on page 813. For the Key Policy parameter, click **Select**, and select the key policy created in Figure 913 on page 807. For the Local Key Server parameter, click **Select**, and select the S/390 key server created in Figure 918. For the Remote Key Servers - Key Server Object, parameter, click **Select**, and select the AS/400 key server created in Figure 920.

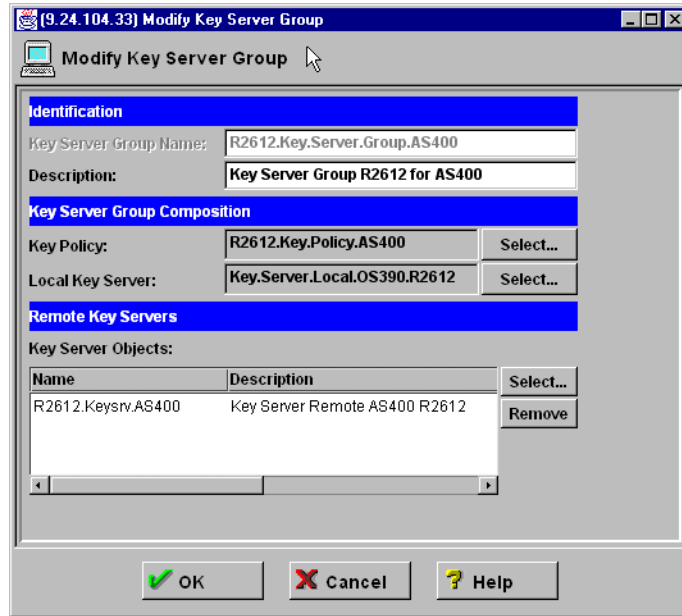


Figure 921. Adding a key server group

35. Click **OK**.

36. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **Network Objects** to display the Network Objects Administration panel.

37. Double-click **New**. The Add Network Objects window appears. Complete the parameters as shown in Figure 922 for the S/390 system.

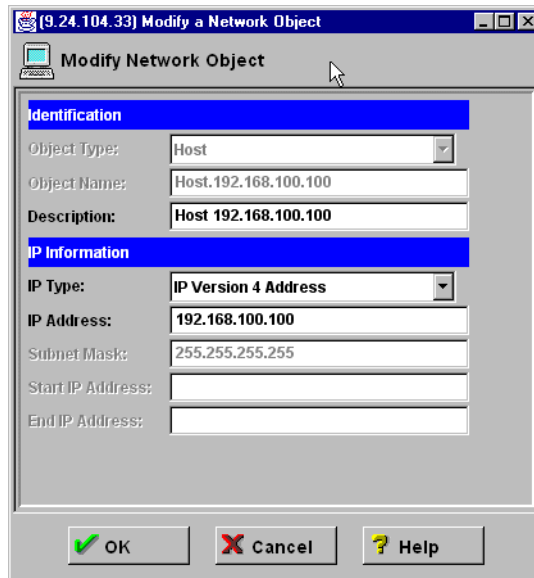


Figure 922. Network object for S/390

38. Click **OK**.

39. Repeat steps 36 through 38 to create another network object for the AS/400 system as shown in Figure 923 on page 814.

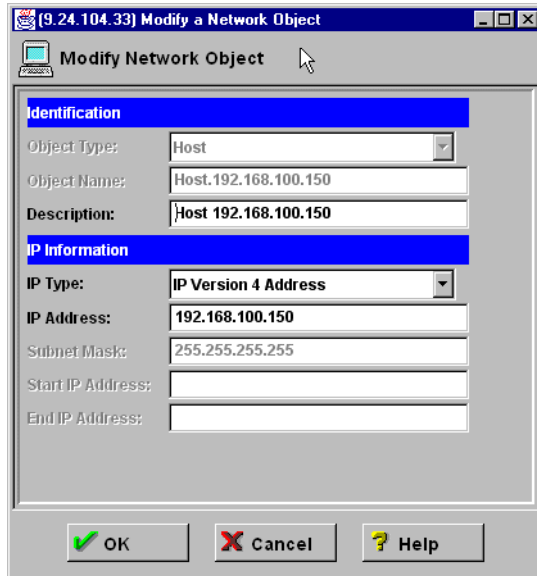


Figure 923. Network object for the AS/400 system

40. Create an anchor filter rule to define the traffic that is permitted to use the tunnel. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), click **Rules**.
41. On the Rules List window, double-click **New**. The Add IP Rule window appears. Complete the parameters as shown in Figure 924 on page 815. In this example scenario, allow all protocols on all source and destination ports. For the Dynamic Tunnel Policy Name parameter, click **Select**, and select the Dynamic Tunnel Policy created in Figure 917 on page 810.

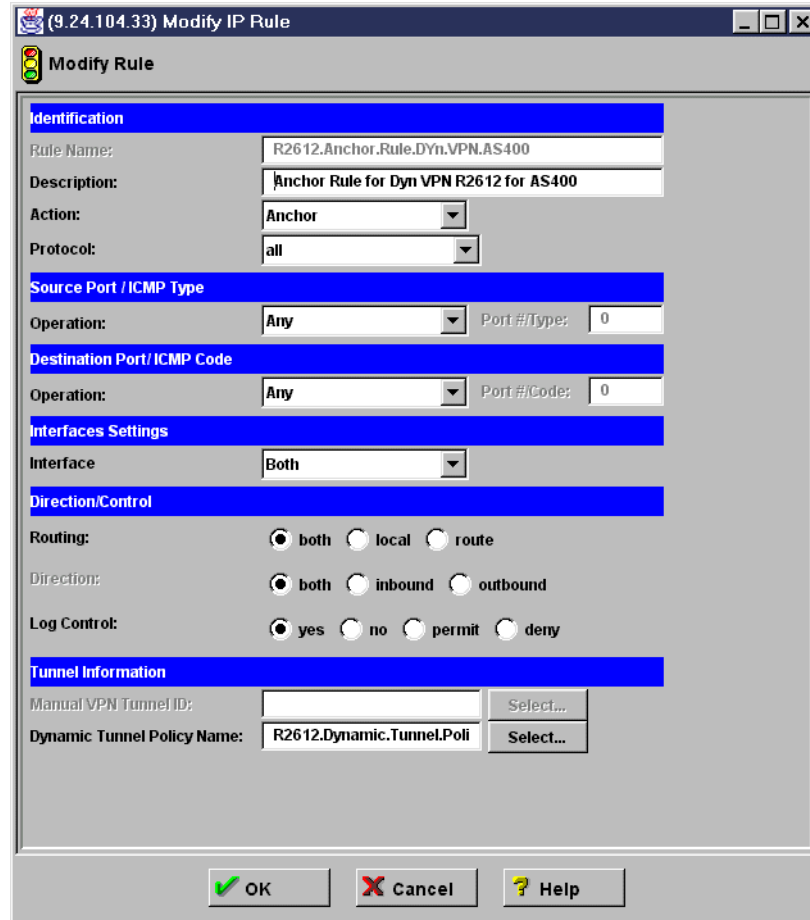


Figure 924. Adding an anchor filter rule

42. Click **OK**.

43. The IP rule created in Figure 924 is linked to a service. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), click **Services**. The Services List window appears.

44. Double-click **New** to access the Add Service window. Complete the parameters as shown in Figure 925 on page 816. For the Rule Objects parameter, click **Select**, and select the IP rule created in Figure 924.

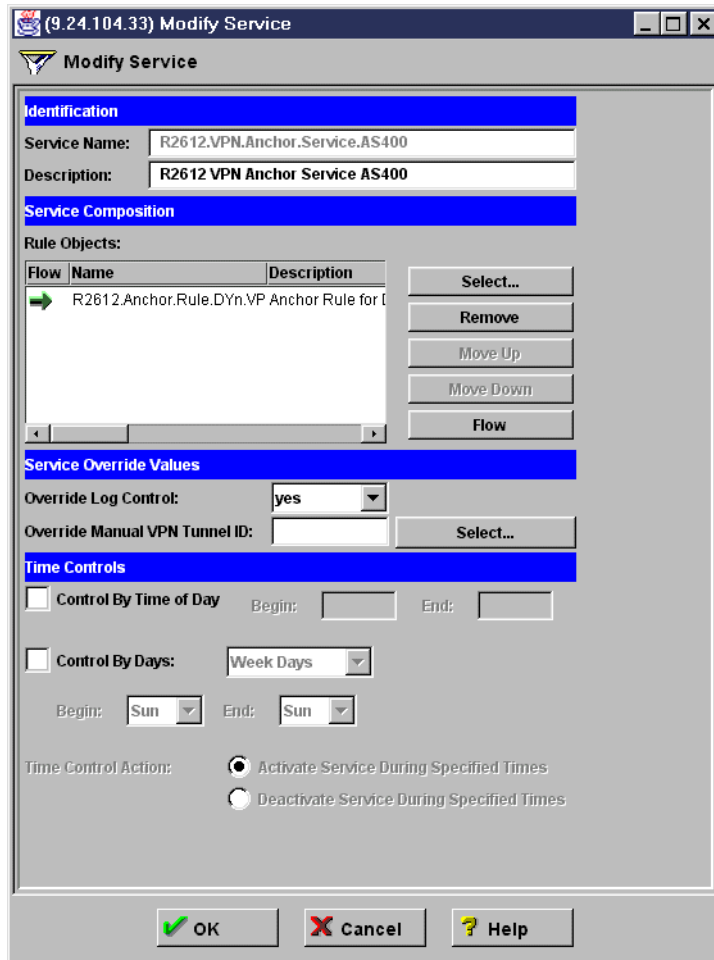


Figure 925. Adding an anchor service

45. Click **OK**.
46. Create an anchor connection for traffic in the outgoing direction that can use the tunnel. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910), click **Connection Setup**. The Connections List window appears. Select **New**.
47. Click **Open**. The Add a Connection window appears. Complete the parameters as shown in Figure 926 on page 817. For the Source parameter, click **Select**, and select the S/390 network object that was created in Figure 922 on page 813. For the Destination parameter, click **Select**, and select the AS/400 network object that was created in Figure 923 on page 814. For the Service Object parameter, click **Select**, and select the service that was created in Figure 925.

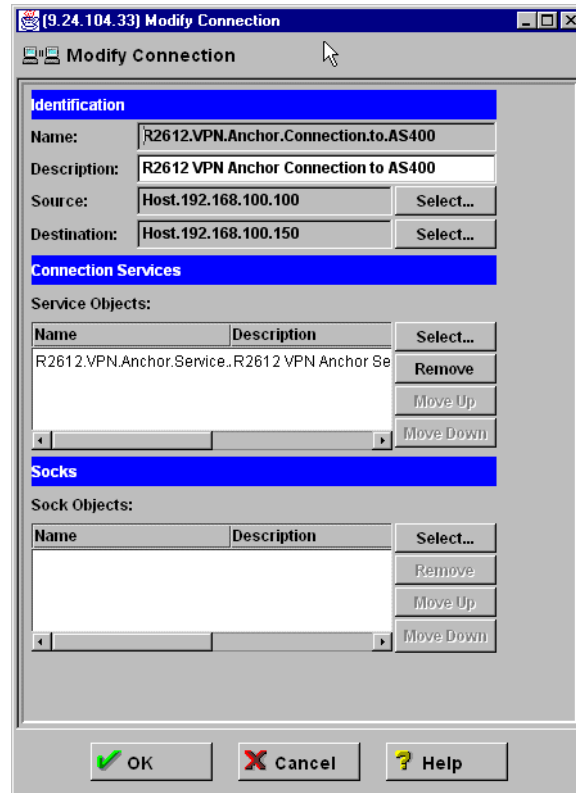


Figure 926. VPN anchor connection - S/390 to AS/400

48. Click **OK**.

49. Create another anchor connection for traffic in the incoming direction that can use the tunnel. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), click **Connection Setup**. The Connections List window appears. Select **New**.

50. Click **Open**. The Add a Connection window appears. Complete the parameters as shown in Figure 927 on page 818. For the Source parameter, click **Select**, and select the AS/400 network object that was created in Figure 923 on page 814. For the Destination parameter, click **Select**, and select the S/390 network object that was created in Figure 922 on page 813. For the Service Objects parameter, click **Select**, and select the service that was created in Figure 925 on page 816.

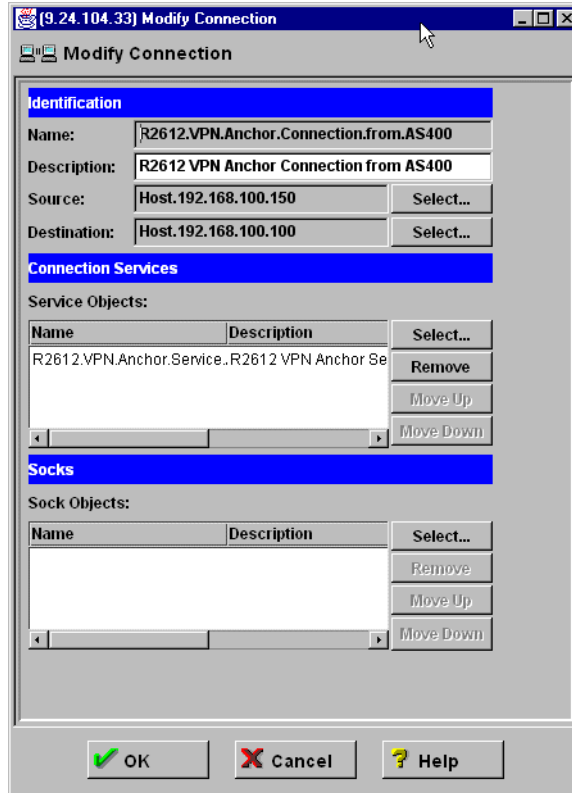


Figure 927. VPN anchor connection - AS/400 to S/390

51. Click **OK**.

52. Create a separate set of IP rules, service, and connection to allow UDP 500, AH, and ESP traffic between the AS/400 and S/390 systems. The exact steps involved are not documented here. However, Figure 928 and Figure 929 on the following pages summarize this configuration.

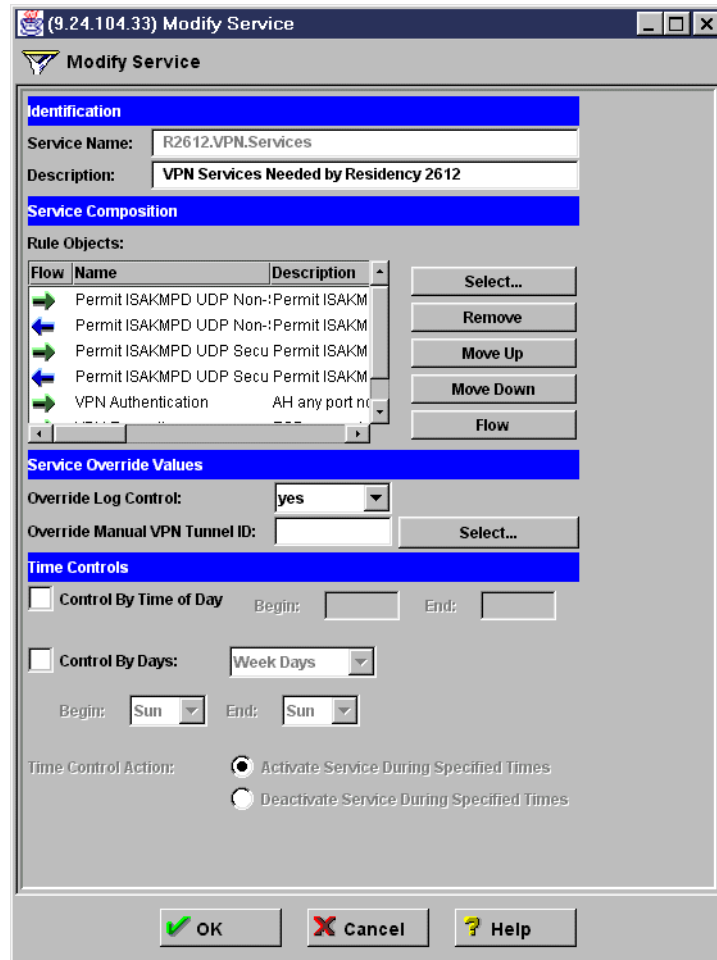


Figure 928. Service for UDP 500, AH, and ESP traffic

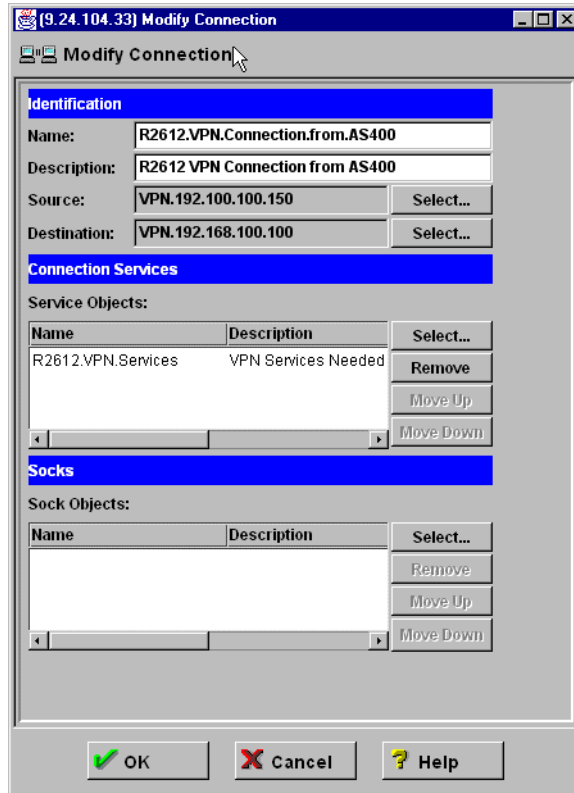


Figure 929. Connection for UDP port 500, AH, and ESP traffic

53. Create a dynamic VPN connection. At the OS/390 Firewall Technologies Configuration Client GUI (Figure 910 on page 805), select **VPN Connection Setup** to display the Dynamic VPN Connection Administration panel.
54. Double-click **New**. The Add Dynamic VPN Connection window appears. Complete the parameters as shown in Figure 930 on page 821. For the Source parameter, click **Select**, and select the S/390 network object that was created in Figure 922 on page 813. For the Destination parameter, click **Select**, and select the AS/400 network object that was created in Figure 923 on page 814. For the Remote Key Server parameter, click **Select**, and select the AS/400 key server created in Figure 919 on page 811. For the Key Server Group parameter, click **Select**, and select the AS/400 key server group created in Figure 921 on page 813.

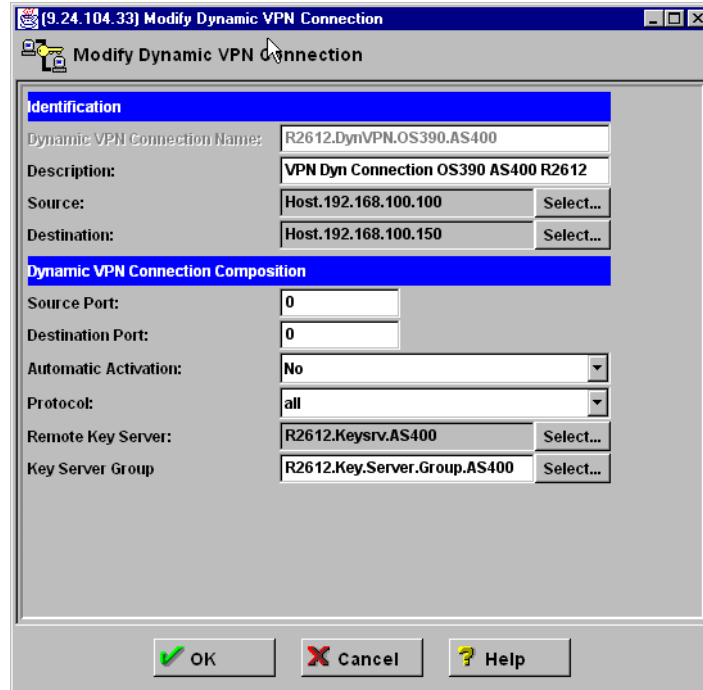


Figure 930. Adding a dynamic VPN connection

55. Click **OK**.

This completes the VPN configuration on the S/390 system.

18.5 AS/400 host-to-host VPN configuration

The following sections explain how to configure the host-to-host dynamic connection on the AS/400 system RALYAS4A to establish a VPN with the OS/390 server.

18.5.1 Completing the AS/400 system planning worksheets

Complete the AS/400 system planning worksheet for the VPN configuration wizard as shown in Table 117.

Table 117. AS/400 system RALYAS4A - Planning worksheet

This is the information needed to create VPN with the New Connection Wizard	Scenario answers
What is the type of connection to be created? – Gateway to Gateway – Host to Gateway – Gateway to Host – Host to Hosts – Gateway to Dynamic IP User – Host to Dynamic IP User	Host to Hosts
What is the name of the connection group?	HtoH4AtoMF

This is the information needed to create VPN with the New Connection Wizard	Scenario answers
What type of security and system performance is required to protect the keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced
How is the local VPN server identified?	IP address
What is the IP address of the local VPN server?	192.168.100.150
How is the remote VPN server identified?	IP address
What is the IP address of the remote VPN server?	192.168.100.100
What is the pre-shared key?	abcd
What type of security and system performance is required to protect the data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	Balanced

Complete the IP filters planning worksheet as shown in Table 118.

Table 118. AS/400 system RALYAS4A - IP filters planning worksheet

This is the information needed to create the IP filters to support the VPN connection	Scenario answers
Is the local VPN server acting as a host or gateway ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, the VPN server acts as a host. If no, the VPN server acts as a gateway.	Host
Is the <i>remote</i> VPN server acting as a host or gateway ?	Host
What is the name used to group together the set of filters that will be created?	VPNIFC
If the local VPN server is acting as a gateway ... – What is the IP address of the local ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>source address</i> on the IPSEC filter.	Not applicable
If the <i>remote</i> VPN server is acting as a gateway ... – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What is the name for these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.	Not applicable
What is the IP address of the local VPN server? – Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters. – Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a host .	192.168.100.150

This is the information needed to create the IP filters to support the VPN connection	Scenario answers
What is the IP address of the remote VPN server? – Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters. – Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a host .	192.168.100.100
What is the name of interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TOKENRING2
What other IP addresses, protocols, and ports are permitted on this interface? Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i> !	10.1.1.0

18.5.2 Configuring a host-to-host VPN on RALYAS4A

Use the VPN New Connection Wizard to create the VPN configuration on RALYAS4A. Perform the following steps:

1. At the Virtual Private Networking GUI menu bar (Figure 931), select **File->New Connection**.

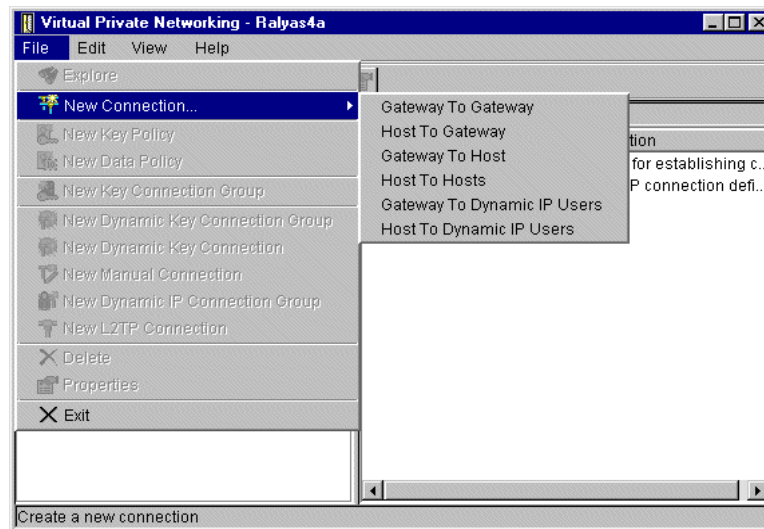


Figure 931. VPN New Connection Wizard

2. Select **Host to Hosts**. This starts the New Connection Wizard for a host-to-host connection (Figure 932 on page 824).

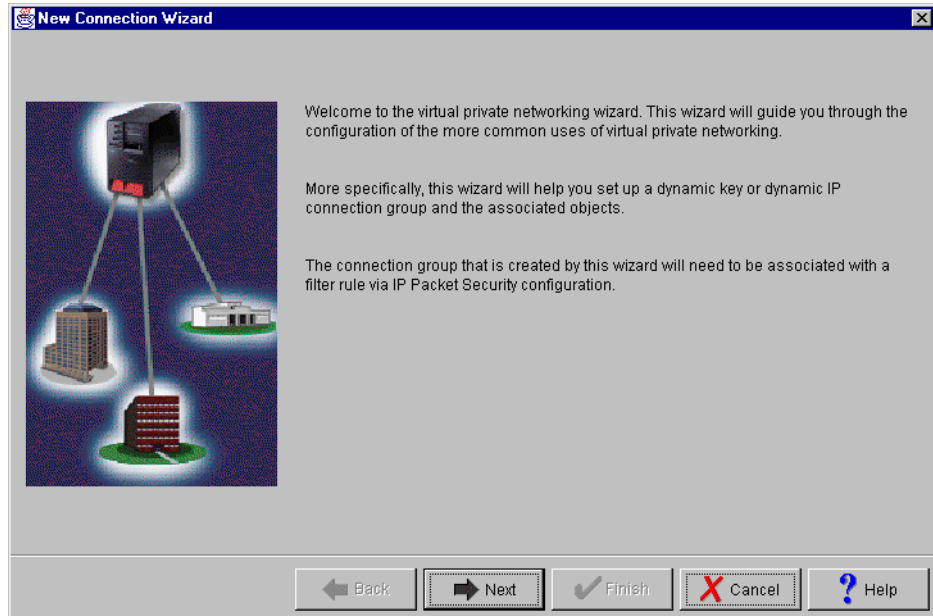


Figure 932. New Connection Wizard welcome window

3. Click **Next** after reading the Welcome window.
4. At the Connection Name window (Figure 933), enter the Name, `HtoH4AtoMF`, for the connection group. Recall that `HtoH4AtoMF` is the name from the worksheet in Table 117 on page 821. This name is used for all objects that the wizard creates for this connection. It is case sensitive. Also enter a description for the configuration.

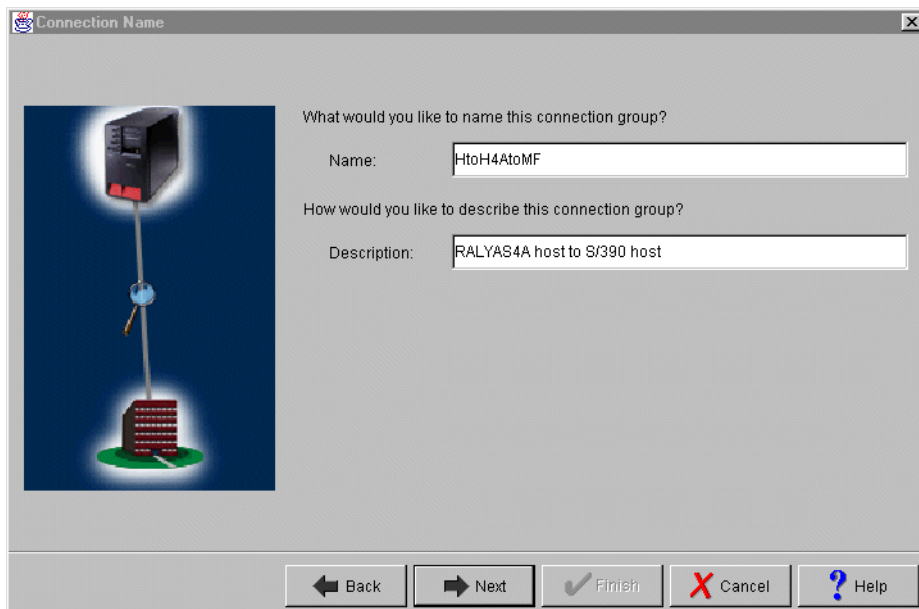


Figure 933. Connection Name window

5. Click **Next**.
6. At the Key Policy window (Figure 934), specify the level of authentication or encryption protection that IKE uses during phase 1 negotiations. Phase 1

establishes the keys that protect the messages that flow during subsequent phase 2 negotiations. Phase 2 protects the data itself. For the purpose of this example, select **Balance security and performance** as specified on the worksheet in Table 117 on page 821. The wizard chooses the appropriate encryption and authentication algorithms based on the selection made here.

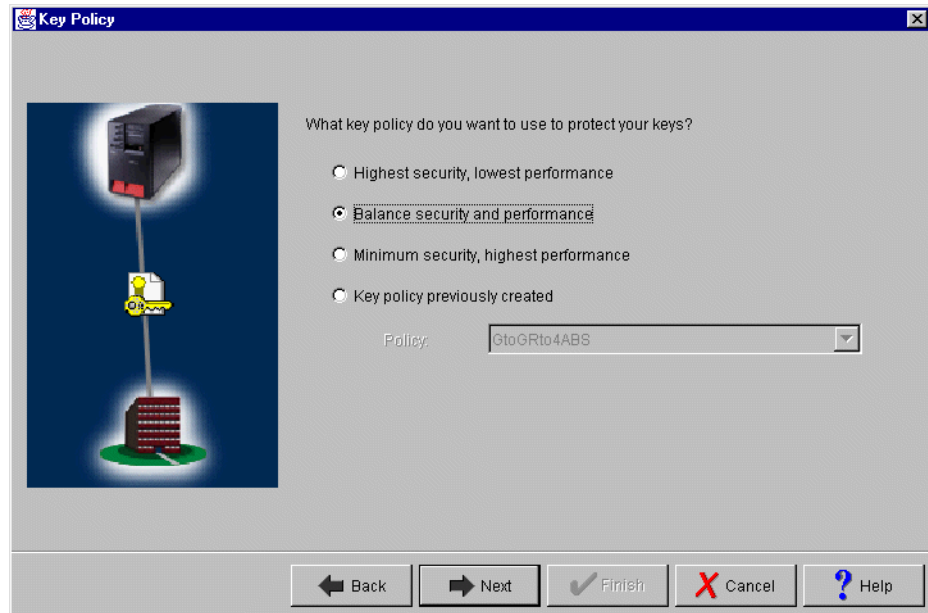


Figure 934. Key Policy window

7. Click **Next**.

8. In the Local Identifier window (Figure 935 on page 826), specify the identity of the local key server. In other words, specify the local AS/400 that acts as the VPN gateway, which, in this case, is RALYAS4A. Leave Identifier type as the default value, **Version 4 IP address**. For the IP Address parameter, use the pull-down menu to select the IP address of the interface that connects to the remote host S/390 system. Refer back to the planning worksheet in Table 117 on page 821 and to the network configuration in Figure 909 on page 801. For RALYAS4A, this is **192.168.100.150**.

Note: Figure 935 shows various IP addresses, such as 9.24.104.21, 9.24.106.18, and so on, that we do not reference anywhere in this scenario. These interfaces are configured on RALYAS4A. However, they are used for other scenarios and projects and should be ignored here.

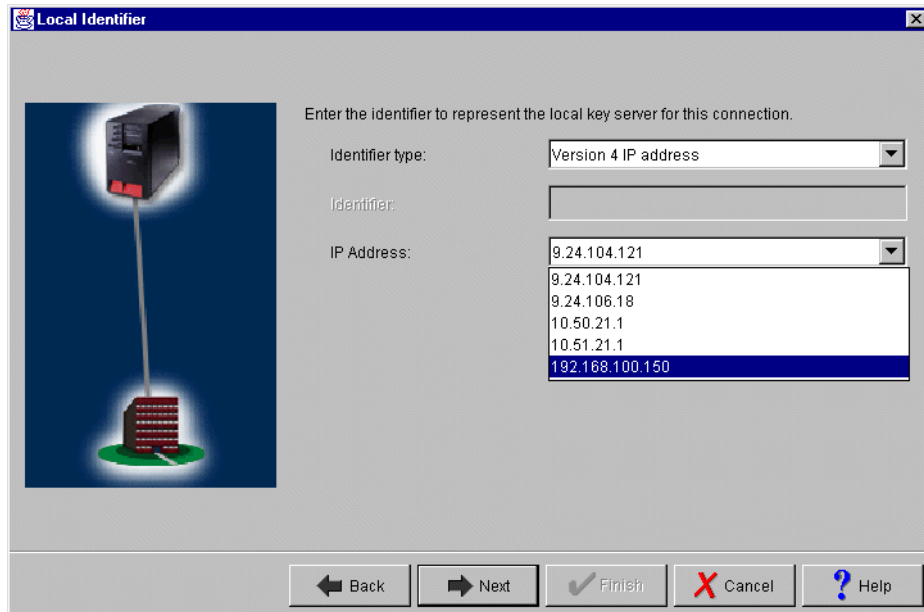


Figure 935. Local Identifier window pull-down list

9. Click **Next**.

10. On the Remote Hosts window (Figure 936), click **Add** to add the remote S/390 host definition.

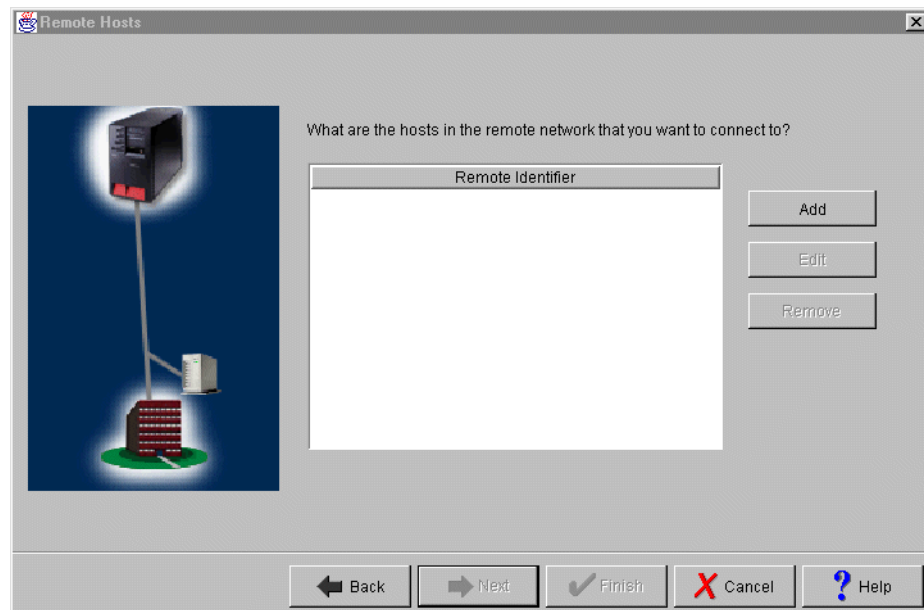


Figure 936. Remote Hosts window

11. At the Remote Identifier window (Figure 937 on page 827), refer to the worksheet in Table 117 on page 821 to define the following parameters:

- **Identifier Type:** Version 4 IP address
- **IP Address:** 192.168.100.100
- **Pre-shared Key:** abcd

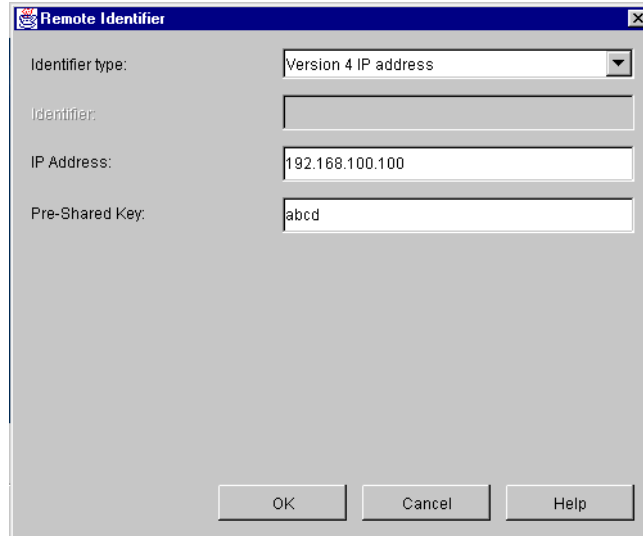


Figure 937. Remote Identifier

12. Click **OK**.

13. Back at the Remote Hosts window (Figure 936), click **Next**.

14. Select **Balance security and performance** on the Data Policy window (Figure 938).

Based on this selection, the wizard selects the appropriate encryption and authentication algorithms, as well as the IPSec protocol for the user data traffic.

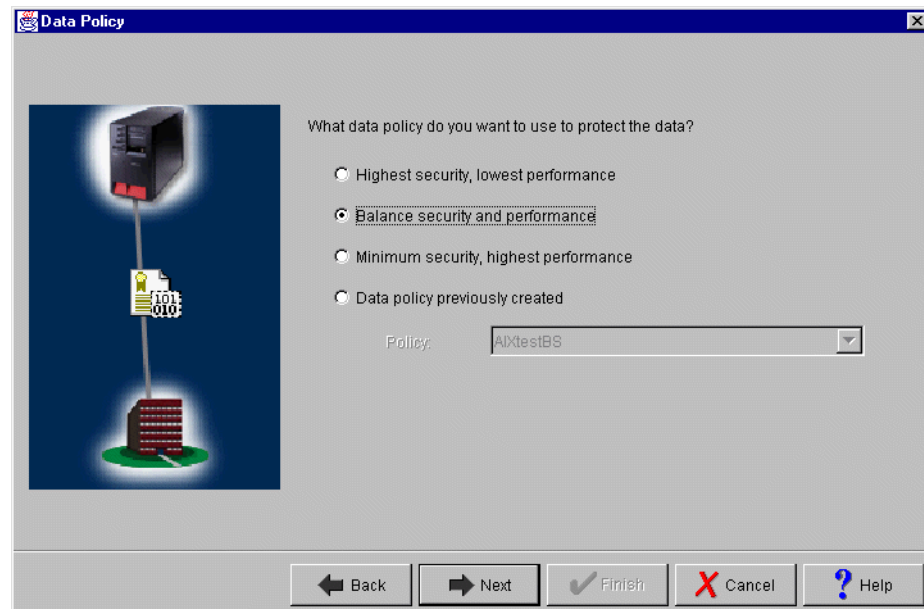


Figure 938. Data Policy

15. Click **Next**.

16. The final window (Figure 939 on page 828) summarizes the configuration values entered. Scroll down to see a list of the configuration objects that the

wizard will create. Check the configuration values against the worksheet. If changes need to be made, click the **Back** button.

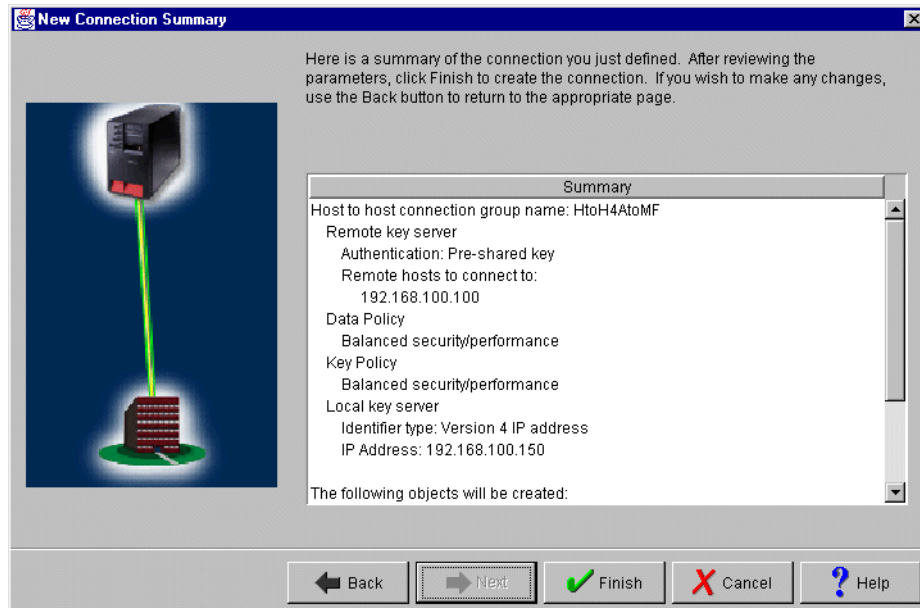


Figure 939. New Connection Summary

17. When you are satisfied with the values, click **Finish**.

This completes the VPN configuration wizard. In the next section, you customize some configuration values created by the wizard to match the S/390 VPN configuration.

18.5.3 Matching the S/390 system VPN configuration

In this example scenario, use the Virtual Private Networking configuration GUI to customize the identity protection and key lifetimes. These values on the AS/400 system must be consistent with those values of the S/390 system. The Virtual Private Networking New Connection Wizard does not provide the option to allow you to configure main mode for identity protection or customize the key lifetime values.

Perform the following steps:

1. At the Virtual Private Networking GUI (Figure 940 on page 829), expand the **IP Security Policies** folder, and click **Key Policies**. This displays a list of key policies, including the one that was just created.
2. Double-click the **HtoH4AtoMF** key policy.

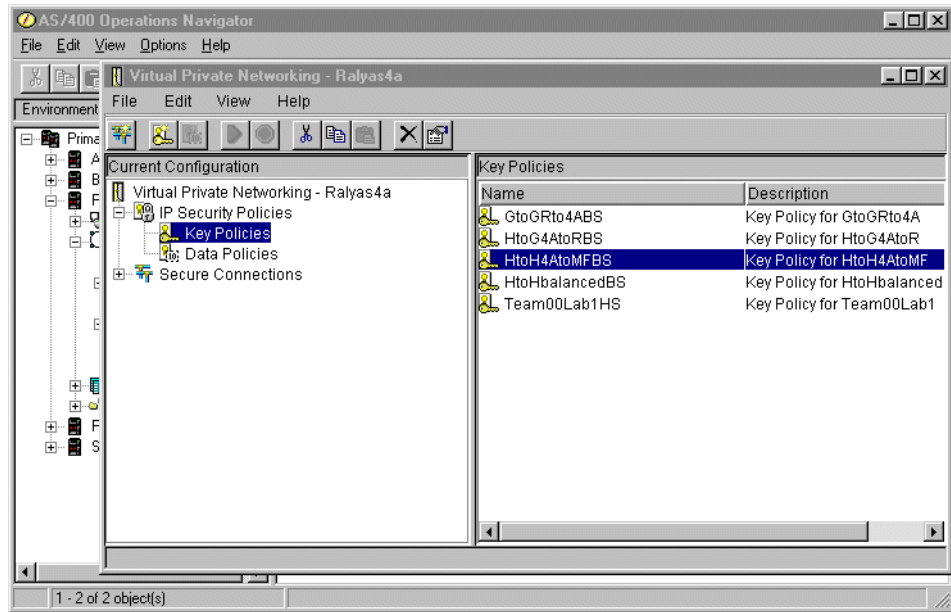


Figure 940. Virtual Private Networking GUI - Key Policies

- At the Key Policy Properties General page (Figure 941), select **Identity protection (ISAKMP main mode negotiation)** for the Initiator Negotiation parameter. Also, select **Require identity protection** for the Responder negotiation parameter.

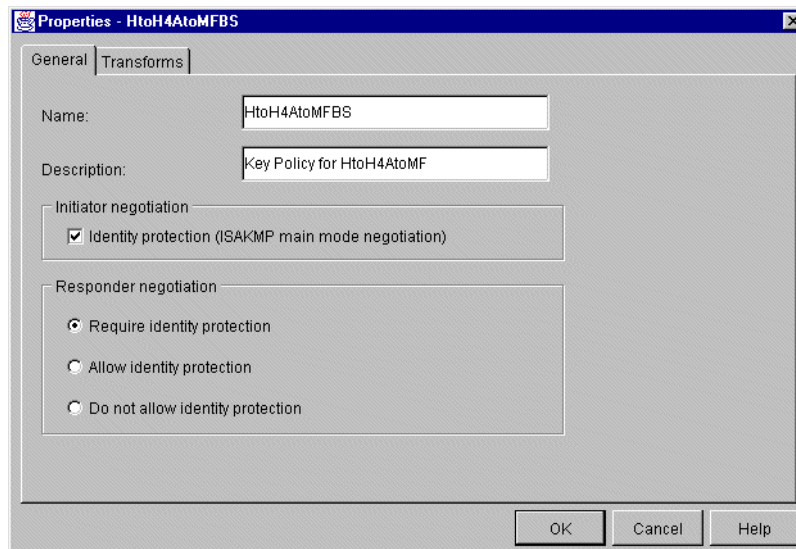


Figure 941. Key Policy Properties General page

- At the Transforms window (Figure 942 on page 830), select the key protection transform, and click **Edit**.

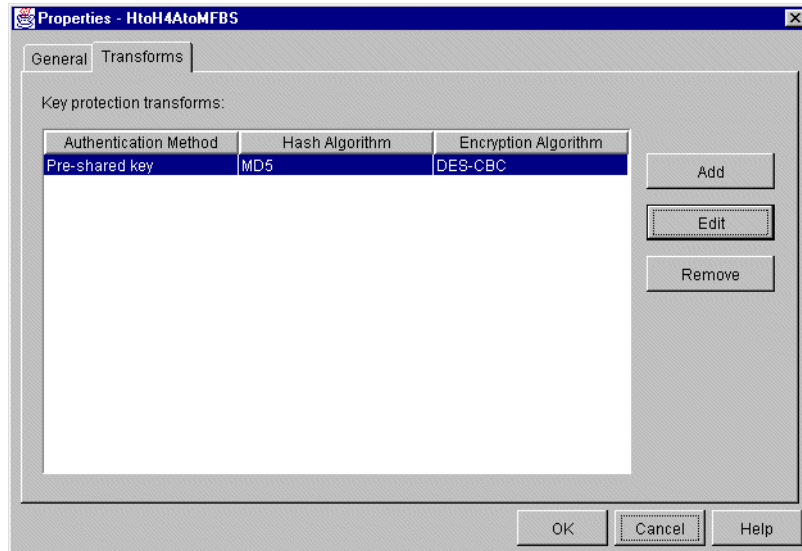


Figure 942. Key Policy Properties Transforms page

- At the Key Protection Transform window (Figure 943), change the Maximum key lifetime value to 1440 and the Maximum size limit value to 1000.

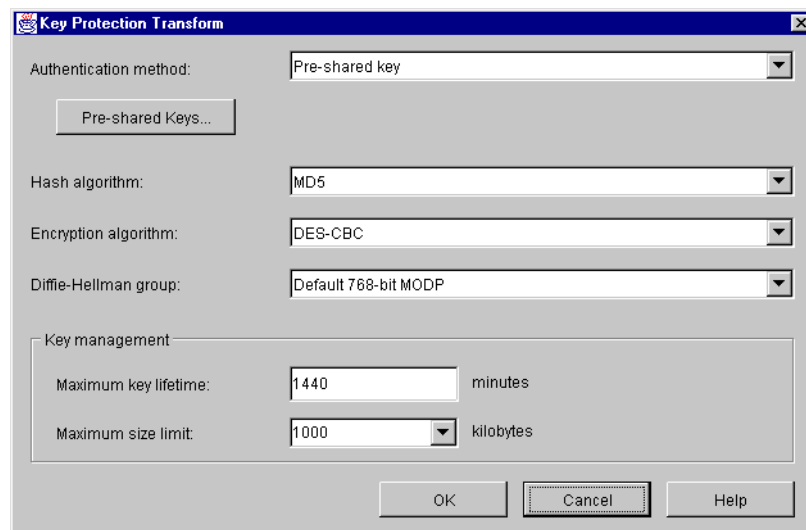


Figure 943. Key Protection Transform window

Note

AS/400 IKE implementation always matches as long as the same attributes are proposed and in the policy. For example, if time is proposed, AS/400 IKE only matches a policy which has time defined. If time and size are proposed, AS/400 IKE only matches a policy that has both time and size defined. This is true for both phase 1 and phase 2.

- Click **OK**.
- Back at the Key Policy Properties window (Figure 942), click **OK**.

8. Back at the Virtual Private Networking GUI window (Figure 944), click **Data Policies** to display a list of data policies.
9. Double-click the **HtoH4AtoMFBS** data policy.

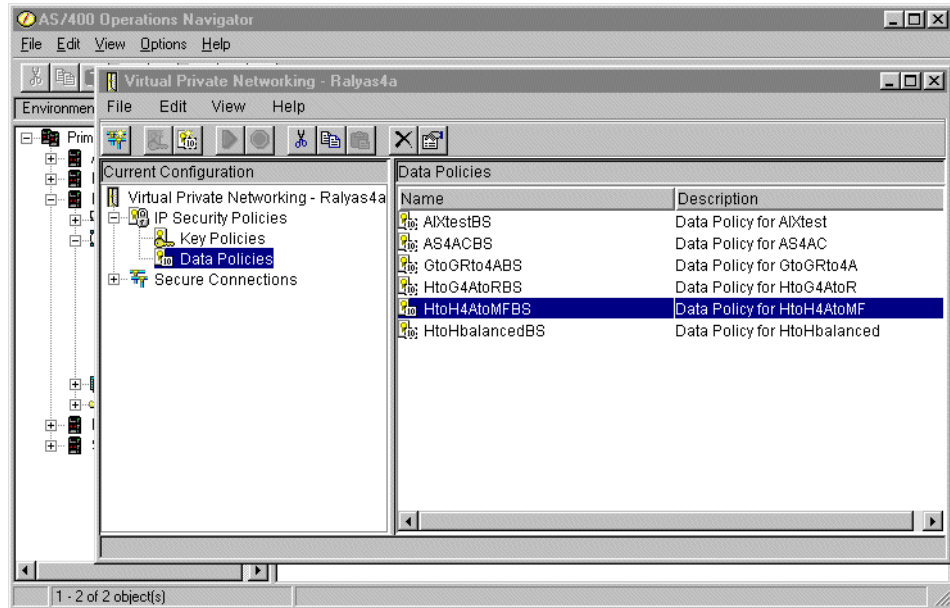


Figure 944. Virtual Private Networking GUI - Data Policies

10. At the Data Policy Properties window (Figure 945), enable **Use Diffie-Hellman perfect forward secrecy**, and select **Default 768-bit MODP** (group 1) for the Diffie-Hellman Group parameter.

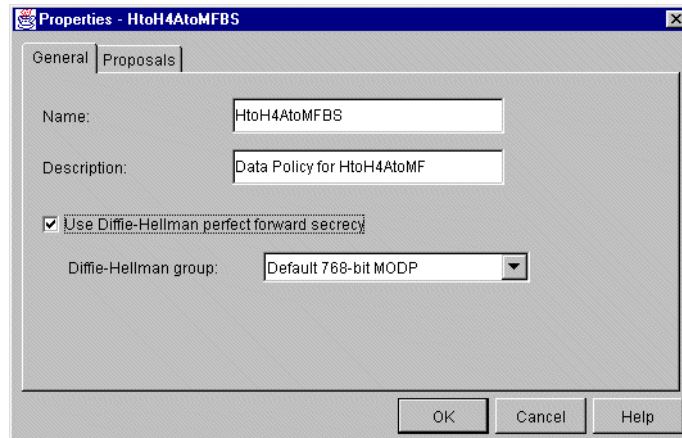


Figure 945. Data Policy Properties window

11. At the Data Policy Properties Proposals window (Figure 946 on page 832), select the data protection proposal, and click **Edit**.

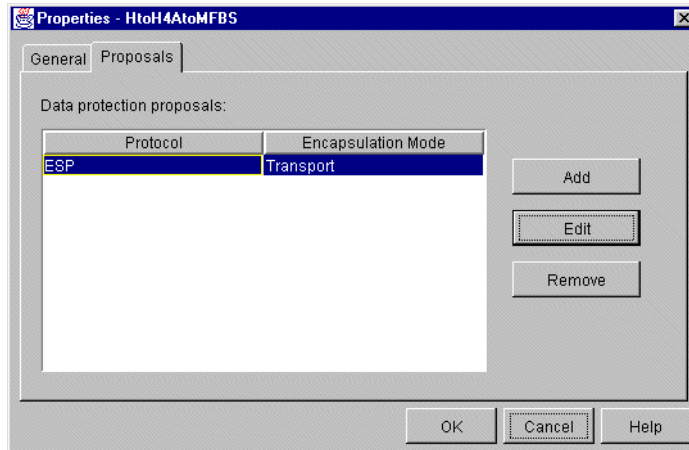


Figure 946. Data Policy Properties Proposals page

12. At the Data Protection Proposal Key Expiration page (Figure 947), change the Expire after parameter value to 60 and Expire at size limit parameter value to 50000.

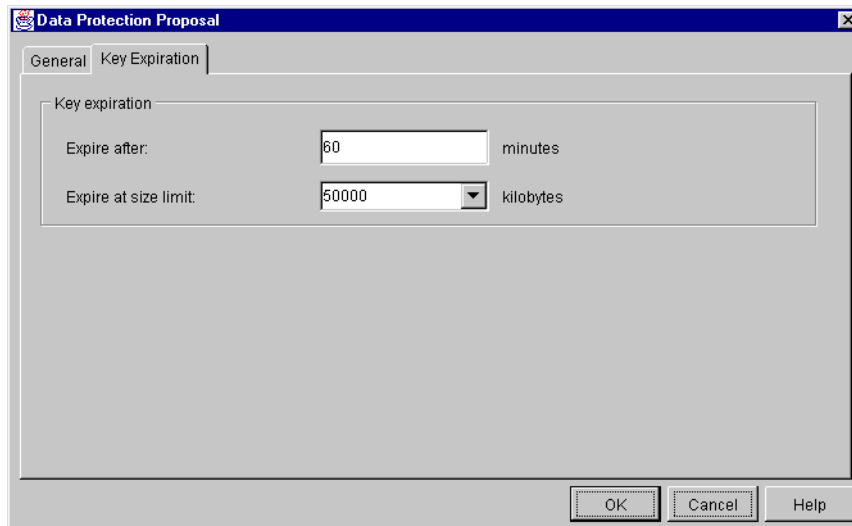


Figure 947. Data Protection Proposal window

13. Click **OK**.

14. Back at the Data Policy Properties window (Figure 946), click **OK**.

The host-to-hosts VPN configuration is now completed for RALYAS4A. In the next task, we configure IP packet security.

18.5.4 Configuring IP packet security on RALYAS4A

The New Connection Wizard does *not* configure IP filters. You must configure filter rules to allow IKE negotiation traffic. You must also configure a filter rule with action IPSec and associate it with the connection group created by the wizard. Use the IP Packet Security GUI in Operations Navigator to configure these filters.

Configure the following filter rules:

- Two filter rules to allow inbound and outbound IKE negotiations.
- One IPSEC filter rule associated with the connection created in 18.5.2, “Configuring a host-to-host VPN on RALYAS4A” on page 823.
- One filter interface associated with the filter rules. This is the physical LAN line TOKENRING2.

Perform the following steps:

1. At the IP Packet Security GUI window (Figure 948), click **Filters**, and select **New Filter**.

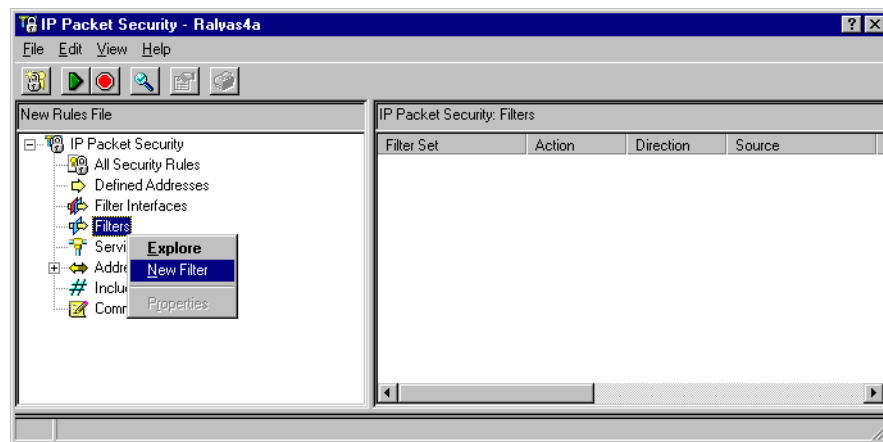


Figure 948. IP Packet Security GUI - Creating a filter rule

2. Configure the outbound IKE filter rule to permit IKE negotiations (Figure 949).

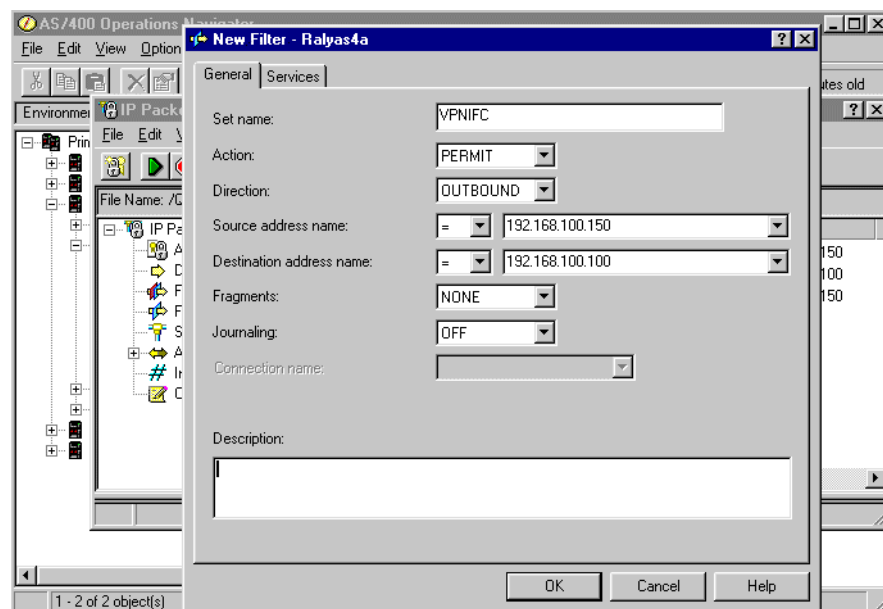


Figure 949. RALYAS05 Outbound IKE filter rule

3. Click the **Services** tab.

- IKE negotiations use protocol UDP and source and destination port 500. Enter the values as shown in Figure 950.

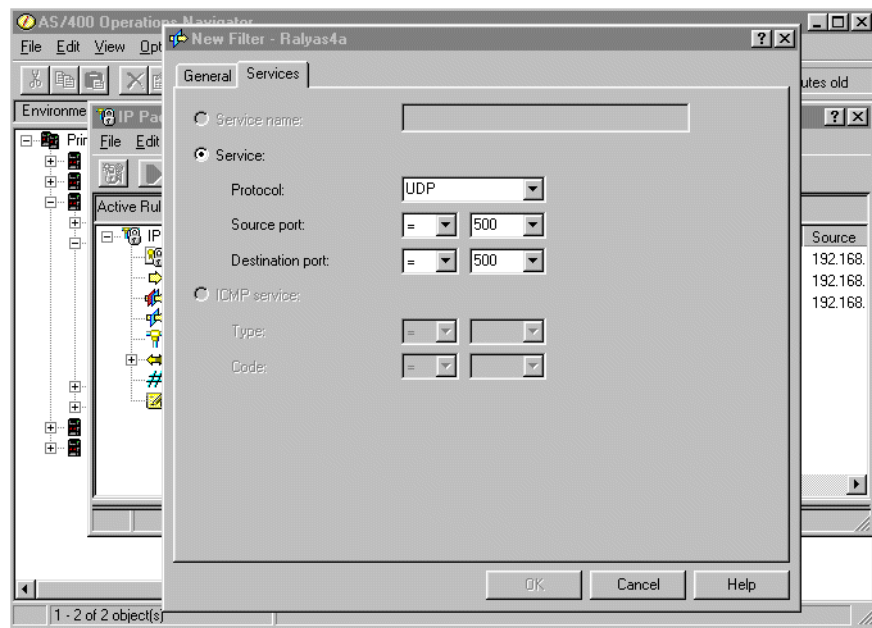


Figure 950. RALYAS4A IKE filter rule services

- Click **OK**.
- Configure the inbound IKE filter rule to permit IKE negotiations (Figure 951).

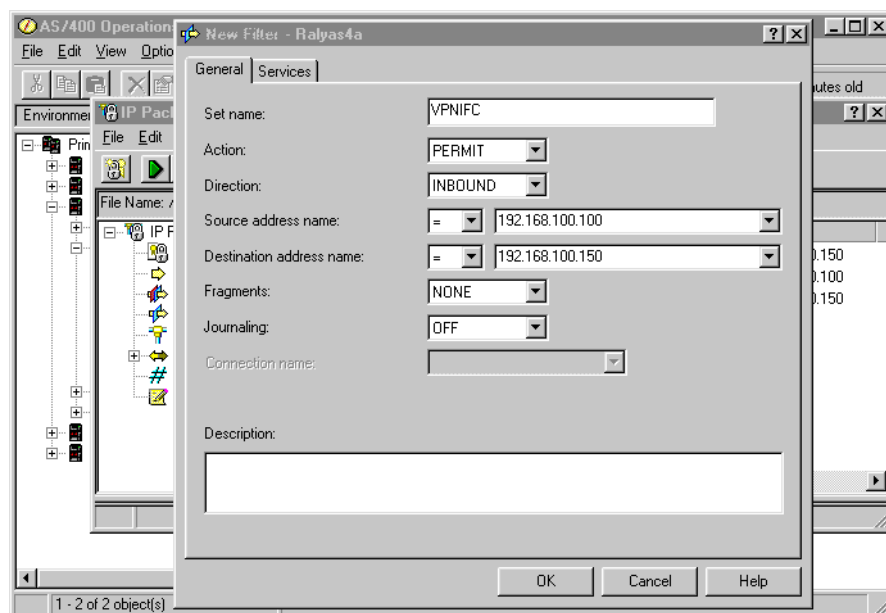


Figure 951. RALYAS4A Inbound IKE filter rule

- Click the **Services** tab.
- IKE negotiations use protocol UDP and source and destination port 500. Enter the values as shown in Figure 952 on page 835.

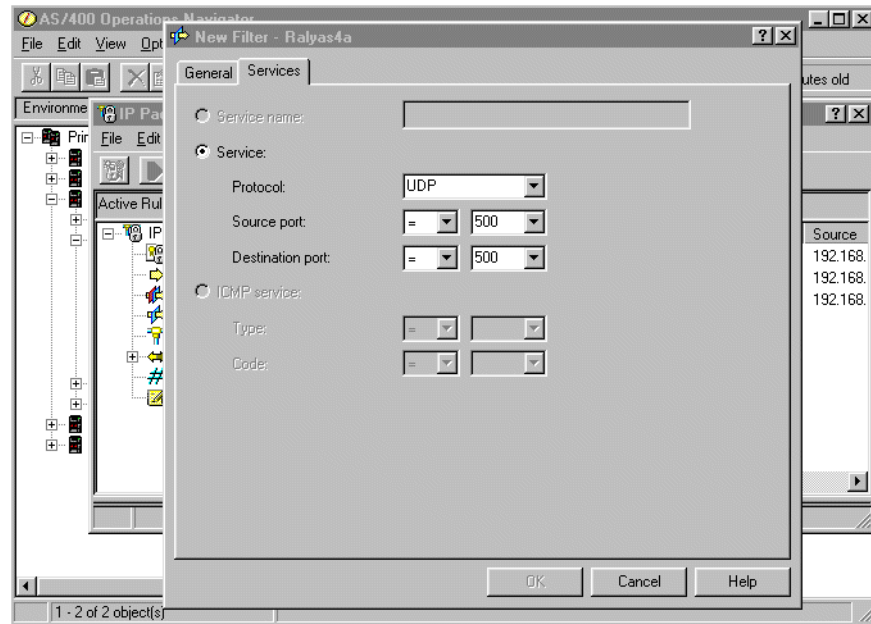


Figure 952. RALYAS4A IKE filter rule services

9. Click **OK**.

Tip

IKE permit rules must appear *before* the first IPSEC filter rule in the file to work properly.

10. Create an IPSEC filter rule (Figure 953 on page 836) to specify the data traffic that will use the VPN tunnel. Use the same filter Set name `VPNIFC`, and select **IPSEC** for the Action field. With an IPSEC filter rule, Direction is always set to **OUTBOUND** and grayed out. Specify `192.168.100.150` in the Source address name field and `192.168.100.100` in the Destination address name field. In a host-to-host VPN, the data endpoint and key server IP addresses are the same. The Connection name is the data connection, which, in this case, is a dynamic key connection group. Use the pull-down menu to list all the data connection names, which were configured on this system, and select **HtoH4AtoMF**.

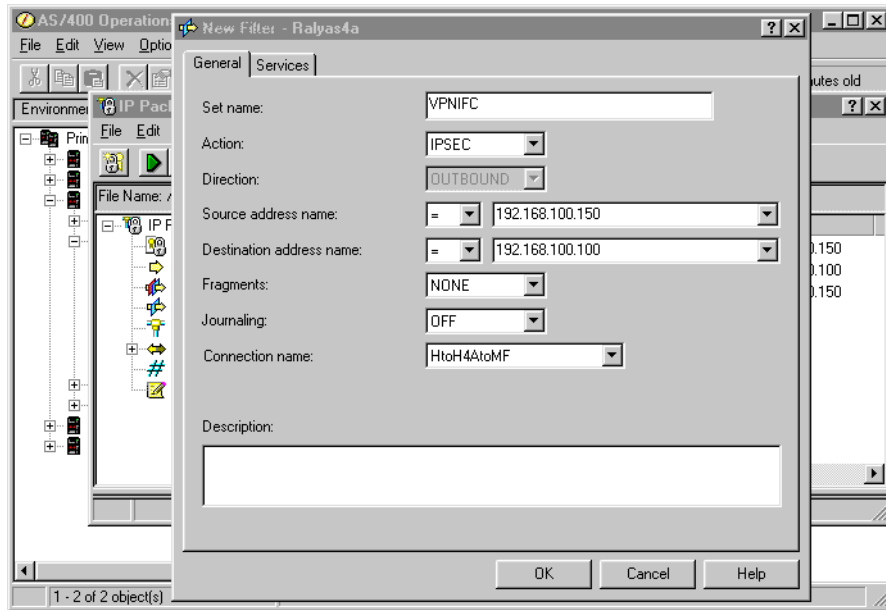


Figure 953. IPSEC filter rule

11. Click on the **Services** tab. The display shown in Figure 954 appears.
12. Select **Service**, and enter a wildcard (*) in the Protocol, Source port, and Destination port fields. This allows all protocols and ports to use the IPsec tunnel.
13. Select **Service** and enter a wildcard (*) in the Protocol, Source port, and Destination port fields. This allows all protocols and ports to use the IPsec tunnel.

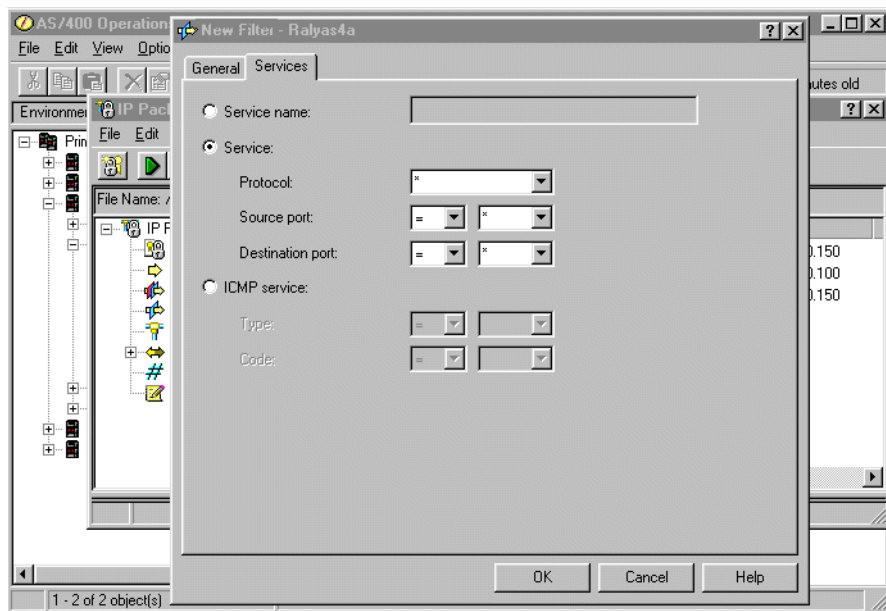


Figure 954. RALYAS4A IPSEC filter rule service

14. Click **OK**.

15. The final rule you must create is a Filter Interface rule, which ties the filter rules you just created to the required interface. Right-click on **Filter Interfaces**, and select **New Filter Interface**.
16. Select **Line name** for the Line radio box, and select **TOKENRING2** from the pull-down menu.
17. Click **Add** to add the filter set name of the filter rules you created previously, which, in this scenario, is **VPNIFC**. See Figure 955.

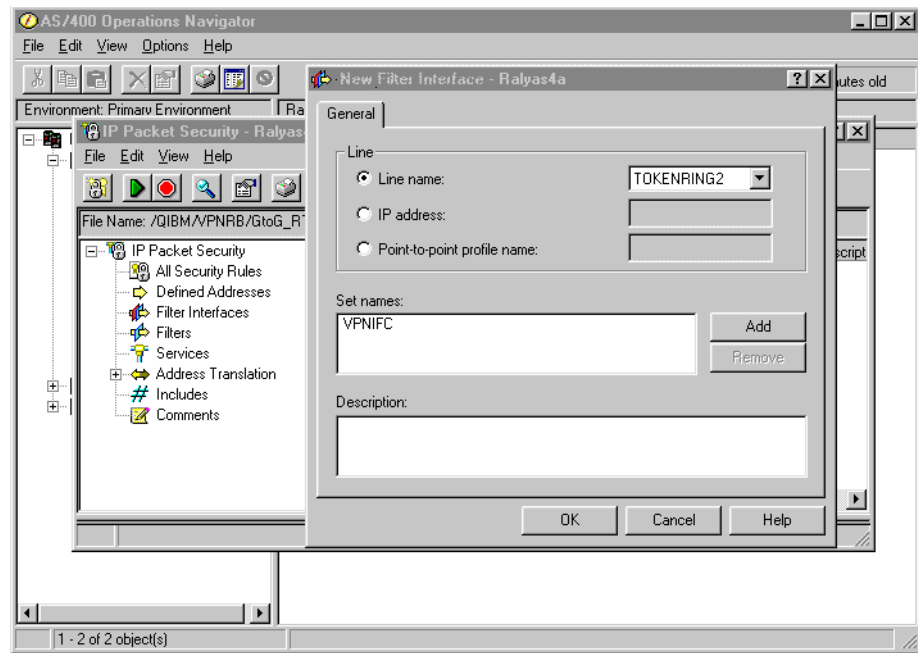


Figure 955. RALYAS4A - Filter interface

18. Click **OK**.
19. Save the filter rules file in the IFS. In this example, we created a subdirectory, **VPNRB**, under the directory **QIBM**. The filter rules were saved as **HtoH_AStoMF.i3p** into **/QIBM/VPNRB**.

This completes the IP Packet Security configuration for the RALYAS4A AS/400 system.

Note

This chapter only describes the IP filters that you need to create to complete the host-to-host VPN configuration in this scenario. You may need to configure additional filters to implement your specific network environment. For example, if the AS/400 system RALYAS4A were connected to the internal network through the same physical interface, TOKENRING2, additional filters would be needed to allow the internal network traffic.

Keep in mind that there is a default action of *Deny All* in a filter rule file. All traffic that you want to allow on an interface with active filters must be explicitly permitted.

The configuration of the firewalls that protect the manufacturer and distributor networks are not included in this chapter. Refer to Chapter 12, “Don’t forget a firewall: Protecting your VPN server” on page 515, for information on how to configure a firewall to allow an IPSec tunnel to flow through it.

18.6 VPN configuration cross-reference table: AS/400 to S/390

Table 119 provides a cross-reference list of the VPN configuration parameters for the AS/400 system and S/390.

Table 119. AS/400 system to S/390 - Configuration cross-reference table

<u>AS/400</u>	<u>S/390</u>
Key Policy	Key Policy, Proposal, Transform
Name = HtoH4AtoMFBS	(2) Initiator Negotiation = Main
Initiator Negotiation = Main Mode (1)	(1) Responder Negotiation = Main
Responder Negotiation = Main Mode only (2)	(3) Authentication Method = Pre-Shared Keys
Key Protection Transforms (5)	Hash Algorithm = MD5 (6)
Authentication Method = Pre-shared key (3)	Encryption Algorithm = DES_CBC_8 (7)
Pre-shared key value = abcd (4)	Diffie-Hellman Group = Group 1 (8)*
Hash Algorithm = MD5 (5)	Maximum Key Lifetime = 1440 min (9)*
Encryption Algorithm = DES-CBC (6)	Maximum Size Limit = 1000 Kilobytes (8)**
Diffie-Hellman Group = Default 768-bit MODP (7)	Size Limit Range = 1-1000 Kilobytes (9)**
Key Management (8)	(13) Data Policy, Proposal, ESP Transform
Maximum key lifetime (minutes) = 1440 (8)	(10) (11) PFS (Perfect Forward Secrecy) = Group 1 (12)
Maximum size limit (kilobytes) = 1000 (9)	ESP Encapsulation Mode = Transport (14)
Data Policy	ESP Authentication Algorithm = HMAC_MD5 (15)
Name = HtoH4AtoMFBS	ESP Encryption Algorithm = DES_CBC_8 (16)*
Use Diffie-Hellman Perfect Forward Secrecy = Yes (10)	ESP Maximum Data Lifetime = 60min (17)*
Diffie-Hellman Group = Default 768-bit MODP (11)	ESP Maximum Size Limit = 50000 Kilobytes (16)**
Data Protection Proposals (12)	ESP Data Lifetime Range = 60-480 min (17)**
Encapsulation mode = Transport (12)	ESP Size Limit Range = 1-50000 Kilobytes (17)**
Protocol = ESP (13)	
Algorithms (14)	Dynamic Tunnel Policy
Authentication Algorithm = HMAC-MD5 (14)	(22) Initiation = Either
Encryption Algorithm = DES-CBC (15)	Connection Lifetime = 0
Key Expiration (16)	
Expire after (minutes) = 60 (16)	Local Key Server
Expire at size limit (kilobytes) = 50000 (17)	Key Server Identity (18)
Key Connection Group	Authentication Identifier Type = IPV4 (19)
Name = HtoH4AtoMF	Authentication Identifier = 192.168.100.100
Remote Key Server (19)	Key Server Location (19)
Identifier Type = Version 4 IP address (18)	IP address = 192.168.100.100
IP address = 192.168.100.100 (19)	
Local Key Server (20)	Remote Key Server
Identifier Type = Version 4 IP address (20)	Key Server Identity (20)
IP address = 192.168.100.150 (21)	Authentication Identifier Type = IPV4 (21)
Key Policy = HtoH4AtoMFBS	Authentication Identifier = 192.168.100.150
Dynamic Key Group	Key Server Location (21)
Name = HtoH4AtoMF	IP address = 192.168.100.150
System Role = Both systems are hosts	
Initiation = Either systems can initiate the connection (22)	Authentication Information
Policy (4)	(3) Authentication Method = Pre-Shared Keys
Data Management Security Policy = HtoH4AtoMFBS	(4) Shared Key = 61626364
Connection Lifetime = Never expires (19)	Dynamic Connection
Local addresses = Filter rule (21)	Source = 192.168.100.100 (21)
Local ports = Filter rule (25)	Destination = 192.168.100.150 (25)
Remote addresses = Filter rule (24)	Source port = 0 (24)
Remote ports = Filter rule (23)	Destination port = 0 (24)
Protocol = Filter rule (21)	Automatic activation = No (23)
	Protocol = All (21)
	Remote Key Server = 192.168.100.150 (21)
Dynamic Key Connection	
Name = HtoH4AtoMF:L1	
Key Connection Group = HtoH4AtoMF	* Used when S/390 system is connection initiator
Start when TCP/IP is started? = No	** Used when S/390 system is connection responder
IP Filters	
Name = HtoH_AStoMF.3ip	
IPSEC rule (21)	
Source address name = 192.168.100.150 (21)	
Destination address name = 192.168.100.100 (19)	
Connection name = HtoH4AtoMF	
Services (23)	
Protocol = * (23)	
Source port = * (24)	
Destination port = * (25)	

18.7 Starting the VPN connection

This section describes how to start the connection at both ends of the tunnel.

18.7.1 Starting the VPN connection on the AS/400 system (RALYAS4A)

Before starting the VPN connection, you must verify that the IP filters and the VPN server are started on the AS/400 system.

If the AS/400 system is the initiator of the connection, perform the following steps:

1. At the Virtual Private Networking GUI (Figure 956), expand **Secure Connections->Data Connections->Dynamic Key Groups**.
2. Click **HtoH4AtoMF**.
3. Right-click the **HtoH4AtoMF:L1** connection, and select **Start** to activate the VPN connection to the S/390 system.

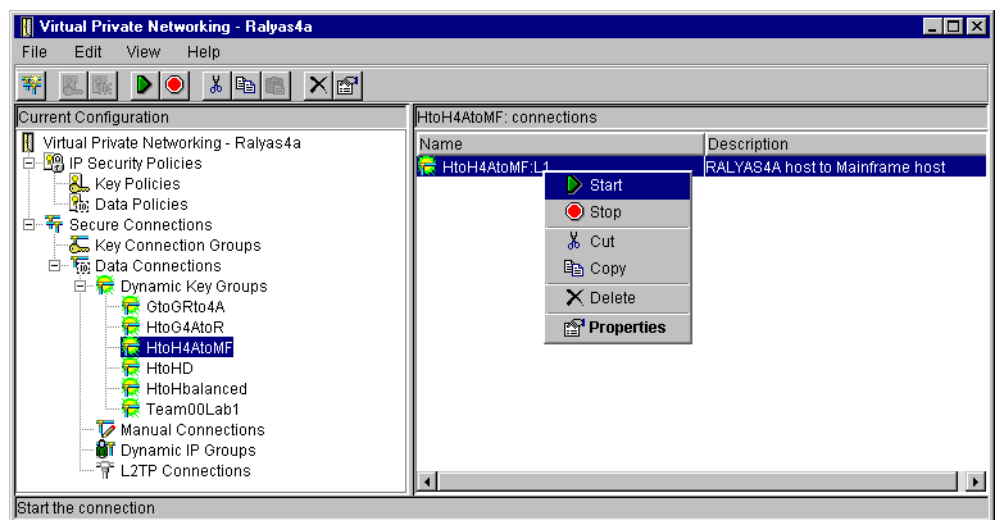


Figure 956. Starting the VPN connection on RALYAS4A

4. Display the active connections to verify that it is active. At the Virtual Private Networking window (Figure 957 on page 841) menu bar, click **View->Active Connections**.

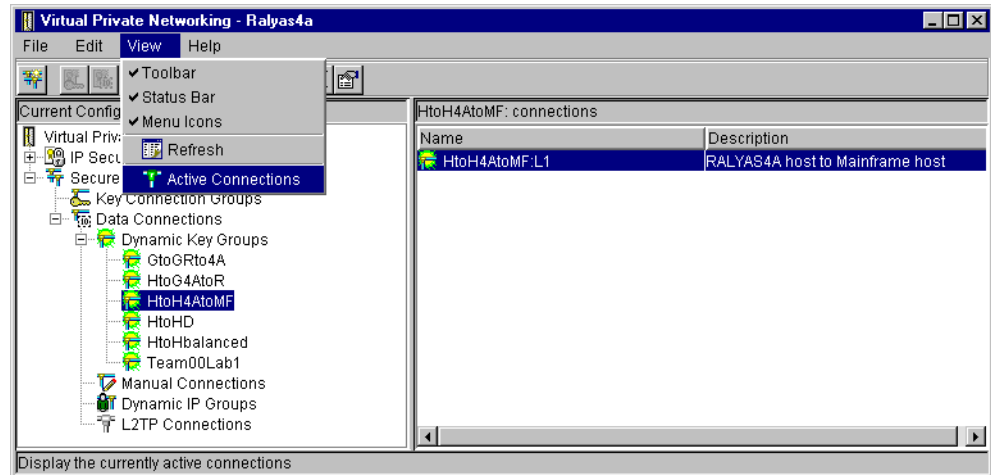


Figure 957. RALYAS4A Viewing active connections

The Active Connections window is shown in Figure 958.

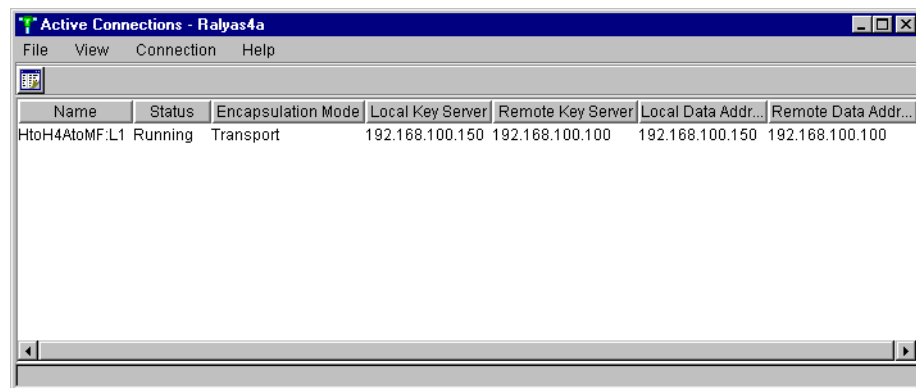


Figure 958. Active Connections window

18.7.2 Starting the VPN connection on the S/390 system

This section describes how to start the connection from the S/390 system if the AS/400 system is the responder and the S/390 system is the initiator. Verify that filters and VPN server jobs are started on the AS/400 system before starting the connection from the S/390 system.

Perform the following steps to initiate the connection on the S/390 system:

1. To activate the dynamic VPN connection, at the OS/390 Firewall Technologies Configuration Client GUI main window (Figure 910), click **Traffic Control->Connection Setup** to display the Dynamic VPN Connection List window shown Figure 959 on page 842.
2. Select the **R2612.DynVPN.OS390.AS400** connection, and click **Activate**.

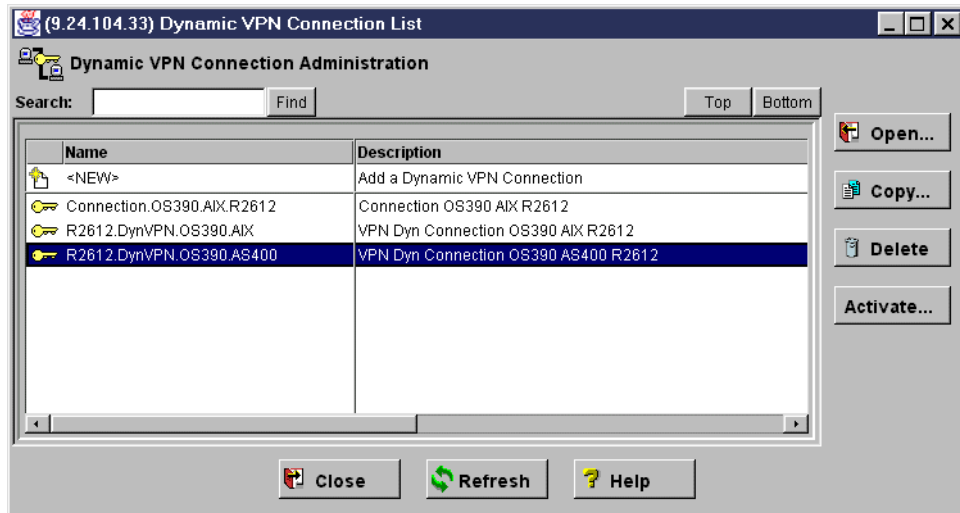


Figure 959. Activating the dynamic VPN connection

- To view the dynamic VPN connection status, at the OS/390 Firewall Technologies Configuration Client GUI main window (Figure 910 on page 805), click **Traffic Control->Connection Activation** to display the Dynamic VPN Connection Activation List window shown in Figure 960. Click **Refresh** if the dynamic connection to the AS/400 system is not shown.

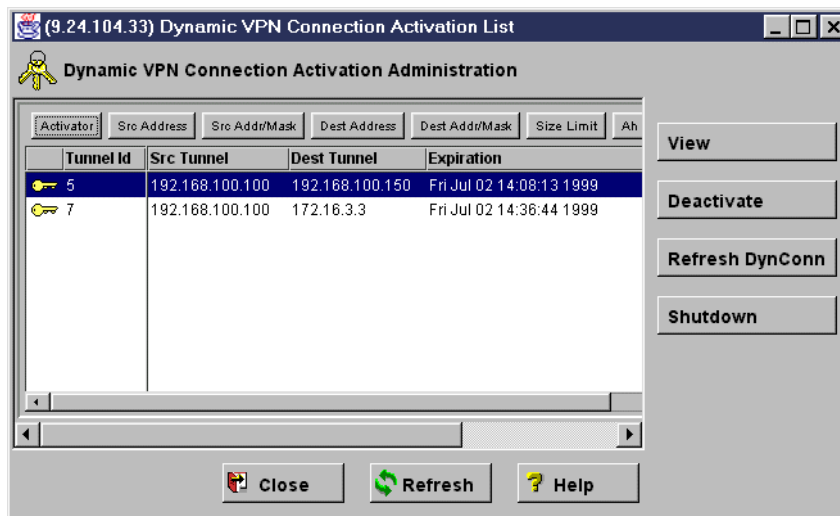


Figure 960. Dynamic VPN connection activation list

- To view the details of the dynamic VPN connection, select the relevant tunnel ID at the Dynamic VPN Connection Activation List window (Figure 960). Then, click **View** to display the View Active Dynamic VPN Connection window shown in Figure 961 on page 843.

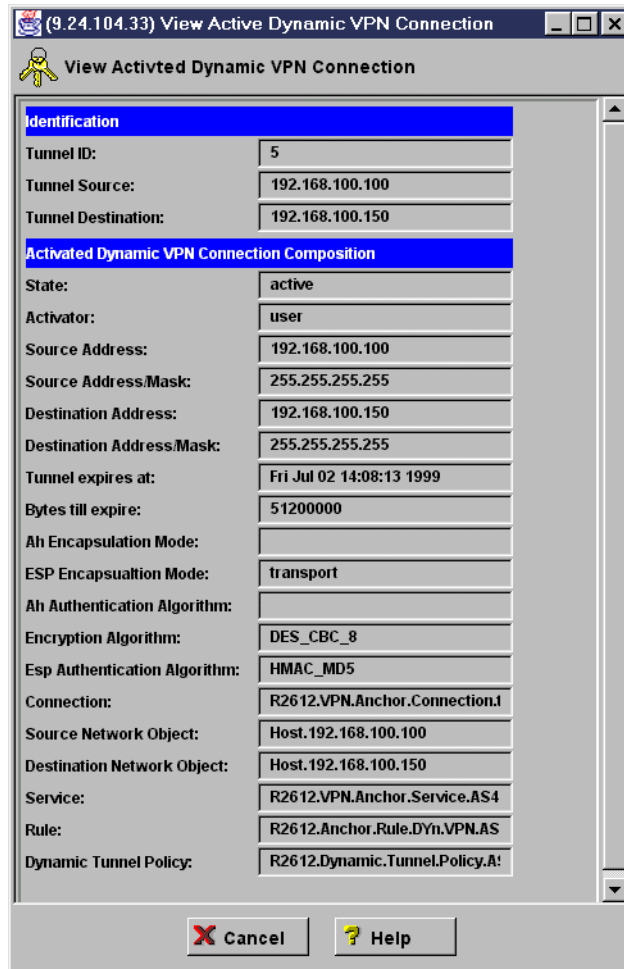


Figure 961. View active dynamic VPN connection

18.8 Performing verification tests

Table 120 presents a summary of the verification tests run after activating the host-to-host VPN configured in this scenario.

Table 120. Verifications tests - RALYAS4A AS/400 host-to-S/390 host scenario

	Start connection	PING	TELNET	FTP
From RALYAS4A to S/390 system	YES	YES	YES	YES
From S/390 system to RALYAS4A	YES	YES	YES	YES

Chapter 19. Manual connection VPN: AS/400 to eNetwork Firewall

You must use manual connections when your AS/400 system's VPN partner does not support the Internet Key Exchange (IKE) protocol. In this case, several connection configuration objects are not negotiated or configured dynamically. The VPN configuration wizard does not support manual connections.

To configure a manual connection, you must use the VPN configuration GUI to configure all of the VPN properties by hand. Both VPN partners need to agree on the value of several parameters that must match both ends of the connection. For example, the outbound Security Parameter Index (SPI) in the local system must match the inbound SPI value of the VPN partner.

Manual connections use static keys that are not refreshed automatically while the connection is active. To change the connection keys, you must stop the manual connection, configure a new key on both ends of the VPN, and re-start the connection.

Because of the administration overhead involved with manual connections, we recommend that you use dynamic connections, which offer a solution to the key refresh issue, are more secure, and easier to maintain.

However, not all VPN implementations support IKE for a dynamic key refresh. Older implementations either don't support a key management protocol at all or support proprietary protocols that are incompatible with the IKE support on the OS/400 VPN. For example, eNetwork Firewall for Windows NTV3.3 does not support IKE, which is the dynamic key refresh protocol supported by the OS/400 VPN implementation.

19.1 Branch office host-to-corporate office gateway VPN

In this scenario, we present a company that connects a branch office AS/400 server to the corporate office gateway through a VPN over the Internet.

19.1.1 Scenario characteristics

The characteristics of this scenario are:

- The branch office network is connected to the Internet through IBM Firewall for AS/400.
- The corporate office is connected to the Internet through eNetwork Firewall for Windows NT.
- The IPSec implementations of IBM Firewall for AS/400 and eNetwork Firewall for Windows NT are incompatible. Therefore, we chose to configure the VPN between OS/400 and eNetwork Firewall for Windows NT V3.3. The filter configuration in the IBM Firewall for AS/400 must allow the IPSec ESP protocol to flow through it. Refer to Chapter 12, "Don't forget a firewall: Protecting your VPN server" on page 515, for information about how to configure a firewall to allow VPN protocols through it.

Figure 962 on page 846 represents this scenario.

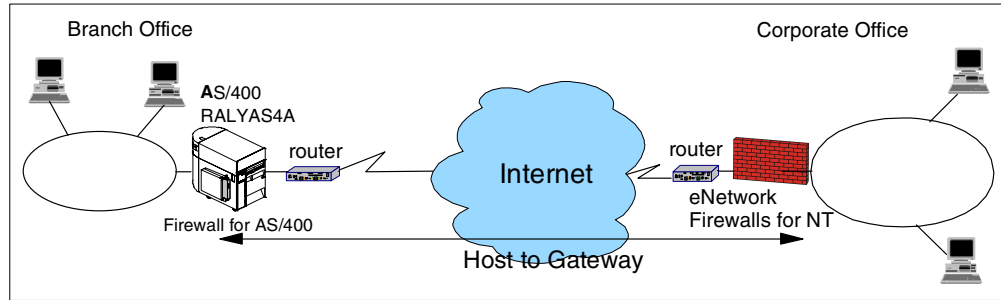


Figure 962. Manual connection VPN - OS/400 to eNetwork Firewall for Windows NT

19.1.2 Scenario objectives

The objectives of this scenario are:

- All traffic between the AS/400 system RALYAS4A and the eNetwork Firewall for Windows NT must be protected by the VPN.
- The corporate office hosts only need access to the AS/400 system RALYAS4A at the branch office. For this reason, we configure RALYAS4A as a VPN *host* instead of a *gateway*.
- All services are allowed between systems at the corporate office network and the AS/400 system RALYAS4A at the branch office.
- Privacy is provided by configuring an ESP tunnel between the AS/400 system and the eNetwork Firewall for Windows NT.
- The networks at both ends of the VPN belong to the same company. Therefore, it is acceptable that data flows in the clear at the corporate office network behind the eNetwork Firewall for Windows NT gateway.

19.1.3 Scenario network configuration

Figure 963 shows the test network used in this scenario.

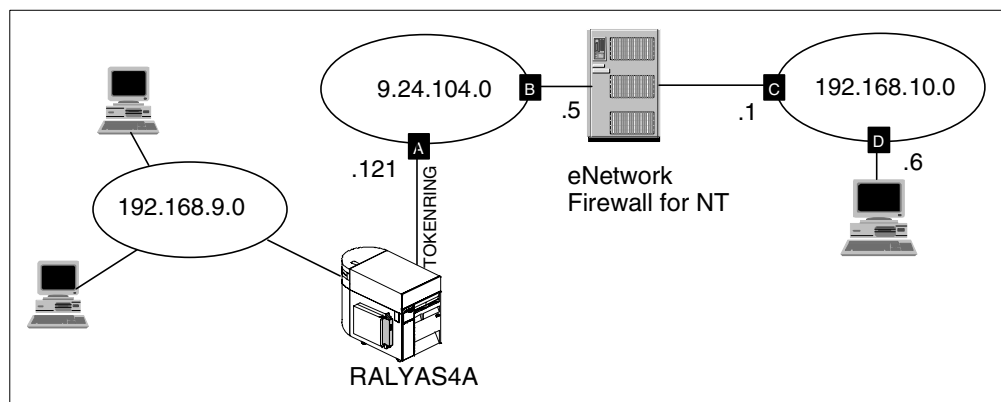


Figure 963. Manual connection VPN - Scenario test network

19.1.4 eNetwork Firewall for Windows NT software

The firewall software used on the corporate side is IBM eNetwork Firewall for Windows NT V3.3.

19.1.5 Implementation tasks: Summary

The following process summarizes the tasks required to implement this VPN host-to-gateway environment:

1. Verify connectivity. Before you start configuring VPN and filters, you must be sure that the underlying TCP/IP network is properly configured and working.
2. Complete the planning worksheet for the eNetwork Firewall for Windows NT.
3. Configure the eNetwork Firewall for Windows NT.
4. Export the eNetwork Firewall VPN configuration to a file.
5. Complete the planning worksheet for the AS/400 system.
6. Configure a host-to-gateway manual connection VPN in the AS/400 system.
7. Configure IP filters in the AS/400 system.
8. Start the VPN connection.
9. Perform the verification tests.

19.1.6 Verifying initial connectivity

Before starting the VPN configuration, verify connectivity and routing between both networks. Generally, this can be accomplished by using the PING command.

However, in a real-life Internet environment, the PING command doesn't always flow through the Internet. PING is often blocked by firewalls and routers.

If you cannot use the PING command, test other service, such as HTTP, or use information in logs to verify that the IP traffic flows properly.

19.2 eNetwork Firewall for Windows NT configuration

The following sections explain how to configure the tunnel in the eNetwork Firewall for Windows NT to establish a VPN with the AS/400 system RALYAS4A. It is beyond the scope of this redbook to provide detailed information about eNetwork Firewall configuration. Refer to *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209, for more information about the firewall product.

19.2.1 eNetwork Firewall for Windows NT planning worksheet

Table 121 shows the planning worksheet with the information required to configure the eNetwork Firewall for Windows NT in this scenario.

Table 121. ENetwork Firewall for Windows NT planning worksheet - Manual connection configuration

This is the information you need to configure eNetwork Firewall for Windows NT V3.3	Scenario answers
Tunnel name	ralyas4a
Filter type	Static

This is the information you need to configure eNetwork Firewall for Windows NT V3.3	Scenario answers
Tunnel endpoints Local tunnel address Remote tunnel address SPI Remote SPI Local SPI	9.24.104.5 9.24.104.121 333 Automatically generated
Authentication (AH) Authentication algorithm	N/A
Encryption (ESP) – Encryption algorithm – Authentication algorithm • Sending encryption key • Receiving encryption key	DES_CBC N/A Automatically generated Automatically generated
Replay prevention Tunnel life time	No 480 sec.
IP filters Permit routed non-encrypted traffic on secure interface – Inbound • From IP address • To IP address • Protocols – Outbound • From IP address • To IP address • Protocols Define traffic to be given to the VPN tunnel – Inbound • From IP address • To IP address • Protocols • Tunnel ID – Outbound • From IP address • To IP address • Protocols • Tunnel ID Permit encrypted traffic between firewall and RALYAS4A – Inbound • From IP address • To IP address • Protocols –Outbound • From IP address • To IP address • Protocols	192.168.10.0 9.24.104.121 any 9.24.104.121 192.168.10.0 any 9.24.104.121 192.168.10.0 any 7 (automatically defined) 192.168.10.0 9.24.104.121 any 7 (automatically defined) 9.24.104.121 9.24.104.5 ESP 9.24.104.5 9.24.104.121 ESP

eNetwork Firewall for Windows NT allows you to configure tunnels with *static* or *dynamic* filters:

Static filters Static filters are user-defined. They allow you to specify additional parameters, such as logging, which are not generated when you configure tunnels with dynamic filters.

Dynamic filters Tunnels with dynamic filters are easier to configure because the eNetwork Firewall for Windows NT generates the filters automatically using the VPN user (data endpoint) and tunnel definitions as input to the configuration. They allow less granular control since parameters, such as logging or time of day filtering, cannot be specified.

The local SPI and the encryption keys are generated automatically by the eNetwork Firewall for Windows NT. We will export those values to a file and use them in the AS/400 VPN configuration.

19.2.2 Configuring eNetwork Firewall for Windows NT

Perform the following steps to configure the gateway-to-host connection on the eNetwork Firewall for Windows NT:

1. To start the eNetwork Firewall for Windows NT configuration GUI, click the Windows **Start** button, and select **Programs->IBM Firewall->Configuration Client** (Figure 964). The eNetwork Firewall configuration client main window starts as shown in Figure 965 on page 850.

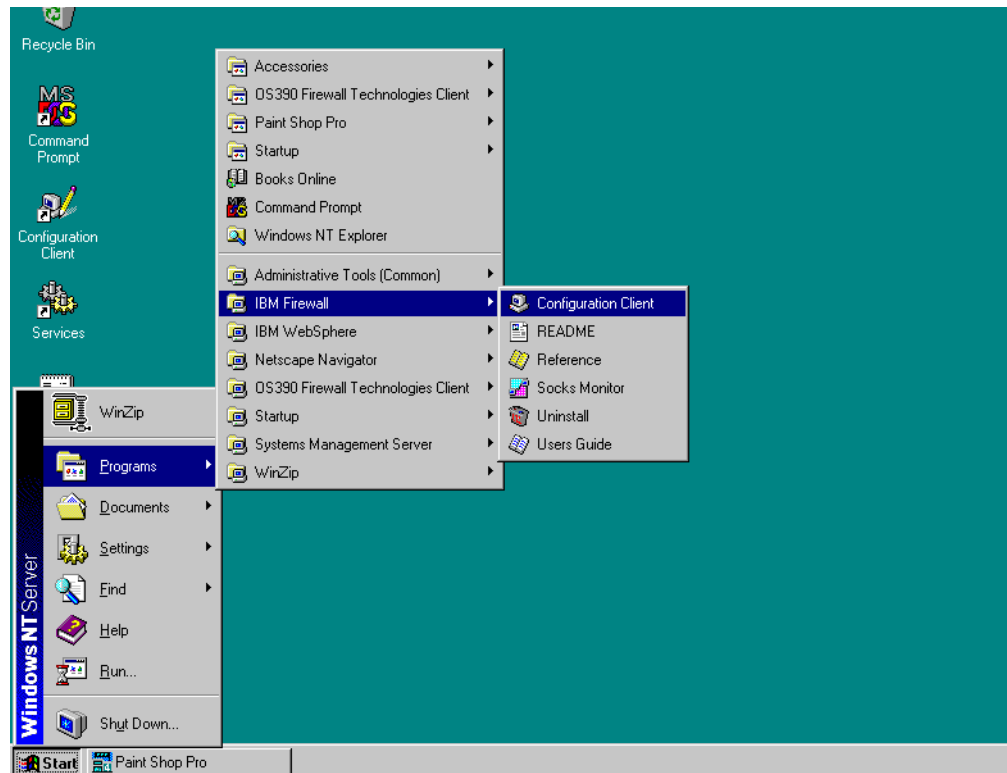


Figure 964. Starting eNetwork Firewall for Windows NT configuration client

2. Click **Traffic Control->Virtual Private Network** to start the VPN configuration (Figure 965 on page 850).

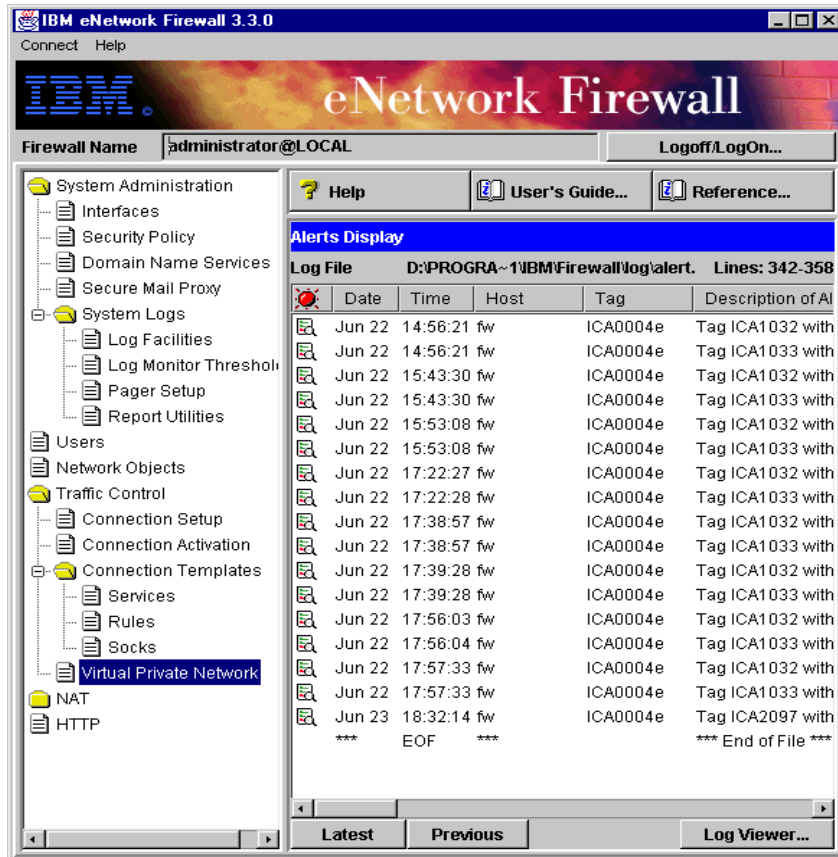


Figure 965. eNetwork Firewall configuration client

3. To create a new tunnel, select **New** in the Virtual Private Network Administration window as shown in Figure 966.

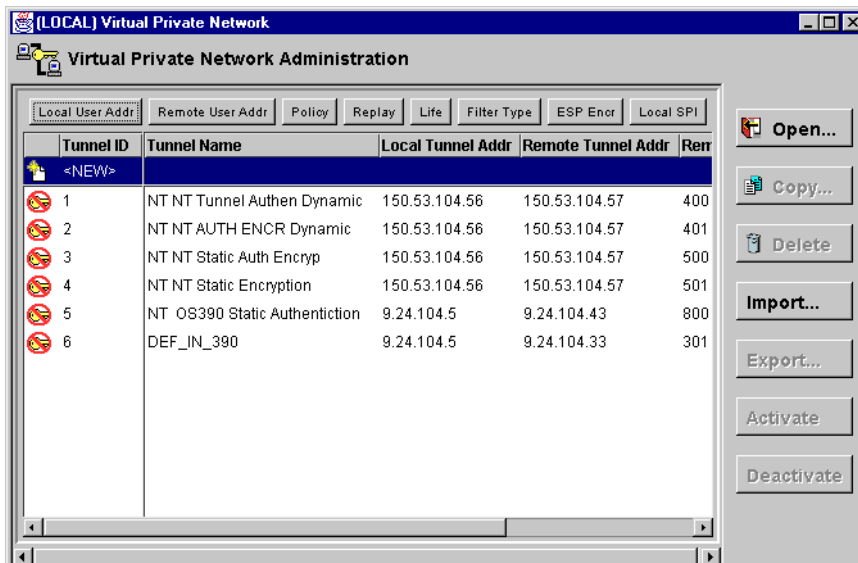


Figure 966. eNetwork Firewall - Virtual Private Network Administration

4. Configure the new tunnel using the values in the planning worksheets in Table 121 on page 847. Refer to Figure 967 on page 851.

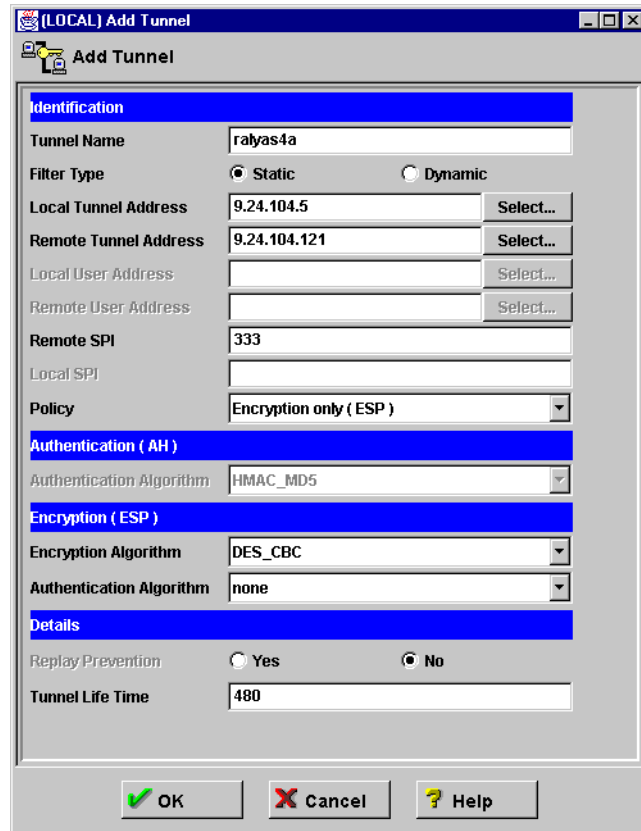


Figure 967. eNetwork Firewall - New tunnel configuration

Note

The local SPI, tunnel ID, authentication, and encryption key values are automatically generated by eNetwork Firewall for Windows NT. To configure the appropriate parameters on the AS/400 system manual connection VPN, export the eNetwork Firewall configuration to a file as discussed in 19.2.3, “Exporting the eNetwork Firewall VPN configuration” on page 851.

19.2.3 Exporting the eNetwork Firewall VPN configuration

eNetwork Firewall for Windows NT allows you to export the manual VPN tunnel configuration to a file that can be imported to the VPN partner. Even though the AS/400 system does not allow you to import this file, the configuration information is helpful for configuring the manual connection on the AS/400 system. Follow these steps:

1. At the Virtual Private Network Administration window, select the tunnel to export, **ralyas4a**, and click **Export...** as shown in Figure 968 on page 852.

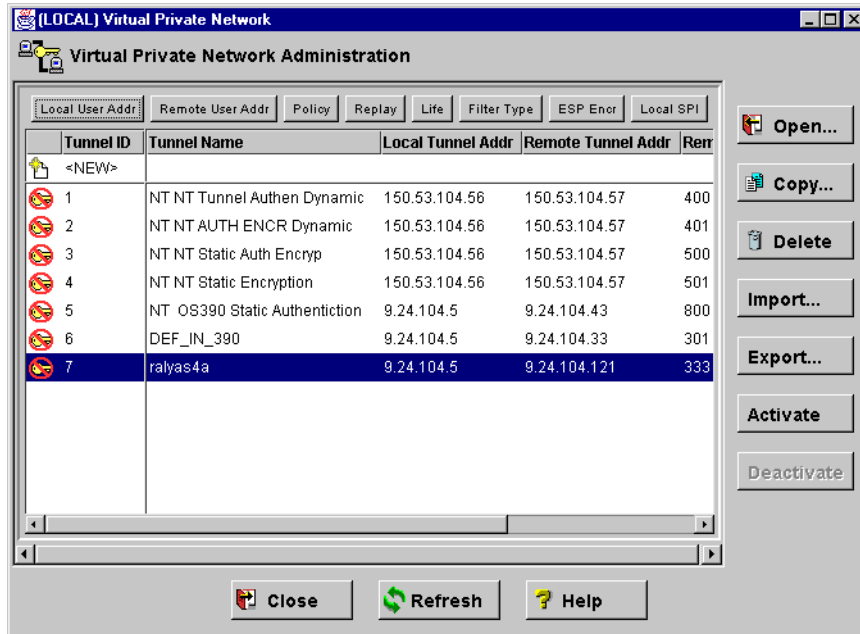


Figure 968. eNetwork Firewall - Exporting tunnel configuration

2. Enter the tunnel ID and the directory where the exported file will be stored as shown in Figure 969.

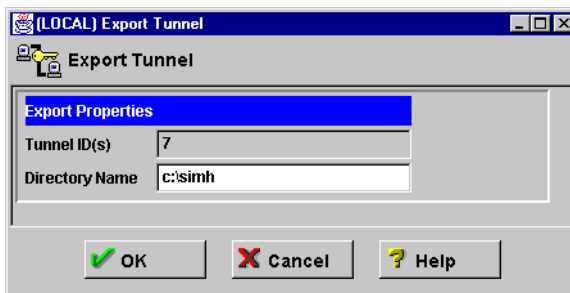


Figure 969. eNetwork Firewall - Export tunnel

Figure 970 on page 853 shows the file resulting from exporting the eNetwork Firewall for Windows NT tunnel configuration.

```

1. 4
2. 9.24.104.5
3. 9.24.104.121
4. 7
5. 333
6. 333
7. 262
8. 262
9. DES_CBC
10. 8
11. 0x427990ab0a9576b2
12. DES_CBC
13. 8
14. 0x27df9fcc52f192d3
15. NONE
16. 0
17. 0x
18. NONE
19. 0
20. 0x
21. 0
22. 28800
23. tunnel
24. tunnel
25. exex
26. 0
27. 1
28. NONE
29. 0
30.
31. NONE
32. 0
33.
34. 0
35. -
36. -
37. ralyas4a
38. 0
39. 0.0.0.0
40. 0.0.0.0
41. 0.0.0.0
42. 0.0.0.0

```

Figure 970. eNetwork Firewall for Windows NT - Tunnel configuration export file

Table 122 shows the description of each line in the tunnel configuration export file.

Table 122. eNetwork Firewall for Windows NT Tunnel configuration export file - Fields description

Line number	Field in export file
1	IP version number
2	Source IP address
3	Destination IP address
4	Tunnel ID
5	Destination encryption SPI
6	Destination authentication SPI

Line number	Field in export file
7	Source encryption SPI
8	Source authentication SPI
9	Receiving encryption algorithm
10	Receiving encryption key length - 8 bytes for DES; 16 bytes for 3DES
11	Receiving encryption key
12	Sending encryption algorithm
13	Sending encryption key length - 8 bytes for DES; 16 bytes for 3DES
14	Sending encryption key
15	Receiving MAC algorithm
16	Receiving MAC key length
17	Receiving MAC key
18	Sending MAC algorithm
19	Sending MAC key length
20	Sending MAC key
21	Start - Defaults to 0
22	Time in seconds that the tunnel will be operational
23	ESP mode, must be tunnel mode
24	AH mode, must be tunnel mode
25	Policy
26	Replay protection, 1=yes, 0=no
27	New header, must be 1
28	Receiving encryption MAC algorithm
29	Receiving encryption MAC key length
30	Receiving encryption MAC key
31	Sending encryption MAC algorithm
32	Sending encryption MAC key length
33	Sending encryption MAC key
34	N/A
35	N/A
36	N/A
37	Tunnel name
38	Filter type, 0=static, 1=dynamic
39	Source tunnel user address (with dynamic filter type only)
40	Source tunnel user mask (with dynamic filter type only)

Line number	Field in export file
41	Destination tunnel user address (with dynamic filter type only)
42	Destination tunnel user mask (with dynamic filter type only)

19.2.4 eNetwork Firewall IP filter configuration

It is beyond the scope of this redbook to provide information about the eNetwork Firewall for Windows NT filters configuration. Refer to *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209, for eNetwork Firewall configuration information.

Configure the IP filters in the eNetwork Firewall to:

- Permit routed traffic to flow in the clear in the internal network (192.168.10.0).
- Funnel the appropriate traffic (to or from the internal network 192.168.10.0 and the AS/400 system RALYAS4A) through the VPN tunnel.
- Encrypt the traffic between the eNetwork Firewall for Windows NT and the AS/400 system RALYAS4A.

Figure 971 shows the tunnel IP filters configured in the eNetwork Firewall for Windows NT in this scenario. In this scenario, the tunnel ID is 7.

```
#Traffic Between SecCliTun and RALYAS4A
#      Service : VPN traffic 1/2
# Description : Permit routed traffic on secure interface (non-encrypted)
permit 192.168.10.0 255.255.255.0 9.24.104.121 255.255.255.255 all any 0 any 0
secure route inbound l=y f=y

permit 9.24.104.121 255.255.255.255 192.168.10.0 255.255.255.0 all any 0 any 0
secure route outbound l=y f=y
#      Service : VPN 2/2 T7
#Description : Route traffic through the VPN
permit 192.168.10.0 255.255.255.0 9.24.104.121 255.255.255.255 all any 0 any 0 non-secure
route outbound l=y f=y t=7
permit 9.24.104.121 255.255.255.255 192.168.10.0 255.255.255.0 all any 0 any 0 non-secure
route inbound l=y f=y t=7

#Traffic Between NonSecInt 9.24.104.5 and RALYAS4A
# Description : Permit encrypted data between eNetwork firewall and RALYAS4A
permit 9.24.104.5 255.255.255.255 9.24.104.121 255.255.255.255 esp any 0 any 0 non-secure
local both l=y f=y
permit 9.24.104.121 255.255.255.255 9.24.104.5 255.255.255.255 esp any 0 any 0 non-secure
local both l=y f=y
```

Figure 971. eNetwork Firewall - Tunnel IP filters

19.3 AS/400 manual connection VPN configuration

The following sections explain how to configure the manual connection in the AS/400 system RALYAS4A to establish a VPN with the eNetwork Firewall for Windows NT.

19.3.1 Completing the AS/400 system planning worksheet

Complete the AS/400 system planning worksheet for manual VPN connections as shown in Table 123 on page 856. The inbound encryption key and SPI values are generated by the eNetwork Firewall for Windows NT and exported to a file as described in 19.2.3, “Exporting the eNetwork Firewall VPN configuration” on page 851.

It is not possible to import the file exported by the eNetwork Firewall for Windows NT in the AS/400 system. We used the values in the exported file to complete the AS/400 planning worksheets before configuring the manual connection. You must wait until after exporting the eNetwork Firewall tunnel configuration to fill in the generated values.

Table 123 shows the data that you must gather before configuring a manual VPN connection on the AS/400 system.

Table 123. AS/400 planning worksheets - Manual connection configuration

This is the information you need to create your VPN manual connection	Scenario answers
Connection name	HtoGWAStoWNT
System role: – Both systems are hosts – Local system is a host, remote system is a gateway – Local system is a gateway, remote system is a host – Both systems are gateways	Local system is a host; Remote system is a gateway
Endpoints – Local connection endpoint • Identifier type • Identifier – Remote connection endpoint • Identifier type • Identifier	IPv4 9.24.104.121 IPv4 9.24.104.5
Policy Encapsulation mode Protocol	Tunnel ESP
Authentication Header (if protocol = AH) Authentication algorithm – Keys • Inbound • Outbound – Security policy index (SPI) • Inbound • Outbound	N/A

This is the information you need to create your VPN manual connection	Scenario answers
Encapsulate Security Payload (if protocol = ESP) Encryption Algorithm – Keys <ul style="list-style-type: none"> • Inbound (local AS/400) from firewall export file • Outbound (remote VPN partner) from firewall export file Authentication algorithm – Keys <ul style="list-style-type: none"> • Inbound • Outbound Security policy index (SPI) – Inbound (VPN partner) from firewall export file – Outbound (local AS/400) from firewall export file	DES-CBC 27DF9FCC52F192D3 427990AB0A9576B2 none N/A N/A 0000014D 00000106
Local Address Identifier type Identifier	IPv4 9.24.104.121
Remote Address Identifier type Identifier	IPv4 9.24.104.5
Services Local port Remote port Protocol	Any Any Any

19.3.2 Configuring a manual VPN connection on the AS/400 system

Use the planning worksheet shown in Table 123 on page 856 to configure the manual connection on the AS/400 system. Perform the following steps:

1. Start Operations Navigator on your desktop.
2. Expand your AS/400 system, which, in this scenario, is **RALYAS4A**.
3. Expand **Network**.
4. Double-click **IP Security**.
5. Double-click **Virtual Private Networking**.
6. Right-click **Manual Connections**, and select **New Manual Connection** (Figure 972 on page 858).

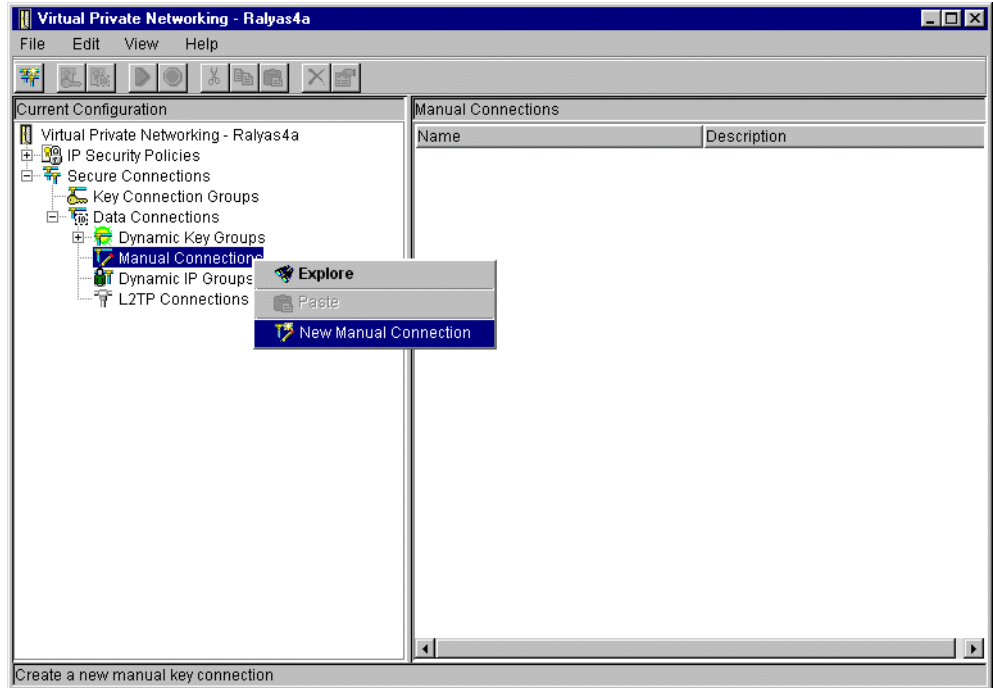


Figure 972. Creating a new manual connection

- At the General window, enter the connection name (HtoGWASToWNT), a description, and the system roles. In this scenario, the local AS/400 system is a host and the remote eNetwork Firewall for Windows NT is a gateway (Figure 973 on page 859).

Note: The default for journaling is *None*. Select **Journaling All** only to debug setup problems.

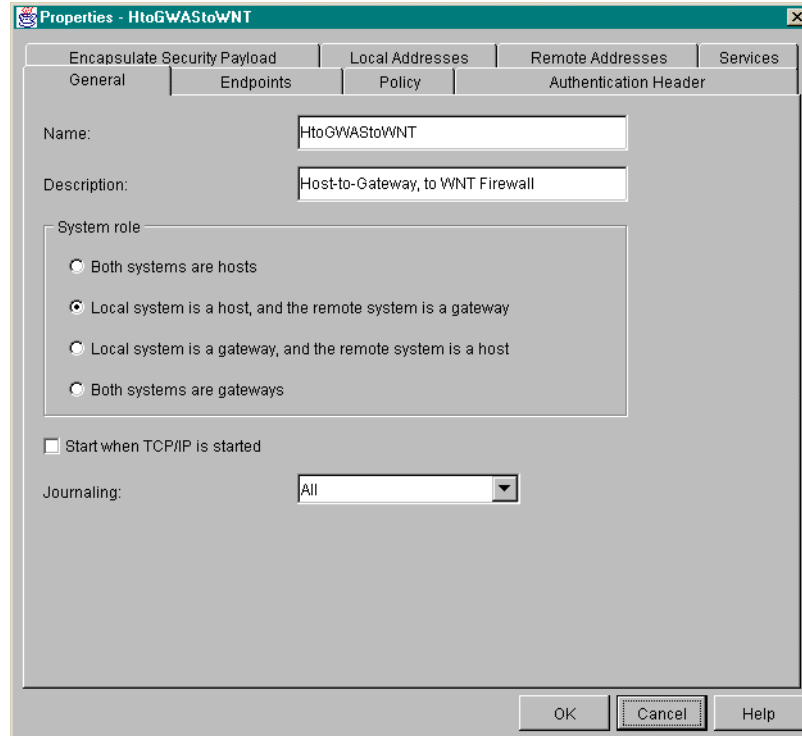


Figure 973. Manual connection - General page

8. Click **Endpoints** to define the connection endpoints.
9. For this scenario, select Version 4 IP address as the identifier type. For Identifier, select the IP addresses of the VPN endpoints as shown in Figure 974 on page 860.

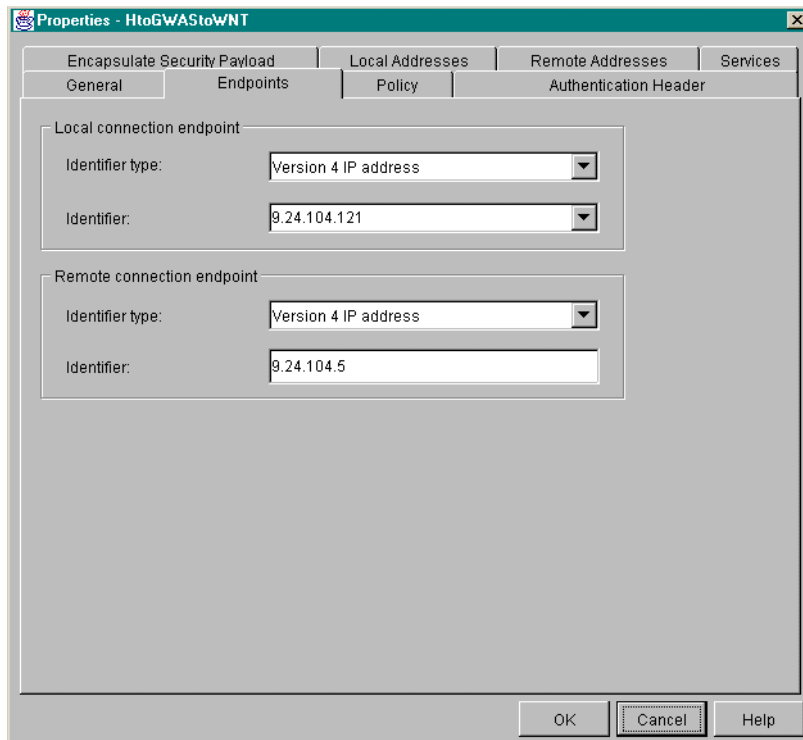


Figure 974. Manual connection - VPN Endpoints configuration

10. Click **Policy**.

11. At the Policy window, enter the encapsulation mode and the protocol to be used in this VPN connection.

When one of the two systems is a gateway (as it is the case in this scenario for the eNetwork Firewall for Windows NT), the encapsulation mode must be **Tunnel**.

We selected **Encapsulation security payload (ESP)** as the VPN protocol for this scenario. See Figure 975 on page 861.

In manual tunnels, the keys are static, and don't change unless an administrator changes them. When the administrator changes them, no traffic flows through the connection. How often you change the keys is a trade-off between security and key management cost. Since this is a manual key connection, you need to devise a procedure to stop the VPN, change the keys on both ends, and restart the VPN.

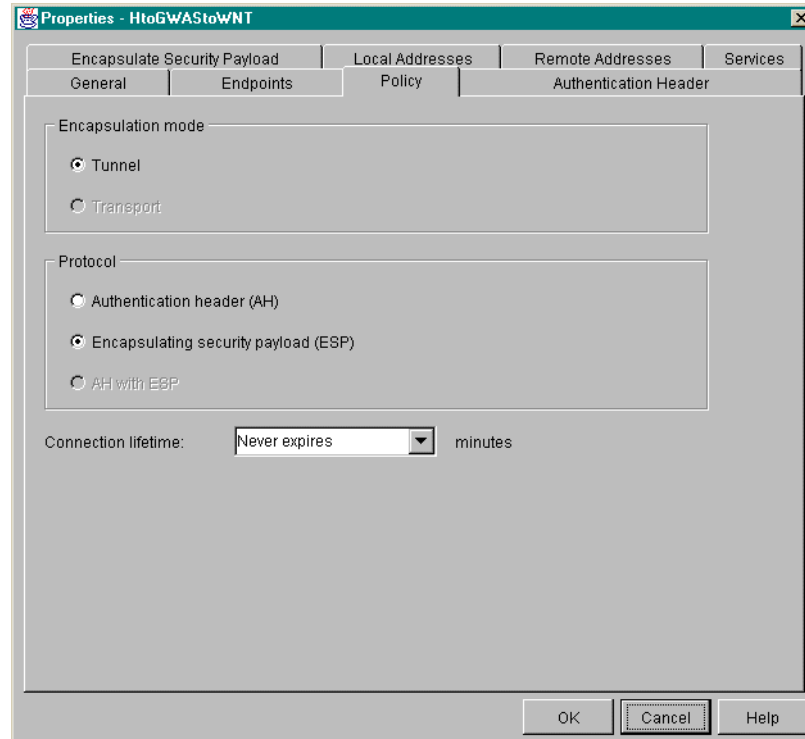


Figure 975. Manual connection - Policy page

12. Click **Authentication Header**. The Authentication Header page shown in Figure 976 on page 862 is displayed.

In this scenario, we did not select AH in the Protocol section of the Policy page (Figure 975). Therefore, all the parameters in the Authentication Header page are grayed out. See Figure 976 on page 862.

With tunnel mode, we may either select AH or ESP. With transport mode we may select AH with ESP.

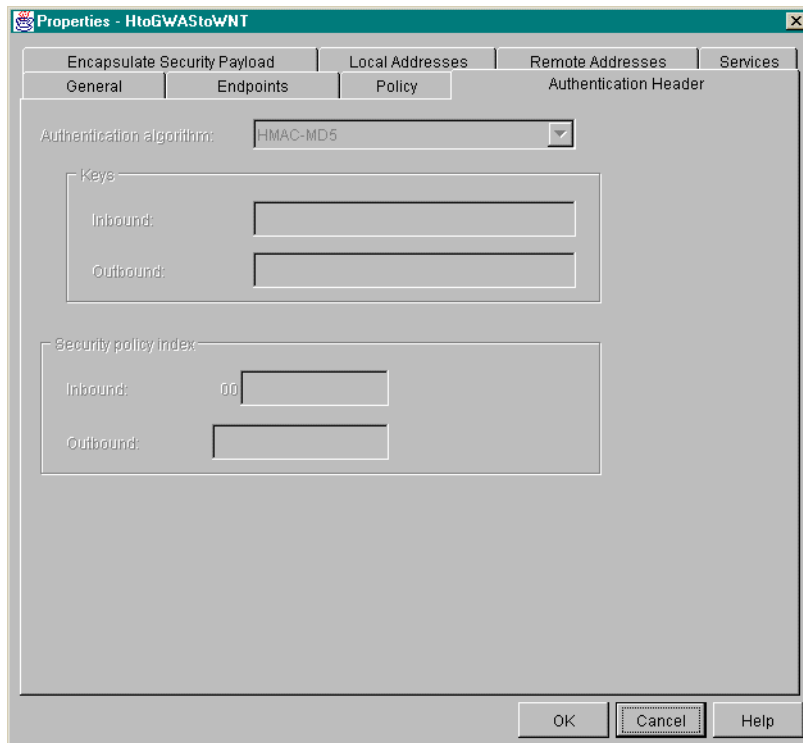


Figure 976. Manual connection - Authentication Header (AH) page

13. Click **Encapsulation Security Payload**. The window shown in Figure 977 on page 864 is displayed.
14. In the Encapsulation Security Payload page, enter the ESP encryption and authentication algorithms, the corresponding keys, and the Security policy index values as determined by the planning worksheet in Table 123 on page 856.

Note

The keys and SPI values are dynamically generated and refreshed by the IKE protocol in dynamic connections. In manual connections, these values must be manually configured. Any refresh of keys is a manual operation. The following procedure can be used to manually refresh keys and SPI values in manual connections:

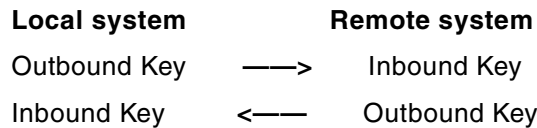
3. Decide how often you want to refresh the keys (once a day, for example).
4. On the eNetwork Firewall for Windows NT, generate seven configurations (enough to cover one week) and export the files.
5. Send the files to the AS/400 system administrator. For example, FTP the files using an existing VPN connection, or mail a diskette with the exported configuration files.
6. The VPN administrators at both ends must agree on when to activate the next configuration switching to the new values. They should select a time when no traffic is flowing through the connection since the connection must be deactivated to change the keys.

As you can see, manual connections are more difficult to manage and, in practice, can only be used with a small number of VPN partners. Use manual connections only when the VPN partner of your AS/400 system does not support IKE.

In this scenario, we selected DES-CBC as the ESP encryption algorithm. We did not choose ESP authentication (none).

The keys must be entered in hexadecimal format. *Inbound* key refers to the local AS/400 system key, and *Outbound* key refers to the remote VPN partner, which, in this scenario, is the eNetwork Firewall for Windows NT.

In other words, the system sending the data uses its Outbound key for IPsec operations. The system receiving the data uses its Inbound key for the same IPsec operation. Therefore, the *local* Outbound key must match the *remote* Inbound key. And, the *local* Inbound key must match the remote Outbound key:



The *Inbound* SPI refers to the value received from the remote system (the eNetwork Firewall for Windows NT in this scenario). The *Outbound* SPI refers to the value sent by the local AS/400 system to the VPN partner.

Tip

The AS/400 configuration requires the Security Policy Index in hexadecimal format while it is in decimal format in the eNetwork Firewall for Windows NT configuration file. Use the values from the eNetwork Firewall for Windows NT tunnel configuration export file to convert these values to hexadecimal values.

Figure 977 shows the values configured in the Encapsulate Security Payload window for this scenario. The first two hexadecimal values of the inbound security policy index have to be zero.

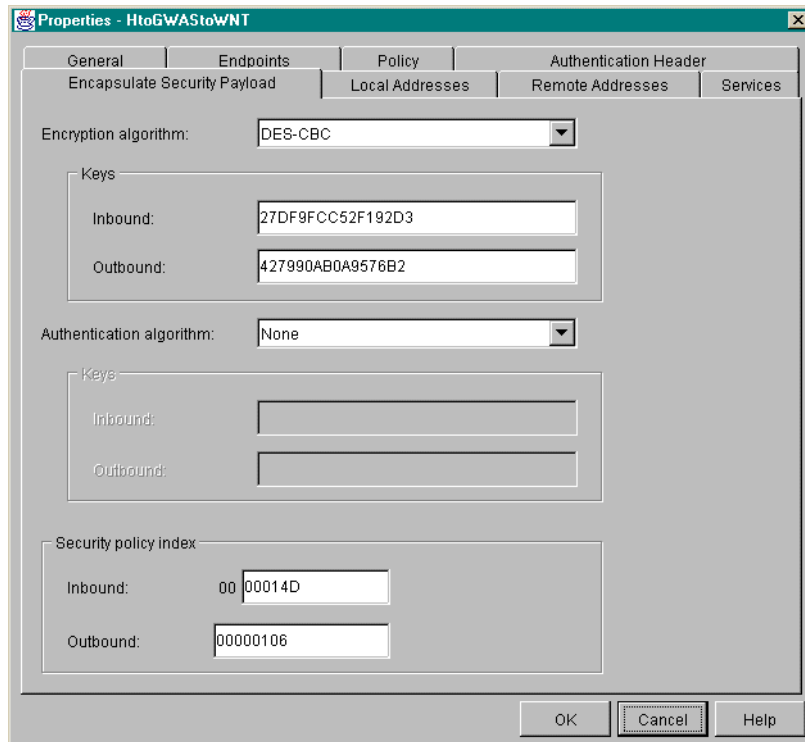


Figure 977. Manual connection - Encapsulate Security Payload page

15. Click the **Local Addresses** tab. The window shown in Figure 978 on page 865 is displayed.
16. At the Local Addresses window, configure the local data endpoint. In this scenario, the local data endpoint (VPN users) is the local host AS/400 system IP address 9.24.104.121 as shown in Figure 978 on page 865.

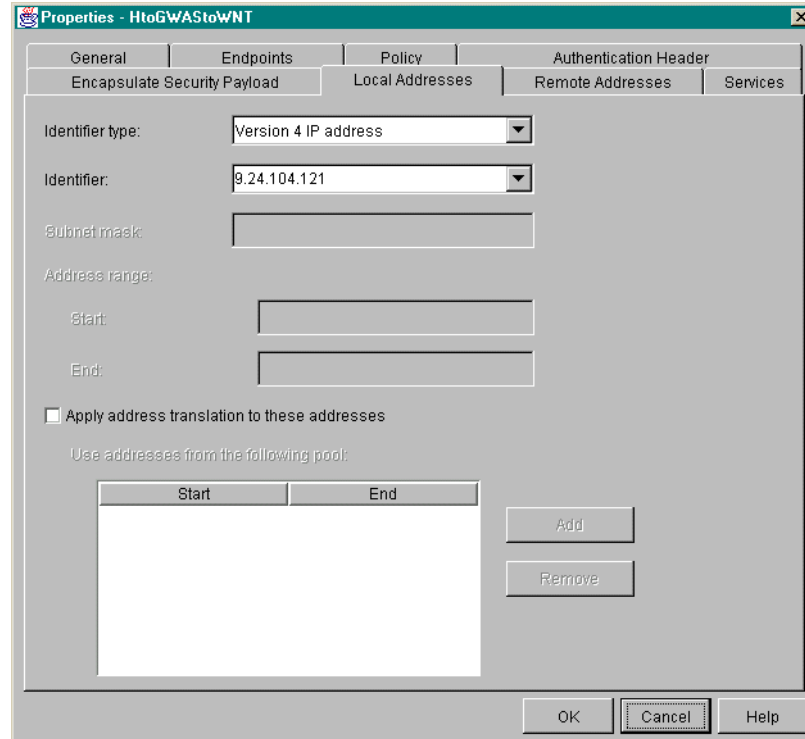


Figure 978. Manual connection - Local data endpoint

17. Click **Remote Addresses**. The window shown in Figure 979 on page 866 is displayed.
18. At the Remote Addresses window, configure the remote data endpoint (remote VPN users). In this scenario, the remote data endpoint is the subnet behind the eNetwork Firewall for Windows NT (192.168.10.0, with subnet mask 255.255.255.0). See Figure 979 on page 866.

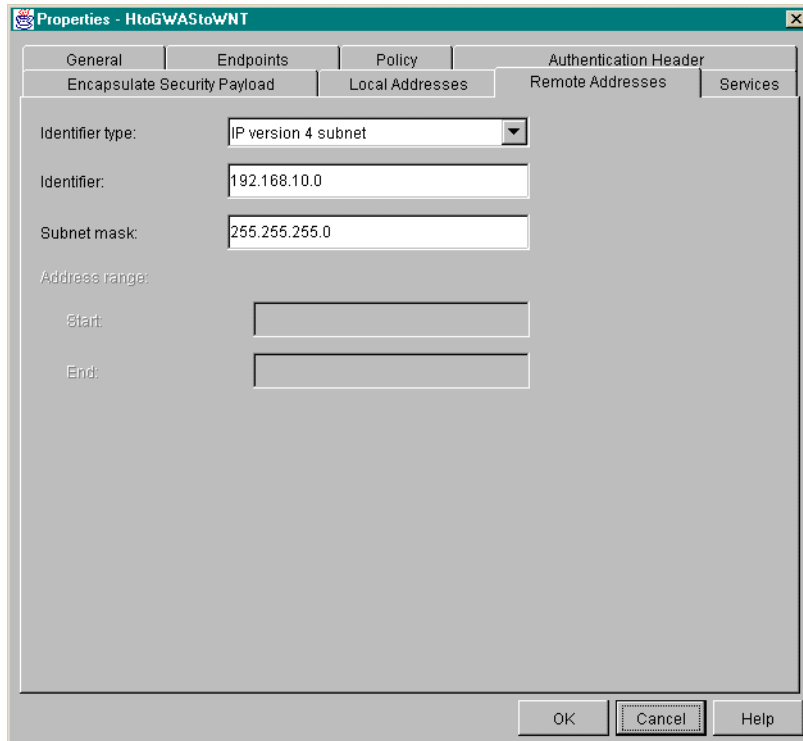


Figure 979. Manual connection - Remote data endpoint

19. Click the **Services** tab. The window shown in Figure 980 on page 867 is displayed.
20. Select **Any port** for the Local and Remote port parameters.
21. Select **Any protocol** for the Protocol parameter.

The Services window shows that there is no restriction in the services allowed through the VPN. See Figure 980 on page 867.

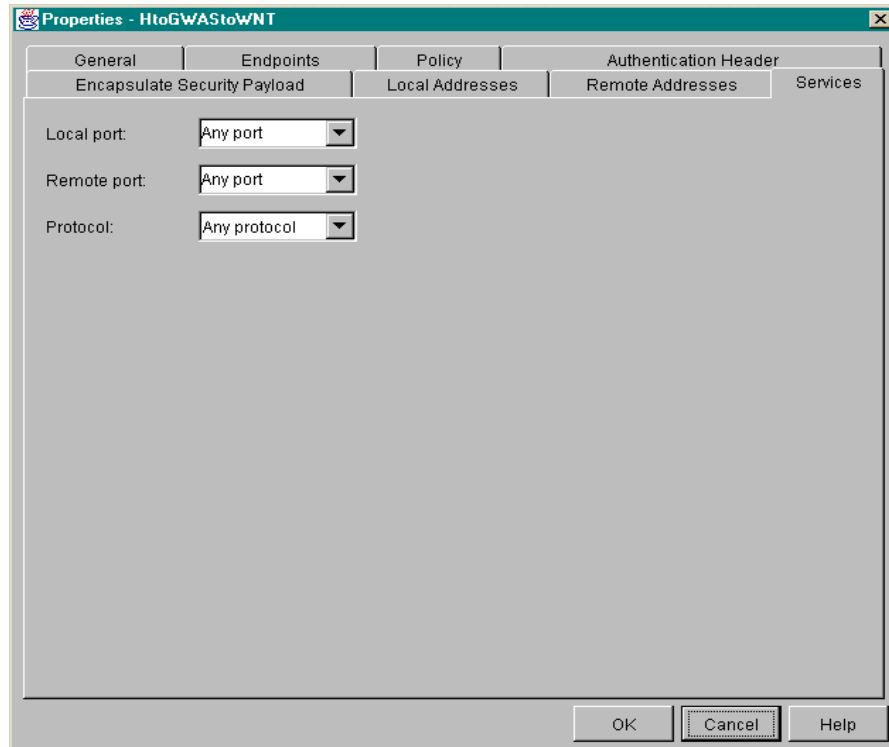


Figure 980. Manual connection - Services page

19.3.3 Configuring IP packet security on RALYAS4A

To complete the VPN configuration in this scenario, you must configure the following IP filters:

- Defined address to represent the corporate subnet.
- IPSec filter rule pointing to the manual connection name created in 19.3.2, “Configuring a manual VPN connection on the AS/400 system” on page 857.
- Filter rules to allow traffic to or from the eNetwork Firewall and the AS/400 system, RALYAS4A. ESP traffic should be allowed.
- Filter interface to tie all filter rules with the same name set together and apply them to a physical line.

Notice that, in a manual connection, there is no need to add the IP filter rules that permit IKE negotiations (UDP 500) since the IKE protocol is not used in manual connections.

Note

Only the filters needed to enable the tunnel between the corporate subnet and RALYAS4A are shown in this section. Additional filter rules may be needed depending on your specific configuration.

Create the following filters:

1. Defined address. A subnet IP address cannot be used in filter rules, so you need to configure a defined address for the corporate subnet as shown in Figure 981.

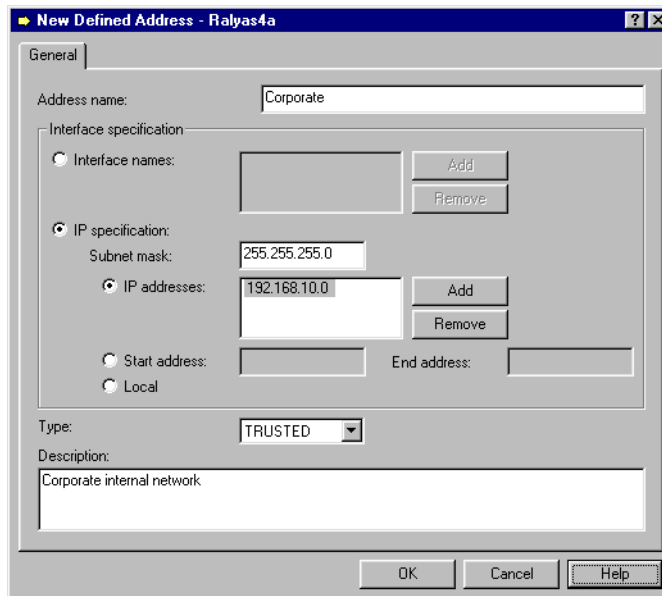


Figure 981. Defining the corporate subnet

2. IPSEC filter rule. Configure the IPSEC filter rule that allows data traffic from RALYAS4A to the corporate subnet to use the VPN. The inbound IPSEC rule is automatically created for you under the covers by the AS/400 system. The Set name must be the same for all the related filter rules (MANUAL in our example). IPSEC filter rule dictates the set or subset of traffic in the connection, and the connection name dictates the data treatment applied to that traffic. The connection must be the one created in 19.3.2, "Configuring a manual VPN connection on the AS/400 system" on page 857. Refer to Figure 982 on page 869.

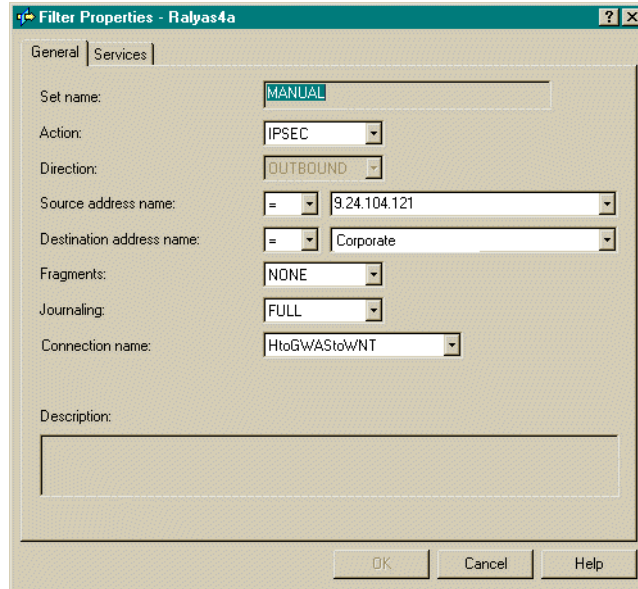


Figure 982. IPSec filter rule - IP traffic between RALYAS4A host and eNetwork Firewall gateway

The corresponding Services window associated with the previously created IPSec filter rule allows all protocols and ports as shown in Figure 983.

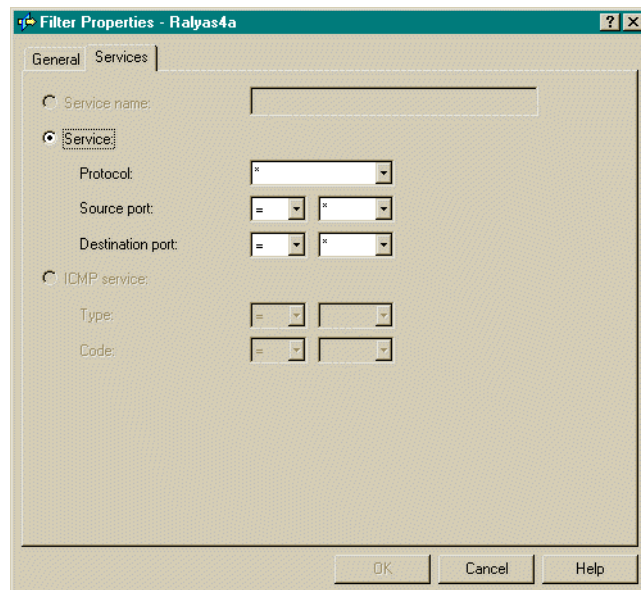


Figure 983. IPSec filter rule - Services page

3. Permit ESP traffic between RALYAS4A and eNetwork Firewall. You must configure inbound and outbound filters to permit the traffic between the AS/400 system host (RALYAS4A) and the eNetwork Firewall gateway as shown in Figure 984 and Figure 985 on page 870.

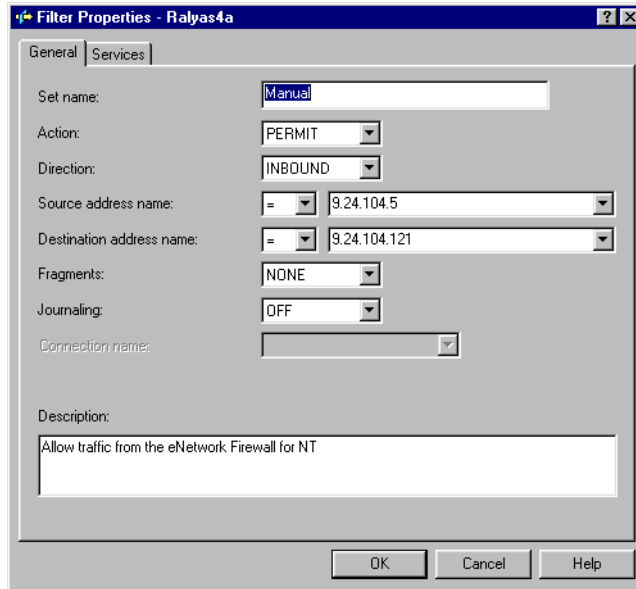


Figure 984. Permit INBOUND ESP traffic between RALYAS4A and firewall - General page

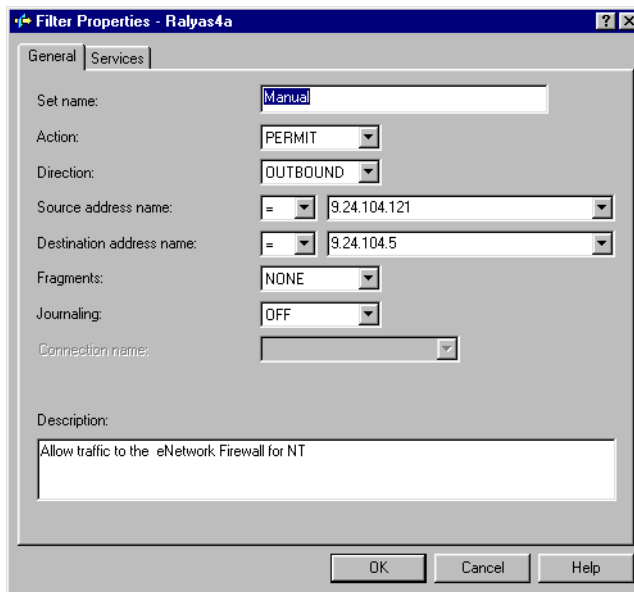


Figure 985. Permit OUTBOUND ESP traffic between RALYAS4A and firewall - General page

4. The services window associated with both filter rules created in Figure 984, allows the tunnel ESP traffic as shown in (Figure 985).

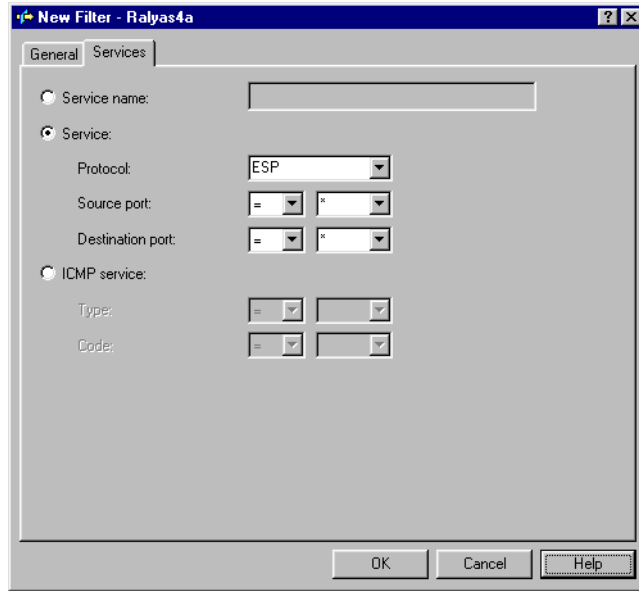


Figure 986. ESP traffic between RALYAS4A and eNetwork Firewall - Services page

5. Filter interface. Finally, you must create the filter interface, which ties all the rules with set name Manual together and applies them to a physical line (Figure 987).

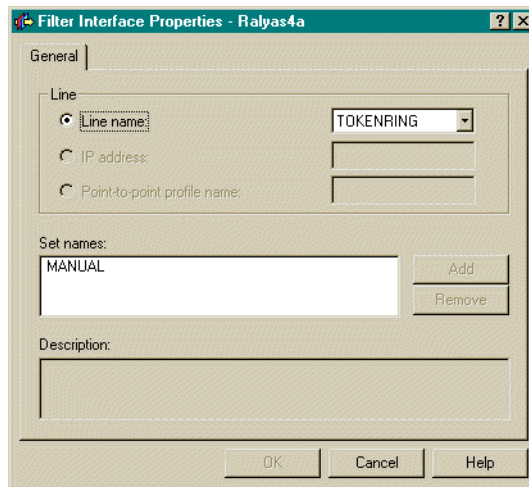


Figure 987. Filter interface - Applies filter rules with Set name MANUAL to line TOKENRING

Figure 988 summarizes the filters configured on RALYAS4AS4A.

```
#Defined Address - Corporate subnet
ADDRESS Corporate IP = 192.168.10.0 MASK = 255.255.255.0 TYPE = TRUSTED
#IPSEC filter rule
FILTER SET Manual ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 9.24.104.21
DSTADDR = Corporate PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE
JRN = OFF CONNECTION_DEFINITION = HtoGWASToWNT
# Allow traffic between RALYAS4A and eNetwork Firewall
FILTER SET Manual ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 9.24.104.5
DSTADDR = 9.24.104.121 PROTOCOL = ESP DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF

FILTER SET Manual ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 9.24.104.121
DSTADDR = 9.24.104.5 PROTOCOL = ESP DSTPORT = * SRCPORT = * FRAGMENTS =NONE JRN = OFF
#Filter interface
FILTER_INTERFACE LINE = TOKENRING SET = Manual
```

Figure 988. RALYAS4A - IP filters summary

You can now start the filter rules files.

19.4 VPN cross-reference configuration table: AS/400 to eNetwork Firewall

Table 124 provides a cross-reference list of the VPN configuration parameters for the AS/400 system and eNetwork Firewall.

Table 124. AS/400 system to eNetwork Firewall for Windows NT - Configuration cross reference

<u>AS/400</u>	<u>eNetwork Firewall</u>
Manual Connection Name = HtoGWASToWNT Role = Local host to remote gateway	Tunnel Name = ralyas4a Filter type = Static
Endpoints Local identifier type = IPv4 Local identifier = 9.24.104.121 (1) Remote identifier type = IPv4 Remote identifier = 9.24.104.5 (2)	Identification Tunnel Addresses Local = 9.24.104.5 (2) Remote = 9.24.104.121 (1) SPI Remote = 333 (11) Local = 262 (12)
Policy Encapsulation mode = Tunnel (3) Protocol = ESP (4) Connection Lifetime = Never expires (5)	Policy = Encryption only (ESP) (4)
Authentication Header n/a (6)	Authentication (AH) Authentication algorithm = n/a (6)
Encapsulate Security Payload Encryption algorithm = DES-CBC (7) Key, inbound = 27DF9FCC52F192D3 (8) Key, outbound = 427990AB0A9576B2 (9) Authentication algorithm = None (10) Security policy index Inbound = 0000014D (11) Outbound = 00000106 (12)	Encryption (ESP) Encryption algorithm = DES_CBC (7) Authentication algorithm = None (10) Sending encryption key = 27df9fcc52f192d3 (8) Receiving encryption key = 427990ab0a9576b2 (9) Replay prevention = No (23) Tunnel Life Time = 480 (5)
Local Addresses Identifier type = IPv4 Identifier = 9.24.104.121 (13)	IP Filters Non-encrypted traffic on secure interface Inbound / outbound From / to IP address = 192.168.10.0 From / to IP address = 9.24.104.121 Protocols = any Traffic to the VPN tunnel Inbound / outbound From / to IP address = 9.24.104.121 (17)(13) From / to IP address = 192.168.10.0 (18)(14) Protocols = any (19)(15)(16) Tunnel ID = 7
Remote Addresses Identifier type = IPv4 subnet Identifier = 192.168.10.0 (14) Subnet mask = 255.255.255.0	Encrypted traffic between tunnel endpoints Inbound / outbound From / to IP address = 9.24.104.121 From / to IP address = 9.24.104.5 Protocols = any
Services Local/remote ports = Any (15) Protocols = Any (16)	
IP Filters Set Name = Manual - Line TOKENRING IPSec Rule Source address = 9.24.104.121 (17) Destination address = 192.168.10.0 (18) Connection name = HtoGWASToWNT	
Services Protocols, ports = * (any) (19)	
Traffic between RALYAS4A and enetwork Firewall Source / destination address = 9.24.104.121 (20) Source / destination address = 9.24.104.5 (21)	
Services Protocols, ports = ESP, * (any) (22)	

eNetwork Firewall for Windows NT supports tunnel mode only. There is no parameter in the firewall configuration to specify transport or tunnel mode.

19.5 Starting the VPN connections and final verification

This section describes how to start the connection at both ends of the tunnel and perform the final verification test.

19.5.1 Starting the VPN tunnel on the eNetwork Firewall for Windows NT

To start the VPN tunnel, perform the following steps:

1. At the Virtual Private Network Administration window, select the tunnel **ralyas4a**.
2. Click **Activate**.

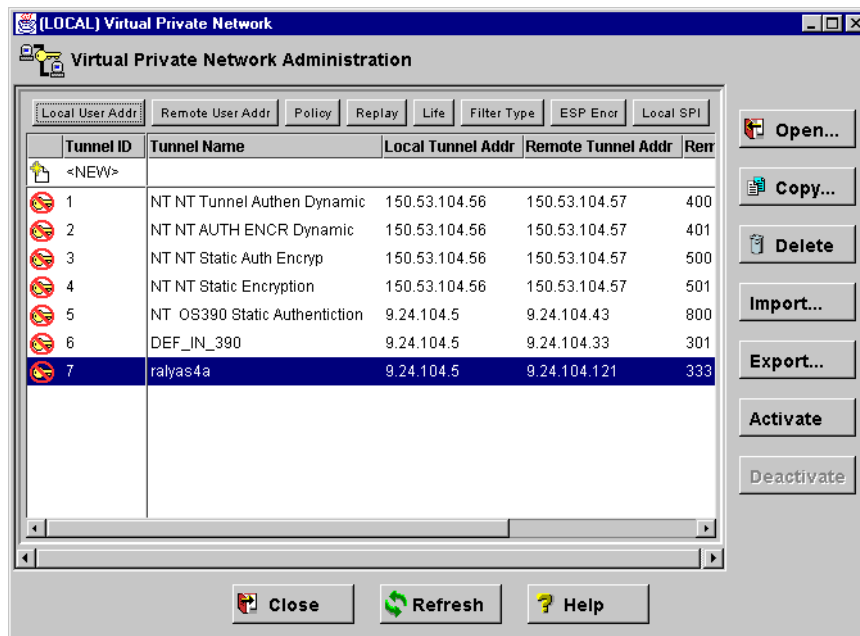


Figure 989. eNetwork Firewall for Windows NT - Starting the VPN tunnel

The status of the tunnel changes as shown in Figure 990 on page 875.

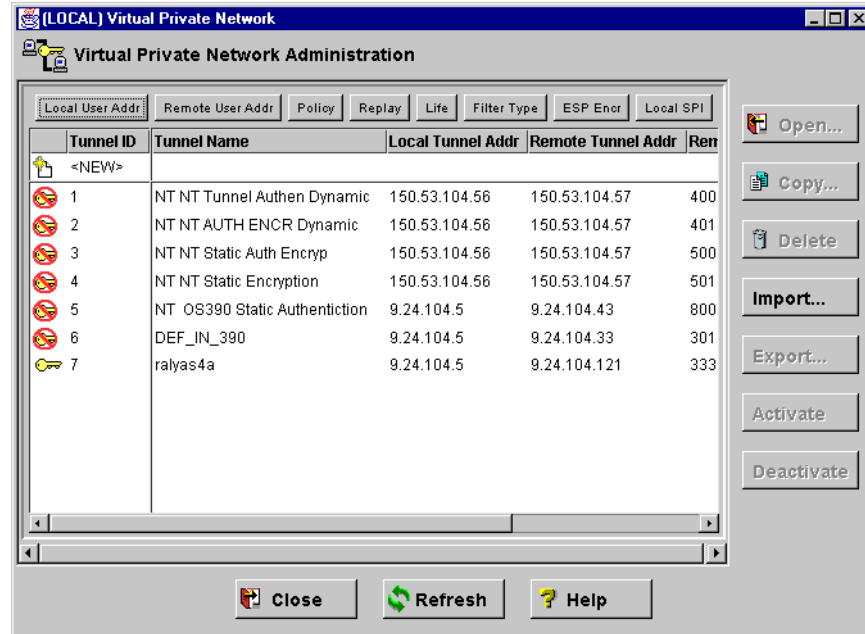


Figure 990. eNetwork Firewall for Windows NT - Active VPN tunnel

3. Activate the filter rules.

19.5.2 Starting the VPN connection on the AS/400 system

Before starting the VPN connection, you must verify that the IP filters and the VPN server are started on the AS/400 system.

To start the manual VPN connection, perform the following steps:

1. Open the Virtual Private Networking window.
2. Select **Secure Connections**.
3. Select **Manual Connections**.
4. Right-click the **HtoGWAStoWNT** connection, and click **Start** from the pull-down menu.
5. Display the connection to verify that it is active. At the Virtual Private Networking window select **View->Active Connections**. The Active Connections window is displayed and shows the status of the VPN connection.

19.5.3 Verification test

To verify the VPN connection, we use the PING command from RALYAS4A to any system in the corporate network and vice versa. In addition, we use the communications trace on the AS/400 system to verify that the data was encrypted and the ESP protocol was being used.

Appendix A. Special notices

This publication is intended to help network administrators, consultants, and AS/400 specialists who plan to design, implement, and configure virtual private networks where AS/400 systems participate. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM Operating System/400. See the PUBLICATIONS section of the IBM Programming Announcement for OS/400 V4R4 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX	AS/400
AT	CT
eNetwork	IBM ®
Netfinity	Operating System/400
OS/390	OS/400
RACF	RS/6000
S/390	SecureWay
SP	SP2
System/390	ThinkPad
XT	400

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere., The Power To Manage., Anything. Anywhere., TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET and the SET logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix B. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

B.1 IBM Redbooks publications

For information on ordering these ITSO publications see “How to get IBM Redbooks” on page 881.

- *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162
- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147
- *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209
- *A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions*, SG24-5234
- *A Comprehensive Guide to Virtual Private Networks, Vol III: IBM Cross-Platform and Key Management Solutions*, SG24-5309
- *IBM Firewall for AS/400: VPN and NAT Support*, SG24-5376
- *Security in OS/390-based TCP/IP Networks*, SG24-5383
- *SecureWay CS for OS/390 V2R8 TCP/IP: Guide to Enhancements*, SG24-5631

B.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at <http://www.redbooks.ibm.com/> for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr Format)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

B.3 Other resources

These publications are also relevant as further information sources:

- *Tips and Tools for Securing Your AS/400*, SC41-5300
- *OS/400 Security Reference V4R4*, SC41-5302
- *OS/390 Firewall Technologies Guide and Reference*, SC24-5835

- Albitz, Paul and Liu, Cricket. *DNS and BIND*. O'Reilly & Associates. 1998. ISBN: 1-56-592512-2
- Graham, Buck and Graham, Norman B. *TCP/IP Addressing: Designing and Optimizing Your IP Addressing Scheme*. Academic Press. 1996. ISBN 0-12-294630-8
- RFC 1027 *Using ARP to Implement Transparent Subnet Gateways*
- RFC 1661 *The Point-to-Point Protocol (PPP)*
- RFC 1700 *Assign Numbers*
- RFC 1858 *Security Considerations for IP Fragment Filtering*
- RFC 1918 *Address Allocation for Private Internets*
- RFC 2401 *Security Architecture for the Internet Protocol*
- RFC 2407 *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2409 *The Internet Key Exchange (IKE)*
- RFC 2410 *The NULL Encryption Algorithm and Its Use With IPsec*
- RFC 2498 *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2661 *Layer Two Tunneling Protocol "L2TP"*
- RFC 2709 *Security Model with Tunnel-mode IPsec for NAT Domains*

B.4 Referenced Web sites

- IBM Redbooks home page: <http://www.redbooks.ibm.com>
- The Internet Engineer Task Force Web site: <http://www.ietf.org>
- For updates on VPN information: <http://www.as400.ibm.com/vpn>
- *AS/400 Performance Capabilities Reference V4R4* for AS/400 VPN performance test results:
<http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R4PDF/AS4PPCP1.PDF>
- For ICSA certification: <http://www.icsa.net>
- Troubleshooting Guide for VPN: <http://www.as400.ibm.com/infocenter>
- For IRE company information and product information on SafeNet Soft-PK:
<http://www.ire.com>
- For information about WinVPN: <http://www.wrs.com>

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** <http://www.redbooks.ibm.com/>

Search for, view, download, or order hardcopy/CD-ROM redbooks from the redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this redbooks site.

Redpieces are redbooks in progress; not all redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

Send orders by e-mail including information from the redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the "How to Order" section at this site: http://www.elink.ibm.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the "How to Order" section at this site: http://www.elink.ibm.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the "How to Order" section at this site: http://www.elink.ibm.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and redbooks by accessing the IBM Intranet Web site at <http://w3.itso.ibm.com/> and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at <http://w3.ibm.com/> for redbook, residency, and workshop announcements.

Index

Symbols

- *CHK value 642
- *END value 642

Numerics

- 2210 router
 - configuration 725
 - gateway-to-gateway VPN 723
 - planning worksheet 725
 - software 724
 - tips 767
 - VPN 729
 - VPN configuration 751
- 2212 router
 - configuration 689
 - planning worksheet 689
 - software 688
 - VPN 693
 - VPN configuration 705
- 3DES 52
- 3DES not a choice for encryption 656
- 5769-AC2 52, 62
- 5769-AC3 52, 62
- 5769-TC1 62
- 5769-XE1 62

A

- A network error has occurred 661
- Active Connections GUI 97
 - customizing view 98
- Active Connections window 628
- Active filter rules fail to deactivate 655
- aggressive mode 28, 61
- Aggressive Mode model 671
- AH (Authentication Header) 12
- AH packet format 14
- AIX server
 - host-to-host VPN 772
 - planning worksheet 771
- AIX software 771
- AIX VPN configuration 771
- All keys are blank 652
- allocating addresses 39
- APP parameter 640, 641
- ARGLIST parameter 641
- AS/400 and SafeNet Soft-PK VPN configuration cross-reference list 509
- AS/400 Client Access Express 62
- AS/400 communication trace example 673
 - with details 676
- AS/400 gateway-to-gateway VPN configuration 742
- AS/400 host-to-AS/400 host 163
- AS/400 host-to-gateway VPN 696
- AS/400 host-to-host VPN 163
- AS/400 host-to-host VPN configuration 778, 821
- AS/400 manual connection VPN configuration 855

- AS/400 Operations Navigator 62, 68
- AS/400 security gateway at the branch office 531
- AS/400 system
 - Gateway to Dynamic IP Users VPN 424
 - Host to Dynamic IP Users VPN 447
 - host-to-gateway VPN 698
 - host-to-host VPN 780, 823
 - IP filtering 709, 754
 - IP filters 430, 452, 791
 - IP packet security 832, 867
 - planning worksheet 424, 446, 696, 742, 778, 821, 856
 - RALYAS4A 474
 - RALYAS4C 494
 - VPN connection 840, 875
- AS/400 VPN gateway 203
 - remote access behind a firewall 540
- AS/400 VPN problem determination 627
- AS/400 VPN problem determination tools 628
- AS/400 VPN server behind the firewall 527
- AS05 routes 260
- AS05 TCP/IP interfaces 260
- AS05 TCP/IP interfaces and routes 537
 - configuration 260
- AS14 and AS20 configuration cross-reference table 196
- AS14 IP filters summary 187
- AS14 routes 259
- AS14 TCP/IP interfaces 259
- AS14 TCP/IP interfaces and routes 536
 - configuration 259
- AS14 VPN NAT source inbound IP filter configuration summary 562
- AS20 IP filters configuration summary 195
- AS20 routes 260
- AS20 TCP/IP interfaces 260
- AS20 TCP/IP interfaces and routes 538
 - configuration 260
- AUTH 671
 - authentication 39
 - authentication data 16
 - Authentication Header (AH) 12, 14
 - transport mode 16
 - tunnel mode 16
 - authentication protocols 22

B

- backup 101
- basic planning 61
- border system 199
- branch office
 - AS/400 security gateway 531
 - connection scenario 7
 - host to corporate office gateway VPN 845
 - network to corporate network connection 323
 - to main office connection scenario 351
 - to main office connection tunnel scenario 263
- branch office VPN connection

- AS/400 gateway to 2210 router gateway 723
- AS/400 host to 2212 router gateway 687
- business partner and supplier scenario 8
- business partner VPN connection 163
 - host-to-host AS/400 to AIX 769
 - host-to-host AS/400 to S/390 799

C

- CFGOBJ parameter 649, 650, 651
- CFGTYPE parameter 649, 650, 651
- cipher 25
- CL command 54
- combining AH and ESP 23
- Commit Bit notification 669
- common problems of AS/400 VPN for early users 651
- communications trace 649
- compulsory tunnel 40, 41
- configuration changes for VPN NAT
 - for servers 617
 - source inbound 565
 - source outbound 581
- configuring a host-to-host VPN 171, 189
- configuring L2TP connections 78
- configuring LNS 266
- configuring the gateway-to-gateway VPN 617
- configuring the manufacturer's AS/400 VPN gateway 590
- configuring IP packet security 179
- CONNECTED notification 669
- Connection is running after you stopped it 657
- Connection lifetime 65, 76
- Connection not displayed in the Active Connections window 658
- Connection overlap with existing connection 659
- connection status 461
- CONNECTION_DEFINITION 665
- CPF9821: Not authorized to program QTFRPRS in QSYS library 652
- Cryptographic Access Provider 62
- cryptographic algorithm 25
- cryptographic support 60
- customizing the VPN configuration 176, 194

D

- data confidentiality 10
- data integrity 10
- data origin authentication 9
- data policy (IKE phase 2) 65
- data protection 751
- Default 1024-bit MODP 61
- Default 768-bit MODP 61
- default security values 169
- deleting a VPN connection 82
- denial of service 26
- DES 52
- destination inbound 584
- dial-in client
 - in an L2TP compulsory tunnel 412
 - verifying interfaces and routes 416
- dial-up network 34

- modern 36
- traditional 34
- Diffie-Hellman Group 61
- Diffie-Hellman Perfect Forward Secrecy 61, 65
- Digital Certificate Manager 61
- digital certificates 59
- distributor's AS/400 VPN gateway 615
- DTADIR parameter 650
- DUN (Windows 95 Dial-Up Networking) 436
- Dynamic IP Connections 51, 63
- Dynamic IP Users 53
- dynamic key connection 51
 - initiation 67
- Dynamic Key Connections 63
 - objects created by the wizard 74

E

- edge system 199
- enabling the VPN journal 635
- Encapsulating Security Payload (ESP) 12, 18
- End Communications Trace (ENDCMNTRC) command 650
- ENDCMNTRC (End Communications Trace) command 650
- ending a VPN connection 68
- ENDTCPSVR 54
- end-to-end connectivity 422, 445, 469
 - verifying 526
- eNetwork Firewall for Windows NT 847, 849
 - planning worksheet 847
 - software 846
 - VPN tunnel 874
- eNetwork Firewall IP filter 855
- eNetwork Firewall VPN, exporting the configuration 851
- ESP (Encapsulating Security Payload) 12, 18
- ESP packet format 18
- ESP transforms 21
- ESP transport mode 20
- ESP tunnel mode 20
- establishing a call 39
- Exchange 664
- Expire after 65, 76
- Expire at size limit 65, 76
- exporting the eNetwork Firewall VPN configuration 851

F

- Failure occurred during phase 1 negotiations 659
- filter set
 - COMPT 379
 - ISP 374
 - to the client 379
 - to the ISP 374
- Filters not loaded correctly on WAN interfaces 655
- firewall
 - AH protocol 57
 - configuration 539
 - ESP protocol 57
 - IP forwarding 57
 - IPSec 57

- permitting IPSec protocols 522
- requirements 518
- firewall filters
 - configuring to permit IPSec protocols 545
 - L2TP compulsory tunnel protected by IPSec 550
 - L2TP voluntary tunnel protected by IPSec 550
- FMTBCD parameter 651
- FMTTCP parameter 651
- format of the Additional information field 664
- fragmentation 536

G

- gateway 696
- Gateway to Dynamic IP Users VPN AS/400 system 424
- Gateway to Hosts VPN New Connection Wizard 369
- Gateway-to-Gateway No Firewall scenario 201
- gateway-to-gateway voluntary tunnel 323
- gateway-to-gateway VPN 199, 206, 558, 564, 574, 581, 592
 - AS/400 to 2210 router 723
 - connection 233
 - on the AS/400 system 744
 - through a firewall 517
 - verification tests 237
- gateway-to-host and host-to-gateway connection groups 238
- gateway-to-host VPN on the Rochester AS/400 system 246
- generic VPN client (PCD) planning worksheet 471

H

- HASH 671
- HDR 670
- hiding IP addresses from your VPN partner 584
- Host to Dynamic IP Users 266
 - connection for ThinkPad C 474, 494
- Host to Dynamic IP Users VPN
 - AS/400 system 447
 - New Connection Wizard 362
- Host to Hosts connection, PC D 483, 495
- host-to-gateway and gateway-to-host connection groups 238
- host-to-gateway L2TP tunnel verification tests 322
- host-to-gateway VPN
 - AS/400 system 698
 - AS/400 to 2212 router 687
 - New Wizard Connection 396
 - on the Rochester AS/400 system 240
- host-to-host connection 187
- host-to-host VPN 167
 - AIX server 772
 - AS/400 system 780, 823
 - AS/400 to AIX server 769
 - AS/400 to S/390 799
 - S/390 system 804

I

- IBM Firewall for AS/400 58

- identity protection 61, 65, 76
 - mode 28
- IDx 670
- IETF (Internet Engineering Task Force) 10
- IKE (Internet Key Exchange) 26
- IKE authentication mechanism 59
- IKE modes 28
- IKE phase 1 27, 670
- IKE phase 1 authentication failed 660
- IKE phase 2 28, 670
- IKE phases 26
- IKE phases overview 670
- IKE protocol overview 670
- incoming calls 39
- initial connectivity 689, 771, 847
- initiator dial-in client IP filters 406
- interfaces 317, 344, 414
- interfaces and routes
 - in L2TP client 320
 - in LNS 317
- Internet Engineering Task Force (IETF) 10
- Internet Key Exchange (IKE) 26
 - protocol 12
- interoperability 10, 58
- Invalid filter rule name 655
- IP address conflicts in a VPN connection 551
- IP address management 45
- IP connectivity 166, 802
- IP destination address 30
- IP filter configuration planning worksheet 557, 564
- IP filter for eNetwork Firewall 855
- IP filter journal 630
- IP filter rules planning worksheet 188, 406
 - to dial-in client 380
 - to ISP 374
- IP filtering 562, 570, 580, 583, 623
 - on the AS/400 system 709, 754
 - on the manufacturer AS/400 VPN gateway 604
- IP filters
 - AS/400 system 430, 452, 791
 - in the L2TP client AS/400 system 333
 - initiator dial-in client 406
 - IPSec-only and L2TP with IPSec clients 464
 - L2TP client AS/400 system 304
 - LNS AS/400 system 279, 333, 374
 - on the Minneapolis AS/400 VPN gateway 232
 - on the Rochester AS/400 VPN gateway 217
 - VPN connection on the AS/400 system 529
 - VPN connection on the branch AS/400 system 533
 - VPN gateway behind a firewall 546
- IP forwarding 277, 358
- IP interfaces in the L2TP client 344
- IP interfaces in the LNS 346
- IP packet filter journaling 630
- IP packet filter rules file backup considerations 101
- IP packet security 55, 194
 - AS/400 system 832, 867
 - operation 84
 - planning 66
 - RALYAS4C 496

- IP Packet Security GUI 53
- IP Security (IPSec) protocols 11
- IPSec 56
- IPSec AH tunnel to the ISP Host to Dynamic IP Users 361
- IPSec configuration concepts 29
- IPSec ESP tunnel
 - to the client gateway to hosts 368
 - to the LNS host to gateway 396
- IPSEC filter rules host-to-gateway and gateway-to-host VPNs 248
- IPSec protocol 51, 59
 - for firewall 522
 - for firewall filters 545
- IPSec security 47
- IPSec specific notifications 669
- IPSec transforms 59
- IPSec tunnel 266
 - to the client Host to Dynamic IP Users 327
- IRE SafeNet Soft-PK 438
 - client on TPA 439
 - ThinkPad C planning worksheet 469
- IRE SafeNet Soft-PK client 511
 - ThinkPad C 499
 - VPN connection status 512
- Item not found 656
- iterated tunneling 23
- iVasion WinVPN client 453

J

- job logs 642
- job logs using Operations Navigator 643

K

- KE 670
- Key Expiration 65, 76
- Key management 65, 76
- key management 10
 - objectives 25
- key policy 61
- key policy (IKE phase 1) 65
- Key policy not offered as a choice in a Dynamic IP Connection Group 656
- key protection 751
- keyed 25
- keys and security parameters index format 59
- keyspace 25
- known limitations in AS/400 VPN V4R4 668

L

- L2TP 37, 55
 - characteristics 48
 - encapsulation 40
 - IP address management 45
 - security with IPSec 47
 - tunnel modes 41
- L2TP (Layer 2 Tunneling Protocol) 33
- L2TP Access Concentrator (LAC) 38, 56
- L2TP and VPN connections

- on the AS/400 LAC 95
- on the AS/400 LNS 93
- L2TP client
 - in a voluntary tunnel 286
 - in a voluntary tunnel protected with IPSec 333
 - interfaces and routes 320
- L2TP compulsory tunnel 351
 - firewall filters 550
 - with IPSec 411
- L2TP connections 51
- L2TP considerations 549
- L2TP error messages 666
- L2TP gateway-to-gateway voluntary tunnel 323
- L2TP host-to-gateway voluntary tunnel 263
- L2TP initiator 291
 - for the WinVPN client 458
 - in an L2TP voluntary tunnel 340
 - in L2TP voluntary tunnel 317
- L2TP Network Server (LNS) 38, 56
- L2TP server job 54
- L2TP terminator profile 273, 327, 354, 452
- L2TP voluntary tunnel
 - firewall filters 550
 - with IPSec 315, 339
- L2TP VPN connection 291
 - on the L2TP initiator 333
- L2TP VPN support 55
- L2TP with IPSec PC client (WinVPN) 461
- L2TPmtclt VPN 450
- LAC (L2TP Access Concentrator) 38, 56
- Layer 2 Tunneling Protocol (L2TP) 33
- limitations in AS/400 VPN V4R4 668
- LNS 56, 79
 - interfaces and routes 317
 - verifying interfaces and routes 414
- LNS (L2TP Network Server) 38
- LNS AS/400 system IP filters 333
- LNS AS05 460
- LNS in a compulsory tunnel protected by IPSec 354
- LNS in a voluntary tunnel protected by IPSec 327
- LNS in an L2TP compulsory tunnel 411
- LNS in an L2TP voluntary tunnel 339
- LNS in L2TP voluntary tunnel 315
- local key server IP address 401
- Local polic 665
- Local role 664

M

- main mode 28, 61, 65, 76
- Main Mode model 671
- main VPN protocols 12
- man-in-the-middle 26
- manual connection 51, 77
- manual connection VPN, AS/400 to eNetwork firewall 845
- Manual Connections
 - automatically starting 92
 - manually starting 92
- manual VPN connection, AS/400 system 857
- matching the 2212 router VPN configuration 705
- Maximum key lifetime 65, 76

- Maximum size limit 65, 76
- MAXSTG parameter 640
- Minneapolis AS/400 VPN gateway 229
 - IP filters 232
 - planning worksheets 229
- miscellaneous planning considerations 67
- mixed-client environment 464
- modern dial-up network 36
- modern private network 4
- mutable 14

N

- NETSTAT 651
- network IP addressing 326
- network routing scheme 326
- New Connection Wizard 53, 63
 - configure Host to Dynamic IP Users VPN 267
 - Gateway to Hosts VPN 369
 - Host to Dynamic IP Users VPN 362
 - host to gateway VPN 396
- New Connection Wizard planning worksheet 563
- no firewall protection 199
- No local pre-shared key found 659
- No remote phase 1 policy 653
- No remote phase 1 policy could be found 659
- No remote phase 2 policy 653
- No remote phase 2 policy could be found 660
- No remote pre-shared key 659
- NONCE 671
- Not authorized to program QTFRPRS in QSYS library 652
- Notation used to describe Oakley mode exchange 670

O

- Oakley Mode 670
- objects created by VPN configuration wizard 213
- outgoing calls 39

P

- P1_PREKEY 665
- Parameter PINBUF is not valid 658
- PC07 TCP/IP configuration 261, 539
- perfect forward secrecy 26
- performance and availability 10
- Phase 1 negotiations timed out 660
- phase 1 SA control 669
- Phase 2 negotiation timed out 660
- planning worksheet 187, 556
 - 2210 router 725
 - 2212 router 689
 - AIX server 771
 - AS/400 system 424, 446, 696, 742, 778, 821, 856
 - distributor AS/400 gateway 615
 - eNetwork Firewall for Windows NT 847
 - for Minneapolis VPN AS/400 gateway 229
 - for Rochester AS/400 gateway 167, 204
 - generic VPN client (PCD) 471
 - IP filter configuration 591
 - IP filter rules 279, 305, 406, 572

- IP filter rules configuration 573, 616
- IP filter rules to dial-in client 380
- IP filter rules to ISP 374
- IRE SafeNet Soft-PK (ThinkPad C) 469
- manufacturer AS/400 gateway 590
- New Connection Wizard 571, 573, 590, 615
- New Connection Wizard gateway to hosts 368
- New Connection Wizard Host to Dynamic IP Users 267
- New Connection Wizard Host to Dynamic IP Users to ISP 362
- RALYAS4A 472
- RALYAS4C 473
- S/390 system 802
- SafeNet Soft-PK client (TPA) 422
- VPN PC clients 422
- WinVPN client 445

- policy values for active connections 272
- PPP dial-in client in a compulsory tunnel with IPsec 389
- PPP dial-up connection to the ISP 286, 333, 389
- Pre-shared key is invalid 655
- Pre-shared key not found on local system 654
- Preshared key not found on remote system 654
- PRF 671
- Print Communications Trace (PRTCMNTRC) command 650
- printing the trace data 650
- private network 3
 - modern 4
 - traditional 3
- protecting your VPN server 515
- proxy ARP 265, 274, 354, 355, 358
- PRTCMNTRC (Print Communications Trace) command 650

Q

- QATOVSOFF file layout 638
- QIPFILTER journal 631
- QRETSVRSEC system value 61
- QTCPIP job 642
- QTOKVPNIKE 54
- QTOKVPNIKE job 642
- QTOVMAN 54
- QTOVMAN job 642
- QTTPANSxxx job 642
- QTPPPCTL 54
- QTPPPCTL job 642
- QTPPPPL2SSN 54
- QTPPPPL2SSN job 643
- QTPPPPL2TP 54
- QTPPPPL2TP job 643
- Quick Mode model 672
- QVPN journal 637

R

- RALYAS4A 474
 - planning worksheet 472
 - VPN connection 500
- RALYAS4C 494

- IP packet security 496
- planning worksheet 473
- VPN connection 505
- RC=14: The local policy does not contain a match 664
- RC=24: IKE phase 1 authentication failed 660
- RC=5: TCP8709 VPN policy processing error 665
- RC=8214: Failure occurred during phase 1 negotiations 659
- RC=8220: No local pre-shared key found 659
- RC=8221: No remote phase 1 policy could be found 659
- RC=8222: No remote pre-shared key 659
- RC=8223: Phase 1 negotiations timed out 660
- RC=8241: No remote phase 2 policy could be found 660
- RC=8242: Phase 2 negotiation timed out 660
- RC=8243 or RC=8252: A network error has occurred 661
- RC=8257: Remote identifier mismatch 661
- recovery 101
- remote access 33
 - scenario 9
- Remote identifier mismatch 661
- remote PC clients
 - with IPSec and L2TP support 444
 - with IPSec-only support 419
- Remote proposal 664
- REMOTE_ID_GROUP 665
- replay protection 10, 60
- requirements for VPN 9
- responder 584
- restricted cipher 25
- restricting services 67
- RMTNETADR parameter 641
- Rochester AS/400
 - gateway-to-host VPN 246
 - host-to-gateway VPN 240
- Rochester AS/400 VPN gateway 203
 - IP filters 217
 - planning worksheets 167, 204
- router configuration 261, 538
- routers 57
 - AH 57
 - ESP 57
 - IP forwarding 57
 - IPSec 57
- routes 317, 344, 414
 - in the L2TP client 345
 - in the LNS 348
- routing 57

S

- S/390 software 801
- S/390 system
 - host-to-host VPN 804
 - planning worksheet 802
 - VPN connection 841
- S/390 VPN configuration 802
- SA 670
- SA (Security Association) 29
- SafeNet Soft-PK and S/400 VPN configuration cross-reference list 509
- SafeNet Soft-PK client (TPA) planning worksheet 422

- scenario
 - branch office connection 7
 - business partner and supplier 8
 - remote access 9
- secret-key algorithm 25
- secure LAN access for PC clients in the intranet 467
- secure remote access for PC clients (Internet) 419
- Secure Sockets Layer (SSL) 13
- security 40
- Security Association (SA) 29
- security associations database (SAD) 31
- Security Parameter Index (SPI) 19, 29, 31
- security policy database (SPD) 31
- security protocol 30
- SET parameter 640, 641
- SKEYID_a 671
- SLTPORT parameter 651
- source inbound 552
- source outbound 552
- SPD (security policy database) 31
- SPI (Security Parameter Index) 19, 29, 31
- SSL (Secure Sockets Layer) 13
- Start Communications Trace (STRCMNTRC) command 649
- starting a VPN connection 67
- starting LNS AS05 460
- starting the communications trace 649
- starting the New Connection Wizard 71
- starting the TCP/IP application trace 640
- starting the VPN connections 196, 570, 583, 624
- Status for a connection in the Active Connection window is blank 658
- stopping the communications trace 650
- stopping the TCP/IP application trace 641
- stopping VPN connections 100
- STRCMNTRC (Start Communications Trace) command 649
- STRTCPSVR 54
- subnetting considerations 519, 542
- symmetric algorithm 25

T

- TC/IP routing 203
- TCP/IP communication 57
- TCP/IP configuration
 - adding information 259
 - additional information 535
- TCP/IP Connectivity Utilities for AS/400 62
- TCP/IP routing 555, 588
- TCP8705 Complete list of reason codes 661
- TCP8705 error processing VPN Connection Manager command 659
- TCP870C proposal not accepted with remote system & 1 664
- TCPIPADR parameter 651
- terminology 61
- test network 541
- TEXT parameter 650
- The local policy does not contain a match 664
- ThinkPad C

- Host to Dynamic IP Users connection 474, 494
- IRE SafeNet Soft-PK client 499
- TITLE parameter 642
- Trace TCP/IP Application (TRCTCPAPP) command 640
- tracing
 - gateway-to-gateway connection 256
 - gateway-to-host connection 258
 - host-to-gateway connection 257
 - VPN tunnels 256
- traditional dial-up network 34
- traditional private network 3
- traffic consolidation 5
- transform 11, 17
- transport adjacency 23
- transport mode 16, 20
- TRCFULL parameter 641, 650
- TRCTCPAPP 54
- TRCTCPAPP (Trace TCP/IP Application) command 640
- tunnel mode 16, 20, 40
- two phases of IKE 26

U

- Unable to communicate with the remote system 652
- Unable to encrypt keys. QRETSVRSEC must be set to 1 651
- Unable to retrieve the connection information in Active Connections window 658
- Unable to update the object 657
- Unexpected columns display in the Active Connections Monitor 658
- using the QIPFILTER journal 631
- using the QVPN journal 637
- USRDTA parameter 650

V

- Valid key policy is required 657
- verification tests 197, 237, 322, 465, 535, 721, 768, 797, 843, 875
- verifying interfaces and routes 344, 414
 - dial-in client 416
- virtual IP addressing and routing 520
- virtual IP and routing, remote access to VPN gateway behind a firewall 542
- virtual point-to-point profile 79
- virtual PPP connection on the L2TP initiator 311, 333
- Virtual Private Network (VPN) 3, 6
- Virtual Private Network Network Address Translation (VPN NAT) 56, 551
- Virtual Private Networking GUI 53
- voluntary tunnel 40, 43
 - protected by IPSec 266
- voluntary tunneling 263
- VPN 9
 - 2210 router 729
 - on the AS/400 system 510
- VPN (Virtual Private Network) 3, 6
- VPN address translation 68
- VPN and L2TP connections on the AS/400 LNS 93
- VPN components 53

- VPN configuration 68
 - customizing objects 75
 - object relationships 74
- VPN configuration cross-reference table
 - AS/400 to 2210 router 762
 - AS/400 to 2212 router 717
 - AS/400 to AIX server 790
 - AS/400 to eNetwork Firewall 873
 - AS/400 to S/390 839
- VPN configuration wizard objects 213
- VPN connection 443, 534, 717, 762, 795, 840, 874
 - AS/400 system 718, 763, 840, 875
 - host-to-gateway and gateway to host 254
 - IP filters on the branch AS/400 system 533
 - IP filters on the corporate AS/400 system 529
 - RALYAS4A 500
 - RALYAS4C 505
 - S/390 system 841
- VPN connection status 343, 511
 - AS/400 system 511
 - IRE SafeNet Soft-PK client 512
- VPN connection type 62
- VPN connections 510
 - automatic ending 100
 - PC clients and AS/400 (intranet) 467
 - status checking 97
- VPN connections operations 90
- VPN connections status 97
- VPN customer value 6
- VPN gateway 199
 - behind a firewall 520, 542
 - IP filters 546
 - platform 515
- VPN graphical user interface (GUI) 53
- VPN GUI default values 76
- VPN implementation 51
- VPN in the 2212 router 693
- VPN journal 634
- VPN key manager job messages 659
- VPN key manager reason codes 659
- VPN NAT (Virtual Private Network Network Address Translation) 56, 551
 - VPN NAT for servers 584, 599
 - VPN NAT for servers implementation 586
 - VPN NAT source inbound 558
 - VPN NAT source inbound implementation 553
 - VPN NAT source outbound 575
 - VPN NAT source outbound implementation 571
- VPN PC clients 68
- VPN PC clients planning worksheet 422
- VPN policy database 54
 - backup 101
- VPN policy processing error 665
- VPN problem determination 627
- VPN problem determination tools 628
- VPN protocols 10
- VPN requirements 9
- VPN server jobs 54
 - status checking 88
- VPN server operations 87

- VPN software prerequisites 52
- VPN terminology 61
- VPN tunnel
 - on eNetwork Firewall for Windows NT 874
 - tracing 256
- VPNAT 52
- VPNSVR parameter 641

W

- Windows 95 Dial-Up Networking (DUN 1.3) for WinVPN 453
- Windows 95 Dial-Up Networking (DUN) 436
- WinVPN client 453
 - L2TP initiator 458
 - planning worksheet 445
- Work with Connection Status (NETSTAT) command 651

IBM Redbooks evaluation

AS/400 Internet Security: Implementing AS/400 Virtual Private Networks
SG24-5404-00

Your feedback is very important to help us maintain the quality of IBM Redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at <http://www.redbooks.ibm.com/>
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?

Customer **Business Partner** **Solution Developer** **IBM employee**
 None of the above

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

What other Redbooks would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

SG24-5404-00

Printed in the U.S.A.

