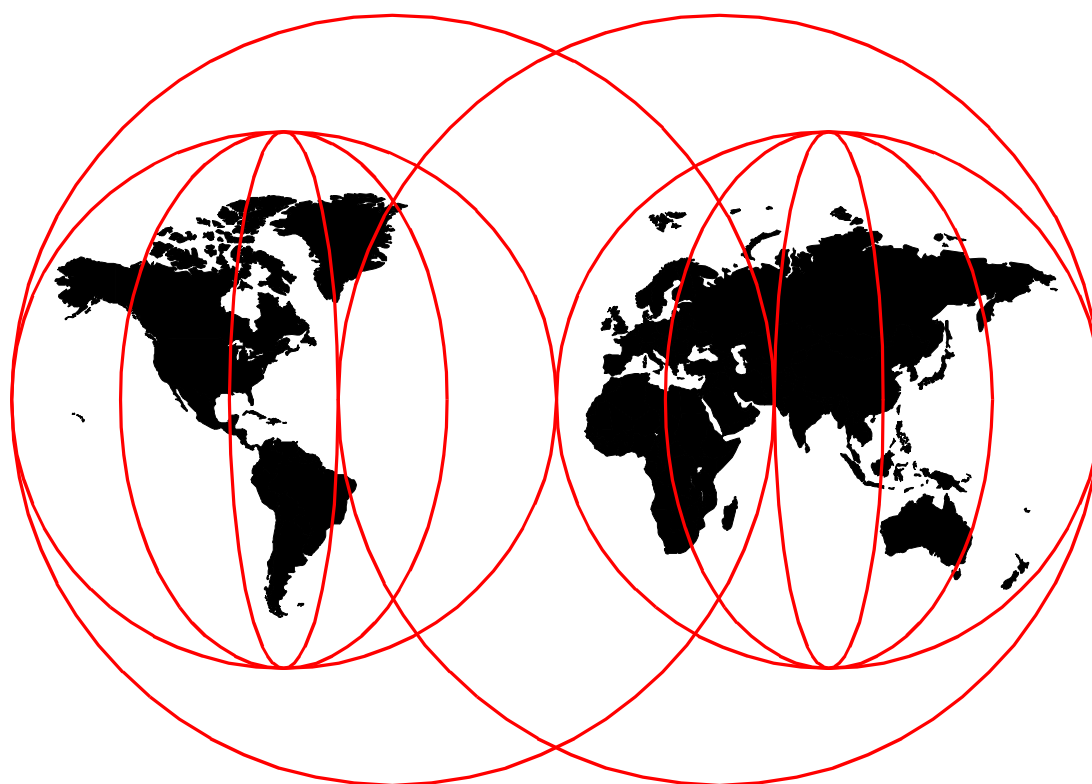


A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management

*Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho
Hyun Jeong Lee, Alexander Schmid*



International Technical Support Organization

<http://www.redbooks.ibm.com>



International Technical Support Organization

SG24-5309-00

**A Comprehensive Guide to
Virtual Private Networks, Volume III:
Cross-Platform Key and Policy Management**

November 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 639.

First Edition (November 1999)

This edition applies to the VPN components of the following IBM products:

- AIX V4.3.2 and V4.3.3
- OS/400 V4R4
- Communications Server and Security Server for OS/390 V2R8
- Nways 2210, 2212 and 2216 routers using MRS/AIS/MAS V3.3

This edition also applies to the VPN components of selected non-IBM products.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

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 | xi |
| How this redbook is organized | xi |
| The team that wrote this redbook | xii |
| Comments welcome | xiii |

Part 1. VPN overview and technology update 1

| | |
|---|----|
| Chapter 1. Virtual private network (VPN) introduction | 3 |
| 1.1 What is a VPN? A quick review | 3 |
| 1.2 VPN benefits | 4 |
| 1.3 VPN requirements | 5 |
| 1.3.1 Security considerations for VPNs | 5 |
| 1.3.2 Performance considerations | 10 |
| 1.3.3 Management considerations | 12 |
| 1.3.4 General purpose encryption | 13 |
| 1.4 A basic approach to VPN design and implementation | 14 |
| 1.5 Common VPN scenarios | 15 |
| 1.5.1 Branch office interconnections | 16 |
| 1.5.2 Business partner/supplier networks | 16 |
| 1.5.3 Remote access scenarios | 18 |
| 1.6 VPN technologies and security policies | 19 |
| 1.6.1 The need for a security policy | 20 |
| 1.6.2 Network security policy | 21 |
| 1.6.3 VPN security policy | 22 |
| Chapter 2. Layer-2 VPN Protocols | 23 |
| 2.1 Layer 2 Tunneling Protocol (L2TP) | 23 |
| 2.1.1 Overview and standards | 23 |
| 2.1.2 L2TP flows | 25 |
| 2.1.3 Compulsory and voluntary tunnel modes | 26 |
| 2.1.4 Securing the tunnels with IPsec | 28 |
| 2.1.5 Multiprotocol support | 30 |
| 2.2 Point-to-Point Tunneling Protocol (PPTP) | 30 |
| 2.3 Layer 2 Forwarding (L2F) | 31 |
| 2.4 Comparing remote access tunneling protocols | 32 |
| 2.5 Layer-2 tunneling authentication and encryption | 33 |
| 2.5.1 Authentication options | 33 |
| 2.5.2 Encryption options | 35 |
| Chapter 3. Layer-3 VPN protocols | 37 |
| 3.1 IP Security Architecture (IPsec) | 37 |
| 3.1.1 Overview and standards | 37 |
| 3.1.2 Security associations | 38 |
| 3.1.3 IP Authentication Header (AH) | 39 |
| 3.1.4 Encapsulating Security Payload (ESP) | 40 |
| 3.1.5 Tunnel and transport mode | 41 |
| 3.1.6 SA combinations | 42 |
| 3.2 Coming to terms with the Internet Key Exchange (IKE) protocol | 45 |
| 3.2.1 Overview and standards | 45 |
| 3.2.2 Key management requirements for IPsec | 46 |
| 3.2.3 IKE Phase 1 overview | 47 |

| | | |
|--|---|-----|
| 3.2.4 | IKE Phase 2 overview | 47 |
| 3.2.5 | ISAKMP message structure | 48 |
| 3.2.6 | General Phase 1 process. | 49 |
| 3.2.7 | General Phase 2 process. | 64 |
| 3.2.8 | Summary of successful IKE negotiation | 66 |
| 3.2.9 | Optional IKE exchanges | 67 |
| 3.3 | IPSec/IKE system processing | 68 |
| 3.3.1 | Outbound IPSec processing for host systems | 69 |
| 3.3.2 | Inbound processing for host systems | 69 |
| 3.3.3 | Outbound processing for gateway systems | 70 |
| 3.3.4 | Inbound processing for gateway systems. | 71 |
| Chapter 4. Certificates and Public Key Infrastructures (PKIs) | | 73 |
| 4.1 | Public key cryptography. | 73 |
| 4.2 | Digital certificates | 73 |
| 4.3 | Registration authority. | 75 |
| 4.4 | Multiple certificate authorities | 76 |
| 4.4.1 | Single root CA | 76 |
| 4.4.2 | Hierarchal topology | 78 |
| 4.4.3 | Peer topology | 80 |
| 4.5 | PKI requirements for IKE. | 83 |
| Chapter 5. Security technologies complementing VPNs | | 85 |
| 5.1 | Authentication for remote access dial-in users. | 85 |
| 5.1.1 | RADIUS operation | 86 |
| 5.1.2 | Using RADIUS with layer-2 tunnels | 88 |
| 5.2 | Network address translation (NAT) | 89 |
| 5.3 | SOCKS | 91 |
| 5.4 | Secure Sockets Layer (SSL) and Transport Layer Security (TLS) | 92 |
| 5.5 | Comparing IPSec to SSL | 94 |
| Chapter 6. Directory-assisted policy management | | 97 |
| 6.1 | The benefits of directory-assisted policy management. | 97 |
| 6.2 | Directory client and servers | 97 |
| 6.2.1 | LDAP schema | 98 |
| 6.2.2 | Directory security. | 98 |
| 6.3 | Nways router policy administration with LDAP | 98 |
| 6.3.1 | LDAP server configuration | 99 |
| 6.3.2 | LDAP client configuration on the IBM Nways 221x routers | 104 |
| 6.3.3 | Secure transmission of LDAP traffic using tunnels | 107 |
| Chapter 7. Network management for VPNs | | 109 |
| 7.1 | Systems management | 109 |
| 7.2 | Design considerations | 110 |
| 7.3 | SNMP management. | 111 |
| 7.4 | SNMP management and VPNs | 113 |
| 7.4.1 | Management objects for Internet VPN | 115 |
| 7.4.2 | Integration into other management tools | 116 |
| 7.5 | Network management objects for IBM Nways routers | 116 |

Part 2. IBM VPN platforms with IKE support 119

| | | |
|---|---|-----|
| Chapter 8. Introduction to IBM VPN solutions | | 121 |
| 8.1 | IBM VPN platforms - IPSec and IKE feature summary | 121 |

| | | |
|--------------------|---|------------|
| 8.2 | IBM VPN platforms - layer-2 tunneling feature summary | 123 |
| 8.3 | IBM VPN platforms - interoperability matrix for IKE | 124 |
| 8.4 | IBM VPN platforms supporting IPSec but not IKE | 124 |
| 8.5 | IBM VPN platforms - interoperability matrix for IPSec without IKE | 125 |
| 8.6 | IBM and OEM VPN platforms - interoperability matrix | 126 |
| | | |
| Chapter 9. | AIX V4.3.2 and V4.3.3 | 129 |
| 9.1 | AIX V4.3.2 | 129 |
| 9.1.1 | IPSec and Internet Key Exchange (IKE) VPN features | 129 |
| 9.1.2 | VPN feature installation on AIX V4.3.2 | 130 |
| 9.1.3 | AIX V4.3.2 IP Security: IKE tunnel basic setup | 131 |
| 9.1.4 | AIX V4.3.2 IP Security IKE advanced setup | 141 |
| 9.1.5 | Use tunnel lifetime and lifesize | 149 |
| 9.1.6 | Packet filtering | 150 |
| 9.1.7 | Manual tunnel setup | 152 |
| 9.2 | AIX V4.3.3 | 154 |
| 9.2.1 | VPN features and improvements in AIX V4.3.3 | 154 |
| 9.2.2 | AIX V4.3.3 VPN feature installation | 155 |
| 9.2.3 | IP Security IKE tunnel basic setup using quick configuration | 157 |
| 9.2.4 | IP Security IKE tunnel advanced setup | 160 |
| 9.2.5 | Manual tunnel configuration using WebSM | 166 |
| 9.2.6 | Filtering capability | 172 |
| 9.2.7 | IKE setup for digital certificate support | 175 |
| 9.3 | Creating a VPN host-to-host connection | 180 |
| | | |
| Chapter 10. | OS/400 V4R4 native VPN support | 189 |
| 10.1 | Overview | 189 |
| 10.2 | VPN software prerequisites | 189 |
| 10.3 | AS/400 VPN components | 190 |
| 10.3.1 | AS/400 Operations Navigator | 190 |
| 10.3.2 | New Connection Wizard | 191 |
| 10.3.3 | VPN server jobs | 191 |
| 10.3.4 | VPN policy database | 191 |
| 10.3.5 | IP packet filtering | 192 |
| 10.4 | Basic planning | 193 |
| 10.5 | VPN configuration | 199 |
| 10.5.1 | AS/400 Operations Navigator | 199 |
| 10.5.2 | Using the New Connection Wizard | 201 |
| 10.5.3 | Changing the New Connection Wizard default values | 204 |
| 10.5.4 | Objects created by the wizard | 204 |
| 10.5.5 | Configuring IP filters | 205 |
| 10.5.6 | Object relationships | 206 |
| 10.6 | VPN management | 207 |
| 10.6.1 | IP packet security | 207 |
| 10.6.2 | VPN server jobs | 209 |
| 10.6.3 | Starting VPN connections | 212 |
| 10.7 | Backup and recovery considerations | 215 |
| 10.7.1 | Creating a VPN host-to-host connection | 215 |
| 10.7.2 | Configuring IP packet security | 223 |
| 10.7.3 | Starting the VPN connection | 230 |
| 10.7.4 | Relationship between the wizard and the configuration objects | 235 |
| | | |
| Chapter 11. | Communications Server V2R8 for OS/390 | 239 |
| 11.1 | Firewall technologies for OS/390 | 239 |

| | | |
|--------------------|--|------------|
| 11.2 | Installation and customization of VPN IKE feature | 240 |
| 11.2.1 | OS/390 SecureWay CS IP services customization | 240 |
| 11.2.2 | UNIX System Services customization | 243 |
| 11.2.3 | OS/390 Security Server and cryptographic services customization | 244 |
| 11.2.4 | OS/390 Firewall USS customization and starting | 257 |
| 11.3 | Dynamic tunnel scenario | 271 |
| 11.3.1 | Creating a dynamic VPN connection using the GUI panels | 280 |
| 11.3.2 | Creating a dynamic VPN using the shell commands | 301 |
| Chapter 12. | Nways routers using MRS/AIS/MAS V3.3 | 307 |
| 12.1 | Policy engine | 307 |
| 12.2 | Configuring IPSec on an Nways router | 309 |
| 12.2.1 | Configuring manual IPSec tunnels | 312 |
| 12.2.2 | Configuring IKE with pre-shared keys | 322 |
| 12.2.3 | IKE with PKI configuration | 337 |

Part 3. VPN scenarios using IBM VPN platforms 359

| | | |
|--------------------|---|------------|
| Chapter 13. | Building branch office VPNs | 361 |
| 13.1 | Design considerations | 361 |
| 13.1.1 | Authenticating backbone traffic | 361 |
| 13.1.2 | Data confidentiality | 361 |
| 13.1.3 | Addressing issues | 362 |
| 13.1.4 | Routing issues | 363 |
| 13.1.5 | Summary: branch office connection | 364 |
| 13.2 | Central site - small enterprise | 365 |
| 13.2.1 | Considerations | 365 |
| 13.2.2 | Gateway-to-gateway tunnel with IPSec between IBM routers | 366 |
| 13.2.3 | Scenario characteristics | 366 |
| 13.2.4 | Implementation tasks - summary | 367 |
| 13.2.5 | Completing the IBM 2216 router planning worksheet | 368 |
| 13.2.6 | Configuring the VPN in the IBM 2216 routers | 372 |
| 13.2.7 | Connection verification and testing | 374 |
| 13.3 | Central site - medium enterprise | 375 |
| 13.3.1 | Considerations | 375 |
| 13.3.2 | Gateway-to-gateway tunnel with IPSec between IBM AIX systems | 376 |
| 13.3.3 | Scenario characteristics | 376 |
| 13.3.4 | Implementation tasks - summary | 378 |
| 13.3.5 | Completing the AIX planning worksheet | 378 |
| 13.3.6 | Configuring the central site gateway | 379 |
| 13.3.7 | Configuring the branch office gateway | 381 |
| 13.3.8 | Connection verification and testing | 381 |
| 13.4 | Central and regional sites - large enterprise | 381 |
| 13.4.1 | Considerations | 381 |
| 13.4.2 | IBM AS/400 to IBM 2210 gateway-to-gateway tunnel with IPSec | 383 |
| 13.4.3 | Scenario characteristics | 383 |
| 13.4.4 | Implementation tasks - summary | 384 |
| 13.4.5 | Completing the 2210 router planning worksheet | 385 |
| 13.4.6 | Completing the AS/400 system planning worksheet | 390 |
| 13.4.7 | VPN configuration cross-reference table - OS/400 to 2210 router | 393 |
| 13.4.8 | Configuring the VPN in the 2210 router | 394 |
| 13.4.9 | Configuring the VPN on the AS/400 system (RALYAS4A) | 396 |
| 13.4.10 | Configuring IP filtering on the AS/400 system (RALYAS4A) | 398 |

| | | |
|--------------------|--|------------|
| 13.4.11 | Starting IP filters | 399 |
| 13.4.12 | Starting the VPN connection | 399 |
| 13.4.13 | Verification tests | 402 |
| Chapter 14. | Building business partner/supplier VPNs | 403 |
| 14.1 | Design considerations | 403 |
| 14.1.1 | Authenticating and encrypting supplier traffic | 404 |
| 14.1.2 | Addressing issues | 406 |
| 14.1.3 | Packet filtering and proxies | 406 |
| 14.1.4 | Summary: intercompany interconnection | 407 |
| 14.2 | Nested tunnel configurations with IKE | 407 |
| 14.2.1 | IBM router configuration | 408 |
| 14.3 | End-to-end tunnels with IPSec | 417 |
| 14.3.1 | Scenario characteristics | 417 |
| 14.3.2 | Implementation tasks - summary | 418 |
| 14.3.3 | Completing the AIX server planning worksheet | 418 |
| 14.3.4 | Completing the AS/400 system planning worksheet | 420 |
| 14.3.5 | Configuring a host-to-host VPN in the AIX server | 422 |
| 14.3.6 | Configuring a host-to-host VPN in the AS/400 system | 424 |
| 14.3.7 | Matching the AIX server VPN configuration | 426 |
| 14.3.8 | Configuring IP filters on the AS/400 system (RALYAS4C) | 428 |
| 14.3.9 | Starting the VPN connection | 431 |
| 14.3.10 | Verification tests | 433 |
| Chapter 15. | Building remote access VPNs | 435 |
| 15.1 | Design considerations | 435 |
| 15.1.1 | Data Confidentiality and authentication | 436 |
| 15.1.2 | Addressing and routing issues | 436 |
| 15.1.3 | Multiprotocol support | 436 |
| 15.1.4 | Summary: remote access | 437 |
| 15.2 | Remote access with IPSec | 437 |
| 15.2.1 | Description of the scenario | 438 |
| 15.2.2 | Configuration of the ISP router | 439 |
| 15.2.3 | Configuration of the VPN Gateway (Center 2216 Router) | 442 |
| 15.2.4 | Configure IPSec action and proposal | 445 |
| 15.2.5 | Configure ISAKMP action and proposal | 447 |
| 15.2.6 | Configuration of the IRE SafeNet VPN Client | 449 |
| 15.2.7 | Testing and verifying the connection | 451 |
| 15.2.8 | Using a private IP address with the IRE SafeNet VPN client | 452 |
| 15.3 | End-to-end connections using L2TP and IPSec | 454 |
| 15.4 | Dial-on-Demand via ISP using L2TP | 454 |
| Chapter 16. | VPN Troubleshooting | 457 |
| 16.1 | Log Files | 457 |
| 16.2 | Alerting and monitoring | 457 |
| 16.3 | Traces, dumps and traffic analysis | 457 |
| 16.3.1 | Traces and dumps | 457 |
| 16.3.2 | Traffic analysis | 458 |
| 16.4 | Interfaces to systems management tools | 467 |
| 16.5 | Ethical Hacking | 467 |
| 16.6 | Troubleshooting for AIX 4.3.x | 468 |
| 16.6.1 | IP Security log file | 468 |
| 16.6.2 | ISAKMPD log file | 471 |
| 16.7 | Troubleshooting for OS/400 | 473 |

| | | |
|--------|--|-----|
| 16.7.1 | Available methods for troubleshooting virtual private networks . . . | 473 |
| 16.7.2 | General guidelines for VPN troubleshooting. | 473 |
| 16.7.3 | Using and customizing the Active Connections window | 474 |
| 16.7.4 | Using the QIPFILTER journal. | 476 |
| 16.7.5 | Using the QVPN journal. | 478 |
| 16.7.6 | The Trace TCP/IP Application (TRCTCPAPP) command | 481 |
| 16.7.7 | Using job logs for problem determination | 482 |
| 16.7.8 | Using the AS/400 communications trace | 483 |
| 16.8 | Troubleshooting for OS/390. | 483 |
| 16.8.1 | Using the firewall log to check the tunnel | 483 |
| 16.9 | Troubleshooting for IBM Nways routers | 484 |
| 16.9.1 | General | 485 |
| 16.9.2 | Order of commands while troubleshooting | 485 |
| 16.9.3 | Useful commands for Policy and IPsec | 486 |
| 16.9.4 | Useful Commands for IKE | 491 |
| 16.9.5 | Useful commands for layer-2 VPNs | 492 |
| 16.9.6 | Authentication commands and RADIUS | 496 |
| 16.9.7 | Useful commands for LDAP | 498 |
| 16.9.8 | Using ELS subsystems | 499 |
| 16.9.9 | Tracing | 499 |

Part 4. OEM VPN platforms and interoperability 501

| | |
|---|------------|
| Chapter 17. Interoperability with Cisco routers | 503 |
| 17.1 Cisco IOS VPN Capabilities | 503 |
| 17.2 Configuring Cisco IOS for IPsec and IKE | 504 |
| 17.2.1 IKE configuration using pre-shared key authentication | 504 |
| 17.2.2 IKE configuration using RSA signature authentication | 508 |
| 17.2.3 IPsec Configuration | 510 |
| 17.2.4 Connection verification. | 512 |
| 17.3 IBM 2216 to Cisco 2612, gateway-to-gateway | 513 |
| 17.3.1 Scenario characteristics. | 513 |
| 17.3.2 Implementation tasks - summary | 514 |
| 17.3.3 Completing the IBM 2216 router planning worksheet | 515 |
| 17.3.4 Configuring the VPN in the IBM 2216 router | 520 |
| 17.3.5 Completing the Cisco router planning worksheet | 522 |
| 17.3.6 Configuring the VPN in the Cisco router. | 523 |
| 17.3.7 Connection verification. | 525 |
| 17.3.8 Verification tests | 527 |
| 17.4 IBM AS/400 to Cisco 2612, gateway-to-gateway | 527 |
| 17.4.1 Scenario characteristics. | 527 |
| 17.4.2 Implementation tasks - summary | 529 |
| 17.4.3 Completing the Cisco router planning worksheet | 530 |
| 17.4.4 Completing the AS/400 system planning worksheet. | 532 |
| 17.4.5 Configuring the VPN in the Cisco router. | 534 |
| 17.4.6 Configuring the VPN on the AS/400 system (RALYAS4A) | 538 |
| 17.4.7 Matching the Cisco router VPN configuration. | 539 |
| 17.4.8 Configuring IP filtering on the AS/400 system (RALYAS4A). | 540 |
| 17.4.9 Starting IP filters | 541 |
| 17.4.10 Starting the VPN connection | 541 |
| 17.4.11 Verification tests | 543 |
| 17.5 IRE SafeNet VPN Client to Cisco 2612, IPsec over PPP dial-up | 543 |
| 17.5.1 Scenario description | 544 |

| | | |
|---|--|------------|
| 17.5.2 | Configuration of the ISP router | 545 |
| 17.5.3 | Completing the Cisco router planning worksheet. | 545 |
| 17.5.4 | Configuring the VPN in the Cisco router | 547 |
| 17.5.5 | Configuration of the IRE SafeNet VPN Client | 548 |
| 17.5.6 | Testing and verifying the connection | 548 |
| 17.6 | Using digital certificates for IKE authentication | 548 |
| 17.6.1 | Generating keys and requesting certificates | 548 |
| 17.6.2 | Creating an IKE policy for certificates | 552 |
| 17.7 | Windows 2000 to Cisco 2612 using voluntary layer-2 tunneling | 553 |
| 17.8 | IBM 2212 to Cisco 2612, L2F dial-up gateway | 554 |
| Chapter 18. Interoperability with Windows 2000 | | 557 |
| 18.1 | Windows 2000 VPN capabilities | 557 |
| 18.1.1 | Windows 2000 IPSec features. | 557 |
| 18.1.2 | Windows 2000 layer-2 tunneling features | 558 |
| 18.2 | Configuring IPSec on Windows 2000 | 559 |
| 18.2.1 | IP Security policy management | 559 |
| 18.2.2 | Configuring IPSec and IKE | 560 |
| 18.2.3 | Enable IPSec for a network connection | 573 |
| 18.2.4 | Starting IPSec connections | 575 |
| 18.2.5 | Using the IP Security Monitor | 575 |
| 18.3 | Windows 2000 to AIX 4.3.2, host-to-host. | 576 |
| 18.3.1 | Scenario characteristics | 576 |
| 18.3.2 | Implementation tasks - summary. | 577 |
| 18.3.3 | Completing the Windows 2000 server planning worksheet | 578 |
| 18.3.4 | Completing the AIX server planning worksheet | 579 |
| 18.3.5 | Configuring a host-to-host VPN in the Windows 2000 server. | 579 |
| 18.3.6 | Configuring a host-to-host VPN in the AIX server | 581 |
| 18.3.7 | Starting the VPN connection | 582 |
| 18.4 | Windows 2000 remote access using L2TP | 583 |
| 18.4.1 | Scenario characteristics | 583 |
| 18.4.2 | Configuring the ISP router. | 584 |
| 18.4.3 | Configuring the center router. | 584 |
| 18.4.4 | Configuring the Windows 2000 client. | 586 |
| 18.4.5 | Starting the VPN connection | 592 |
| 18.4.6 | Verification tests | 593 |
| 18.4.7 | Using IPSec inside an L2TP tunnel | 595 |
| Chapter 19. Interoperability with OEM VPN products | | 597 |
| 19.1 | IRE SafeNet VPN client | 597 |
| 19.1.1 | SafeNet VPN client capabilities | 597 |
| 19.1.2 | Client installation. | 598 |
| 19.1.3 | Client configuration for LAN connections. | 599 |
| 19.1.4 | Building a LAN connection | 602 |
| 19.1.5 | Client configuration for certificates | 603 |
| 19.1.6 | Configuring manual IPSec tunnels. | 608 |
| 19.2 | WinVPN client from Wind River Systems | 612 |
| 19.2.1 | WinVPN client capabilities. | 613 |
| 19.2.2 | Client installation. | 613 |
| 19.2.3 | Client configuration | 614 |
| 19.2.4 | Building the connection | 616 |
| 19.3 | Network TeleSystems TunnelBuilder. | 618 |
| 19.3.1 | NTS TunnelBuilder capabilities | 619 |

| | | |
|--------|---|------------|
| 19.3.2 | Client installation | 619 |
| 19.3.3 | Client configuration | 620 |
| 19.3.4 | Building the connection | 623 |
| 19.4 | IBM router configuration for the OEM VPN client scenarios | 625 |
| 19.4.1 | ISP router | 625 |
| 19.4.2 | Center router | 625 |
| 19.4.3 | Switching between configurations | 635 |
| 19.5 | IBM server configuration for the OEM VPN client scenarios | 635 |
| 19.6 | VPN solutions for Linux and OS/2 | 636 |
| 19.6.1 | Linux VPN implementations | 636 |
| 19.6.2 | OS/2 VPN implementations | 637 |
| | Appendix A. Special notices | 639 |
| | Appendix B. Related publications | 643 |
| B.1 | IBM Redbooks | 643 |
| B.2 | Redbooks on CD-ROMs | 643 |
| B.3 | Other publications | 644 |
| B.3.1 | IBM publications | 644 |
| B.3.2 | Internet standards and drafts | 644 |
| B.3.3 | Further reading | 645 |
| B.3.4 | Referenced Web sites | 646 |
| | How to get IBM Redbooks | 647 |
| | IBM Redbook fax order form | 648 |
| | List of abbreviations | 649 |
| | Index | 655 |
| | IBM Redbook evaluation | 669 |

Preface

The Internet nowadays is not only a popular vehicle to retrieve and exchange information in traditional ways, such as e-mail, file transfer and Web surfing. It is being used more and more by companies to replace their existing telecommunications infrastructure with virtual private networks (VPNs) by implementing secure IP tunnels across the Internet between corporate sites as well as to business partners and remote users.

This redbook closely examines the functionality of the Internet Key Exchange protocol (IKE), which is derived from the Internet Security Associations Key Management Protocol (ISAKMP) and the Oakley protocol. IKE provides a framework and key exchange protocol for virtual private networks that are based on the IP Security Architecture (IPSec) protocols. An overview of VPN technologies based on the latest standards is provided in Part I.

This redbook also helps you understand, install and configure the most current VPN product implementations from IBM, in particular AIX, OS/400, Nways routers, OS/390, and several client and OEM platforms. After reading this redbook, you will be able to use these products to implement different VPN scenarios. An overview of the functions and configuration of the VPN components of these products is provided in Part II.

The main focus of this redbook is on how to implement complete VPN solutions using state-of-the-art VPN technologies, and to document IBM product interoperability. This redbook is therefore not meant to be an exhaustive VPN design guide. The authors would like to refer the reader to IBM security and network consulting services for that purpose.

A basic understanding of IP security and cryptographic concepts and network security policies is assumed.

How this redbook is organized

This redbook is Volume III in the series on virtual private networks (VPNs).

- Volume I provides the reader with an understanding of the architecture and underlying technologies, including cryptographic concepts used in IP security. It also presents VPN scenarios based on IBM solutions using manually keyed IPSec.
- Volume II is a practical guide for use in configuring IPSec tunnels and applications of these tunnels with IBM Nways Multiprotocol Routers.
- This redbook (Volume III) illustrates interoperability scenarios based upon the full range of IBM VPN platforms that currently implement IPSec and IKE. It also includes interoperability with a variety of OEM VPN solutions.

The structure of this redbook presents itself as follows:

1. Part I discusses VPN architectures and technologies in general.
2. Part II describes the capabilities of IBM VPN solutions and illustrates their basic configuration steps based on simple scenarios.
3. Part III discusses complex VPN scenarios based on IBM products with an emphasis on cross-platform interoperability.

4. Part IV discusses VPN scenarios involving IBM and selected OEM VPN solutions.

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, Raleigh Center. The leader of this project was Martin W. Murhammer.

Martin W. Murhammer is a Senior I/T Availability Professional at the ITSO Raleigh Center. Before joining the ITSO in 1996, he was a Systems Engineer in the Systems Service Center at IBM Austria. He has 14 years of experience in the personal computing environment including areas such as heterogeneous connectivity, server design, system recovery, and Internet solutions. He is an IBM Certified OS/2 and LAN Server Engineer and a Microsoft Certified Professional for Windows NT. Martin has co-authored a number of redbooks at the ITSO Raleigh and Austin centers. His latest publications are *TCP/IP Tutorial and Technical Overview*, Sixth Edition, GG24-3376, and *IP Network Design Guide*, Second Edition, SG24-2580.

Orcun Atakan is an IT Security Specialist in Information Systems, IBM Turkey, where he has been working for four years. His areas of expertise include IP security, security implementations, Java and electronic commerce. Orcun has previously co-authored the redbook *TCP/IP Tutorial and Technical Overview*, Sixth Edition, GG24-3376.

Zikrun Badri is a Networking Systems Specialist working in IBM Australia's Networking Systems Division. His responsibilities include initial network design, migration, implementation and ongoing support of IBM's networking customers. He is one of IBM Australia's Networking Division's VPN and IP Security specialists. He has had nine years of experience with IBM, the last five with the Networking Division. He holds a degree in Computing Studies from the University of Canberra. His area of expertise includes the complete range of IBM's networking offerings, particularly IBM's campus networking offerings. He has extensive experience in ATM networks and previously co-authored the redbook *IBM 8260 As a Campus ATM Switch*, SG24-5003.

Beomjun Cho is an IT Architect in Network Services, IBM Korea. He has eight years of experience in network SI and managed network services. His areas of expertise include network and system management and system and security solution design.

Hyun Jeong Lee is an IT Specialist in Network Services, IBM Korea, where she has been working for eight years. She has six years of experience in the networking environment. She holds a Master degree in computer sciences from Yonsei University, Korea. Her areas of expertise include network analysis, design, SI, troubleshooting.

Alexander Schmid is a Senior Consultant for Information and Technology Management with IBM Unternehmensberatung GmbH (IBM UBG) in Germany. Before joining IBM UBG he did network design and sales support within IBM Global Network. He has 10 years of experience in the networking environment including network operations, systems programming, design, architecture and consulting. He holds a degree in computer sciences from the University of

Erlangen, Germany. During his studies he worked in the IBM Zurich Research Lab for several months. He is currently studying toward a degree in Master of Business Administration (MBA) at the Open University in Milton Keynes, UK.

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

Thomas Barlen, Jorge Ferrari, Erol Lengerli, Tatsuhiko Kakimoto, Tim Kearby, Michael Haley, Margaret Ticknor, Shawn Walsh, Tate Renner, Linda Robinson, Gail Christensen
International Technical Support Organization, Raleigh Center

Marcela Adan
International Technical Support Organization, Rochester Center

Stephan Imhof
IBM Switzerland

Chia Weng Wai
IBM Singapore

Giancarlo Rodolfi
IBM Brazil

Skip Booth, John Crawbuck, Bruce Dillon, Don Grosser, Christophe Henrion, Charles Kunzinger, Susanne Vergara, John Walczyk
IBM Research Triangle Park

Jackie Wilson, Shawn Mullen, Unnikrishnan Rama, Parag Salvi, Guha Prasad Venkataraman
IBM Austin

Edward Boden, Franklin Gruber, Frank Paxhia, Richard Planutis, Scott Sylvester, David Wierbowski, Mike Williams
IBM Endicott

Mark Davis
IBM Rochester

John Alling, Jim Alumbaugh, Peter Fritz, Ulrich Hamm
Cisco Systems

Bill Moore, Ed Irvine, Jim Pickering
Network TeleSystems

Titus Peedikayil
RouterWare

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 Redbook evaluation" on page 669 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 overview and technology update

Chapter 1. Virtual private network (VPN) introduction

This chapter provides an overview of the most important technologies employed to build VPNs today and emphasizes those used across the IBM product portfolio. The descriptions and explanations given in this chapter are based on the latest available standards for the discussed protocols and solutions and thus provide a valuable refresh and an update to existing VPN publications that are referenced as appropriate.

1.1 What is a VPN? A quick review

A virtual private network (VPN) is an extension of an enterprise's private intranet across a public network such as the Internet, creating a secure private connection, essentially through a private tunnel. VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network, as shown in Figure 1 on page 4.

It will help you to understand the concepts discussed in this redbook to summarize and return to the basic concepts that distinguish VPNs from other components of a networking infrastructure as well as from mere application security solutions:

It is virtual:

This means that the physical infrastructure of the network has to be transparent to any VPN connection. In most cases it also means that the physical network is not owned by the user of a VPN but is a public network shared with many other users. To facilitate the necessary transparency to the upper layers, protocol tunneling techniques are used. To overcome the implications of not owning the physical network, service level agreements with network providers should be established to provide, in the best possible way, the performance and availability requirements needed by the VPN.

It is private:

The term "private" in the VPN context refers to the privacy of the traffic that is to flow over the VPN. As mentioned before, VPN traffic often flows over public networks (hence the confusion with the word "private") and therefore, precautions must be met to provide the necessary security that is required for any particular traffic profile that is to flow over a VPN connection. Those security requirements include:

- Data encryption
- Data origin authentication
- Secure generation and timely refresh of cryptographic keys needed for encryption and authentication
- Protection against replay of packets and address spoofing

It is a network:

Even though not physically existent, a VPN must effectively be perceived and treated as an extension to a company's network infrastructure. This means that it must be made available to the rest of the network, to all or a specified

subset of its devices and applications, by regular means of topology such as routing and addressing.

Having said all that, "secure tunneled connections" may be a more appropriate term to describe what a VPN technically is, but the term VPN has prevailed.

1.2 VPN benefits

With the explosive growth of the Internet, companies are beginning to ask: "How can we best exploit the Internet for our business?" Initially, companies were using the Internet to promote their image, products, and services by providing World Wide Web (WWW) access to corporate Web sites. Today, however, the Internet potential is limitless, and the focus has shifted to e-business, using the global reach of the Internet for easy access to key business applications and data that reside in traditional I/T systems. Companies are looking for the best solution to securely and cost-effectively extend the reach of their applications and data across the world. While Web-enabled applications can be used to achieve this, a virtual private network offers more comprehensive and secure solutions.

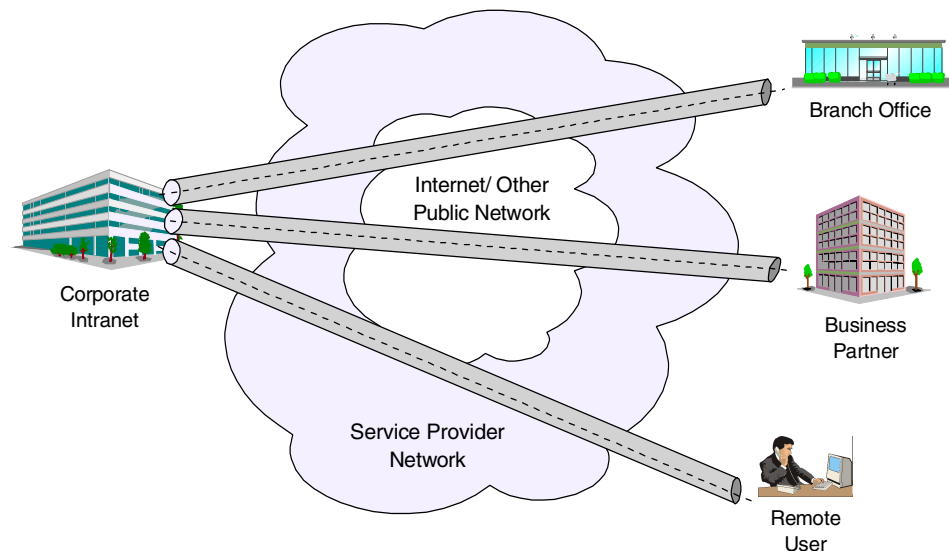


Figure 1. Virtual private network (VPN)

VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network, as shown in Figure 1. Internet service providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive, leased lines, long-distance calls, and toll-free telephone numbers.

A 1997 VPN Research Report, by Infonetics Research, Inc., estimates savings from 20% to 47% of wide area network (WAN) costs by replacing leased lines to remote sites with VPNs. And, for remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs. Additionally, Internet access is available worldwide where other connectivity alternatives may not be available.

Although the technology to implement these virtual private networks is just becoming standardized, not all the products in the market support all VPN methods. While some VPN methods can be used in conjunction with each other, some are alternative solutions to each other. A proper VPN solution should be determined according to your needs by taking the following issues into consideration:

- Business need
- Security
- Performance
- Interoperability of the solution with your current systems

The key to maximizing the value of a VPN is the ability for companies to evolve their VPNs as their business needs change and to easily upgrade to future technology. Vendors who support a broad range of hardware and software VPN products provide the flexibility to meet these requirements. IPSec-based VPN solutions today run mainly in the IPv4 environment, but it is important that they have the capability of being upgraded to IPv6 to remain interoperable with your business partner's and/or supplier's VPN solutions. Perhaps equally critical is the ability to work with a vendor who understands the issues of deploying a VPN. The implementation of a successful VPN involves more than technology. The vendor's networking experience plays heavily into this equation.

1.3 VPN requirements

Before implementing virtual private networks, you should not only be aware of the potential benefits of such a solution but also of potential exposures and how you can successfully thwart them. In this section we deal with problems that are commonly attributed to VPNs. We explain those considerations and what can be done to prevent them from jeopardizing a VPN solution.

Most of the time, security is seen as the biggest problem with VPNs, but we think that with today's advanced cryptographic features and with careful planning and comprehensive security policies, this is the easiest problem to overcome when implementing VPNs. We will therefore discuss this topic first.

1.3.1 Security considerations for VPNs

The use of VPNs raises several security concerns beyond those that were present in traditional corporate networks. A typical end-to-end data path might contain:

- Several machines not under control of the corporation (for example, the ISP access box in a dial-in segment and the routers within the Internet).
- A security gateway (firewall or router) that is located at the boundary between an internal segment and an external segment.
- An internal segment (intranet) that contains hosts and routers. Some could be malicious, and some will carry a mix of intracompany and intercompany traffic.
- An external segment (Internet) that carries traffic not only from your company's network but also from other sources.

In this heterogeneous environment, there are many opportunities to eavesdrop, to change a datagram's contents, to mount denial-of-service attacks, or to alter a datagram's destination address, as outlined in the following sections. The IBM solutions provide the tools to counter these threats.

Let us have a look at a typical end-to-end path next so that we will be able to understand the security considerations raised with common scenarios.

1.3.1.1 A typical end-to-end path

To understand the issues with VPN end-to-end security, we look at the elements along an end-to-end path. While not all the elements may appear in a given path, some of them will appear in every VPN configuration. End-to-end traffic will usually flow over a mix of three basic segments: a dial-in segment, an external segment (Internet), and an internal segment (intranet).

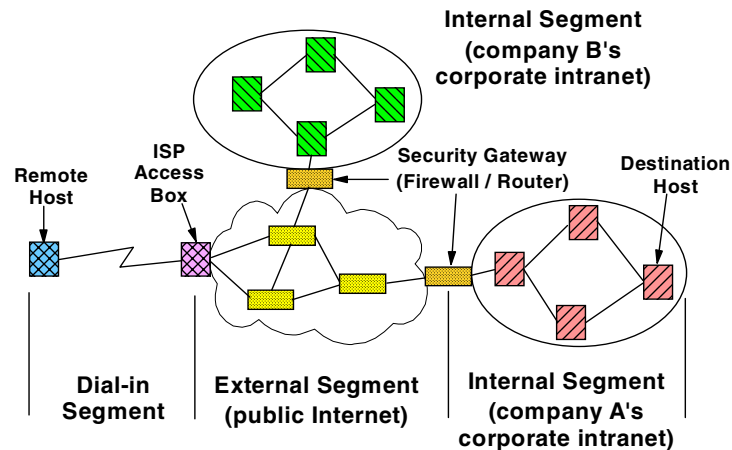


Figure 2. Typical elements in an end-to-end path

As shown in Figure 2, a path might include a first-hop dial-in connection to an Internet service provider (ISP), who in turn uses the backbone public Internet to carry the user's traffic back to a gateway at the perimeter of the corporate network. Then, the traffic eventually flows within an intranet to its ultimate destination. As we also see in Figure 2, intercompany communication can create a path that includes two separate intranets (for example, company A's and company B's).

For discussion purposes in this redbook, we refer to these elements as outlined below:

- **Dial-in segment:** In today's environment, remote access has become a necessity. Both work-at-home and on-the-road employees want convenient and secure dial-in access to their company's networks; and sometimes they even need to communicate with hosts located inside another company's network. We refer to both work-at-home and on-the-road users as *remote users*. This segment extends from a remote user's machine to an access box provided by the ISP. The protocols and procedures used on this link are specified by the Internet service provider. Today, most ISPs support the Point-to-Point Protocol (PPP) suite of protocols on this segment.
- **External network (Internet):** The Internet is not owned or operated by any single entity but is a collection of distinct routing domains, each operated by a different authority. The unifying factor is the standardized IP communications protocols defined by the Internet Engineering Task Force (IETF). The Internet Protocol (IP) suite of protocols will route data traffic at the network layer over a path that may span several ISPs' routing domains. Since IP is a

connectionless technology, each user datagram could potentially follow a different path. And in fact, traffic from several different companies could all flow simultaneously through a given backbone router in the Internet. For example, a datagram that originated in company A's intranet and a datagram that originated in company B's intranet could both flow through a common router located somewhere in the Internet. A company's traffic on the Internet can no longer be considered to be isolated from the outside world, as it would have been on a dedicated private network, since flows from different VPNs will be intermixed on the Internet backbone.

- **Internal network (intranet):** This segment appears at an endpoint of the communications path. It is under the control of the corporation, which typically operates and manages it. Traditionally, almost all traffic flowing within a corporate network was generated by the corporation's employees; very little traffic entered or exited the corporate network; and the protocols in the intranet were proprietary.

Today, IP is becoming a popular protocol for use within corporate intranets, and data traffic enters and exits the corporate intranet regularly (consider Web browsers, FTP, or Telnet applications). In today's world of e-business, there are emerging requirements for external suppliers and business partners to have access to data stored on another company's internal servers. Since traffic flowing within an intranet at any given time may have been generated by several different companies, today it may no longer be possible to categorize a given intranet as *trusted* or *untrusted*. A company may consider its own intranets to be trusted, but at the same time its business partners may consider it to be untrusted. In this environment, a VPN designer may need to provide network security functions both on the intranet segments and on the Internet segment.

As shown in Figure 2, there are four classes of machines that occur along the path:

- Remote hosts (dial-up)
- Fixed hosts (sources and destinations, or clients and servers)
- ISP access box
- Security gateways (firewalls and/or routers)

Protocols in these machines are used to provide address assignment, tunneling, and IP security. Viable security solutions can be constructed by deploying IP security in some combination of remote hosts, firewalls, routers, and fixed hosts. But since each company should be responsible for its own security, there is no requirement for the ISP boxes or the routers in the Internet backbone to support IP security.

1.3.1.2 Exposures in a dial-in client

The dial-in client is where the communication starts so protection is on the physical access to the dial-in client. The client has to protect his or her PC/notebook when left unattended. A simple measure such as password protection, even when he or she leaves for a short duration, should be enforced. Locking up the physical PC and/or room must also be considered.

1.3.1.3 Exposures in a dial-in segment

The dial-in segment in Figure 2 delivers a user's data traffic directly to an Internet service provider (ISP). If the data is in cleartext (that is, not encrypted), then it is

very easy for the ISP to examine sensitive user data, or for an attacker to eavesdrop on the data as it travels over the dial-in link.

Link-layer encryption between the remote host and the ISP can protect against passive eavesdropping, but it does not protect against a malicious ISP. Since the ISP can decrypt the user's data stream, sensitive data is still available to the ISP in cleartext format.

1.3.1.4 Exposures in the Internet

In some remote-access scenarios, an ISP builds a tunnel to extend the reach of the PPP connection so that its endpoints will be the access box and the security gateway. If the tunneling protocol does not incorporate robust security features, a malicious ISP could easily build a tunnel that terminates somewhere other than at the correct security gateway (see Figure 3). Thus, a user's data could be delivered via a false tunnel to a malicious impostor gateway where it could be examined or even altered.

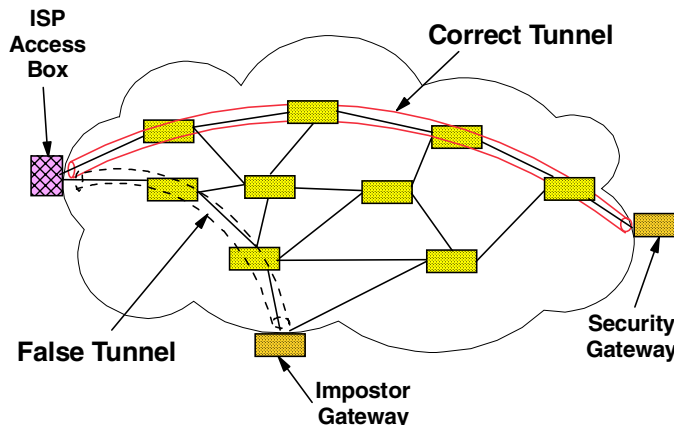


Figure 3. Exposures in the external (Internet) segment

There are also dangers as the datagram travels within the tunnel. As illustrated in Figure 3, user datagrams pass through routers in the Internet as they travel along a path toward the tunnel endpoint. If the datagrams are in cleartext, any of these routers could easily examine or modify the datagram, and passive attackers could eavesdrop on any of the links along the path.

Link-by-link encryption at each hop in the Internet backbone can thwart eavesdroppers but does not protect the user's data from a malicious router, since each router along the path would be capable of decrypting the user's data stream. Nor does link-by-link encryption protect against false tunnels, since the false tunnel endpoint would have access to cleartext data.

Even popular tunneling protocols such as Layer 2 Tunneling Protocol (L2TP) do not provide robust security. Therefore, the IETF has recommended that the tunnel traffic should be protected with the IPSec protocols.

1.3.1.5 Exposures in a security gateway

The security gateway (firewall/router) shown in Figure 2 also creates security exposures. Its main purpose is to enforce an access control policy (that is, to accept only the desired inbound traffic, to reject undesired inbound traffic, and to

prevent internally generated traffic from indiscriminately leaving the corporate network). The firewall or router is under the control of the corporate network, but an internal attacker still has an opportunity to examine any traffic that the gateway decrypts and then forwards into the intranet in cleartext form.

Noncryptographic authentication provides some protection against unwanted traffic entering or leaving the network. Common techniques are passwords, packet filtering, and network address translation. However, these can be defeated by a variety of well-known attacks, such as address spoofing, and new attacks are being developed regularly. Each time a new packet filter is designed to thwart a known attack, hackers will devise a new attack, which in turn demands that a new filter rule be generated.

Because the cryptography-based authentication techniques require a long time to break, even with powerful computers, it becomes prohibitively expensive, both in time and in computer power, for a hacker to attempt to attack them. Hence, companies can deploy them with the confidence that they will provide robust protection against a hacker's attacks.

Link-by-link encryption does not prevent an intermediate box along the path from monitoring, altering, or rerouting valid traffic, since each intermediate box will have access to the cleartext form of all messages. Even host-to-gateway encryption suffers from the same weakness; the gateway still has access to cleartext.

1.3.1.6 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 VPN connections traverse firewalls or routers that perform IP packet filtering as in Figure 4, the firewall or router configurations must be changed to allow VPN traffic across the firewalls or routers.

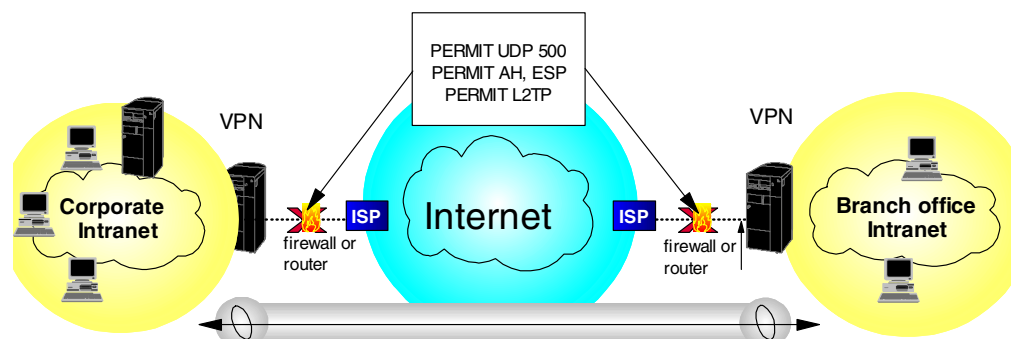


Figure 4. Allowing VPN traffic through firewalls

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

- Enable IP forwarding
- Permit UDP port 500 for IKE
- Permit IP protocols 50 and 51 for ESP and AH
- Permit UDP port 1701 for L2TP and L2F
- Permit IP protocol 47 (GRE) and TCP port 1723 for PPTP

Note

To be effective, the firewall or router filter rules need to support filtering of the relatively new VPN protocols.

1.3.1.7 Exposures in an intranet

Although there is a popular belief that most security threats will occur in the public Internet, there have been studies showing that many of the attacks actually arise internally. Unless every host, gateway, and router within the intranet of Figure 2 can be fully trusted, it is possible for a malicious employee to modify an internal box, making it possible to monitor, alter, or reroute datagrams that flow within the corporate network. When data from several different networks flows within the intranet (for example, in the case where the VPN interconnects a manufacturer's intranet with the intranets of several suppliers) threats within the intranet need to be guarded against. Even if company A trusts that its own intranet is secure, the external supplier or business partner whose traffic must flow through company A's intranet may not trust it; after all, the partner's data is at risk if company A's intranet is in fact compromised in any fashion.

1.3.1.8 Conclusions

There are security exposures everywhere along an end-to-end path: on the dial-up link, in an ISP's access box, in the Internet, in the firewall or router, and even in the corporate intranet.

Previously, security solutions were developed to address just a subset of the exposures discussed in this section, but there was no framework that could protect against all these exposures using a single approach.

IP Security Architecture (IPSec) is the first definition of a comprehensive, consistent solution. It can provide end-to-end protection as well as segment-by-segment protection. Based on the work of the Internet Engineering Task Force (IETF) IBM chose to use IPSec for its VPN solutions.

In addition to IPSec, technologies such as layer-2 tunneling and remote access authentication servers provide the necessary flexibility to apply adequate security to any given VPN scenario.

1.3.2 Performance considerations

Next to security, performance is among the most critical requirements for virtual private networks. Again the problem lies in the task of finding a way to map a service guarantee from a private network to a virtual connection running over a public network.

1.3.2.1 Quality of Service (QoS)

In a virtual private network, just as in a conventional network, there will be a desire to provide distinct transport characteristics (quality of service) for packets as they travel from source to destination. The IP protocol provides Type of Service (TOS) bits that can be used for this purpose. The details of how to use these bits is a work in progress in the IETF Differentiated Services working group, but so far no firm standard solutions exist today.

As opposed to Integrated Services such as RSVP which guarantee a quality of service for an entire path, differentiated services provide a class of service within domains where it is guaranteed that a certain TOS bit pattern will always be mapped to a certain level of service. Between DS domains - typically across the corporate-ISP boundary and between ISPs, service level agreements (SLAs) have to be in place to map TOS bits from one DS domain to another to guarantee the same level of service.

The problem with QoS is how to determine if it is required or if it is really provided when promised. Unless there are network congestions it is hardly possible to prove that specific QoS guarantees are in place. And unless you have time-critical applications you may not even experience congestions if only you provide enough bandwidth. Until QoS standards and adherent technologies are in place, ISPs and carriers in some parts of the world tend to pursue the bandwidth option rather than finding elaborate ways to guarantee service levels. Whether this is enough for the type of VPN you have in mind - and the bandwidth and response time requirements of the applications that ultimately drive this network - is only for you to find out by putting VPNs to the test.

However, looking forward to future requirements, the IPsec's AH protocol treats the TOS bits as mutable, thus allowing them to be changed as needed while an IPsec-protected datagram travels through the Internet. Thus, IPsec is already positioned to take advantage of the emerging QoS work as soon as it matures.

1.3.2.2 The toll of encryption processing

One of the key issues with respect to performance will be the encryption factor. For example, if triple DES is employed, then the resources required to cipher and decipher will be significant. One solution is to use a hardware-based encryption card or adapter to off-load the VPN gateway. The performance of this hardware, however, is also limited. A reasonably good encryption hardware can drive up to 25 Mbps, which is a lot of 64 kbps lines.

For determining the impact of encryption processing overhead you should distinguish the following types of systems that are incurring such overhead:

- End systems, typically VPN clients and servers with occasional VPN access, will most likely not notice much performance toll by using encryption because they only run one or up to a couple of concurrent connections.
- Servers with permanent VPN access will notice some encryption overhead run to a degree where it is advisable to separate the server from the encryption device. Where this point is reached needs to be determined per platform and cannot be generalized or measured in the number of concurrent tunnels or amount of traffic over time.
- VPN gateways will certainly absorb most of the encryption processing in almost any VPN scenario. Therefore, adding special encryption hardware or using dedicated VPN devices should be considered as an alternative before your firewall is breaking down or your router is no longer routing because it is bogged down by performing VPN operations.

1.3.2.3 The toll of logging

In a similar way, the logging of messages and events that relate to VPN traffic is likely to cause a performance impact. This impact will again be different on clients, servers and gateways. The problem to solve in this case is quite delicate:

1. If you abandon logging altogether, you risk compromising the security of your network because you will be unable to detect intrusion attempts and other attacks. A good security policy always includes a certain amount of logging.
2. If you log excessively you will lose a significant amount of processing power which will cause traffic delays and potential buffer or log space overflows. This may render your VPN systems inoperable and your whole VPN solution impractical.

It is good practice to set up a testbed for the systems that you want to deploy later to build your VPN environment. During a test phase, determine what can be logged by any of those systems, how much performance is lost due to logging and what the logs can actually tell you. That will provide you with a fair understanding of which events are significant to log permanently and which events should only be logged in case there are specific problems.

VPN gateways of several leading vendors also have the capability to log to a dedicated log server in order to avoid local resource overruns. That way you can collect and evaluate logging information in a central location which makes intrusion detection and trend determination much easier.

1.3.2.4 Conclusions

Some performance issues, such as encryption, are easier to tackle than others, such as quality of service. Standards are maturing toward providing the latter across public networks, but at the moment you are left to try a VPN to find out if your application requirements can be met, either in full or partially, or not at all. Encryption overhead can be easily absorbed by modern hardware encryption and dedicated VPN devices up to multiple T1 speeds, which should be adequate for most VPN scenarios.

1.3.3 Management considerations

With a private network, management used to be a piece of cake if done properly but could be a nightmare if you had no clue what you were doing. With VPNs, the bandwidth of error is much narrower because there is not enough technology available today to provide comprehensive VPN management. This sounds like bad news, but in fact it is good news because it shows that the topic of VPN management is not a rushed one. Customers are unlikely to implement large VPNs in great numbers overnight. That is why vendors first provided the tools to build VPNs rather than to manage them. Once customers have had hands-on experience with VPNs, total management solutions will be in place as both standards and products.

For the time being, vendors of VPN technology provide you with limited features to manage some VPN functions within their particular VPN device, while network management vendors are still thinking of how VPNs can be included in their respective management suites. Expect a broader portfolio for the coming six to twelve months as the VPN market is spinning very fast.

What you can do today with IBM VPN products is explained in more detail in Chapter 7, "Network management for VPNs" on page 109.

1.3.4 General purpose encryption

Encryption is an efficient way to make data unreadable to unintended recipients. If handled properly, it is a very effective way to provide security. However, if handled poorly, encryption can be a threat to your data rather than a protection. Remember that encryption requires keys to transform cleartext into ciphertext and vice versa. If those keys get lost or stolen, for instance by a system administrator who leaves the company without handing in encryption keys previously in his or her custody, your data is compromised and, what is worse, you may not be able to access it anymore (but your competitors might).

Therefore, as part of your security policy, you should clearly define if encryption is at all necessary, and if so, for what types of data, at what points in the network, and who should be authorized to use it.

There are generally two ways to protect against the loss or theft of encryption keys:

Key escrow

This technique provides for the storage and retrieval of keys and data in case keys get lost or stolen. Keys are stored with a trusted third party (recovery agent or key guardian), as a whole or in parts, on independent storage media, to be retrieved as required. The trusted third party could be a company key administrator located on company premises, or an external agency. This ensures that the keys remain in a company's possession even after a system administrator or whoever used the keys leaves the company.

Key recovery

This technique was designed to allow law enforcement agencies (LEAs) to recover the keys for decrypting secret messages of suspicious parties. Of course, you can also use this approach to recover your own keys yourself, but it is a rather complicated process and less practical than key escrow.

One way of implementing key recovery is by inserting key recovery blocks in the data stream at random intervals and/or when the keys change. Those key recovery blocks are encrypted with the public key of a trusted third party (key recovery agent). The key recovery agents can decrypt keys with their private keys, then encrypt retrieved keys with the public key of an LEA and send them to the LEA. LEAs can decrypt keys with their private keys and then decrypt the previously retrieved ciphertext messages.

1.3.4.1 Export/import regulations

Whenever you choose to use encryption you have to make sure what level of encryption is legally allowed to be used in your country and for the nature of your business. Usually, banks can employ higher levels of encryptions than home office users, and some countries are more restrictive than others. In the United States encryption is regulated by the Department of Commerce.

1.3.4.2 Dangers of end-to-end encryption

When end-to-end encryption is allowed, this opens up the firewalls to an untrusted zone. When implemented, the end-to-end encrypted traffic will not be seen even by the customer who implemented this except for the designated server/client. This also means once the intruder gets access to one end, the intruder can gain access all the way to the corporate intranet. Denial-of-service

support on the VPN gateway or firewall will also be of no use then, and therefore the intruder can disrupt an important server/service.

1.4 A basic approach to VPN design and implementation

We mentioned in the preface that this redbook is not meant to be a VPN design guide so we will limit ourselves to a few words on the general process of VPN design and implementation. This will help you to put the remainder of this redbook in proper perspective.

What VPN scenarios are to be implemented?

To get started on VPNs, it helps to know which environment you want to implement:

- Branch office (intranet) VPN
- Business partner/supplier (extranet) VPN
- Remote access VPN
- Multiple combinations

Later in this chapter (see 1.5, “Common VPN scenarios” on page 15), we introduce you briefly to the characteristics of this redbook, and in Part 3, “VPN scenarios using IBM VPN platforms” on page 359 and in Part 4, “OEM VPN platforms and interoperability” on page 501, we demonstrate how you can implement each of those scenarios using IBM VPN solutions and complementing solutions from other vendors.

What is your application mix?

We mentioned that applications ultimately drive any network, hence they do the same for VPNs. You have to evaluate the benefits of a VPN solution in light of the requirements of the applications and application infrastructure that you want to support and/or provide over a VPN. Things you should consider include:

- Are your applications based on a 2-tier or a 3-tier model?
- Are your applications Web-enabled? If yes, what is the motivation for VPNs?
- Does the network need to provide end-to-end services?
- Are applications time-critical or bandwidth-intensive?
- Are security features such as authentication and encryption provided by applications or is the network expected to take care of that? This leads to a choice between specific or generic security technologies.

What are the required levels of protection?

This leads to the implementation of a security policy that covers all of the following:

- Authentication
- Encryption
- Key exchange and key refresh intervals
- Perfect forward secrecy (PFS) and replay protection
- End-to-end protection
- Performance
- Event logging
- Legal issues

What is the projected growth of the VPN topology to be deployed?

Scalability is often an important criterion for a network. With a VPN this includes issues such as the following:

- Dynamic (IKE) versus manual tunnels
- Pre-shared keys versus certificates
- Public key infrastructure (PKI)
- Geographical span
- Cost of implementation, migration and ownership

What is the VPN infrastructure going to look like and who will support it?

This includes topics such as the following:

- ISP bandwidth, geographical presence and access plans
- VPN technology support by ISPs (Layer-2 tunneling, IPSec, PKI, LDAP)
- Network transition
- VPN gateway placement
- Quality of Service (QoS) and service level agreements (SLAs)
- Public key infrastructure (PKI)
- Cost of implementation and service

How will the VPN be managed?

This includes, among others, the following issues:

- Policies and configuration definition and delivery
- Directory infrastructure (for example, LDAP)
- Public key infrastructure (PKI)
- Monitoring, alerting and logging
- Authentication and accounting (for example, RADIUS)
- Virtual-to-physical network mappings
- Routing and backup paths
- Load balancing of traffic and devices
- Virus and content screening and intrusion detection
- Cost of implementation, migration, ownership and service

Which products are you finally going to settle on?

Best-of-breed or one-size-fits-all or single vendor? What is the cost factor and is it the ultimate decision criterion?

How will roll-out and maintenance be conducted?

In-house by your I/S department or outsourced using a service contractor or ISP? Again, what about the cost factor?

As you can see, making all these decisions is not easy and takes time and there is no guarantee that you will do everything right. This redbook helps you during several of the steps mentioned above. It describes VPN scenarios, technologies and products and it illustrates how you can use those products to implement VPNs.

1.5 Common VPN scenarios

In this section we look at the three most likely business scenarios well suited to the implementation of a VPN solution:

- Branch office connection network
- Business partner/supplier network

- Remote access network

1.5.1 Branch office interconnections

The branch office scenario securely connects two trusted intranets within your organization. Your security focus is on both protecting your company's intranet against external intruders and securing your company's data while it flows over the public Internet. For example, suppose corporate headquarters wants to minimize the costs incurred from communicating to and among its own branches. Today, the company may use frame relay and/or leased lines but wants to explore other options for transmitting its internal confidential data that will be less expensive, more secure, and globally accessible. By exploiting the Internet, branch office connection VPNs can be easily established to meet the company's needs.

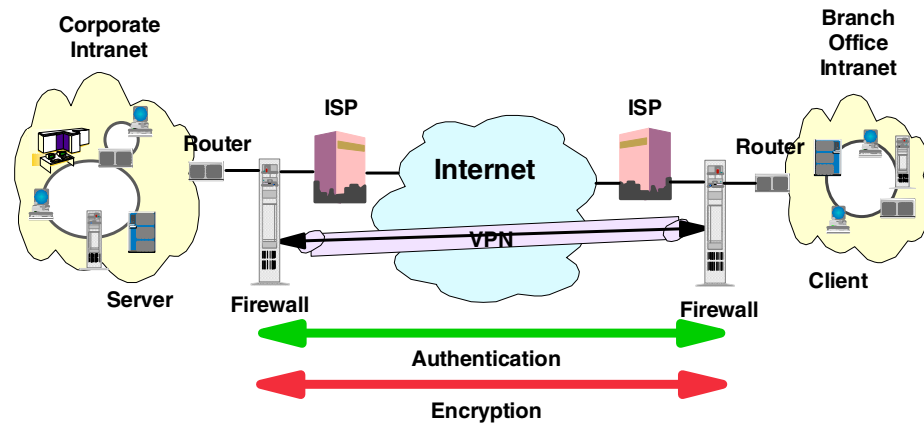


Figure 5. Branch office VPN

As shown in Figure 5, one way to implement this VPN connection between the corporate headquarters and one of its branch offices is for the company to purchase Internet access from an ISP. Firewalls, or routers with integrated firewall functionality, or in some cases a server with IPSec capability, would be placed at the boundary of each of the intranets to protect the corporate traffic from Internet hackers. With this scenario, the clients and servers need not support IPSec technology, since the IPSec-enabled firewalls (or routers) would be providing the necessary data packet authentication and encryption. With this approach, any confidential information would be hidden from untrusted Internet users, with the firewall denying access to potential attackers.

With the establishment of branch office connection VPNs, the company's corporate headquarters will be able to communicate securely and cost effectively to its branches, whether located locally or far away. Through VPN technology, each branch can also extend the reach of its existing intranet to incorporate the other branch intranets, building an extended, enterprise-wide corporate network. And this company can easily expand this newly created environment to include its business partners, suppliers, and remote users, through the use of open IPSec technology.

1.5.2 Business partner/supplier networks

Industry-leading companies will be those that can communicate inexpensively and securely to their business partners, subsidiaries, and vendors. Many

companies have chosen to implement frame relay and/or purchase leased lines to achieve this interaction. But this is often expensive, and geographic reach may be limited. VPN technology offers an alternative for companies to build a private and cost-effective extended corporate network with worldwide coverage, exploiting the Internet or other public network.

Suppose you are a major parts supplier to a manufacturer. Since it is critical that you have the specific parts and quantities at the exact time required by the manufacturing firm, you always need to be aware of the manufacturer's inventory status and production schedules. Perhaps you are handling this interaction manually today, and have found it to be time consuming, expensive and maybe even inaccurate. You would like to find an easier, faster, and more effective way of communicating. However, given the confidentiality and time-sensitive nature of this information, the manufacturer does not want to publish this data on its corporate Web page or distribute this information monthly using an external report.

To solve these problems, the parts supplier and manufacturer can implement a VPN, as shown in Figure 6 on page 17. A VPN can be built between a client workstation, in the parts supplier's intranet, directly to the server residing in the manufacturer's intranet. The clients can authenticate themselves either to the firewall or router protecting the manufacturer's intranet, directly to the manufacturer's server (validating that they are who they say they are), or to both, depending on your security policy. Then a tunnel could be established, encrypting all data packets from the client, through the Internet, to the required server.

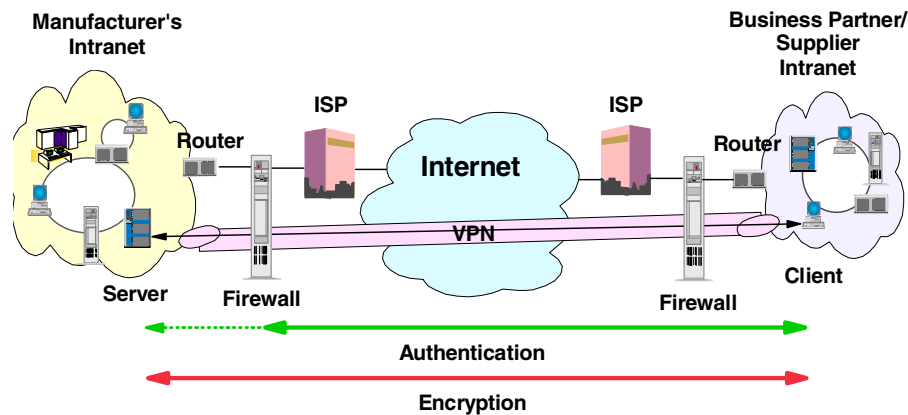


Figure 6. Extranet VPN

Optionally, the tunnels into the intranet could be terminated at a special VPN gateway in a DMZ. This would allow additional security checks, such as virus protection and content inspection, to be performed before data from an external system was allowed into the corporate network.

With the establishment of this VPN, the parts supplier can have global, online access to the manufacturer's inventory plans and production schedule at all times during the day or night, minimizing manual errors and eliminating the need for additional resources for this communication. In addition, the manufacturer can be assured that the data is securely and readily available to only the intended parts supplier(s).

One way to implement this scenario is for the companies to purchase Internet access from an Internet service provider (ISP), then, given the lack of security of the Internet, either a firewall or IPSec-enabled router, or a server with IPSec capability can be deployed as required to protect the intranets from intruders. If end-to-end protection is desired, then both the client and server machines need to be IPSec-enabled as well.

Through the implementation of this VPN technology, the manufacturer would be able to easily extend the reach of its existing corporate intranet to include one or more parts suppliers (essentially building an extended corporate network) while enjoying the cost-effective benefits of using the Internet as its backbone. And, with the flexibility of open IPSec technology, the ability for this manufacturer to incorporate more external suppliers is limitless.

1.5.3 Remote access scenarios

A remote user, whether at home or on the road, wants to be able to communicate securely and cost effectively back to his or her corporate intranet. Although many still use expensive long-distance and toll-free telephone numbers, this cost can be greatly minimized by exploiting the Internet. For example, you are at home or on the road but need a confidential file on a server within your intranet. By obtaining Internet access in the form of a dial-in connection to an ISP, you can communicate with the server in your intranet and access the required file.

One way to implement this scenario is to use a remote access tunneling protocol such as L2TP, PPTP or L2F. Another way is to use an IPSec-enabled remote client and a firewall, as shown in Figure 7. Ideally, you may wish to combine both solutions, which will provide the best protection and the most cost-effective way of remote access. The client accesses the Internet via dial-up to an ISP, and then establishes an authenticated and encrypted tunnel between itself and the firewall at the intranet boundary.

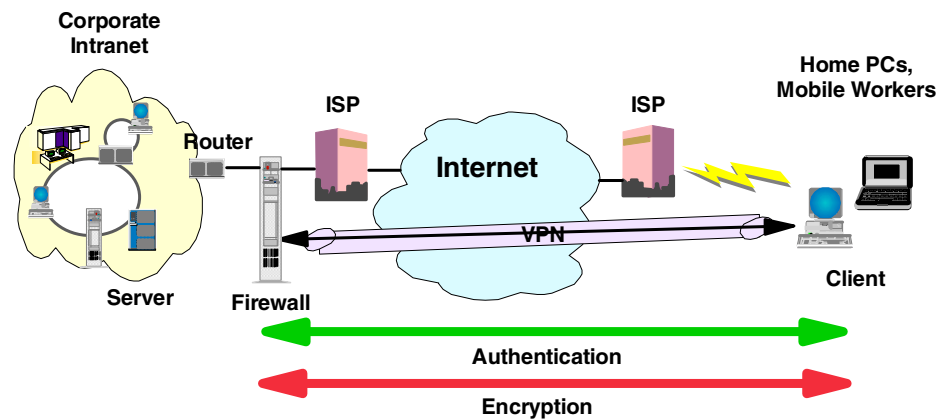


Figure 7. Remote access VPN

By applying IPSec authentication between the remote client and the firewall, you can protect your intranet from unwanted and possibly malicious IP packets. And by encrypting traffic that flows between the remote host and the firewall, you can prevent outsiders from eavesdropping on your information.

1.6 VPN technologies and security policies

The following protocols and systems are commonly used to provide various degrees of security services in a computer network. Some of them are described in more detail in later chapters in this redbook. This section provides an overview of what security technologies are available today and commonly used, which creates confidence, and which ones may be suitable for VPNs.

- IP packet filtering
- Network Address Translation (NAT)
- IP Security Architecture (IPSec)
- SOCKS
- Secure Sockets Layer (SSL)
- Application proxies
- Firewalls
- Kerberos, RADIUS, and other authentication systems
- Antivirus, content inspection and intrusion detection systems

Figure 8 on page 19 illustrates where those security solutions fit within the TCP/IP layers:

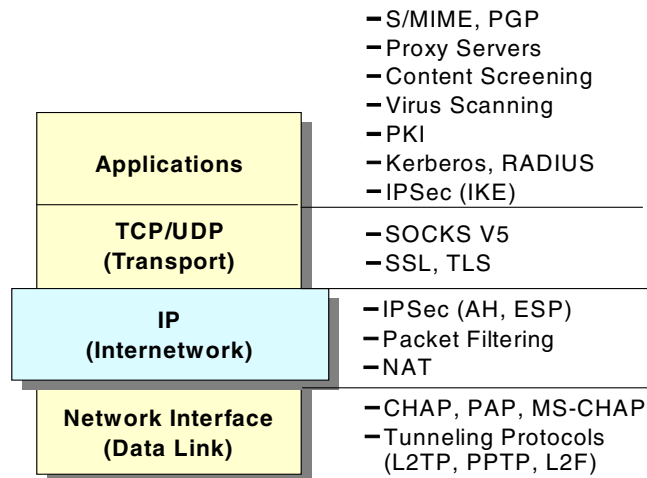


Figure 8. Security solutions in the TCP/IP layers

Figure 9 on page 20 summarizes the characteristics of some of the security solutions mentioned earlier and compares them to each other in light of specific VPN requirements. This should help anyone who needs to devise a security strategy to determine what combination of solutions will achieve a desired level of protection.

| <i>Solution</i> | <i>Access Control</i> | <i>Encryption</i> | <i>Authenti- cation</i> | <i>Integrity Checking</i> | <i>Key Exchange</i> | <i>Concealing Internal Addresses</i> | <i>Replay Protection</i> | <i>Session Monitoring</i> | <i>UDP Support</i> |
|------------------------------|-----------------------|-------------------|-----------------------------|-------------------------------|-------------------------|--|------------------------------|-------------------------------|------------------------|
| IP Filtering | Y | N | N | N | N | N | N | N | Y |
| NAT | Y | N | N | N | N | Y | N | Y (connection) | Y |
| L2TP | Y (connection) | Y (PPP link) | Y (call) | N | N | Y | N | Y (call) | Y |
| IPSec | Y | Y (packet) | Y (packet) | Y (packet) | Y | Y | Y | N | Y |
| SOCKS | Y | optional | Y (client/user) | N | N | Y | N | Y (connection) | Y |
| SSL | Y | Y (data) | Y (system/ user) | Y | Y | N | Y | Y | N |
| Application Proxy | Y | normally no | Y (user) | Y | normally no | Y | normally no | Y (connection & data) | normally no |
| AAA Server | Y (connection) | some | Y (user) | N | normally no | N | N | N | Y |

Figure 9. Characteristics of IP security technologies

As mentioned earlier, an overall security solution can, in most cases, only be provided by a combination of the listed options, for instance by using a firewall. However, what your particular security requirements are needs to be specified in a security policy.

1.6.1 The need for a security policy

It is important to point out that you cannot implement security if you have not decided what needs to be protected and from whom. You need a security policy, a list of what you consider allowable and what you do not consider allowable, upon which to base any decisions regarding security. The policy should also determine your response to security violations.

An organization's overall security policy must be determined according to security analysis and business requirements analysis. Since a firewall, for instance, relates to network security only, a firewall has little value unless the overall security policy is properly defined. The following questions should provide some general guidelines:

- Exactly who do you want to guard against?
- Do remote users need access to your networks and systems?
- How do you classify confidential or sensitive information?
- Do the systems contain confidential or sensitive information?
- What will the consequences be if this information is leaked to your competitors or other outsiders?
- Will passwords or encryption provide enough protection?

- Do you need access to the Internet?
- How much access do you want to allow to your systems from the Internet and/or users outside your network (business partners, suppliers, corporate affiliates, etc.)?
- What action will you take if you discover a breach in your security?
- Who in your organization will enforce and supervise this policy?

This list is short, and your policy will probably encompass a lot more before it is complete. Perhaps the very first item you need to assess is the depth of your paranoia. Any security policy is based on how much you trust people, both inside and outside your organization. The policy must, however, provide a balance between allowing your users reasonable access to the information they require to do their jobs, and totally disallowing access to your information. The point where this line is drawn will determine your policy.

1.6.2 Network security policy

If you connect your system to the Internet then you can safely assume that your network is potentially at risk of being attacked. Your gateway or firewall is your greatest exposure, so we recommend the following:

- The gateway should not run any more applications than is absolutely necessary, for example, proxy servers and logging, because applications have defects that can be exploited.
- The gateway should strictly limit the type and number of protocols allowed to flow through it or terminate connections at the gateway from either side, because protocols potentially provide security holes.
- Any system containing confidential or sensitive information should not be directly accessible from the outside.
- Generally, anonymous access should at best be granted to servers in a demilitarized zone.
- All services within a corporate intranet should require at least password authentication and appropriate access control.
- Direct access from the outside should always be authenticated and accounted.

The network security policy defines those services that will be explicitly allowed or denied, how these services will be used and the exceptions to these rules. Every rule in the network security policy should be implemented on a firewall and/or Remote Access Server (RAS). Generally, a firewall uses one of the following methods:

Everything not specifically permitted is denied.

This approach blocks all traffic between two networks except for those services and applications that are permitted. Therefore, each desired service and application should be implemented one by one. No service or application that might be a potential hole on the firewall should be permitted. This is the most secure method, denying services and applications unless explicitly allowed by the administrator. On the other hand, from the point of users, it might be more restrictive and less convenient.

Everything not specifically denied is permitted.

This approach allows all traffic between two networks except for those services and applications that are denied. Therefore, each untrusted or potentially harmful service or application should be denied one by one. Although this is a flexible and convenient method for the users, it could potentially cause some serious security problems.

Remote access servers should provide authentication of users and should ideally also provide for limiting certain users to certain systems and/or networks within the corporate intranet (authorization). Remote access servers must also determine if a user is considered roaming (can connect from multiple remote locations) or stationary (can connect only from a single remote location), and if the server should use callback for particular users once they are properly authenticated.

1.6.3 VPN security policy

While a simple network security policy specifies which traffic is denied and which traffic is permitted to flow and where, a VPN security policy describes the characteristics of protection for a particular traffic profile. In a sense, it is a subset of a network security policy because it is more granular and it depends on the former to allow traffic between certain destinations before it can be protected. It should also be noted that traffic that should flow through a VPN and therefore be protected should not be allowed to flow otherwise, probably through unsecured channels.

A VPN security policy typically describes the traffic profile to be protected (source and destination, protocols and ports) and the security requirements for the protection itself (authentication, encryption, transforms, key lengths and lifetimes, and so forth). VPN policies can be defined per device but should be implemented in a centralized directory to provide better scalability and management. Essentially, both devices need to have matching policies for the same traffic profile before such traffic can be allowed to flow between them. One policy can be more granular or restrictive than the other as long as both parties can agree on the same set of protection suites at any point in time.

Chapter 2. Layer-2 VPN Protocols

In this chapter we discuss protocols that allow a layer-2 connection, typically PPP, to be tunneled over another network, typically IP. This sounds like a complicated approach involving a lot of overhead, but several benefits can be derived from this approach which are useful or even invaluable for building VPNs. In fact, the number of Internet VPN scenarios or variations thereof would be quite limited without the use of layer-2 tunneling techniques.

2.1 Layer 2 Tunneling Protocol (L2TP)

The Layer 2 Tunneling Protocol (L2TP) is one of the emerging techniques for providing a remote connection to the corporate intranet. The L2TP protocol has been developed merging two different protocols: the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F).

The remote dial-in user scenario is the most common situation for using L2TP. Remote users do not need to make a long-distance call or use a toll-free number to connect directly to the corporate servers but cost constraints suggest the use of ISPs' points of presence (POPs) as a more cost-effective solution. In this case the dial-in user connects to the nearest POP provided by the ISP and then the session is routed through the ISPs and/or the Internet cloud to reach the corporate LAN access. This environment has more than one point of critical security and reliability issues.

L2TP provides a technique for building a Point-to-Point Protocol (PPP) tunnel connection that, instead of being terminated at the ISP's nearest POP, is extended to the final corporate intranet access gateway. The tunnel can be initiated either by the remote host or by the ISP's gateway access. L2TP provides a reliable way of connecting remote users in a virtual private network that can support multiprotocol traffic, that is, all the network layer protocols supported by the PPP protocol. Moreover, it provides support for any network layer private addressing scheme for the connection over the Internet.

2.1.1 Overview and standards

L2TP can support remote LAN access using any network layer protocol supported by PPP over the tunnel session, and this is managed by terminating the PPP connection directly in the corporate intranet access gateway.

L2TP is defined in RFC 2661.

There are some elements that take part in the L2TP protocol scenario:

L2TP Access Concentrator (LAC)

The LAC is located at the ISP's POP to provide the physical connection of the remote user. In the LAC the physical media are terminated and can be connected to more public switched telephone network (PSTN) lines or integrated services digital network (ISDN) lines. Over these media the user can establish the L2TP connection that the LAC routes to one or more L2TP servers where the tunnels are terminated. Any 221x Nways router can support LAC functionality and based on the connection capabilities a 2210 Nways

multiprotocol router or a 2212 Nways Access Utility can be correctly positioned on a different ISP's POPs as a LAC for the L2TP.

L2TP Network Server (LNS)

The LNS terminates the calls arriving from the remote users. Only a single connection can be used on the LNS to terminate multiple calls from remote users, placed on different media as ISDN, asynchronous lines, V.120, etc. The 221x Nways routers can support LNS capabilities. A 2216 Multiaccess Concentrator can be used also as LNS when it is used as the corporate intranet access gateway.

Network Access Server (NAS)

The NAS is the point-to-point access device that can provide on-demand access to the remote users across PSTN or ISDN lines.

The L2TP protocol is described in Figure 10. The session and tunnel establishments are handled in the following phases:

- The remote user initiates a PPP connection to the NAS.
- The NAS accepts the call.
- The end user authentication is provided by means of an authorization server to the NAS.
- The LAC is triggered by the end user's attempt to start a connection with the LNS for building a tunnel with the LNS at the edge of the corporate intranet. Every end-to-end attempt to start a connection is managed by the LAC with a session call. The datagrams are sent within the LAC LNS tunnel. Every LAC and LNS device keeps track of the connected user's status.
- The remote user is authenticated also by the authentication server of the LNS gateway before accepting the tunnel connection.
- The LNS accepts the call and builds the L2TP tunnel.
- The NAS logs the acceptance.
- The LNS exchanges the PPP negotiation with the remote user.
- End-to-end data is now tunneled between the remote user and the LNS.

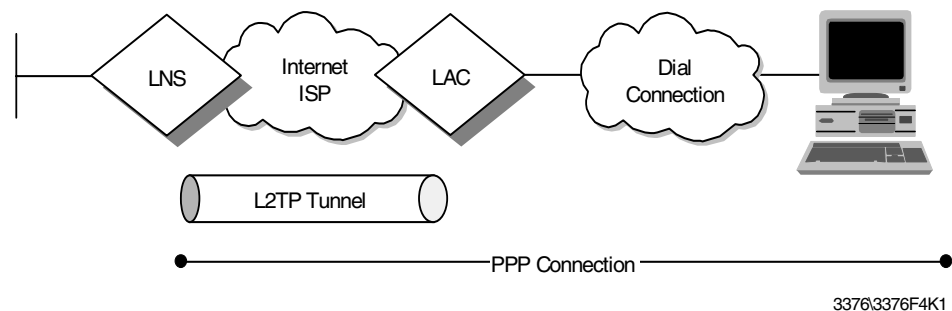


Figure 10. Layer 2 Tunnel Protocol (L2TP) scenario

L2TP can support the following functions:

- Tunneling of single user dial-in clients

- Tunneling of small routers, for example, a router with a single static route to set up based on an authenticated user's profile
- Incoming calls to an LNS from a LAC
- Multiple calls per tunnel
- Proxy authentication for PAP and CHAP
- Proxy LCP
- LCP restart in the event that proxy LCP is not used at the LAC
- Tunnel endpoint authentication
- Hidden attribute value pair (AVP) for transmitting a proxy PAP password
- Tunneling using a local lookup table
- Tunneling using the PPP user name lookup in the AAA subsystem

2.1.2 L2TP flows

There are a number of steps that occur for L2TP:

- Establish control connection and tunnel
- Initiate call
- Establish L2TP session
- Forward PPP packets

Between two devices there may be more than one tunnel and each tunnel must have its own control connection. The control connection can be initiated by either the LSN or LAC.

Within the tunnel there can be many L2TP sessions and each session represents a single PPP stream between the LNS and the LAC. Normally this session is established by the LAC.

2.1.2.1 Control connection and tunnel

Below are the flows for establishing the control connection and its associated tunnel.

Table 1. L2TP control session establishment flow

| LAC or LNS | | LAC or LNS |
|------------------------------------|--------|--------------------------------|
| Start_Control_Connection_Request | 1 ---> | |
| | <--- 2 | Start_Control_Connection_Reply |
| Start_Control_Connection_Connected | 3 ---> | |
| | <--- 4 | ZLB_Acknowledge |

As you can gather from the table above either the LAC or LNS can set up the control connection and its tunnel. A series of messages are simply transferred between the peers requesting the setup of the connection. Message 4 is a Zero Length Body (ZLB) message which simply acknowledges receipt of the last message.

During this process authentication of the tunnel occurs. Note that this step is optional. This is achieved by sending a challenge in either message 1 or 2, and

sending the reply in the following message. A shared secret is needed between the peers to generate and validate the challenge.

2.1.2.2 Establish session

A separate session must be established for each PPP stream. It is normally initiated by the receipt of a call from the LAC. This session can only be established after the control connection and its tunnel have been set up. The following shows the flows that occur in this process:

Table 2. L2TP incoming session establishment flow

| LAC | | LNS |
|-------------------------|--------|---------------------|
| Call detected | | |
| Incoming_Call_Request | 1 ---> | |
| | <--- 2 | Incoming_Call_Reply |
| Incoming_Call_Connected | 3 ---> | |
| | <--- 4 | ZLB_Acknowledge |

During this process the LAC can defer answering the call until it receives message 2 to ensure that this session should be established. LAC can answer the call and negotiate the LCP and PPP authentication and then use this information to choose the LNS to which it needs to establish a session.

The above flows show the process for establishing a session from the LAC. This is called an incoming call establishment. L2TP, however, allows you to establish a call from the other direction, that is, from the LNS. This is called an outgoing call request:

Table 3. L2TP outgoing session establishment flow

| LAC | | LNS |
|-------------------------|--------|-----------------------|
| | <--- 1 | Outgoing_Call_Request |
| Outgoing_Call_Reply | 2 ---> | |
| Perform call operation | | |
| Outgoing_Call_Connected | 3 ---> | |
| | <--- 4 | ZLB_Acknowledge |

Once the session is established PPP packets can flow over the tunnel.

2.1.3 Compulsory and voluntary tunnel modes

L2TP supports two types of tunnels, the compulsory model and the voluntary model.

2.1.3.1 L2TP compulsory tunnels

With this model, the L2TP tunnel is established between a LAC, an ISP and an LNS at the corporate network. This requires the cooperation of a service provider that has to support L2TP in the first place and has to determine based upon authentication information whether L2TP should be used for a particular session, and where a tunnel should be directed. However, this approach does not require any changes at the remote client, and it allows for, centralized IP address

assignment to a remote client by the corporate network. Also, no Internet access is provided to the remote client other than via a gateway in the corporate network that allows for better security control and accounting.

An L2TP compulsory tunnel, illustrated in Figure 11, is established as follows:

1. The remote user initiates a PPP connection to an ISP.
2. The ISP accepts the connection and the PPP link is established.
3. The ISP now undertakes a partial authentication to learn the user name.
4. ISP-maintained databases map users to services and LNS tunnel endpoints.
5. LAC then initiates an L2TP tunnel to LNS.
6. If LNS accepts the connection, LAC then encapsulates PPP with L2TP and forwards the appropriate tunnel.
7. LNS accepts these frames, strips L2TP, and processes them as normal incoming PPP frames.
8. LNS then uses PPP authentication to validate the user and then assigns the IP address.

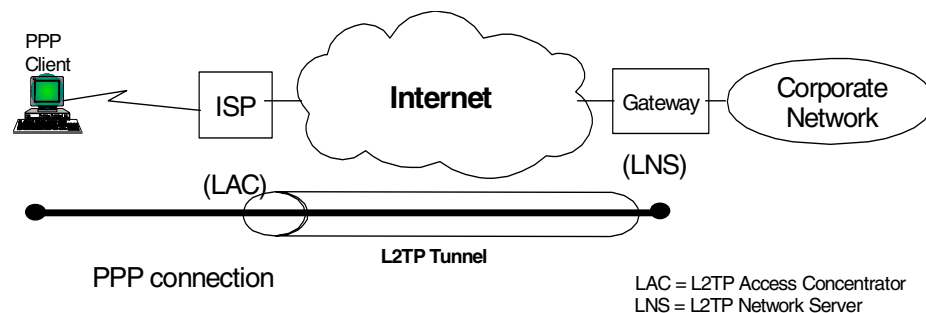


Figure 11. L2TP compulsory tunnel model

2.1.3.2 L2TP voluntary tunnels

With this model, the L2TP tunnel is established between a remote client (which is effectively acting as a LAC) and an LNS at a corporate network. This method is similar to PPTP and is essentially transparent to an ISP but requires L2TP support at the client. This approach allows the remote client to have Internet access as well as one or multiple VPN connections at the same time. However, the client ultimately ends up being assigned multiple IP addresses; one from the ISP for the original PPP connection, and one per L2TP VPN tunnel assigned from a corporate network. This opens the client as well as the corporate networks to potential attacks from the outside, and it requires client applications to determine the correct destinations for their data traffic.

An L2TP voluntary tunnel, illustrated in Figure 12 on page 28, is established as follows:

1. The remote user has a pre-established connection to an ISP.
2. The L2TP Client (LAC) initiates the L2TP tunnel to LNS.
3. If LNS accepts the connection, LAC then encapsulates PPP and L2TP, and forwards through a tunnel.

4. LNS accepts these frames, strips L2TP, and processes them as normal incoming frames.
5. LNS then uses PPP authentication to validate the user and then assign the IP address.

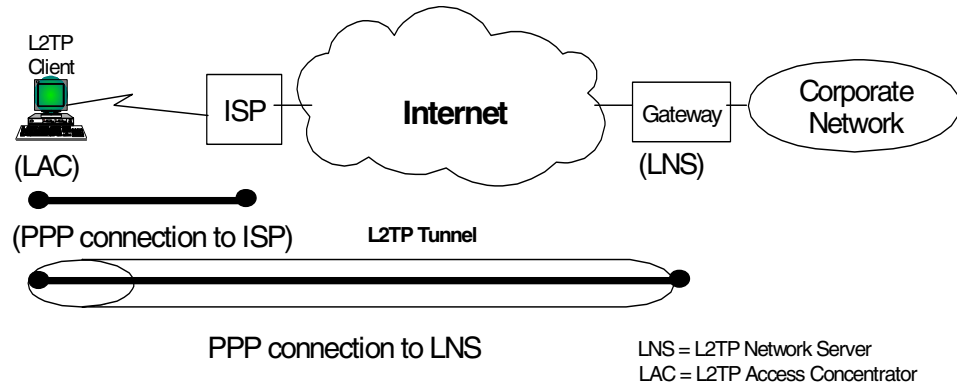


Figure 12. L2TP voluntary tunnel model

2.1.4 Securing the tunnels with IPSec

The L2TP protocol can provide a cost-effective solution for the remote access scenario using the virtual private network technology, but there are some issues mainly concerned with security. An L2TP tunnel is created by encapsulating an L2TP frame inside a UDP packet, which in turn is encapsulated inside an IP packet whose source and destination addresses define the tunnel's endpoints as can be seen in Figure 13. Since the outer encapsulating protocol is IP, clearly IPSec protocols can be applied to this composite IP packet, thus protecting the data that flows within the L2TP tunnel. The Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE) protocols can all be applied in a straightforward way.

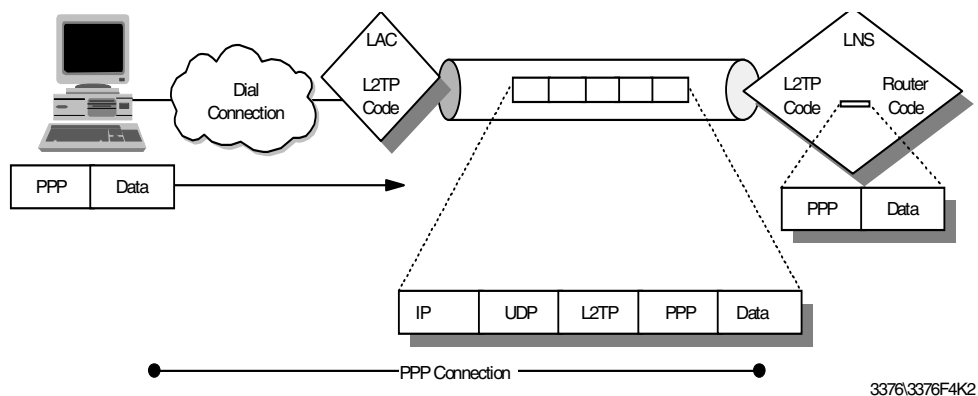


Figure 13. L2TP tunnel encapsulation

In fact a proposed solution to the security issues has been developed in the PPP Extensions Working Group in the IETF to make use of the IPSec framework to provide the security enhancements to the L2TP protocol. The use of IPSec technologies in conjunction with the L2TP protocol can provide a secured

end-to-end connection between remote users and the corporate intranet that can support remote LAN connections (not only remote IP). The following reference provides additional information on how to use IPsec in conjunction with L2TP:

<http://search.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-security-04.txt>

The IPsec framework can add to the L2TP protocol the per packet authentication mechanism and integrity checks instead of the simple authentication of the ending point of the tunnel that is not secured from attack by internetwork nodes along the path of the tunnel connection. Moreover, the IPsec framework adds to the L2TP protocol the encryption capabilities for hiding the cleartext payload and a secured way for an automated generation and exchange of cryptographic keys within the tunnel connection.

We have discussed above the benefits of using L2TP for cost-effective remote access across the Internet. The shortcomings of that approach are the inherently weak security features of L2TP and the PPP connection that is encapsulated by L2TP. The IETF has therefore recommended to use IPsec to provide protection for the L2TP tunnel across the Internet as well as for the end-to-end traffic inside the tunnel.

Figure 14 on page 29 illustrates how IPsec can be used to protect L2TP compulsory tunnels between a remote client and a corporate VPN gateway:

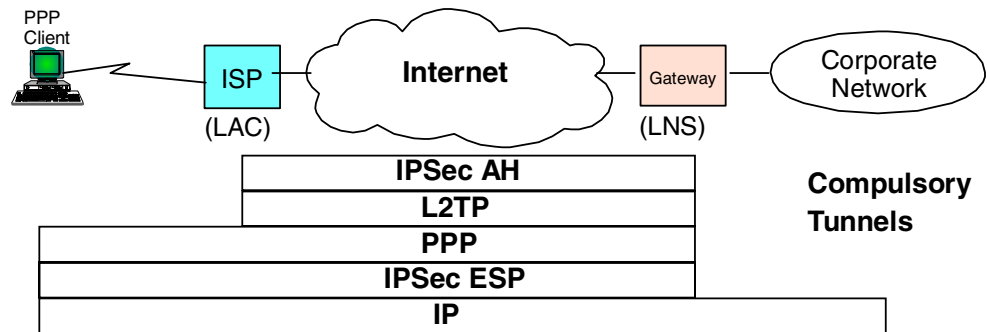


Figure 14. IPsec protection for L2TP compulsory tunnel to VPN gateway

Figure 15 on page 29 illustrates how IPsec can be used to protect L2TP voluntary tunnels between a remote client and a corporate VPN gateway:

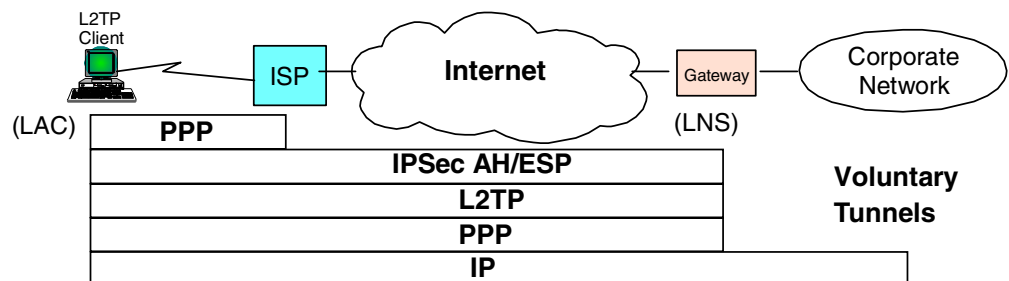


Figure 15. IPsec protection for L2TP voluntary tunnel to VPN gateway

Figure 16 illustrates how IPSec can be used to protect L2TP compulsory tunnels between a remote client and an IPSec-enabled system inside a corporate network:

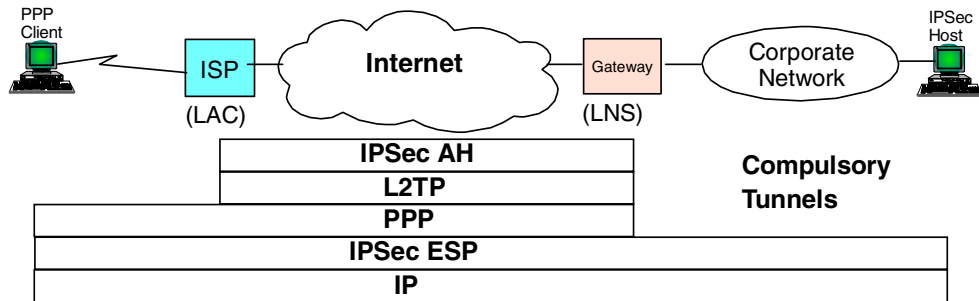


Figure 16. IPSec protection for L2TP compulsory tunnel end-to-end

Figure 17 illustrates how IPSec can be used to protect L2TP voluntary tunnels between a remote client and an IPSec-enabled system inside a corporate network:

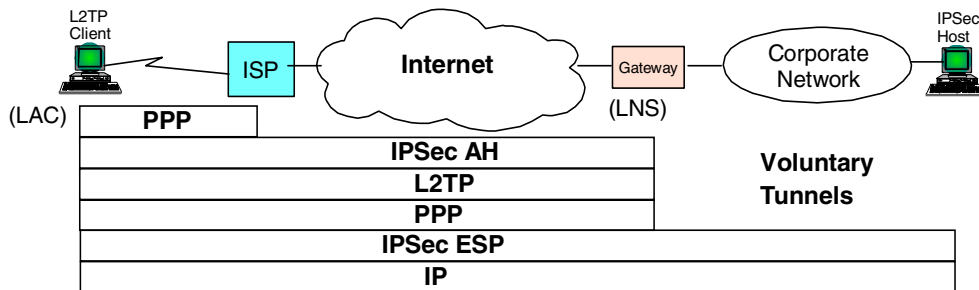


Figure 17. IPSec protection for L2TP voluntary tunnel end-to-end

When planning the use of VPN access in large environments the choice of whether or not to differentiate the functionalities of the corporate firewall, which provides the traditional Internet access from the VPN gateway, should be evaluated to simplify the management and the critical requirement of these resources. If the existing filtering policies are not changed when introducing the IPSec VPN remote access, then the IPSec authentication mechanisms will keep non-VPN traffic from accessing the corporate intranet.

2.1.5 Multiprotocol support

Because L2TP tunnels PPP sessions, any protocol that is supported over PPP can be tunneled by L2TP. Protocols such as SNA, IPX and others are carried as a PPP payload and therefore transparent to L2TP. This makes L2TP a good choice for connecting corporate networks that require multiprotocol support.

2.2 Point-to-Point Tunneling Protocol (PPTP)

One of the more "established" techniques for remote connection is the Point-to-Point Tunneling Protocol (PPTP). PPTP is a vendor solution that meets

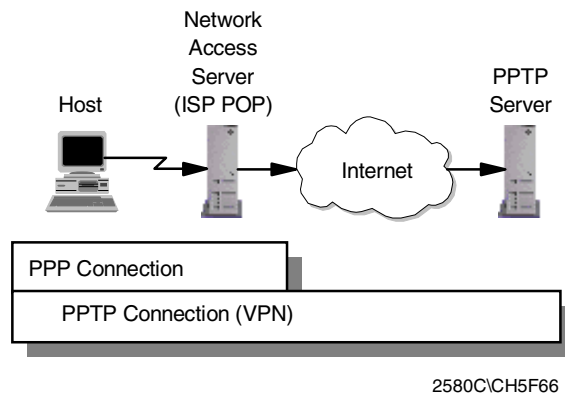
the requirements for a VPN. It has been implemented by Microsoft on the Windows NT, Windows 98 and Windows 95 (OSR2) platforms.

PPTP is an extension of the basic PPP protocol (see Figure 18). It is due to this fact that PPTP does not support multipoint connections, connections must be point-to-point.

PPTP supports only IP, IPX, NetBIOS and NetBEUI. Because these are the most commonly implemented network protocols, it is rarely an issue, especially for this book as we are concerned with IP network design. However, this must be considered when designing the network, more so when upgrading an existing network.

PPTP does not change the PPP protocol. PPTP only defines a new way, a tunneled way, of transporting PPP traffic.

PPTP is currently being replaced by implementations of L2TP. Microsoft has announced that Windows 2000 will support L2TP. However, some vendors are still developing solutions with PPTP.



2580C\CH5F66

Figure 18. PPTP system overview

PPTP is defined in RFC 2637.

2.3 Layer 2 Forwarding (L2F)

Layer 2 Forwarding (L2F) was developed by Cisco Systems at the same time that PPTP was being developed. It is another protocol that enables remote hosts to access an organization's intranet through public infrastructure, with security and manageability maintained.

Cisco submitted this technology to the Internet Engineering Task Force (IETF) for approval as a standard, and it is defined in RFC 2341.

As with PPTP, L2F enables secure private network access through public infrastructure by building a "tunnel" through the public network between the client and the host. The difference between PPTP and L2F is that L2F tunneling is not dependent on IP; it is able to work with other network protocols natively, such as frame relay, ATM or FDDI. The service requires only local dial-up capability,

reducing user costs and providing the same level of security found in private networks.

An L2F tunnel supports more than one connection, a limitation of PPTP. L2F is able to do this as it defines connections within the tunnel. This is especially useful in situations where more than one user is located at a remote site, only one dial-up connection is required. Alternatively, if tunneling is used only between the POP and the gateway to the internal network, fewer connections are required from the ISP, reducing costs. See Figure 19.

L2F uses PPP for client authentication, as does PPTP, however, L2F also supports TACACS+ and RADIUS for authentication. L2F authentication comprises two levels, first when the remote user connects to the ISP's POP, and then when the connection is made to the organization's intranet gateway.

L2F passes packets through the virtual tunnel between endpoints of a point-to-point connection. L2F does this at the protocol level. A frame from the remote host is received at the POP; the linked framing/transparency bytes are removed. The frame is then encapsulated in L2F and forwarded over the appropriate tunnel. The organization's gateway accepts the L2F frame, removes the L2F encapsulation, and processes the incoming frame. Because L2F is a layer-2 protocol, it can be used for protocols other than IP, such as IPX and NetBEUI.

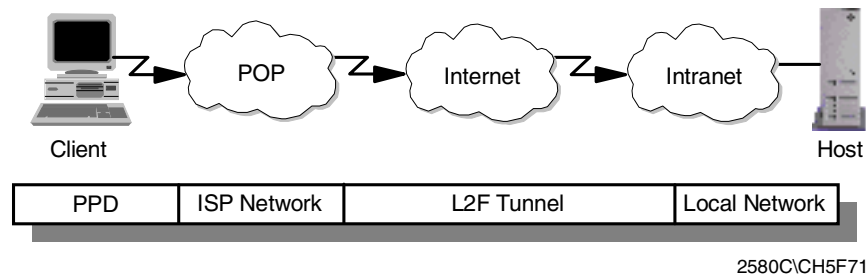


Figure 19. L2F tunnel from POP to intranet gateway

With L2F, a complete end-to-end secure VPN can be created and used. It is a reliable and scalable solution. However, it has shortcomings that are addressed with L2TP.

2.4 Comparing remote access tunneling protocols

The following table provides a quick comparison of the three predominant remote access tunneling protocols, L2TP, PPTP and L2F:

Table 4. Comparing remote access tunneling protocols

| Feature | PPTP | L2F | L2TP |
|-----------------|-----------------------------|-----------------------------|-------------------------------|
| Standard/Status | RFC 2637 (informational) | RFC 2341 (informational) | RFC 2661 (standards track) |
| Carrier | IP/GRE | IP/UDP, FR, ATM | IP/UDP, FR, ATM |

| Feature | PPTP | L2F | L2TP |
|-----------------------------|-------------------------------------|--|--|
| Private address assignments | Yes | Yes | Yes |
| Multiprotocol support | Yes | Yes | Yes |
| Call types | Incoming and outgoing | Incoming | Incoming and outgoing |
| Control protocol | Control over TCP Port 1723 | Control over UDP Port 1701 | Control over UDP Port 1701 |
| Encryption | Microsoft PPP encryption (MPPE) | PPP encryption (MPPE); IPSec optional | PPP encryption (MPPE/ECP); IPSec optional |
| Authentication | PPP authentication (user) | PPP authentication (user); IPSec optional (packet) | PPP authentication (user); IPSec optional (packet) |
| Tunnel modes | Typically voluntary tunneling model | Compulsory tunneling model | Compulsory and voluntary models |
| Multiple calls per tunnel | No | Yes | Yes |
| PPP multilink support | No | Yes | Yes |

2.5 Layer-2 tunneling authentication and encryption

In this section we discuss the options for authentication and encryption that are available with the aforementioned layer-2 tunneling protocols.

2.5.1 Authentication options

Authentication is one of the key requirements for VPNs. The following sections discuss some commonly used remote access authentication techniques and highlight their suitability for VPNs.

2.5.1.1 Password Authentication Protocol (PAP)

PAP was, and maybe still is, the most common authentication protocol for dial-up connection to ISPs. It authenticates the PPP user before a connection can be established, but it sends the user information and password in the clear which makes it entirely unsuitable to VPNs. PAP also authenticates the user only once, at connection establishment. Once connected, a cracker could potentially take over the connection and would not have to worry about further authentication requirements (even though they would be easy to meet with PAP if the cracker already listened in on the original authentication exchange).

2.5.1.2 Challenge Handshake Protocol (CHAP)

CHAP fixes some of the problems with PAP in that it requires the user and access server to have a shared secret between them. The server challenges the client for identification upon which the client responds with a hashed value (usually using MD5) of the secret. If that matches at the server where the same hash on

the presumed secret is performed, the client is authenticated. This effectively avoids having to send cleartext passwords over the line. CHAP also provides for multiple authentication challenges by the server during a connection which makes it harder for crackers to take over. In the case of Microsoft PPTP, the secret shared between the client and the access server is the Windows NT domain password of the user at the client.

2.5.1.3 Microsoft CHAP (MS-CHAP)

MS-CHAP works the same way as CHAP but uses the RSA MD4 or DES hash functions instead of MD5. MD4 is the hash algorithm used by Windows NT as well as Windows 95 and Windows 98 dial-up networking clients for logon verification. DES is used by older Windows dial-up clients. Using MS-CHAP is fine if you have only Microsoft clients but is not supported by any other client platforms. However, it is the required PPP authentication option if you also want to use MPPE encryption (see 2.5.2.1, “Microsoft Point-to-Point Encryption (MPPE)” on page 35).

2.5.1.4 Shiva Password Authentication Protocol (SPAP)

SPAP is a proprietary method for authenticating DIALs clients and some Microsoft clients. It provides a two-way handshake between client and server with an encrypted password. In some scenarios, SPAP can provide additional functionalities such as callback, change password, and virtual connections.

2.5.1.5 Extensible Authentication Protocol (EAP)

EAP (defined in RFC 2284) provides a more generic way to authenticate a remote user during PPP connection establishment. As opposed to other authentication methods such as PAP and CHAP, EAP is not performed during LCP setup but takes place after LCP has been completed and the PPP authentication phase begins. This allows for more connection parameters to be exchanged that can be used as authentication information. EAP offers a tie-in of back-end authentication servers in a similar way as RADIUS and TACACS, but EAP itself does not provide for authentication mechanisms. To use EAP, existing PPP implementations must be changed.

2.5.1.6 IP Security Architecture (IPSec)

IPSec has two protocols that offer authentication, the Authentication Header (AH) and the Encapsulating Security Payload (ESP) protocols. Both provide authentication per packet as long as a session is active, instead of per user at session establishment or at numerous times during a session. AH and ESP also provide replay protection. This makes IPSec authentication much more secure than traditional PPP authentication options, but it incurs a slightly higher processing overhead at the performing devices. IPSec is the recommended security protocol for L2TP and can be used with L2F and theoretically with PPTP as well. For more information on IPSec AH and ESP, please read 3.1, “IP Security Architecture (IPSec)” on page 37.

2.5.1.7 RADIUS and TACACS

RADIUS and TACACS provide centralized authentication for remote access users. Both technologies work in a similar way: A remote access server implements a RADIUS or TACACS client that forwards authentication requests to a central server where the request is processed and access granted or denied. That provides great flexibility and scalability over large numbers of access servers which is typically required by ISPs and large corporations. RADIUS and

TACACS also allow to pass on configuration information to the client from a central database which is convenient from a management standpoint. RADIUS can optionally be tied into other central authentication systems such as Kerberos, DCE or RACF.

2.5.1.8 SecureID

SecureID is developed by Security Dynamics, Inc. and is based on the principle of two-factor authentication. A user requires not only a password to authenticate successfully but also a secret PIN code in the form of a random number that changes over time. The password is stored in a database at the server and compared to that entered by a user at logon. The random number is generated at the server for each user and typically changes once every minute. The user is provided with a device in the form of a key chain token or smart card in which a microchip performs the same random number calculations as the server. That chip has a fairly synchronized clock to the server so the user is generally able to log on successfully by entering the password and the PIN that is displayed on the token device. SecureID is based on a client/server model similar to RADIUS and TACACS in that an access server acts as a SecureID client/proxy that forwards authentication requests to the central server called ACE/Server. SecureID can also be used as a secondary authentication system for RADIUS.

2.5.2 Encryption options

Encryption and key exchange are two of the key requirements for VPNs. In the following sections we discuss some commonly used remote access encryption techniques and highlight their suitability for VPNs.

2.5.2.1 Microsoft Point-to-Point Encryption (MPPE)

MPPE uses the MD4 hash created during MS-CHAP authentication (see 2.5.1.3, “Microsoft CHAP (MS-CHAP)” on page 34) to derive a secret session key for a PPP connection. This is typically used for PPTP with Microsoft clients. The encryption algorithm used by MPPE is RC4 with 40-bit keys, which is considered very weak by the standard of today’s cracking techniques. Microsoft also offers a 128-bit key version for the U.S. market. Microsoft implementations of PPTP refresh a key every 256 packets, though the PPTP standards allow other intervals.

2.5.2.2 Encryption Control Protocol (ECP)

ECP can be used to negotiate encryption for a PPP link once the link is established and authenticated. ECP allows for using different encryption algorithms in each direction, but it does not provide key refresh. The standard encryption algorithm defined in the standard is DES, but vendors are free to implement any algorithm they wish. ECP is defined in RFC 1968.

2.5.2.3 IPSec

IPSec offers encryption with the Encapsulating Security Payload (ESP) protocols and uses the Internet Key Exchange (IKE) protocol for key generation and refresh. ESP provides encryption per packet as long as a session is active and offers a choice of low, medium, strong and very strong encryption algorithms, ranging from 40-bit DES to 192-bit triple DES. IKE authenticates the parties that need to exchange secret information based on strong authentication algorithms and also encrypts the key refresh messages. The keys generated by IKE are then used by ESP (and also by AH). ESP optionally provides authentication per packet

and replay protection. This makes IPSec encryption much more flexible and secure than traditional PPP authentication options, but it incurs a higher processing overhead at the performing devices. IPSec is the recommended security protocol for L2TP and can be used with L2F and theoretically with PPTP as well. For more information on IPSec AH and ESP, please read 3.1, “IP Security Architecture (IPSec)” on page 37.

Chapter 3. Layer-3 VPN protocols

In this chapter we discuss IPSec, a VPN technology that operates on the network layer, and its supporting component, the Internet Key Exchange (IKE) protocol. Even though IPSec is the architecture that implements layer-3 security and IKE uses an application running at or above layer-5, there is an inherent relationship between the two. IPSec protocols require symmetric keys to secure traffic between peers, but IPSec itself does not provide a mechanism for generating and distributing those keys. This is the role that IKE is playing to support IPSec peers by enabling key management for security associations. IKE, as you will see later, provides security for its own traffic in addition to providing IPSec protocols with the necessary cryptographic keys for authentication and encryption.

3.1 IP Security Architecture (IPSec)

In this section, we provide a brief overview of the Security Architecture for the Internet Protocol (IPSec) because this is the technology upon which the majority of VPN solutions are based, though a more detailed discussion of this topic is already available in *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions*, SG24-5201. This section presents a valuable addition to this redbook because it is based on the latest Internet standards.

3.1.1 Overview and standards

The IP Security Architecture (IPSec) provides a framework for security at the IP layer for both IPv4 and IPv6. By providing security at this layer, higher layer transport protocols and applications can use IPSec protection without the need of being changed. This has turned out to be a major advantage in designing modern networks and has made IPSec one of the most, if not the most attractive technologies to provide IP network security.

IPSec is an open, standards-based security architecture (RFC 2401-2412, 2451) that offers the following features:

- Provides authentication, encryption, data integrity and replay protection
- Provides secure creation and automatic refresh of cryptographic keys
- Uses strong cryptographic algorithms to provide security
- Provides certificate-based authentication
- Accommodation of future cryptographic algorithms and key exchange protocols
- Provides security for L2TP and PPTP remote access tunneling protocols

IPSec was designed for interoperability. When correctly implemented, it does not affect networks and hosts that do not support it. IPSec uses state-of-the-art cryptographic algorithms. The specific implementation of an algorithm for use by an IPSec protocol is often called a transform. For example, the DES algorithm used in ESP is called the ESP DES-CBC transform. The transforms, as the protocols, are published in RFCs and in Internet drafts.

3.1.2 Security associations

The concept of a security association (SA) is fundamental to IPSec. An SA is a unidirectional (simplex) logical connection between two IPSec systems, uniquely identified by the following triple:

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

The definition of the members is as follows:

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 range 1 to 255 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, currently SA management mechanisms are defined only for unicast addresses.

Security Protocol This can be either AH or ESP.

An SA can be in either of two modes: transport or tunnel, depending on the mode of the protocol in that SA. You can find the explanation of these protocol modes later in this chapter.

Because SAs are simplex, for bidirectional communication between two IPSec systems, there must be two SAs defined, one in each direction.

An SA gives security services to the traffic carried by it either by using 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 could use an AH SA between itself and a firewall and a nested ESP SA that extends to a host behind the firewall.

An IPSec implementation maintains two databases related to SAs:

Security Policy Database (SPD) The Security Policy Database specifies what security services are to be offered to the IP traffic, depending on factors such as source, destination, whether it is inbound, outbound, etc. It contains an ordered list of policy entries, separate for inbound and/or outbound traffic. These entries might specify that some traffic must not go through IPSec processing, some must be discarded and the rest must be processed by the IPSec module. Entries in this database are similar to the firewall rules or packet filters.

Security Associations Database (SAD) The Security Associations Database contains parameter information about each SA, such as AH or ESP algorithms and keys, sequence numbers, protocol mode and SA lifetime. For outbound processing, an SPD entry points to an entry in the SAD. That is, the SPD determines which SA is to be used for a given packet. For inbound processing, the SAD is consulted to determine how the packet must be processed.

Notes:

1. The user interface of an IPSec implementation usually hides or presents these databases in a more friendly way and makes the life of the administrator easier.
2. While IPSec SAs are unidirectional as described above, ISAKMP SAs used by IKE (see 3.2.1, “Overview and standards” on page 45) are essentially bidirectional because an IKE peer can usually act as both initiator or responder. For ISAKMP SAs, the cookies generated by the peers to identify the ongoing exchange are also used as SPI values.

3.1.3 IP Authentication Header (AH)

AH provides origin authentication for a whole IP datagram and is an effective measure against IP spoofing and session hijacking attacks. AH has the following features:

- Provides data integrity and replay protection
- Uses hashed message authentication codes (HMAC), based on shared secrets
- Cryptographically strong but economical on CPU load
- Datagram content is not encrypted
- Does not use changeable IP header fields to compute integrity check value (ICV), which are:
 - TOS, Flags, Fragment Offset, TTL, Checksum

AH adds approximately 24 bytes per packet that can be a consideration for throughput calculation, fragmentation, and path MTU discovery. AH is illustrated in Figure 20:

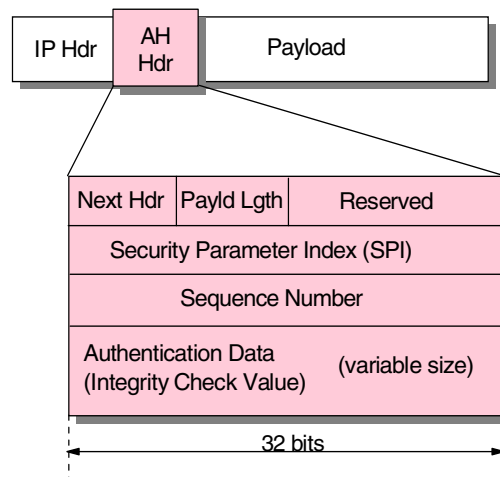


Figure 20. IPsec Authentication Header (AH)

The following transforms are supported with AH:

- Mandatory authentication transforms
 - HMAC-MD5-96 (RFC 2403)
 - HMAC-SHA-1-96 (RFC 2404)
- Optional authentication transforms

- DES-MAC
- Obsolete authentication transforms
 - Keyed-MD5 (RFC 1828)

AH can be used in tunnel or transport mode (see 3.1.5, “Tunnel and transport mode” on page 41) and also in combination with ESP (see 3.1.6, “SA combinations” on page 42).

3.1.4 Encapsulating Security Payload (ESP)

ESP encrypts the payload of an IP packet using shared secrets. The Next Header field actually identifies the protocol carried in the payload. ESP also optionally provides data origin authentication, data integrity, and replay protection in a similar way as AH. However, the protection of ESP does not extend over the whole IP datagram as opposed to AH.

ESP adds approximately 24 bytes per packet that can be a consideration for throughput calculation, fragmentation, and path MTU discovery. ESP is illustrated in Figure 21:

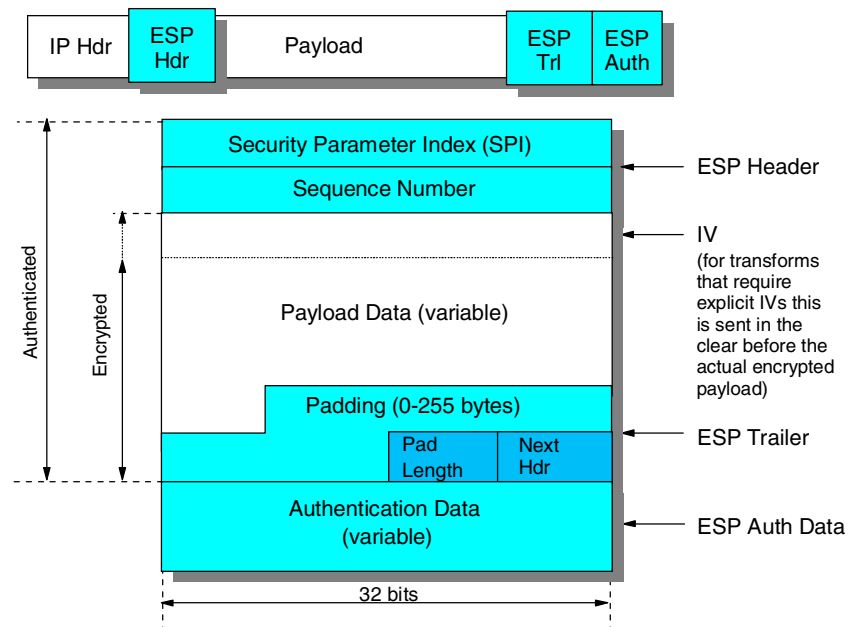


Figure 21. IPsec Encapsulating Security Payload (ESP)

The following transforms are supported with ESP:

- 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: The NULL transform cannot be used for both encryption and authentication at the same time.

ESP can be used in tunnel or transport mode (see 3.1.5, “Tunnel and transport mode” on page 41) and also in combination with AH (see 3.1.6, “SA combinations” on page 42).

3.1.5 Tunnel and transport mode

IPSec protocols can implement security associations in two modes, transport mode and tunnel mode.

3.1.5.1 IPSec transport mode

In transport mode the original IP datagram is taken and the IPSec header is inserted right after the IP header, as it is shown in Figure 22. In the case of ESP, the trailer and the optional authentication data are appended at the end of the original payload. If the datagram already has IPSec header(s), then the new header would be inserted before any of those, but that is hardly ever the case and it would be better to use tunnel mode.

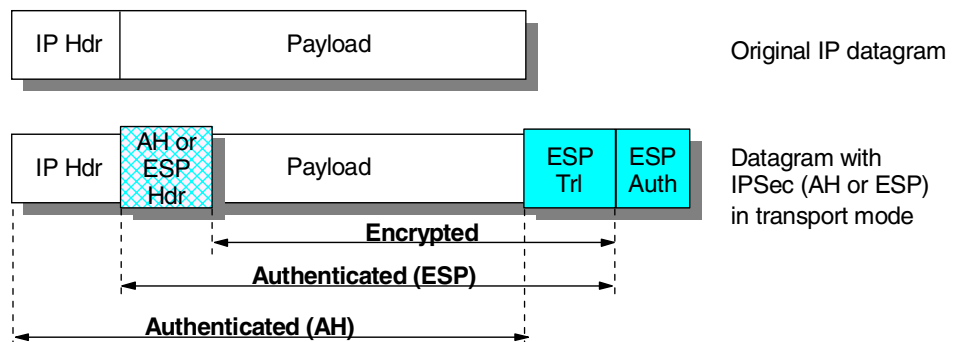


Figure 22. IPSec - transport mode

The transport mode is used by hosts, not by gateways. Gateways are not even required to support transport mode.

The advantage of the transport mode is less processing overhead.

One disadvantage is that the mutable fields are not authenticated. ESP in transport mode provides neither authentication nor encryption for the IP header. This is a disadvantage, since false packets (spoofing attack) might be delivered for ESP processing. Another disadvantage of transport mode is that the addresses of the original IP datagram must be used for delivery. This can be a problem where private IP addresses are used, or where internal addressing structures need to be hidden in the public network.

3.1.5.2 IPSec tunnel mode

With this mode the tunneling concept is applied, which means that a new IP datagram is constructed and the original IP datagram is made the payload of it. Then IPSec in transport mode is applied to the resulting datagram. See Figure 23 for an illustration. In the case of ESP, the original datagram becomes the payload data for the new ESP packet, and therefore its protection is total if both encryption and authentication are selected. However, the new IP header is still not protected.

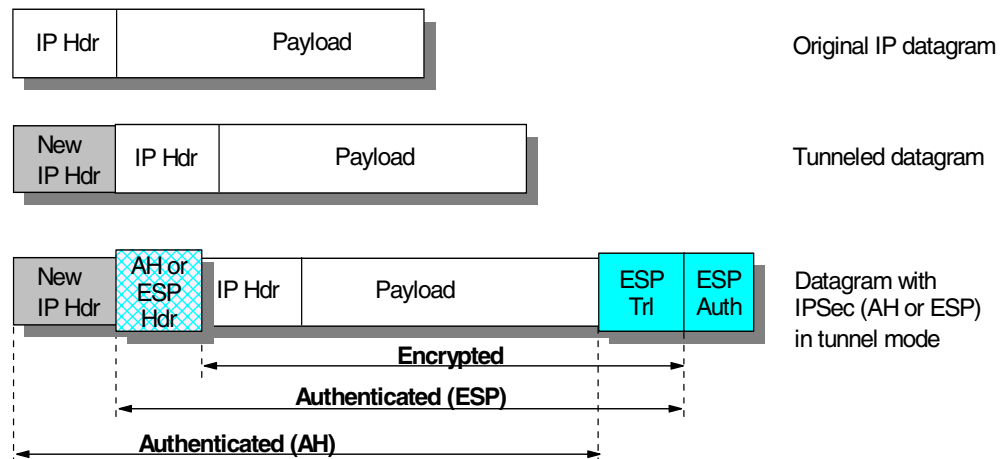


Figure 23. IPSec - tunnel mode

Tunnel mode is used whenever either end of a security association is a gateway. Thus, between two firewalls tunnel mode is always used for traffic that is passing through the firewalls between the secure networks through an IPSec tunnel.

Although gateways are supposed to support tunnel mode only, often they can also work in transport mode. This mode is allowed when the gateway acts as a host, that is, in cases when traffic is destined to itself. Examples are SNMP commands or ICMP echo requests.

In tunnel mode the outer headers' IP addresses do not need to be the same as the inner headers' addresses. For example, two security gateways may operate an AH tunnel which is used to authenticate all traffic between the networks they connect together. This is a very typical mode of operation. Hosts are not required to support tunnel mode, but often they do, and they have to support it for certain remote access scenarios.

The advantages of the tunnel mode are total protection of the encapsulated IP datagram and the possibility of using private addresses. However, there is an extra processing overhead associated with this mode.

3.1.6 SA combinations

The AH and ESP protocols can be applied alone or in combination. Given the two modes of each protocol, there is quite a number of possible combinations. To make things even worse, the AH and ESP SAs do not need to have identical endpoints, so the picture becomes rather complicated. Luckily, out of the many possibilities only a few make sense in real-world scenarios.

Combinations of IPSec protocols are realized with SA bundles and there are two approaches for their creation:

3.1.6.1 Transport adjacency

Both security protocols are applied in transport mode to the same IP datagram. This method is practical for only one level of combination.

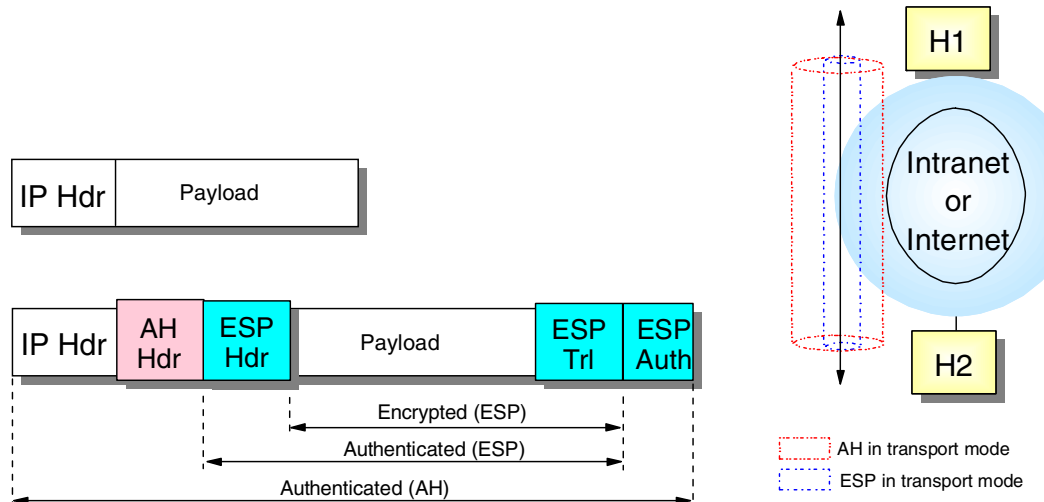


Figure 24. IPSec - transport adjacency

The IPSec standard dictates that transport adjacency can only be used in the way shown above. This means that for outbound packets, encryption (inner SA) has to be performed before authentication (outer SA), whereas for inbound packets authentication has to be performed before encryption. This is a logical sequence and also spares a system the load of decryption in case authentication of the packet fails in the first place.

3.1.6.2 Iterated (nested) tunneling

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.

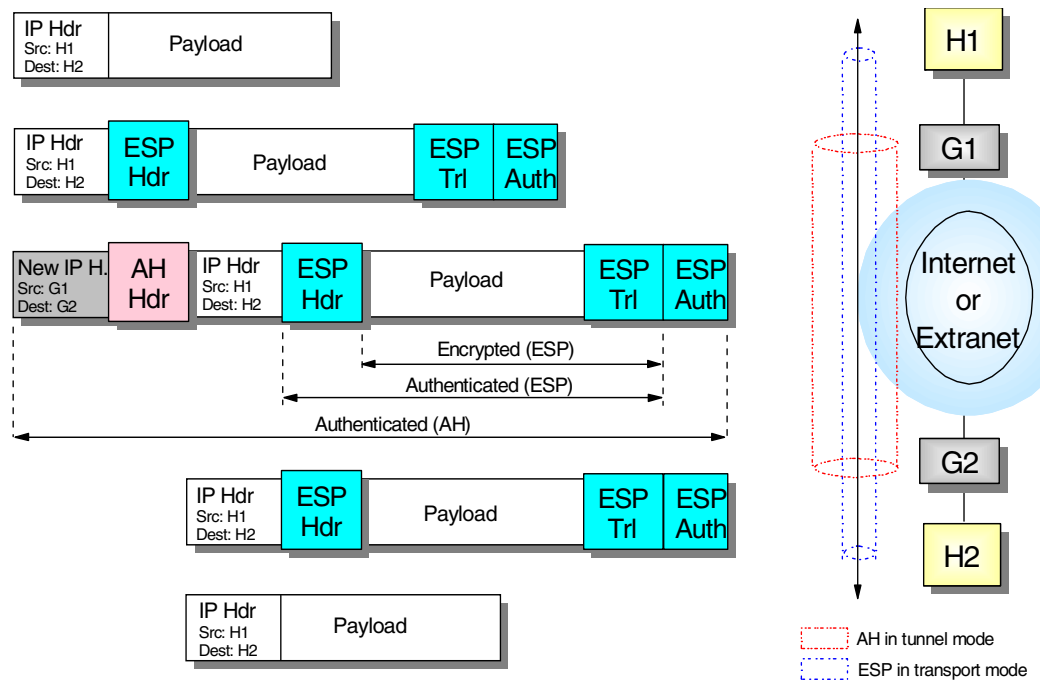


Figure 25. IPsec - iterated tunnels

3.1.6.3 Design considerations

SA bundle approaches can be combined. For example, an IP packet with transport adjacency IPsec headers can be sent through nested tunnels.

When designing a VPN, you should limit the IPsec processing stages applied to a certain packet to a reasonable level. In our view three applications is that limit over which further processing has no benefits. Two stages are sufficient for almost all the cases. Many times even only one stage using ESP with both authentication and encryption will be the level implemented in modern VPNs to reduce processing overhead. In that case, any spoofed packets would eventually fail ESP authentication though they may illegitimately enter the secure network.

Note that to be able to create an SA bundle in which the SAs 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. IKE provides for negotiation of such situations by allowing the peers to use different IDs for Phase 1 (the outer tunnel) and Phase 2 (the end-to-end traffic).

The practical principle of the combined usage is that upon the receipt of a packet with both protocol headers, the IPsec processing sequence should be authentication followed by decryption. It is a common sense decision not to bother with the decryption of packets of uncertain origin. In fact, the IPsec standards prescribe that the sender first apply ESP and then AH to the outbound traffic for transport mode.

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

3.2 Coming to terms with the Internet Key Exchange (IKE) protocol

The following explanations and illustrations of the Internet Key Exchange (IKE) protocol reflect the latest developments.

3.2.1 Overview and standards

Internet Key Exchange (IKE), defined in RFC 2409, is the protocol used to establish security associations that are needed by various services, for example IPsec uses IKE to establish the security associations needed to generate and refresh its keys. To establish security associations, keys need to be formed in a secure and protected manner and IKE provides the mechanism to achieve this.

IKE was originally called ISAKMP/Oakley. Internet Security Association and Key Management Protocol (ISAKMP), defined in RFC 2408, provides the framework to establish security associations and cryptographic keys. The framework is not dependent on any technology and is able to be used with any security mechanism that may be available at the time. Since ISAKMP does not actually define the security mechanism, this is where Oakley, specified in RFC 2412, is used to define the key exchange protocol within ISAKMP.

IKE still uses ISAKMP as its framework but incorporates Oakley and SKEME as its key exchange protocol. IKE does not implement the whole Oakley and SKEME protocol but rather a subset of it.

IKE is made up of two phases as defined in the ISAKMP framework, and within these phases Oakley defines a number of modes that can be used.

Phase 1 is the process where the ISAKMP security association must be established. It assumes that no secure channel currently exists and therefore it must initially establish one to protect any ISAKMP messages. This SA is different from other SAs that are negotiated for other services in that it is owned by ISAKMP.

Phase 2 is where subsequent security associations required by various services are negotiated on their behalf. The ISKMP SA generated in Phase 1 protects all subsequent ISAKMP messages.

Two modes are available for use in Phase 1, main mode and aggressive mode. Support for main mode is a mandatory requirement for IKE, while aggressive mode is optional. Main mode has the advantage of being able to protect the identities of the parties trying to establish the SA, while aggressive mode has the advantage of being able to use three rather than six message flows to establish the ISAKMP SA.

Within Phase 2, quick mode is used to negotiate the SAs for the services.

Informational mode is used to give the other party some information, normally abnormal conditions due to failures. For example, if signature verification failed, none of the proposals offered were acceptable or decryption failed. This exchange is normally associated with an SA that was negotiated in Phase 2.

The other mode is new group mode, which is used to negotiate private groups for Diffie-Hellman exchanges. Although protected by a Phase 1 exchange, this is not part of a Phase 2 exchange.

The IKE mechanism is quite efficient in that it is able to negotiate many security associations with relatively few messages. With a single Phase 1 negotiation, multiple Phase 2 negotiations can occur. And within a single Phase 2 negotiation, multiple security associations can be negotiated so an implementation is able to use the same number of message flows to negotiate several security associations as it would need to negotiate one.

3.2.2 Key management requirements for IPSec

The IPSec protocols AH and ESP require that shared secrets are known to all participating parties that require either manual key entry or out-of-band key distribution. The problem is that keys can become lost, compromised or simply expire. Moreover, manual techniques do not scale when there are many security associations to manage (for example, for an extranet VPN). A robust key exchange mechanism for IPSec must therefore meet the following requirements:

- Independent of specific cryptographic algorithms
- Independent of a specific key exchange protocol
- Authentication of key management entities
- Establish SA over "unsecured" transport
- Efficient use of resources
- Accommodate on-demand creation of host and session-based SAs

The Internet Key Exchange (IKE) protocol has been designed to meet those requirements. It is based on the Internet Security Associations and Key Management Protocol (ISAKMP) framework and the Oakley key distribution protocol. IKE offers the following features:

- Key generation and identity authentication procedures
- Automatic key refresh
- Solves the "first key" problem
- Each security protocol (that is, AH, ESP) has its own Security Parameter Index (SPI) space
- Built-in protection
 - Against resource-clogging (denial-of-service) attacks
 - Against connection/session hijacking
- Perfect forward security (PFS)
- Two-phased approach
 - Phase 1 - Establish keys and SA for key exchanges
 - Phase 2 - Establish SAs for data transfer
- Implemented as application over UDP, port 500
- Supports host-oriented (IP address) and user-oriented (long-term identity) certificates
- Uses strong authentication for ISAKMP exchanges
 - Pre-shared keys
 - No actual keys are shared, only a token used to create keying material
 - Digital signatures (using either DSS or RSA methods)
 - Public key encryption (RSA and revised RSA)

- For performance reasons revised RSA uses a generated secret key instead of a public/private key during the second Phase 1 exchange.

The differences between those authentication methods is illustrated in Figure 26:

| Authentication method | How authentication is performed | Advantages | Disadvantages |
|--|---|--|---|
| <i>Pre-shared keys</i> | By creating hashes over exchanged information | ▸ Simple | ▸ Shared secret must be distributed out-of-band prior to IKE negotiations ▸ Can only use IP address as ID |
| <i>Digital signatures (RSA or DSS)</i> | By signing hashes created over exchanged information | ▸ Can use IDs other than IP address ▸ Partner certificates need not be available before IKE negotiations | ▸ Requires certificate operations (inline or out-of-band) |
| <i>RSA public key encryption</i> | By creating hashes over nonces encrypted with public keys | ▸ Better security by adding public key operation to DH exchange ▸ Allows ID protection with aggressive mode | ▸ Public keys (certificates) must be available before IKE negotiations ▸ Performance-intensive public key operations |
| <i>Revised RSA public key encryption</i> | Same as above | ▸ Same as above ▸ Fewer public key operations by using an intermediate secret | ▸ Public keys (certificates) must be available before IKE negotiations |

Figure 26. Comparing IKE authentication methods

As mentioned before, IKE requires two phases be completed before traffic can be protected with AH and/or ESP.

3.2.3 IKE Phase 1 overview

During Phase 1, the partners exchange proposals for the ISAKMP SA and agree on one. This contains specifications of authentication methods, hash functions and encryption algorithms to be used to protect the key exchanges. The partners then exchange information for generating a shared master secret:

- Cookies that also serve as SPIs for the ISAKMP SA
- Diffie-Hellman values
- Nonces (random numbers)
- Optionally exchange IDs when public key authentication is used

Both parties then generate keying material and shared secrets before exchanging additional authentication information.

Note: When all goes well, both parties derive the same keying material and actual encryption and authentication keys without ever sending any keys over the network.

3.2.4 IKE Phase 2 overview

During Phase 2, the partners exchange proposals for protocol SAs and agree on one. This contains specifications of authentication methods, hash functions and encryption algorithms to be used to protect packets using AH and/or ESP. To

generate keys, both parties use the keying material from a previous Phase 1 exchange and they can optionally perform an additional Diffie-Hellman exchange for PFS.

The Phase 2 exchange is protected by the keys that have been generated during Phase 1, which effectively ties a Phase 2 to a particular Phase 1. However, you can have multiple Phase 2 exchanges under the same Phase 1 protection to provide granular protection for different applications between the same two systems. For instance, you may want to encrypt FTP traffic with a stronger algorithm than Telnet, but you want to refresh the keys for Telnet more often than those for FTP.

Systems can also negotiate protocol SAs for third-parties (proxy negotiation) which is used to automatically create tunnel filter rules in security gateways.

3.2.5 ISAKMP message structure

ISAKMP defines a very flexible method of building messages that can be adapted to almost any type of service, not just IPsec. ISAKMP messages are very modular in that all components are contained in various types of payloads. Currently there are 14 payload types defined:

- Security Association Payload
- Proposal Payload
- Transform Payload
- Key Exchange Payload
- Identification Payload
- Certificate Payload
- Certificate Request Payload
- Hash Payload
- Signature Payload
- Nonce Payload
- Notification Payload
- Delete Payload
- Vendor ID Payload

These payloads are the basic building blocks of an ISAKMP message. Each payload has a generic header indicating what the next payload is and the length of the payload. This gives the ability to chain payloads together and to nest payloads within another payload.

The following example shows the payload structure of message 1 of an aggressive mode exchange with pre-shared keys where two transforms are proposed.

ISAKMP Header

SA Payload, (next payload = Key Exchange Payload)

Proposal Payload, (next payload = none)

Transform Payload, (next payload = Transform Payload)

Transform Payload, (next payload = none)
Key Exchange Payload, (next payload = Nonce Payload)
Nonce Payload, (next payload = Identification Payload)
Identification Payload, (next payload = none)

In addition to the payloads there is the ISAKMP Header which has the cookies to protect against denial-of-service attacks, the exchange type to indicate what type of flow is occurring (aggressive mode, for example), and a message ID to uniquely identify the message against an SA negotiation.

Payloads may also require certain attributes to be defined, and ISAKMP defines how data attributes are to be formatted within the payload.

How these payloads are coded or formatted are dependent on the services using ISAKMP. These definitions are known as the Domain of Interpretation (DOI) and also contain, for example, exchange types and naming conventions. Therefore, if IPsec is the service being used the IPsec DOI for ISAKMP defines how the payloads are coded.

In conjunction with the DOI there is also the concept of a situation. A situation allows a device to make policy decisions with regard to security services that are being negotiated. For example, the IPsec DOI defines three situations:

- Identity only
- Secrecy
- Integrity

The DOI is documented in RFC 2407. The detailed specifications of the protocol structures and message constructs are useful for implementors of IKE software as well as for system administrators who have to debug IKE errors. To discuss the details of this specification would be far beyond the scope of this document and you are therefore kindly referred to study the RFC on this subject.

3.2.6 General Phase 1 process

As described earlier, during this phase the ISAKMP SA is established, which provides a secure mechanism for subsequent ISAKMP messages to flow. This phase assumes no protection whatsoever and must establish a secure and private channel where no privacy currently exists.

The objective of this phase is to establish keying material that can be used to derive keys that encrypt and authenticate ISAKMP messages, and to derive keys that will be used for non-ISAKMP security associations. In addition to this, Phase 1 also authenticates the two parties involved in the exchange.

There are four methods of authentication available (see Figure 26 on page 47):

1. Digital signatures
2. Public key encryption
3. Revised public key encryption
4. Pre-shared keys

During Phase 1 only a single SA is negotiated, that is the ISAKMP SA. Only one proposal is offered always proposing Oakley as the key exchange method. Within that proposal multiple transforms can be offered which negotiate the following parameters:

- Authentication method
- Lifetime/lifesize of the SA
- Diffie-Hellman group
- Hash algorithm
- Encryption algorithm

Using main mode there are basically six message flows:

In the first two messages a proposal is offered by the initiator with one or more transforms, and the responder accepts the proposal with the chosen transform. Additionally, cookies are generated to incorporate into the ISAKMP header. The cookies ensure protection against denial of service attacks and the pair of cookies (the initiator's cookie and responder's cookie) identify the ISAKMP SA.

During the next two messages an exchange occurs as a Diffie-Hellman key exchange along with some nonces. After these two messages each party now has the keying material to generate keys for encryption and authentication of subsequent ISAKMP messages. Keying material is also derived which will be used to generate keys for other non-ISAKMP SAs in Phase 2. All ISAKMP messages from this point are then encrypted.

In the last two messages of Phase 1 authentication occurs. Depending on the chosen authentication method the appropriate messages and identities are exchanged here so that each party can authenticate the other.

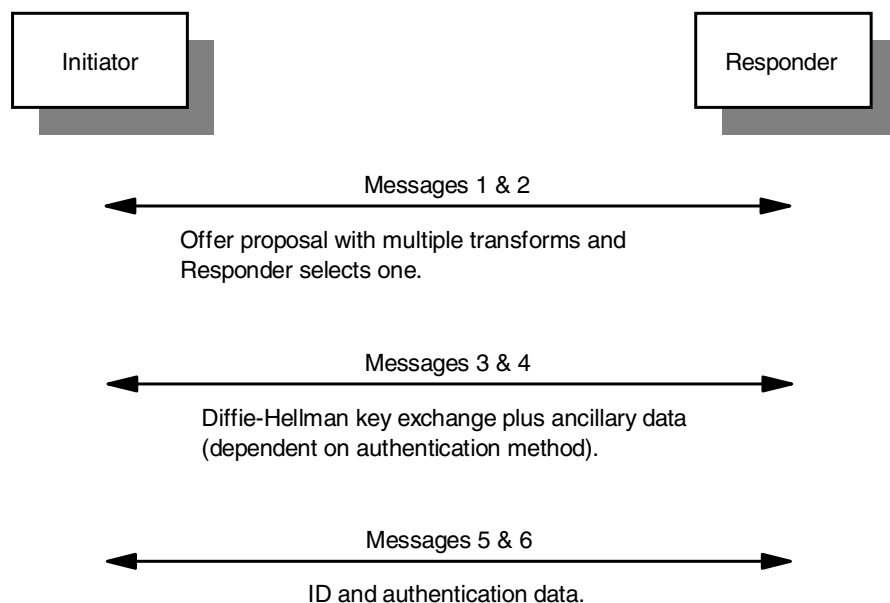


Figure 27. Basic Phase 1 main mode flows

In aggressive mode only a total of three messages are needed to establish the SA, however, the identities of the parties involved are revealed.

In the first message the initiator sends the proposal, Diffie-Hellman key exchange, nonce and ID to the responder.

At this point the responder can generate its nonce and Diffie-Hellman key exchange, and in conjunction with what it has just received from the initiator has all the components to generate the keying material. The responder on the second messages also sends the same information to the initiator so that it can generate the keying material, but also attaches the information to be able to authenticate it.

When the initiator receives the second message it is able to generate the keying material and authenticate the responder. All that is required is for the responder to authenticate the initiator. To achieve this the initiator sends the last Phase 1 message to the responder containing information that will enable the responder to authenticate the initiator.

As with main mode, the information that is exchanged to facilitate authentication is dependent on the negotiated authentication method.

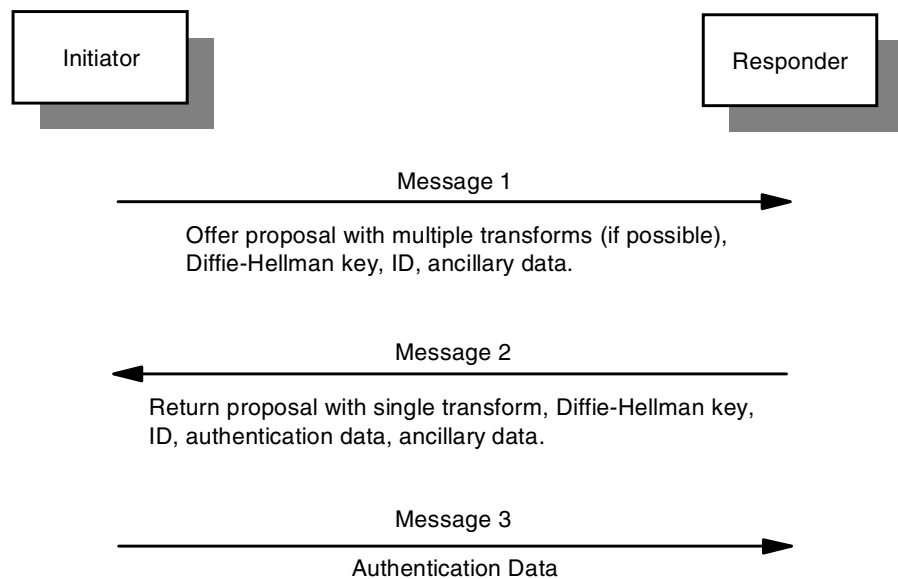


Figure 28. Basic Phase 1 aggressive mode flows

Note

The convention used in this chapter describes the information that is transferred or used in a particular function. Therefore, the same identifier used in this book may represent both the payload in one area or the actual value in another area.

For example, when a Diffie-Hellman public key is transferred, a Key Exchange payload containing the Diffie-Hellman public value is actually passed in the message, or when a nonce is transferred, a Nonce Payload containing the nonce is actually passed.

In the examples that show the inputs to a pseudo-random function, the actual value rather than the payload is normally used. For example, the actual value of a nonce is used as an input rather than the Nonce Payload with its associated headers.

Although the actual payload and information are strictly different entities, this chapter identifies them in the same way for readability. For example, an initiator's nonce contained in a Nonce payload is identified in the same way as the actual value being used as an input to a pseudo-random function, that is, $\text{Nonce}_{\text{initiator}}$.

3.2.6.1 Derivation of keying material

In all message flows keying material and hashing methods must be derived. The only difference is the algorithm that is used.

In main mode the keying material is derived after the exchange of messages 3 and 4, while the hash is used in the authentication process at messages 5 and 6. In aggressive mode the responder is able to derive the keying material after the receipt of message 1, and the initiator after the receipt of message 2. The hash is used in the authentication, which is used in message 2 and message 3.

When deriving keys and authenticating, a pseudo-random function is used. It generates a deterministic output that appears pseudorandom. Potentially the pseudo-random function could be negotiated, but the current standard does not define it. As such the HMAC version of the negotiated hash function is used, for example, HMAC-MD5. The function has two inputs, the key and message and is written in the form $\text{prf}(\text{key}, \text{message})$.

A value called SKEYID needs to be generated which is derived in different ways depending on the keying authentication method. This value is a string derived from secret information established during the exchange and is used to derive additional keying material. The following lists how SKEYID is determined for the different authentication methods:

- Digital signatures

$\text{prf}(\text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}}, \text{DH}_{\text{shared_secret}})$

The pseudo-random function is applied using concatenation of the nonces as the key, and the Diffie-Hellman shared secret as the message.

- Public key encryption

$\text{prf}(\text{hash}(\text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}}), \text{Cookie}_{\text{initiator}} + \text{Cookie}_{\text{responder}})$

The pseudo-random function is applied using a hash of the concatenation of the nonces as the key, and the concatenation of the cookies as the message. The hash function used here is the negotiated hash function in the SA.

- Pre-shared keys

$\text{prf}(\text{pre-shared-key}, \text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}})$

The pseudo-random function is applied using the pre-shared key as the key and the concatenation of the nonces as the message.

Once SKEYID has been derived the keying material can then be derived. Three sets of keying material are derived:

1. SKEYID_d. This is the keying material used to derive keys material for non-ISAKMP security associations, IPSec, for example. It is derived from the application of the pseudorandom function in the following manner:

$\text{prf}(\text{SKEYID}, \text{DH}_{\text{shared_secret}} + \text{Cookie}_{\text{initiator}} + \text{Cookie}_{\text{responder}} + 0)$

The pseudo-random function is applied using SKEYID as the key and the concatenation of the Diffie-Hellman shared secret, the two cookies and the single octet value "0".

2. SKEYID_a. This is keying material used by ISAKMP to generate keys to authenticate its messages. It is derived from the application of the pseudorandom function in the following manner:

$\text{prf}(\text{SKEYID}, \text{SKEYID}_d + \text{DH}_{\text{shared_secret}} + \text{Cookie}_{\text{initiator}} + \text{Cookie}_{\text{responder}} + 1)$

The pseudo-random function is applied using SKEYID as the key and the concatenation of the SKEYID_d, the Diffie-Hellman shared secret, the two cookies and the single octet value "1".

3. SKEYID_e. This is keying material used by ISAKMP to generate keys to encrypt its messages. It is derived from the application of the pseudo random in the following manner:

$\text{prf}(\text{SKEYID}, \text{SKEYID}_a + \text{DH}_{\text{shared_secret}} + \text{Cookie}_{\text{initiator}} + \text{Cookie}_{\text{responder}} + 2)$

The pseudo-random function is applied using SKEYID as the key and the concatenation of the SKEYID_d, the Diffie-Hellman shared secret, the two cookies and the single octet value "2".

How the keying material is used to derive the actual keys is dependent on the encryption algorithm that is being used. Detailed information can be found in the appropriate RFCs, however, an example will be described here. The encryption key used to encrypt ISAKMP messages using DES-CBC is derived from the first 8 bytes of SKEYID_e. The initialization vector that is to be used with the encryption (for use in protecting Phase 1 messages) is derived from a hash of the concatenation of the initiator's public Diffie-Hellman value and responder's public Diffie-Hellman value, using the negotiated hash function, that is:

$\text{hash}(\text{DH}_{\text{initiator_public_value}} + \text{DH}_{\text{responder_public_value}})$

3.2.6.2 Derivation of hashes for authentication

During the authentication process the initiator and responder have to derive hash values. The initiator needs to derive the value HASH_I by:

$$\text{prf}(\text{SKEYID}, \text{DH}_{\text{initiator_public_value}} + \text{DH}_{\text{responder_public_value}} + \text{Cookie}_{\text{initiator}} + \text{Cookie}_{\text{responder}} + \text{SA}_{\text{initiator}} + \text{ID}_{\text{initiator}})$$

This is the application of the pseudo-random function using SKEYID as the key and the concatenation of the initiator's Diffie-Hellman public value, the responder's Diffie-Hellman public value, the initiator's cookie, the responder's cookie, the whole SA payload (including all proposals and transforms) that was offered originally by the initiator and the complete ID payload of the initiator, as the message.

The responder needs to derive the value HASH_R by:

$$\text{prf}(\text{SKEYID}, \text{DH}_{\text{responder_public_value}} + \text{DH}_{\text{initiator_public_value}} + \text{Cookie}_{\text{responder}} + \text{Cookie}_{\text{initiator}} + \text{SA}_{\text{initiator}} + \text{ID}_{\text{responder}})$$

This is the application of the pseudo-random function using SKEYID as the key and the concatenation of the responder's Diffie-Hellman public value, the initiator's Diffie-Hellman public value, the responder's cookie, the initiator's cookie, the whole SA payload (including all proposals and transforms) that was offered originally by the initiator and the complete ID payload of the initiator, as the message.

How HASH_I and HASH_R are used for authentication is dependent on the authentication process. If digital signatures are used, HASH_I and HASH_R are signed, and that signature is passed to the other party to be verified. While using public key encryption and pre-shared keys, the respective hash values are produced and passed to the other party where it is verified. Production of the correct hash value directly authenticates the other party in the public key encryption and pre-shared key authentication methods.

3.2.6.3 Phase 1 message flows - pre-shared keys

The following table shows the message flows when pre-shared key authentication is used in main mode:

Table 5. IKE Phase 1 - main mode exchange using pre-shared keys

| Initiator | | Responder |
|--|--------|--|
| ISAKMP_Header _{main_mode} SA _{multiple_transforms} | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{main_mode} SA _{single_transform} Note the transform that is returned would be the chosen proposal with pre-shared key authentication and other acceptable parameters. |
| ISAKMP_Header _{main_mode} DH _{initiator_public_value} Nonce _{initiator} | 3 ---> | |
| | <--- 4 | ISAKMP_Header _{main_mode} DH _{responder_public_value} Nonce _{responder} |
| ISAKMP_Header _{main_mode} (ID _{initiator} HASH_I) ^{Key_SKEYID_e} | 5 ---> | |

| Initiator | | Responder |
|-----------|--------|---|
| | <--- 6 | ISAKMP_Header _{main_mode} (ID _{responder} , HASH_R) ^{Key_SKEYID_e} |

Note

The whole ISAKMP payload in messages 5 and 6 (shown in the table above in italics) is encrypted with the key derived from SKEYID_e.

The following table shows the message flows when pre-shared key authentication is used in aggressive mode:

Table 6. IKE Phase 1 - aggressive mode exchange using pre-shared keys

| Initiator | | Responder |
|---|--------|---|
| ISAKMP_Header _{aggressive_mode} SA _{multiple_transforms} DH _{initiator_public_value} Nonce _{initiator} ID _{initiator} Only one Diffe-Helman group can be offered since the first Diffe-Helman value is sent in message 1. | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{aggressive_mode} SA _{single_transform} DH _{responder_public_value} Nonce _{responder} ID _{responder} HASH_R Note the transform that is returned would be the chosen proposal with pre-shared key authentication and other acceptable parameters. |
| ISAKMP_Header _{aggressive_mode} HASH_I | 3 ---> | |

With main mode the ID is exchanged only in messages 5 and 6. With pre-shared key authentication the identity of the party must be known before this so that HASH_I and HASH_R can be computed. Therefore, only the IP address can be used to identify the peer if main mode is going to be used.

With aggressive mode this does not exist since the ID is exchanged as part of the first messages.

3.2.6.4 Phase 1 message flows - digital signatures

The following table shows the message flows when digital signature authentication is used in main mode:

Table 7. IKE Phase 1 - main mode exchange using digital signatures

| Initiator | | Responder |
|--|--------|---|
| ISAKMP_Header _{main_mode} SA _{multiple_transforms} | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{main_mode} SA _{single_transform} Note the transform that is returned would be the chosen proposal with digital signature authentication and other acceptable parameters. |
| ISAKMP_Header _{main_mode} DH _{initiator_public_value} Nonce _{initiator} Certificate_Request | 3 ---> | |
| | <--- 4 | ISAKMP_Header _{main_mode} DH _{responder_public_value} Nonce _{responder} Certificate_Request |
| ISAKMP_Header _{main_mode} <i>(ID_{initiator}</i> <i>Certificate_{initiator}</i> <i>Signature_{initiator})</i> Key_SKEYID_e | 5 ---> | |
| | <--- 6 | ISAKMP_Header _{main_mode} <i>(ID_{responder}</i> <i>Certificate_{responder}</i> <i>Signature_{responder})</i> Key_SKEYID_e |

Note

The whole ISAKMP payload in messages 5 and 6 (shown in the table above in italics) is encrypted with the key derived from SKEYID_e.

The following table shows the message flows when digital signature authentication is used in aggressive mode.

Table 8. IKE Phase 1 - aggressive mode exchange using digital signatures

| Initiator | | Responder |
|--|--------|---|
| ISAKMP_Header _{aggressive_mode} SA _{multiple_transforms} DH _{initiator_public_value} Nonce _{initiator} ID _{initiator} Certificate_Request Only one Diffie-Hellman group can be offered since the first Diffe-Helman value is sent in message 1. | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{aggressive_mode} SA _{single_transform} DH _{responder_public_value} Nonce _{responder} ID _{responder} Certificate _{responder} Signature _{responder} Certificate_Request Note the transform that is returned would be the chosen proposal with digital signature authentication and other acceptable parameters. |
| ISAKMP_Header _{aggressive_mode} Certificate _{initiator} Signature _{initiator} | 3 ---> | |

When digital signatures are used there will normally be a requirement to transfer certificates. It is a requirement that the transfer of certificates does not increase the number of message flows in the exchange. The tables above show when the certificate requests and actual certificates flow during the exchange. If the certificates have already been acquired by some other means then the certificate request payload and certificate payload would not be exchanged. IKE does not specify how these certificates are to be acquired, potentially an online method like PKIX could be used. Almost all current implementations require the transfer of certificates during the ISAKMP exchange process.

3.2.6.5 Phase 1 message flows - public key encryption

The following table shows the message flows when public key encryption authentication is used in main mode:

Table 9. IKE Phase 1 - main mode exchange using public key encryption

| Initiator | | Responder |
|---|--------|-----------|
| ISAKMP_Header _{main_mode} SA _{multiple_transforms} | 1 ---> | |

| Initiator | | Responder |
|---|--------|---|
| | <--- 2 | ISAKMP_Header _{main_mode} SA _{single_transform} Note the transform that is returned would be the chosen proposal with public key encryption authentication and other acceptable parameters. |
| ISAKMP_Header _{main_mode} DH _{initiator_public_value} <i>(ID_{initiator})^{PK_Responder}</i> <i>(Nonce_{initiator})^{PK_Responder}</i> | 3 ---> | |
| | <--- 4 | ISAKMP_Header _{main_mode} DH _{responder_public_value} <i>(ID_{responder})^{PK_Initiator}</i> <i>(Nonce_{responder})^{PK_Initiator}</i> |
| ISAKMP_Header _{main_mode} <i>(HASH_I)^{Key_SKEYID_e}</i> | 5 ---> | |
| | <--- 6 | ISAKMP_Header _{main_mode} <i>(HASH_R)^{Key_SKEYID_e}</i> |

Note

The ID payload and the Nonce payload in message 3 (shown in the table above in italics) are encrypted with the responder's public key.

The ID payload and the Nonce payload in message 4 (shown in the table above in italics) are encrypted with the initiator's public key.

The whole ISAKMP payload in messages 5 and 6 (shown in the table above in italics) is encrypted with the key derived from SKEYID_e.

The following table shows the message flows when public key encryption authentication is used in aggressive mode:

Table 10. IKE Phase 1 - aggressive mode exchange using public key encryption

| Initiator | | Responder |
|---|--------|--|
| ISAKMP_Header _{aggressive_mode} SA _{multiple_transforms} DH _{initiator_public_value} <i>(ID_{initiator})^{PK_Responder}</i> <i>(Nonce_{initiator})^{PK_Responder}</i> Note only one Diffie-Hellman group can be offered since the first Diffie-Hellman value is sent in message 1. Public key encryption authentication is the only authentication method that can be offered since the message already contains information encrypted with the public key. | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{aggressive_mode} SA _{single_transform} DH _{responder_public_value} <i>(ID_{responder})^{PK_Initiator}</i> <i>(Nonce_{responder})^{PK_Initiator}</i> HASH_R Note the transform that is returned would be the chosen proposal with public key encryption authentication and other acceptable parameters. |
| ISAKMP_Header _{aggressive_mode} HASH_I | 3 ---> | |

Note

The ID payload and the Nonce payload in message 1 (shown in the table above in italics) are encrypted with the responder's public key.

The ID payload and the Nonce payload in message 2 (shown in the table above in italics) are encrypted with the initiator's public key.

Notice that with this method of authentication an aggressive mode exchange can occur without having to reveal the identities in the clear. This is the main advantage of using public key encryption. Another advantage is that additional security is incorporated in that an attacker has to break the Diffie-Hellman exchange as well as the RSA public key encryption.

The disadvantage is that there is no nonrepudiation, that is, there is nothing in the flows that can prove that either party participated in the exchange, whether in main or aggressive mode. This is because each party can reconstruct all the messages. For example, let us take message 2 in aggressive mode that was sent by the responder. If you examine the contents in this message there is nothing there that cannot be reconstructed by the initiator, since the encrypted fields used the initiator's public key as the key, which obviously could have been constructed by the initiator. If you look at the equivalent message with digital signatures, the responder had to put a signature in the message. If this signature is valid, only the responder could have produced it and therefore the exchange cannot be repudiated.

This method of authentication assumes that each party already has the public key of the other side. There may be cases when the responder has multiple public keys. If this is the case the initiator must also include a hash of the responder's certificate containing the public key being used. This will allow the responder to determine which public key the initiator used. This hash is sent as part of message 3 in main mode or message 1 in aggressive mode.

3.2.6.6 Phase 1 message flows - revised public key encryption

This authentication method was incorporated to reduce the number of asymmetric key operations (encryption/decryption with public key cryptography), as they are significantly more expensive with regard to the processing power. The original public key encryption authentication method requires that each party perform four public key operations (two encryptions and two decryptions). The revised method will cut that in half.

The following table shows the message flows when revised public key encryption authentication is used in main mode:

Table 11. IKE Phase 1 - main mode exchange using revised public key encryption

| Initiator | | Responder |
|--|--------|---|
| ISAKMP_Header _{main_mode} SA _{multiple_transforms} | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{main_mode} SA _{single_transform} Note the transform that is returned would be the chosen proposal with revised public key encryption authentication and other acceptable parameters. |
| ISAKMP_Header _{main_mode} (Nonce _{initiator}) ^{PK_Responder} (DH _{initiator_public_value}) ^{KE_Initiator} (ID _{initiator}) ^{KE_Initiator} | 3 ---> | |

| Initiator | | Responder |
|---|--------|---|
| | <--- 4 | $ISAKMP_Header_{main_mode}$ $(Nonce_{responder})^{PK_Initiator}$ $(DH_{responder_public_value})^{KE_Responder}$ $(ID_{responder})^{KE_Responder}$ |
| $ISAKMP_Header_{main_mode}$ $(HASH_I)^{Key_SKEYID_e}$ | 5 ---> | |
| | <--- 6 | $ISAKMP_Header_{main_mode}$ $(HASH_R)^{Key_SKEYID_e}$ |

Note

The Nonce payload in message 3 (shown in Table 11 on page 60 in italics) is encrypted with the responder's public key.

The initiator's Diffie-Hellman public value and the initiator's ID in message 3 (shown in Table 11 on page 60 in italics) are encrypted with the initiator's derived symmetric key KE_Initiator.

The Nonce payload in message 4 (shown in Table 11 on page 60 in italics) is encrypted with the initiator's public key.

The responder's Diffie-Hellman public value and the responder's ID in message 3 (shown in Table 11 on page 60 in italics) are encrypted with the responder's derived symmetric key KE_Responder.

The whole ISAKMP payload in messages 5 and 6 (shown in Table 11 on page 60 in italics) is encrypted with the key derived from SKEYID_e.

The following table shows the message flows when revised public key encryption authentication is used in aggressive mode:

Table 12. IKE Phase 1 - aggressive mode exchange using revised public key encryption

| Initiator | | Responder |
|--|--------|---|
| ISAKMP_Header _{aggressive_mode} SA _{multiple_transforms} Nonce _{initiator} ^{PK_Responder} (DH _{initiator_public_value}) ^{KE_Initiator} (ID _{initiator}) ^{KE_Initiator} Note only one Diffie-Hellman group can be offered since the first Diffie-Hellman value is sent in message 1. The revised public key authentication method is the only authentication method that can be offered since information is sent encrypted with the public key and symmetric key. The hash and encryption algorithm cannot be negotiated since the message already contains information encrypted with the symmetric key, with a key derived from the hash algorithm that will be used. | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{aggressive_mode} SA _{single_transform} (Nonce _{responder}) ^{PK_Initiator} (DH _{responder_public_value}) ^{KE_Responder} (ID _{responder}) ^{KE_Responder} HASH_R Note the transform that is returned would be the chosen proposal with revised public key encryption authentication and other acceptable parameters. |
| ISAKMP_Header _{aggressive_mode} HASH_I | 3 ---> | |

Note

The Nonce payload in message 1 (shown in Table 12 on page 62 in italics) is encrypted with the responder's public key.

The initiator's Diffie-Hellman public value and the initiator's ID in message 1 (shown in Table 12 on page 62 in italics) are encrypted with the initiator's derived symmetric key KE_Initiator.

The Nonce payload in message 2 (shown in Table 12 on page 62 in italics) is encrypted with the initiator's public key.

The responder's Diffie-Hellman public value and the responder's ID in message 2 (shown in Table 12 on page 62 in italics) are encrypted with the responder's derived symmetric key KE_Responder.

As you can see from the flows above only two asymmetric key operations are needed, and the other components are encrypted using symmetric key operations with the keys KE_Initiator and KE_Responder. The keying material to produce these keys:

- Keying material for KE_Initiator

$\text{prf}(\text{Nonce}_{\text{initiator}}, \text{Cookie}_{\text{initiator}})$

The pseudo-random function is applied using the initiator's nonce as the key, and the initiator's cookie as the message.

- Keying material for KE_Responder

$\text{prf}(\text{Nonce}_{\text{responder}}, \text{Cookie}_{\text{responder}})$

The pseudo-random function is applied using the responder's nonce as the key, and the responder's cookie as the message.

Remember the cookies are contained in the ISAKMP header and are generated before each party sends its first message. The pair of cookies identify the ISAKMP security association.

The keys are derived from the keying material in exactly the same way described earlier in 3.2.6.1, "Derivation of keying material" on page 52, that is, it is dependent on the encryption algorithm. If a CBC algorithm is used the initialization vector will be set to zero.

If the responder has a variety of public keys to use, the hash of the certificate containing the public key that is being used can be sent in the same manner as in the original public key encryption authentication method.

The initiator's certificate can be sent to allow the responder to use the correct public key of the initiator. If this is done it is sent in message 3 with main mode or message 1 with aggressive mode. The certificate, however, is encrypted using KE_initiator.

3.2.7 General Phase 2 process

Phase 2 is where the SA is negotiated on behalf of other services, for example, IPSec. It requires that Phase 1 be successfully completed since it uses the ISAKMP SA established in Phase 1 to protect all Phase 2 messages.

The objective of this phase is to refresh keying material established in Phase 1, which can be used to derive keys needed required by the service. For example, these keys could be used to encrypt and authenticate messages.

Although perfect forward security (PFS) must be supported, its use is optional. If PFS is required another Diffie-Hellman exchange is performed to achieve this.

Phase 2 can negotiate multiple security associations in a single exchange. This is achieved by incorporating multiple SA payloads into the message.

In each of the three messages a different hash is passed to guarantee the two parties' identities. Nonces are exchanged in messages 1 and 2, and the Diffie-Hellman exchange occurs in messages 1 and 2 if PFS is required. Additionally, the SA is also offered in message 1, and the chosen proposal is returned in message 2.

The following table shows the message flows with quick mode:

Table 13. IKE Phase 2 - quick mode exchange

| Initiator | | Responder |
|--|--------|---|
| ISAKMP_Header _{quick_mode} <i>(HASH_1</i> <i>SA_{multiple_transforms}</i> <i>Nonce_{initiator}</i> <i>DH_Temp_{initiator_public_value}</i> <i>ID_Client_{initiator}</i> <i>ID_Client_{responder})Key_SKEYID_e</i> | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{quick_mode} <i>(HASH_2</i> <i>SA_{single_transform}</i> <i>Nonce_{responder}</i> <i>DH_Temp_{initiator_public_value}</i> <i>ID_Client_{initiator}</i> <i>ID_Client_{responder})Key_SKEYID_e</i> |
| ISAKMP_Header _{quick_mode} <i>(HASH_3)Key_SKEYID_e</i> | 3 ---> | |

Note

The whole ISAKMP payload in messages 2 and 3 (shown in Table 13 in italics) is encrypted with the key derived from SKEYID_e.

The IDs of the negotiated SA in Phase 2 are normally the IP addresses of the ISAKMP peers, and therefore, IDs do not need to be exchanged. There may be cases where ISAKMP is acting as a client negotiator on behalf of another party. In these situations the identities of the other parties must be passed in the exchange as shown above in messages 1 and 2 (ID_Client_{initiator} and

ID_Client_{responder}). This would normally be the case for IPsec in gateway implementations since the services that want the IPsec security are the various IP addresses and subnets attached to the routers.

Although PFS must be supported it is not mandatory that it be used. If PFS is not required the flows are the same except the key exchange payloads carrying the temporary Diffie-Hellman public values in messages 2 and 3 are not exchanged.

PFS is achieved by incorporating a temporary Diffie-Hellman exchange. It is important that the Diffie-Hellman values that are generated are strictly temporary and only exist during this exchange. The value generated here must have absolutely no relationship with other Diffie-Hellman values in other exchanges, for example, the Diffie-Hellman values used during Phase 1.

During the flows three different hash values are derived to authenticate the exchange:

- Hash_1

$\text{prf}(\text{SKEYID_a}, \text{Message_ID} + \text{Everything_after_Hash_1_in_Message_1})$

The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the Message_ID and everything after Hash_1 in message 1, as the message.

- Hash_2

$\text{prf}(\text{SKEYID_a}, \text{Message_ID} + \text{Nonce}_{\text{initiator}} + \text{Everything_after_Hash_2_in_Message_2})$

The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the Message_ID, initiator's nonce and everything after Hash_2 in message 2, as the message.

- Hash_3

$\text{prf}(\text{SKEYID_a}, 0 + \text{Message_ID} + \text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}})$

The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the single octet value "0", the Message_ID, the initiator's nonce and the responder's nonce, as the message.

SKEYID_a was generated during Phase 1 as described in 3.2.6.1, "Derivation of keying material" on page 52. The message ID is a unique identifier generated by the initiator during Phase 2 negotiations and is contained in the ISAKMP header. *Everything_after_Hash_x_in_Message_x* includes the Diffie-Hellman key exchange payload and client identity payloads if they exist.

The keying material that is derived for the SA being negotiated in Phase 2 if PFS was not required is:

$\text{prf}(\text{SKEYID_d}, \text{Protocol} + \text{SPI} + \text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}})$

The pseudo-random function is applied using SKEYID_d as the key and a concatenation of the Protocol, the SPI, the initiator's nonce and the responder's nonce, as the message.

The keying material that is derived for the SA being negotiated in Phase 2 if PFS was required is:

$$\text{prf}(\text{SKEYID_d}, \text{DH_Temp}_{\text{shared_secret}} + \text{Protocol} + \text{SPI} + \text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}})$$

The pseudo-random function is applied using SKEYID_d as the key and a concatenation of the temporary Diffie-Hellman shared secret, the Protocol, the SPI, the initiator's nonce and the responder's nonce, as the message.

The Protocol is carried in the proposal payload and indicates the protocol being negotiated, for example, IPsec ESP. The SPI (Security Parameter Index) is a locally generated number, also carried in the proposal payload, that identifies the SA. Note that in a single SA negotiation, two SAs are generated, one for each direction, which implies two SPIs. Therefore, there are also two keys that are generated, one for each direction. The keying material for each side will differ for each side of the SA because a different SPI value will be used in the pseudo-random function. The SA from the initiator to responder will use the SPI generated by the responder, while the SA from the responder to the initiator will use the SPI generated by the initiator.

3.2.8 Summary of successful IKE negotiation

Once Phase 1 and Phase 2 exchanges have successfully completed, the peers have reached a state where they can start to protect traffic with IPsec according to applicable policies and traffic profiles. They have done all of the following:

1. Agreed on a proposal to authenticate each other and to protect future IKE exchanges
2. Exchanged enough secret and random information to create keying material for later key generation
3. Mutually authenticated the exchange
4. Agreed on a proposal to authenticate and protect data traffic with IPsec
5. Exchanged further information to generate keys for IPsec protocols
6. Finally confirmed the exchange and generated all necessary keys

This is illustrated in Figure 29 on page 67.

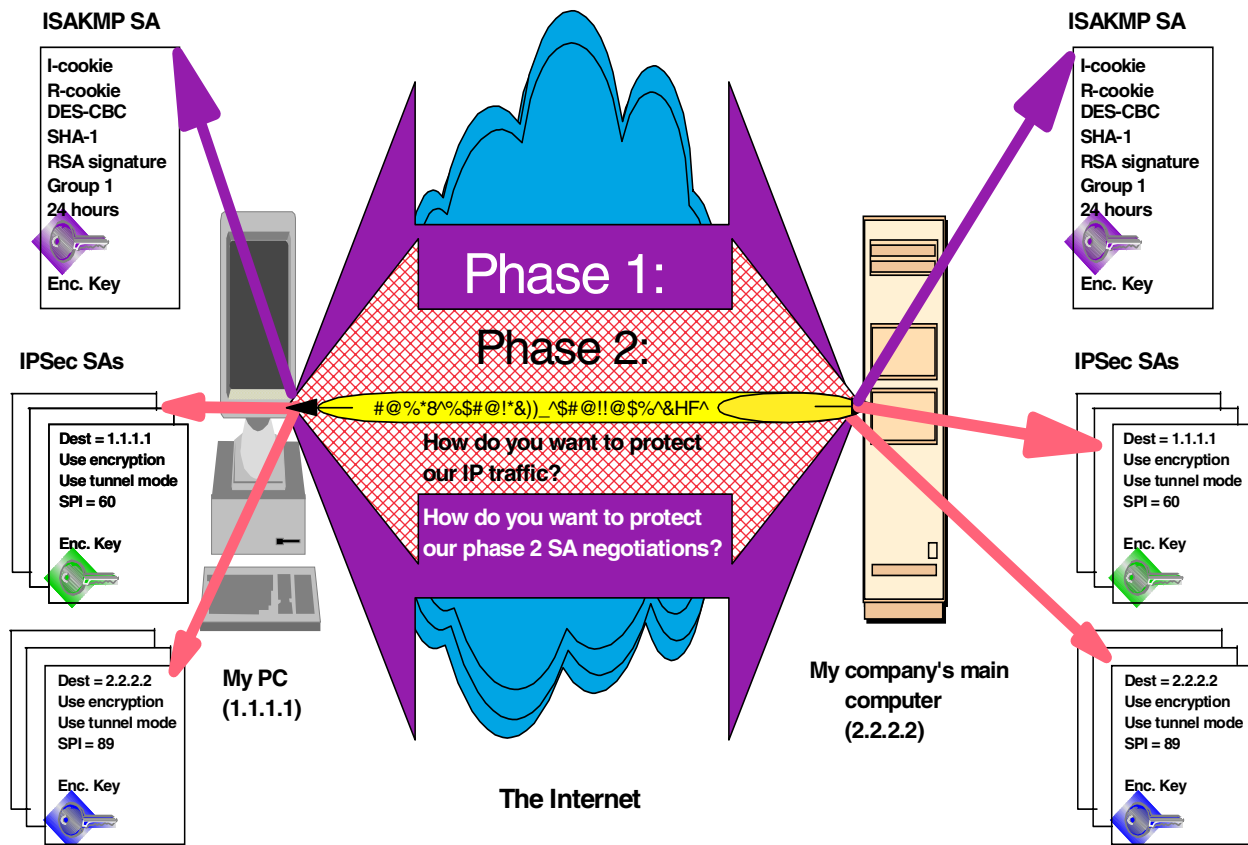


Figure 29. IKE negotiation summary

3.2.9 Optional IKE exchanges

Apart from main, aggressive and quick mode, IKE offers additional functionality with the new group and informational modes. However, the actual product implementation of those modes are up to the vendor.

3.2.9.1 New group mode

IKE defines four Oakley groups with which to do a Diffie-Hellman exchange. The first group must be supported in all implementations while the others are optional. IKE defines a way to negotiate other groups if required.

Note that this exchange can only occur after a successful Phase 1 exchange, however, group mode is *not* a Phase 2 exchange.

The following table describes the flows for a new group mode exchange:

Table 14. IKE Phase 2 - New group mode exchange

| Initiator | | Responder |
|---|--------|--|
| ISAKMP_Header _{group_mode} (HASH_1 SA _{multiple_transforms}) ^{Key_SKEYID_e} | 1 ---> | |
| | <--- 2 | ISAKMP_Header _{group_mode} (HASH_2 SA _{single_transform}) ^{Key_SKEYID_e} |

Note

The whole ISAKMP payload in messages 1 and 2 (shown in Table 14 on page 67 in italics) is encrypted with the key derived from SKEYID_e.

During the flows two different hash values are derived to authenticate the exchange:

- Hash_1

$\text{prf}(\text{SKEYID_a}, \text{Message_ID} + \text{SA}_{\text{multiple_transforms}})$

The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the Message_ID and the SA with all the proposals offered, as the message.

- Hash_2

$\text{prf}(\text{SKEYID_a}, \text{Message_ID} + \text{SA}_{\text{single_transform}})$

The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the Message_ID and SA reply, as the message.

3.2.9.2 Informational messages

Informational exchanges are used to convey status information to the other party, for example, to let the other party know that decryption was not successful. This exchange can only occur after a successful Phase 1 exchange, however, it is associated with a particular Phase 2 exchange.

The following table describes the flows for an informational mode exchange:

Table 15. IKE Informational Exchange

| Initiator | | Responder |
|--|--------|-----------|
| <i>ISAKMP_Header_{informational_mode} (HASH_1 Notify_or_Delete)_{Key_SKEYID_e}</i> | 1 ---> | |

Note

The whole ISAKMP payload in message 1 (shown in Table 15 in italics) is encrypted with the key derived from SKEYID_e.

During the flow HASH_1 is derived to authenticate the exchange:

$\text{prf}(\text{SKEYID_a}, \text{Message_ID} + \text{Notify_or_Delete})$

The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the Message_ID and the SA with all the proposals offered, as the message.

3.3 IPSec/IKE system processing

It is important to understand how systems process datagrams when it comes to using IPSec and IKE. With IP security in place, datagrams can no longer be

simply processed, forwarded or discarded but must be subject to a security policy to determine if additional IPSec processing is required and when it has to occur. Even though there are slight differences among platforms as to how they implement IPSec on their particular IP stacks, the general principle of IPSec processing for host and gateway systems can be summarized as follows:

3.3.1 Outbound IPSec processing for host systems

With IPSec active, any outbound packet is subject to the Security Policy Database (SPD) to determine if IPSec processing is required or what else to do with the packet. If IPSec is required, the Security Associations Database (SAD) is searched for an existing security association (SA) for which the packet matches the profile. If that is not the case and IKE as well as on-demand outbound SAs are supported, a new IKE negotiation is started that ultimately results in the establishment of the desired SA(s) for this packet. Finally, IPSec is applied to the packet as required by the SA and the packet is delivered. This process is illustrated in Figure 30.

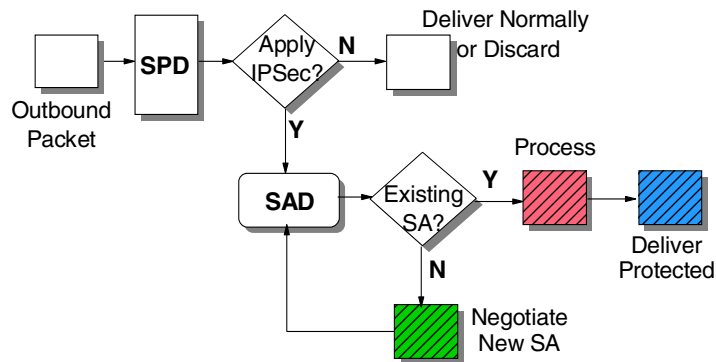


Figure 30. IPSec - outbound processing for host systems

Note

In general, the routing table is consulted to determine if the packet can be delivered at all. If no route is found, IPSec processing should not be performed but the user should be informed of this problem.

We are assuming, however, that host systems usually have a default router defined so that packets get sent in any case.

3.3.2 Inbound processing for host systems

With IPSec active, any inbound packet is subject to the SPD to determine if IPSec processing is required or what else to do with the packet. If IPSec is required, the SAD is searched for an existing security parameter index (SPI) to match the SPI value contained in the packet. If that is not the case, there are essentially two options:

1. Silently discard the packet (do not inform the sender but log the event if configured). This is the default action performed by most of today's IPSec implementations.

2. If IKE as well as on-demand inbound SAs are supported, a new IKE negotiation is started that ultimately results in the establishment of SA(s) to the sender of the original packet. In this case, it does not matter if the original packet was IPSec protected or in the clear, which only depends upon the local policy. However, it requires that the sender of the original packet respond to the IKE negotiations, and it means that packets are discarded until an SA is established.

Finally, IPSec is applied to the packet as required by the SA and the payload is delivered to the local process. This is illustrated in Figure 30.

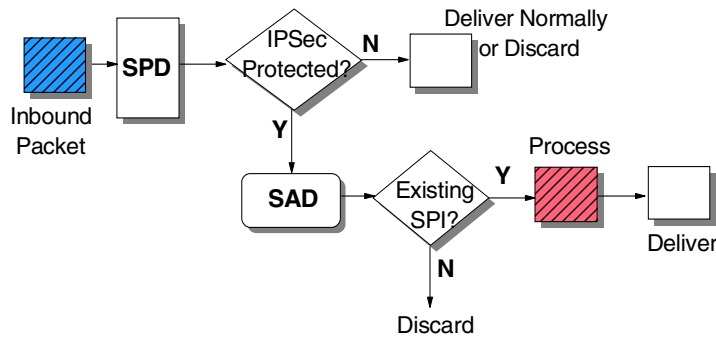


Figure 31. IPSec - inbound processing for host systems

3.3.3 Outbound processing for gateway systems

On a gateway system, any outbound packet is usually subject to the SPD of the secure interface to determine what to do with it. If the decision is to route the packet, the routing table is consulted to determine if the packet can be delivered at all. If no route is found, IPSec processing should not be performed, but the original sender may be informed of this problem using ICMP network unreachable messages.

We are assuming, however, that gateway systems either employ routing protocols or have a default router defined so that a successful routing decision can be made.

From this stage on, processing is essentially the same as on host systems. The packet is then forwarded to the SPD of a nonsecure interface to determine if IPSec processing is required or what else to do with the packet. If IPSec is required, the SAD is searched for an existing SA for which the packet matches the profile. If that is not the case and IKE as well as on-demand outbound SAs are supported, a new IKE negotiation is started that ultimately results in the establishment of the desired SA(s) for this packet. Finally, IPSec is applied to the packet as required by the SA and the packet is delivered. This process is illustrated in Figure 30 on page 69.

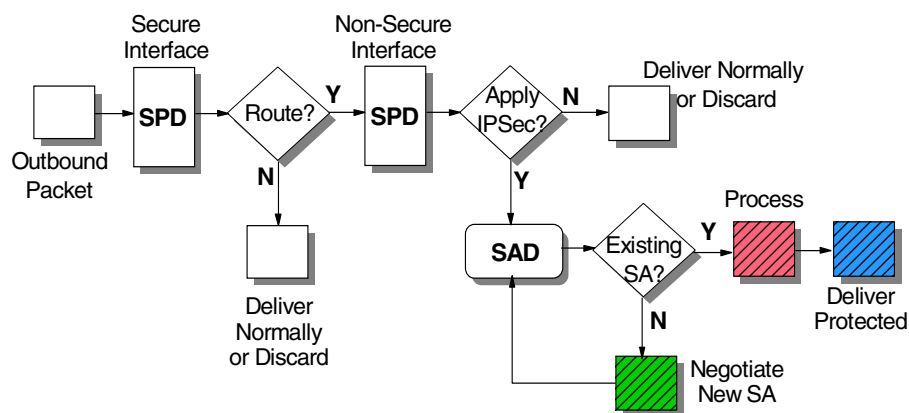


Figure 32. IPSec - outbound processing for gateway systems

3.3.4 Inbound processing for gateway systems

On a gateway system with IPSec active, any inbound packet is subject to the SPD to determine if IPSec processing is required or what else to do with the packet. If IPSec is required, the SAD is searched for an existing SPI to match the SPI value contained in the packet. If that is not the case, there are essentially two options:

1. Silently discard the packet (do not inform the sender but log the event if configured). This is the default action performed by most of today's IPSec implementations.
2. If IKE as well as on-demand inbound SAs are supported, a new IKE negotiation is started that ultimately results in the establishment of SA(s) to the sender of the original packet. In this case, it does not matter if the original packet was IPSec protected or in the clear, which only depends upon the local policy. However, it requires that the sender of the original packet respond to the IKE negotiations, and it means that packets are discarded until an SA is established.

Once the packet has been successfully processed by IPSec, which may be an iterative process for SA bundles, a routing decision has to be made as to what to do with the packet next. If the packet is destined to another host it is delivered over the appropriate interface according to the routing tables. If the packet is destined to the gateway itself, the payload is delivered to the local process. This is illustrated in Figure 30 on page 69.

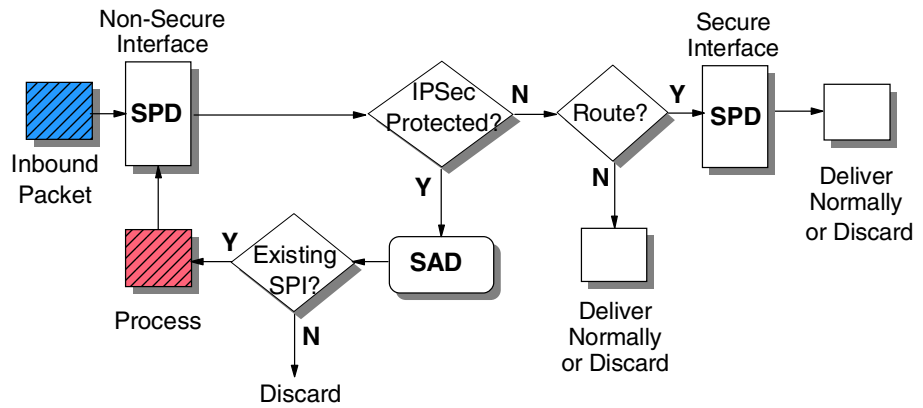


Figure 33. IPSec - inbound processing for gateway systems

Note

If the gateway receives a packet with IPSec applied in an iterated tunnel SA bundle, it only has to process the outer SA which is carried in a datagram destined to the gateway. The inner SA is carried in a datagram destined to another host and will therefore be forwarded by the gateway (provided the policy permits it), irrespective of its IPSec protection.

Chapter 4. Certificates and Public Key Infrastructures (PKIs)

A certificate is an electronic document that binds an entity's identity with its public key. A Public Key Infrastructure (PKI) is an infrastructure that deploys digital certificates. The following will describe the various components of certificates and PKIs.

4.1 Public key cryptography

Public key cryptography (also known as asymmetric cryptography) is a method of encryption where there are two keys involved. These two keys are mathematically related where one is the inverse of the other and are known as the private and public keys or key pair. If one encrypts some information with the public key, that information can only be decrypted with its private key. The converse also applies, that is, if some information is encrypted with the private key it can only be decrypted with its public key.

The public and private keys are generated at the same time. Once generated the private key leaves the entity that produced it only in certain circumstances, such as when a central authority generates, distributes and safeguards all keys for a PKI. The public key, however, is freely distributed to any device or location.

Public key cryptography has the advantage over secret key cryptography in that it allows the public distribution of the public key while still being able to maintain the security or confidentiality of information. If you wish to send information to a person all you have to do is encrypt the information with that person's public key (which is freely available) and send it to that person. That person can then decrypt the message with his or her private key. Even if the message is intercepted, an attacker would not be able to decrypt it because he or she does not have the private key.

With secret key cryptography the process is more difficult because both parties must have a common secret key which will be used to encrypt and decrypt the information. Before information can be transferred securely another secure method must be used to distribute the secret key.

The main disadvantage of public key cryptography is that it takes significantly more processing power to perform the encryption/decryption process. Therefore, a common implementation is to use public key cryptography to securely transmit a secret key, and it is the secret key that is used to encrypt and decrypt the information.

4.2 Digital certificates

There is a problem with using public key cryptography in that you cannot be confident of the authenticity of the public key. If the key was obtained from a public source it could have been forged or modified by an attacker. Digital certificates are used to solve this very problem. Note that the rest of this book will refer to digital certificates as simply certificates.

Certificates bind the identity of a person to his or her public key. The nature of a certificate is similar to that of a credit card. A credit card binds a person's identity

to a credit card number. When you wish to purchase something from a shop without cash, the shopkeeper will ask for your credit card and then perform a series of checks on it, such as:

- Examine the card to see if it is a forgery or has been tampered with
- Check if it was issued from an organization with whom the merchant has a relationship
- Check if the credit card has been revoked
- Confirm your identity by challenging you to write your signature

A certificate is an electronic document that has the same characteristics as those described above. In order for an electronic document to have these characteristics hashing and digital signatures are used.

Hashing is a mathematical function which summarizes a large piece of data into something small, for example, 128 bits. The hash function has certain characteristics:

1. If a single bit in the original message changes, on average, half the bits in the hash also change.
2. It is almost impossible to find two data streams that will provide the same hash value.
3. For a given hash value, it is almost impossible to determine the original message.

Hashes can be used to determine whether a document or data stream has been altered, whether intentionally by an attacker or inadvertently through transmission errors. The hash of a document simply needs to be sent with the original data stream. When the recipient receives the message and hash, he or she simply performs the same hash function on the message and compares that result with the one that was sent with the message. The problem now is that an attacker could intercept the message, modify it, perform a hash on the altered message and send the altered message and the new hash. This is where we have the concept of a digital signature.

A digital signature is simply the encryption of the hash with the sender's private key. The encrypted hash along with the original document is then sent to the recipient. The recipient performs the same hash function on the document, decrypts the hash that was sent with the sender's public key and compares the two results. If they are the same then the recipient is guaranteed that it was sent by the real sender and was not altered in any way in transit.

A certificate is simply a document that contains a person's identity and public key, and is digitally signed by a trusted organization, that is, a Certificate Authority (CA). A certificate has the same characteristics described earlier for a credit card:

- Tampering is prevented through the use of hashing.
- Forgery is prevented through the use of digital signatures.
- Certificates are issued by CAs, which the communicating parties trust, and therefore, trust certificates issued by that CA.
- Certificates which have been revoked can be checked by examining the Certificate Revocation Lists (CRLs) published by the CA.

- Your identity can be confirmed by the other party challenging you to encrypt a random message. If the public key contained in the certificate successfully decrypts the message, then you must be the same person as the one contained in the certificate.

Certificates can be used to determine the identity of a person or entity. This process is called authentication. When used in authentication the two parties typically exchange their certificates. Alternatively, you may go to a CA's repository to obtain the certificate. During authentication the CA does not have to be online. By examining the other party's certificate you are able to confirm his or her identity without any real-time interaction with the CA. A certificate contains a number of other items, but the essence has been described here.

4.3 Registration authority

The purpose of a CA is to issue certificates. To ensure the integrity of a PKI, the CA must initially validate the identity of an entity before it issues a certificate. For small implementations this process of validating the identity of person can be done by the CA itself. However, in large implementations this may not be practical nor will the required performance levels be met.

To implement large PKIs the validation step is delegated to Registration Authorities (RAs). Typically, RAs are distributed over a wide area to perform the validation. When an entity wishes to request a certificate, it must first generate a public and private key pair. The entity then submits the certificate request to the RA along with its public key. There the RA validates the identity of the person through any method it chooses. Once validated the RA requests a certificate from the CA on the person's behalf. Since the CA trusts all the RAs it has deployed, the CA does not need to validate the user but simply ensure that it is communicating with one of its authorized RAs. Once the CA receives the certificate request from one of its authorized RAs it issues the certificate containing the identity of the person and his or her public key.

The CA can also place the new certificate in a publicly available repository where any entity can request a copy of a certificate it issued. CRL is also published in this central repository.

The same process of requesting certificates is used for certificate renewal or certificate revocation.

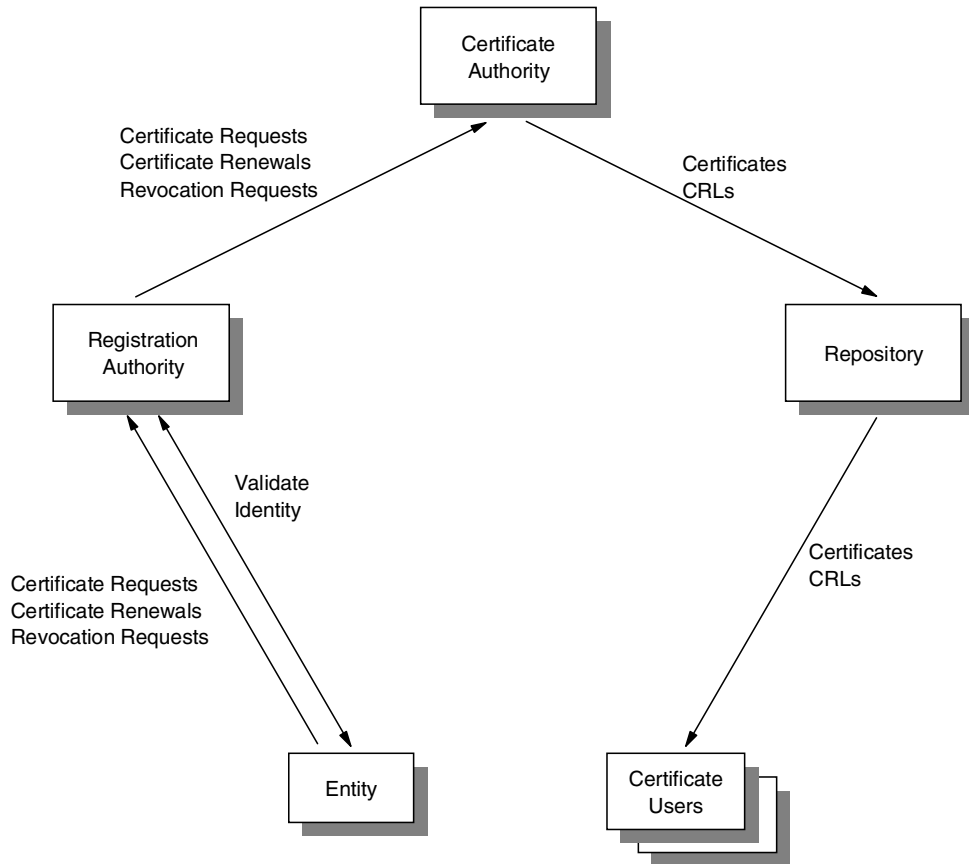


Figure 34. Relationship of the RA and CA

4.4 Multiple certificate authorities

In large implementations of PKIs, particularly worldwide implementations, it is not practical or possible to use a single CA. In these implementations multiple CAs must be used and a chain of trust must exist before entities will accept certificates from different CAs.

4.4.1 Single root CA

Let us first examine what is needed if there is only a single CA (see Figure 35 on page 77).

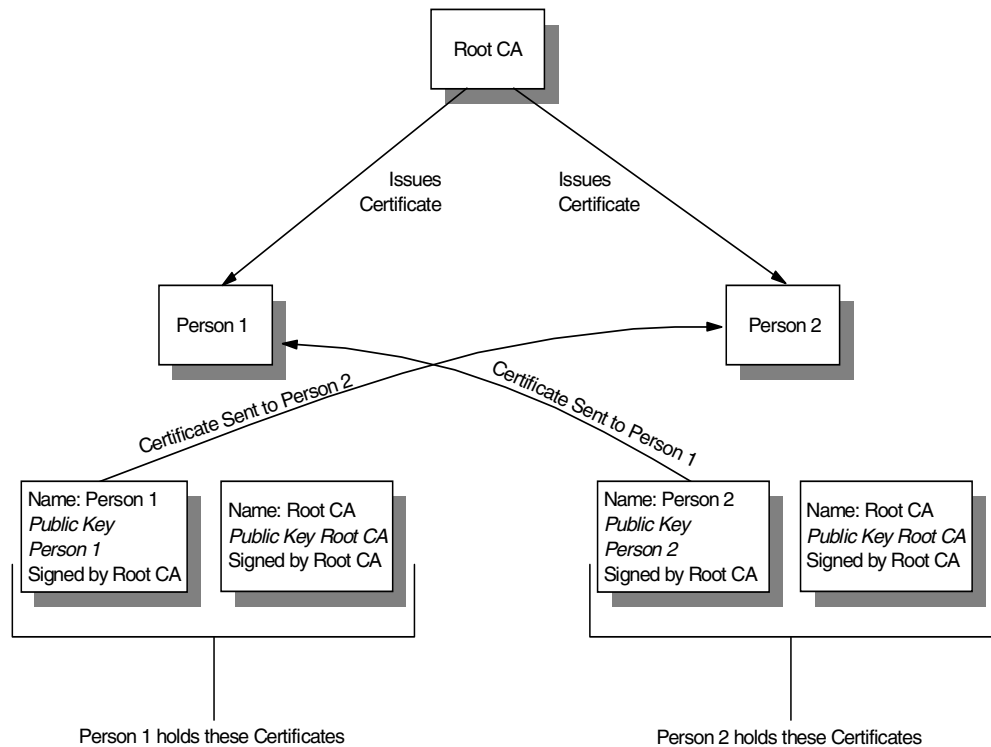


Figure 35. Single Root CA PKI

This scenario is the basic PKI infrastructure where there is a single CA issues all the certificates. Person 1 must hold all the relevant certificates so that he or she can authenticate Person 2 and vice versa. This assumes that the parties do not want to go through the process of requesting certificates from a CA or other repository. If two people wish to authenticate each other, each person must have the following certificates:

1. His or her own certificate, which was signed by the root CA.
2. The certificate of the root CA, which was self signed.

The first certificate is given to another person so that he or she can authenticate you. The second certificate is used so a person can validate a certificate that was given to him or her before trying authentication. If Person 1 wishes to authenticate Person 2 the following steps occur:

1. Person 2 sends his or her certificate to Person 1.
2. Person 1 checks the validity of Person 2's certificate using the public key in his or her copy of the root CA's certificate.
3. Person 1 challenges Person 2 to encrypt a random message.
4. Person 2 sends the encrypted message back to Person 1.
5. Person 1 decrypts the message with the public key in Person 2's certificate.
6. If decryption was successful, then Person 2 has been successfully authenticated.

A similar process occurs when Person 2 wants to authenticate Person 1; in fact they normally happen at the same time as each party wants to be sure of the identity of the other.

Note that the CA does not have to be online for authentication to occur. However, if the parties want to check if the certificate has been revoked they must check the CRL that was published by the CA. Typically the CRL is housed in a repository that is online since the CRL is a dynamic list.

4.4.2 Hierarchical topology

When there are multiple CAs a hierarchical structure can be implemented (see Figure 36):

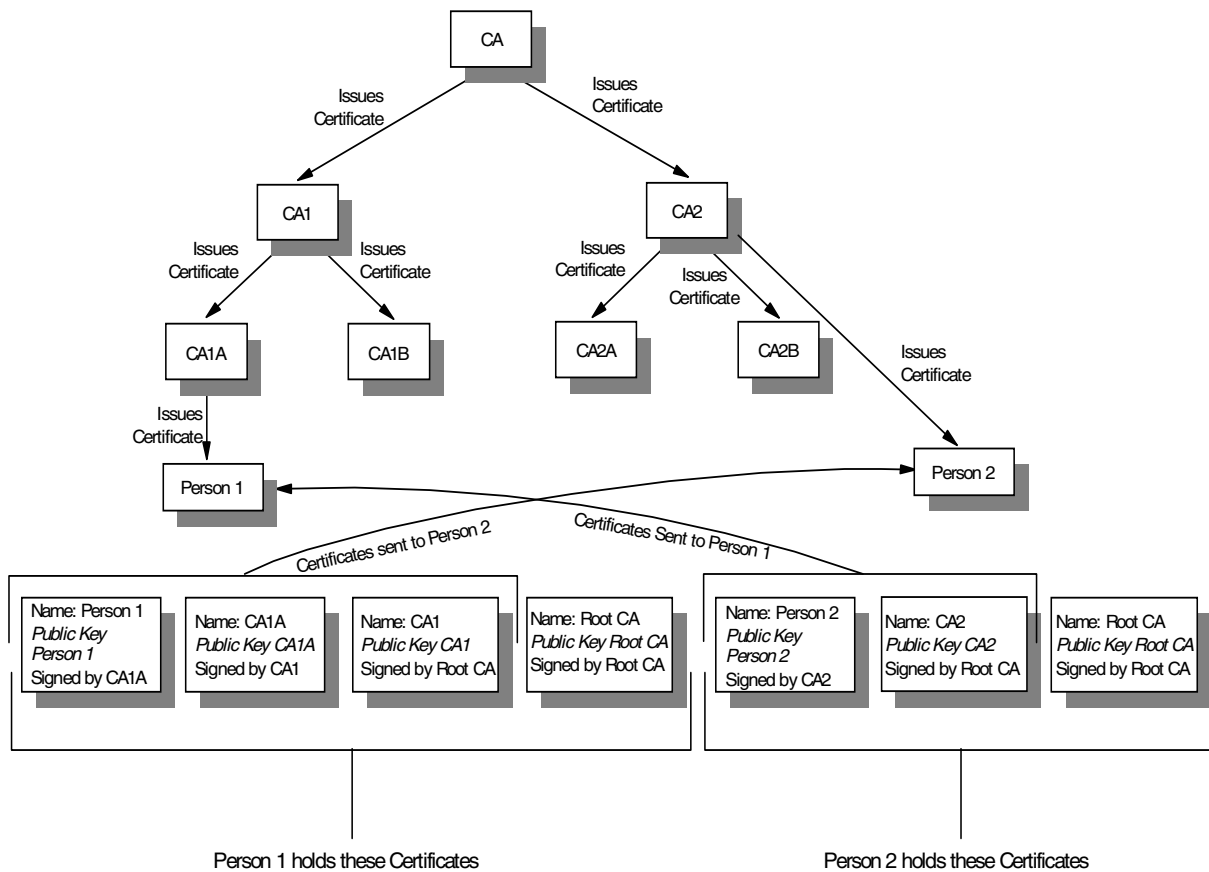


Figure 36. Hierarchical PKI

With a hierarchical PKI infrastructure a single root CA exists, which ultimately every other CA trusts, and therefore, every person who was issued a certificate by a CA in the tree will also trust. For two parties to communicate with each other a chain of trust ultimately to the root CA must exist.

Let us suppose that Person 1 and Person 2 want to authenticate each other, but their certificates are issued by two different CAs (CA1A and CA2 respectively). As in the single root CA example, Person 1 and Person 2 must hold all the relevant certificates so they can authenticate any person who wishes to communicate with them and be able to provide the relevant certificates to that other person so that person can provide authentication (again assuming that the parties do not want to

go through the process of requesting certificates from a CA or other repository). Therefore, Person 1 needs to hold the following certificates:

1. His or her own certificate signed by CA1A
2. CA1A's certificate, which was signed by CA1
3. CA1's certificate, which was signed by the root CA
4. The root CA's certificate, which was self signed

On the other hand, Person 2 needs to have the following certificates:

1. His or her own certificate signed by CA2
2. CA2's certificate, which was signed by the root CA
3. The root CA's certificate, which was self signed

All certificates except the root CA's certificate are used to give to another person so that other person can establish a chain of trust to the root CA. The root CA certificate is used so a person can validate a chain of certificates that establishes a chain of trust to the root CA.

Note that Person 2 does not need to hold certificates for CAs under CA2, even if Person 2 wants to communicate with a person whose certificate was issued by one of the CAs under CA2, CA2a, for example.

During authentication all the required certificates are exchanged, except that of the root CA since Person 1 and Person 2 both have a copy of it. At the end of the exchange Person 1 will have the required certificates to be able to trust Person 2:

1. Person 2's certificate signed by CA2
2. CA2's certificate, which was signed by the root CA
3. The root CA's certificate, which was self signed

These certificates allow Person 1 to establish a chain of trust for Person 1 to the root CA and therefore, be able to trust Person 2:

1. Person 2 has a certificate issued by CA2.
2. CA2 has a certificate issued by the root CA.
3. Since Person 1 trusts the root CA, he or she can therefore trust Person 2.

A similar operation occurs for Person 2. At the end of the exchange Person 2 will have the required certificates to be able to trust Person 2:

1. Person 1's certificate signed by CA1A
2. CA1A's certificate, which was signed by CA1
3. CA1's certificate, which was signed by the root CA
4. The root CA's certificate, which was self signed

These certificates allow Person 2 to establish a chain of trust for Person 1 to the root CA and therefore, be able to trust Person 1:

1. Person 1 has a certificate issued by CA1A.
2. CA1A has a certificate issued by CA1.
3. CA1 has a certificate issued by the root CA.

4. Since Person 2 trusts the root CA, he or she can therefore trust Person 1.

As in the single root CA example a final challenge of encrypting a random message must occur to confirm the identity of the other person. Again CRLs need to be checked. The parties must be able to go to a repository where these CAs are published. The location of the CRLs for each CA could potentially be stored in the certificate itself as an extension.

It is worth noting that if the two parties had their certificates issued from one branch of the hierarchy, for example, CA1A and CA1B, the parties need only establish a chain of trust to a common root rather than the root CA. In this example it would be CA1. However, to ensure that a person is able to communicate with any person, he or she must hold all the certificates that establish a chain of trust to the root CA.

4.4.3 Peer topology

A PKI infrastructure can also support multiple CAs in a peer arrangement. This is where all the CAs are considered root CAs and there is an any-to-any relationship between them (see Figure 37):

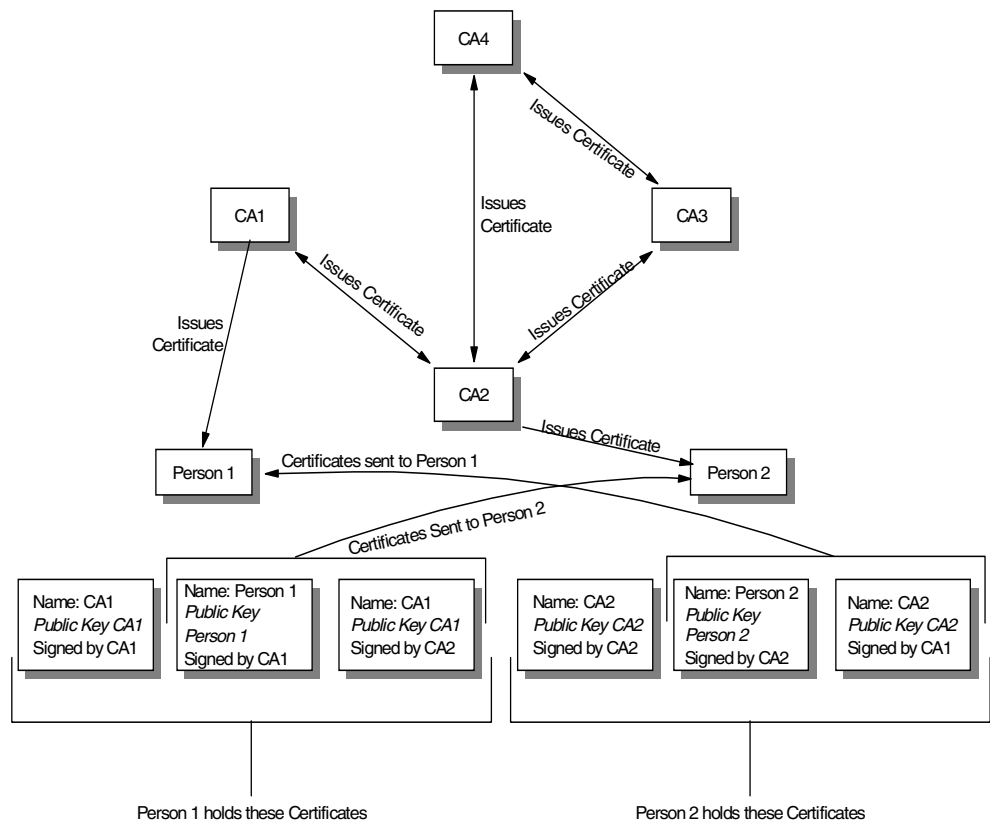


Figure 37. Peer PKI (adjacent CAs)

For two parties to communicate with each other who have certificates issued by different CAs, a chain of trust must be established between the two CAs. This can be achieved by the two CAs providing cross-certificates for each other. Let us consider the example where Person 1 wishes to communicate with Person 2. In

this example, CA1 and CA2 must cross-certify each other, that is, CA1 must issue a certificate for CA2 and CA2 must issue a certificate for CA1.

For Person 1 to communicate with Person 2, Person 1 must establish a chain of trust with the CA that issued Person 2's certificate, that is, CA2. The chain of trust is established in the following manner:

1. Person 1 trusts his or her own CA: CA1.
2. Since Person 1 trusts CA1, he or she will also trust all certificates issued by CA1.
3. Person 1 will trust CA2 if there is a certificate for CA2, which was issued by CA1.
4. If Person 1 trusts CA2, then he or she will trust all certificates issued by CA2, and thus the chain of trust is established.

In a similar way Person 2 can establish a chain of trust to CA1.

For authentication to occur Person 1 and Person 2 must hold the required certificates so that they can authenticate any person who wishes to communicate with them, and be able to provide the relevant certificates to the other person so that person can provide authentication (again assuming that the parties do not want to go through the process of requesting certificates from a CA or other repository). Person 1 must have:

1. CA1's certificate signed by CA1
2. His or her own certificate signed by CA1
3. CA1's certificate signed by CA2

Person 2 must have the following certificates:

1. CA2's certificate signed by CA2
2. His or her own certificate signed by CA2
3. CA2's certificate signed by CA1

During the authentication Person 1 and Person 2 will exchange certificates 2 and 3 between themselves. Therefore, Person 1 will have the required certificates to trust Person 2, thereby allowing Person 1 to establish a chain of trust to Person 2:

1. Person 2's certificate signed by CA2
2. CA2's certificate signed by CA1
3. CA1's certificate signed by CA1

Similarly Person 2 will have the following certificates to trust Person 1:

1. Person 1's certificate signed by CA1
2. CA1's certificate signed by CA2
3. CA2's certificate signed by CA2

This allows Person 2 to establish a chain of trust to Person 1.

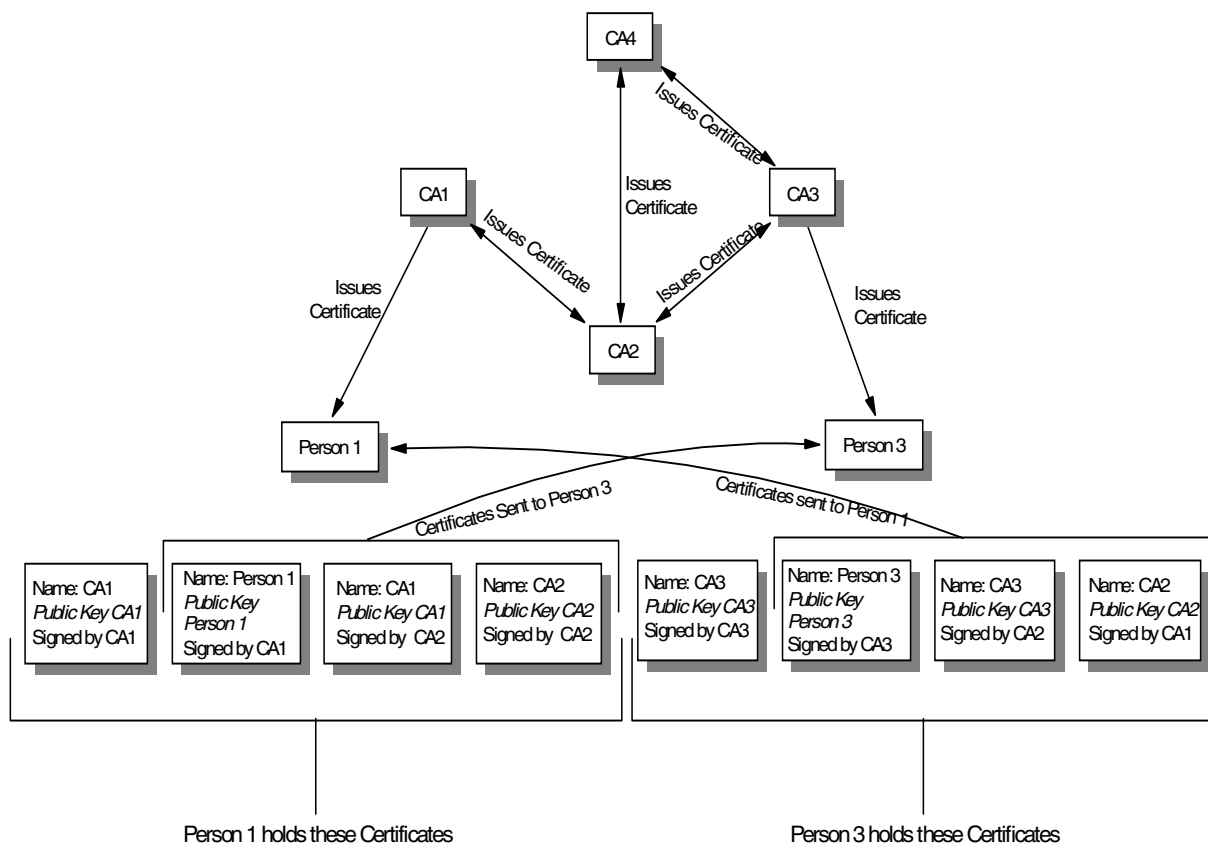


Figure 38. Peer PKI (nonadjacent CAs)

The scenario gets even more complicated if there is no direct exchange of cross-certificates between the two issuing CAs, that is, that the CAs are not adjacent to each other (see Figure 38). For example, if Person 1 wishes to communicate with Person 3, a chain of trust must be established through an intermediate CA. Person 1 must establish a chain of trust to CA3:

1. Person 1 trusts his or her own CA: CA1.
2. Since Person 1 trusts CA1, he or she will also trust all certificates issued by CA1.
3. Person 1 will trust CA2 if there is a certificate for CA2 that was issued by CA1.
4. If Person 1 trusts CA2, then he or she will trust all certificates issued by CA2.
5. Since Person 1 trusts all certificates issued by CA2, he or she will trust CA3 if there is a certificate for CA3 that was issued by CA2.
6. If Person 1 trusts CA3, then he or she will trust all certificates issued by CA3, and thus the chain of trust is established.

Similarly Person 3 can establish a chain of trust to CA1.

The chain of trust is achieved by a series of cross-certificates between CA1/CA2 and CA2/CA3. Again, for authentication to occur Person 1 and Person 3 must hold the required certificates so that they can authenticate any person who wishes to communicate with them, and be able to provide the relevant certificates

to the other person so that person can provide authentication. In this example, Person 1 must have:

1. CA1's certificate signed by CA1
2. His or her own certificate signed by CA1
3. CA1's certificate signed by CA2
4. CA2's certificate signed by CA3

Person 3 must have the following certificates:

1. CA3's certificate signed by CA3
2. His own certificate signed by CA3
3. CA3's certificate signed by CA2
4. CA2's certificate signed by CA1

During authentication Person 1 and Person 3 will exchange certificates 2, 3, and 4 between themselves. Therefore, Person 1 will have the required certificates to trust Person 3, thereby allowing Person 1 to establish a chain of trust to Person 3:

1. Person 3's certificate signed by CA3
2. CA3's certificate signed by CA2
3. CA2's certificate signed by CA1
4. CA1's certificate signed by CA1

Similarly Person 3 will have the following certificates after the exchange:

1. Person 1's certificate signed by CA1
2. CA1's certificate signed by CA2
3. CA2's certificate signed by CA3
4. CA3's certificate signed by CA3

This allows Person 3 to establish a chain of trust to Person 1.

As with previous examples the last step in authentication is to challenge the partner by asking him or her to encrypt a random message to ensure his or her identity, and to check the CRL to ensure the certificates have not been revoked.

As you can see, with a peer topology, the PKI scalability becomes an issue. The entities that wish to communicate with each other must hold a large number of certificates to communicate with other entities in the PKI, if there is no mechanism to request certificates dynamically from CAs or other repositories. With a hierarchal topology each entity simply needs to hold the certificates that establish the chain of trust to the root CA.

4.5 PKI requirements for IKE

As described in 3.2.2, "Key management requirements for IPsec" on page 46, IKE can be used with certificate-based authentication methods during a Phase 1 exchange to provide mutual authentication for the participating peers. While IKE does not specify how a device obtains a certificate, there are certain

requirements that must be met before certificates can be used by IKE. These are essentially specified in the Internet draft at:

`draft-ietf-ipsec-pki-req-02.txt`

The most important fact to notice about IKE and certificates is that IKE requires the ID of a device used in Phase 1 exchanges to be stored in the `subject_alternate_name` field of an X.509 certificate. Some CAs do not support that, so even if you included that field in your certificate request the certificate that will be returned to you by that CA does not include that field. Make sure, therefore, if you are going to deploy a public key infrastructure for IKE, or plan on using an existing one, that all CAs and devices in that PKI properly support `subject_alternate_name`.

Chapter 5. Security technologies complementing VPNs

In previous chapters we have discussed security technologies that can be used to build virtual private networks. While those technologies are usually efficient and sufficient to the task, there are cases where those technologies alone will not fulfill the request for a complete VPN solution. One such case is the use of digital certificates for authentication and encryption, which has already been described. This chapter briefly presents additional security technologies that can either complement a VPN solution or coexist in a VPN environment under certain circumstances.

5.1 Authentication for remote access dial-in users

Remote dial-in to the corporate intranet, as well as to the Internet, has made the Remote Access Server (RAS) a very vital part of today's internetworking services. As mentioned previously, more and more mobile users are requiring access not only to central-site resources but to information sources on the Internet. The widespread use of the Internet and the corporate intranet has fueled the growth of remote access services and devices. There is an increasing demand for a simplified connection to corporate network resources from mobile computing devices such as notebook computers or palm-sized devices.

The emergence of remote access has caused significant development work in the area of security. The Authentication, Authorization and Accounting (AAA) security model has been developed to address the issues of remote access security. AAA answers the questions who, what, and when, respectively. A brief description of each of the three As in the AAA security model is presented below:

Authentication

This is the action of determining who a user (or entity) is. Authentication can take many forms. Traditional authentication utilizes a name and a fixed password. Most computers work this way. However, fixed passwords have limitations, mainly in the area of security. Many modern authentication mechanisms utilize one-time passwords or a challenge-response query. Authentication generally takes place when the user first logs on to a machine or requests a service from it.

Authorization

This is the action of determining what a user is allowed to do. Generally authentication precedes authorization, but again, this is not required. An authorization request may indicate that the user is not authenticated, that we do not know who he or she is. In this case it is up to the authorization agent to determine if an unauthenticated user is allowed the services in question. In current remote authentication protocols authorization does not merely provide yes or no answers, but it may also customize the service for the particular user.

Accounting

This is typically the third action after authentication and authorization. But again, neither authentication nor authorization is required. Accounting is the action of recording what a user is doing, and when he or she has done it.

In the distributed client/server security database model, a number of communication servers, or clients, authenticate a dial-in user's identity through a single, central database, or authentication server. The authentication server stores all the information about users, their passwords and access privileges. Distributed security provides a central location for authentication data that is more secure than scattering the user information on different devices throughout a network. A single authentication server can support hundreds of communication servers, serving up to tens of thousands of users. Communication servers can access an authentication server locally or remotely over WAN connections.

Several remote access vendors and the Internet Engineering Task Force (IETF) have been in the forefront of this remote access security effort, and the means whereby such security measures are standardized. The Remote Authentication Dial-In User Service (RADIUS) and the Terminal Access Controller Access Control System (TACACS) are two such cooperative ventures that have evolved out of the Internet standardizing body and remote access vendors.

Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a distributed security system developed by Livingston Enterprises. RADIUS was designed based on a previous recommendation from the IETF's Network Access Server Working Requirements Group. An IETF Working Group for RADIUS was formed in January 1996 to address the standardization of the RADIUS protocol; RADIUS is now an IETF-recognized dial-in security solution (RFC 2058 and RFC 2138).

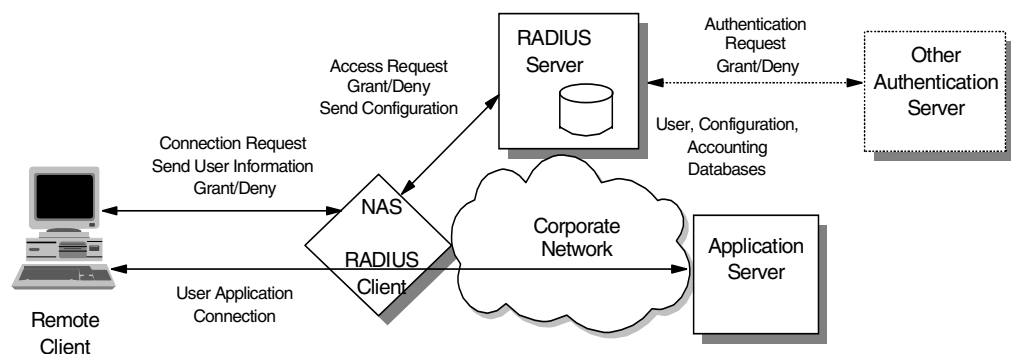


Figure 39. RADIUS

Terminal Access Controller Access Control System (TACACS)

Similar to RADIUS, Terminal Access Controller Access Control System (TACACS) is an industry-standard protocol specification, RFC 1492. Similar to RADIUS, TACACS receives authentication requests from a network access server (NAS) client and forwards the user name and password information to a centralized security server. The centralized server can be either a TACACS database or an external security database. Extended TACACS (XTACACS) is a version of TACACS with extensions that Cisco added to the basic TACACS protocol to support advanced features. TACACS+ is another Cisco extension that allows a separate access server (the TACACS+ server) to provide independent authentication, authorization, and accounting services.

5.1.1 RADIUS operation

RADIUS was originally developed by Livingston Enterprises but is now in the domain of the IETF and is an open protocol and a reference implementation

distributed in source code format that can be modified by anyone. Any client that supports the RADIUS client protocol can talk to the corresponding RADIUS server.

Although RADIUS was originally developed for the administration of NAS products support was recently added for further devices/applications such as firewalls, access to individual Web pages, e-mail accounts and other authentication-related Internet security situations.

RADIUS consists of two parts: There is the RADIUS client, for example, the NAS or any other software such as a firewall, that sends an AAA request to the RADIUS server. On the other hand, there is the RADIUS server, which checks the request according to preconfigured data. The RADIUS standard specifies the format and traffic flow of the packets between these devices that provides AAA services.

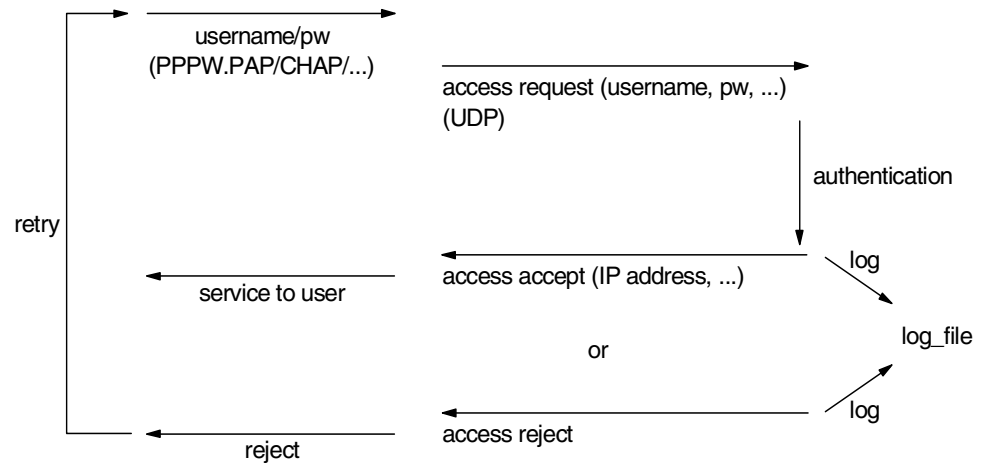
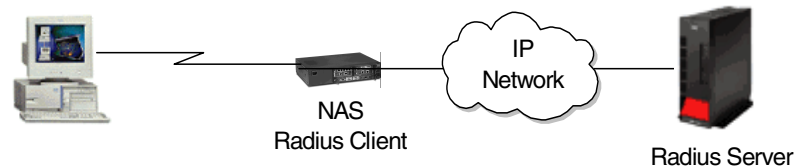


Figure 40. Traffic flow in RADIUS

Although RADIUS and TACACS authentication servers can be set up in a variety of ways, depending upon the security scheme of the network they are serving, the basic process for authenticating a user is essentially the same. Using a modem, a remote dial-in user connects to a remote access server (also called the network access server or NAS), with a built-in analog or digital modem. Once the modem connection is made, the NAS prompts the user for a name and password. The NAS then creates the so-called authentication request from the supplied data packet, which consists of information identifying the specific NAS device sending the authentication request, the port that is being used for the modem connection, and the user name and password.

A very important role is performed by the authentication server, which is a server in the network that validates user IDs and passwords for the network. If a device is configured for authentication through an authentication server and the device receives a packet from an authentication protocol, the device passes a user ID and password to the server for authentication.

If the user ID and password are correct, the server responds positively. The device can then communicate with the originator of the request. If the server does not find the user ID and password that it receives from the device, it responds negatively to the device. The device then rejects the session from which it got the authentication request.

The authentication server can be the RADIUS server itself or a different server based on other central authentication technologies such as Kerberos, DCE, SecureID (by Security Dynamics) or RACF. A RADIUS server can be configured to forward authentication requests to such a central authentication server and pass access or deny information and configuration back to the client.

For protection against eavesdropping by hackers, the NAS, acting as the RADIUS or TACACS client, encrypts the password before it sends it to the authentication server. If the primary security server cannot be reached, the security client or NAS device can route the request to an alternate server. When an authentication request is received, the authentication server validates the request and then decrypts the data packet to access the user name and password information. If the user name and password are correct, the server sends an authentication acknowledgment packet. This acknowledgment packet may include additional filters, such as information on the user's network resource requirements and authorization levels. The security server may, for instance, inform the NAS that a user needs TCP/IP and/or Internet Packet Exchange (IPX) using PPP, or that the user needs SLIP to connect to the network. It may include information on the specific network resource that the user is allowed to access.

To circumvent snooping on the network, the security server sends an authentication key, or signature, identifying itself to the security client. Once the NAS receives this information, it enables the necessary configuration to allow the user the necessary access rights to network services and resources. If at any point in this log-in process all necessary authentication conditions are not met, the security database server sends an authentication reject message to the NAS device and the user is denied access to the network.

5.1.2 Using RADIUS with layer-2 tunnels

RADIUS can be used to authenticate layer-2 tunnels as well as PPP connections which is important for VPNs. There are two models of layer-2 tunnels, voluntary and compulsory. RADIUS can be used in both cases to authenticate a user and grant or deny a tunnel setup or session establishment. This adds one layer of security to the layer-2 VPN scenario because unless the tunnel is up and the session established, no traffic can flow over the tunnel, and authentication and access to those tunnels can be centrally controlled.

Figure 41 on page 89 illustrates yet another way of using RADIUS in a VPN environment where compulsory tunnels are used that involve an ISP to establish a tunnel or start a new session over an existing tunnel on behalf of a remote client. The ISP can use a RADIUS proxy server to forward client authentication

back to the corporate authentication server so that there is no need to maintain user information at two locations, the ISP and the corporate server.

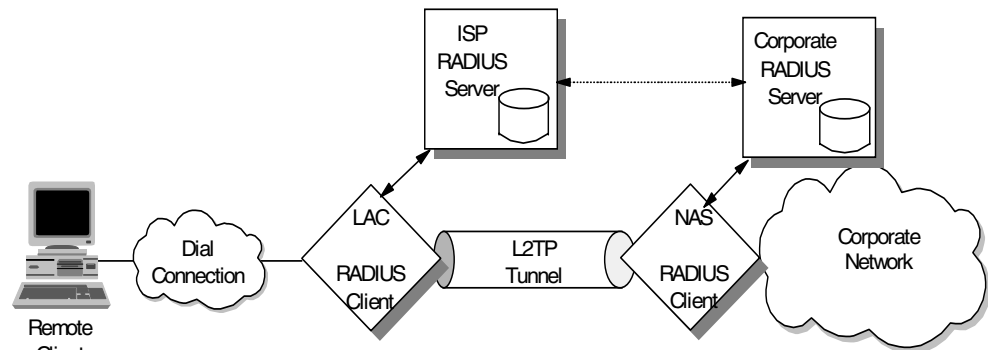


Figure 41. Using RADIUS with layer-2 tunnels

5.2 Network address translation (NAT)

Originally NAT was suggested as a short-term solution to the problem of IP address depletion. In order to ensure any-to-any communication on the Internet, all IP addresses have to be officially assigned by the Internet Assigned Numbers Authority (IANA). This is becoming increasingly difficult to achieve, because the number of available address ranges is now severely limited. Also, in the past, many organizations have used locally assigned IP addresses, not expecting to require Internet connectivity. The idea of NAT is based on the fact that only a small part of the hosts in a private network is communicating outside of that network. If each host is assigned an IP address from the official IP address pool only when it needs to communicate, then only a small number of official addresses are required.

NAT might be a solution for networks that have private IP address ranges or illegal addresses and want to communicate with hosts on the Internet. In fact, most of the time, this can be achieved also by implementing a firewall. Hence, clients that communicate with the Internet by using a proxy or SOCKS server do not expose their addresses to the Internet, so their addresses do not have to be translated. However, for any reason, when proxy and SOCKS are not available or do not meet specific requirements, NAT might be used to manage the traffic between the internal and external network without advertising the internal host addresses.

Consider an internal network that is based on the private IP address space, and the users want to use an application protocol for which there is no application gateway. The only option is to establish IP-level connectivity between hosts in the internal network and hosts on the Internet. Since the routers in the Internet would not know how to route IP packets back to a private IP address, there is no point in sending IP packets with private IP addresses as source IP addresses through a router into the Internet. As shown in Figure 42 on page 90, NAT handles this by taking the IP address of an outgoing packet and dynamically translating it to an official address. For incoming packets it translates the official address to an internal address.

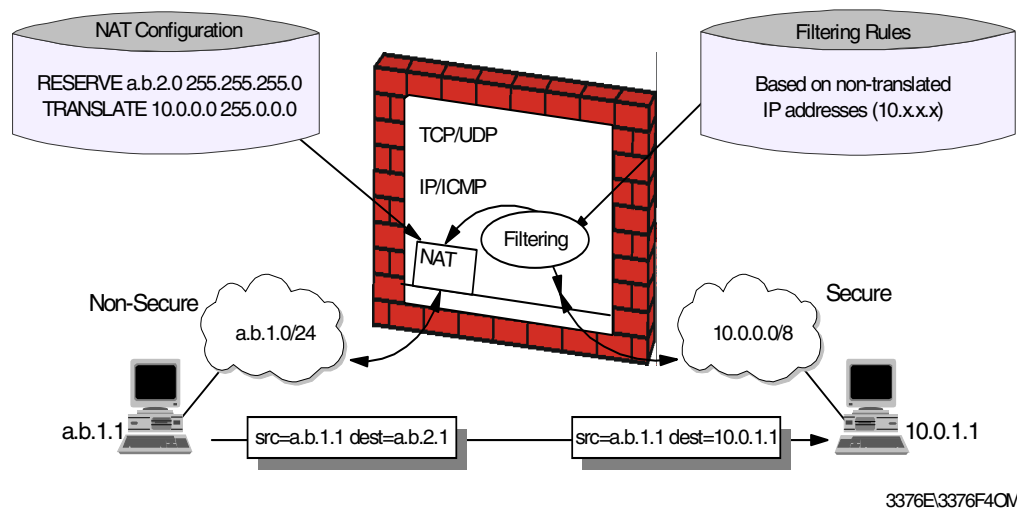


Figure 42. Network Address Translation (NAT)

From the point of two hosts that exchange IP packets with each other, one in the secure network and one in the nonsecure network, NAT looks like a standard IP router that forwards IP packets between two network interfaces (see Figure 43).

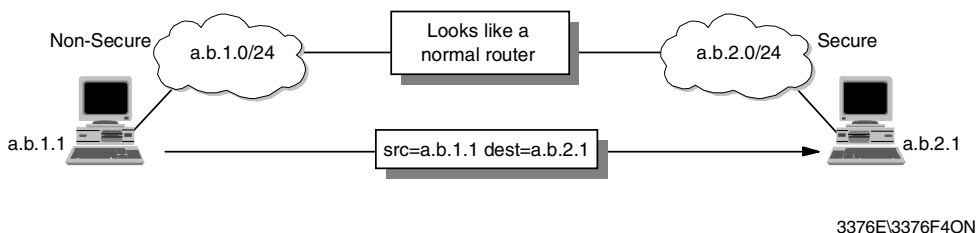


Figure 43. NAT seen from the non-secure network

5.2.0.1 Using NAT with VPNs

NAT works fine for IP addresses in the IP header. Some application protocols exchange IP address information in the application data part of an IP packet, and NAT will generally not be able to handle translation of IP addresses in the application protocol. Currently, most of the implementations handle the FTP protocol. It should be noted that implementation of NAT for specific applications that have IP information in the application data is more sophisticated than the standard NAT implementations.

Another important limitation of NAT is that NAT changes some or all of the address information in an IP packet. When end-to-end IPSec authentication is used, a packet whose address has been changed will always fail its integrity check under the Authentication Header (AH) protocol, since any change to any bit in the datagram will invalidate the integrity check value that was generated by the source. Since IPSec protocols offer some solutions to the addressing issues that were previously handled by NAT, there is no need for NAT when all hosts that compose a given virtual private network use globally unique (public) IP addresses. Address hiding can be achieved by IPSec's tunnel mode. If a company uses private addresses within its intranet, IPSec's tunnel mode can

keep them from ever appearing in cleartext on the public Internet, which eliminates the need for NAT.

5.3 SOCKS

A circuit level gateway relays TCP and also UDP connections and does not provide any extra packet processing or filtering. A circuit level gateway is a special type of application level gateway. This is because the application level gateway can be configured to pass all information once the user is authenticated, just as the circuit level gateway (see Figure 449). However, in practice, there are significant differences between them:

- Circuit level gateways can handle several TCP/IP applications as well as UDP applications without any extra modifications on the client side for each application. Thus, this makes circuit level gateways a good choice to satisfy user requirements.
- Circuit level gateways do not provide packet processing or filtering. Thus, a circuit level gateway is generally referred to as a transparent gateway.
- Application level gateways have a lack of support for UDP.
- Circuit level gateways are often used for outbound connections, whereas application level gateways (proxy) are used for both inbound and outbound connections. Generally, in cases of using both types combined, circuit level gateways can be used for outbound connections and application level gateways can be used for inbound connections to satisfy both security and user requirements.

A well-known example of a circuit level gateway is SOCKS. Because data that flows over SOCKS is not monitored or filtered, a security problem may arise. To minimize the security problems, trusted services and resources should be used on the outside network (untrusted network).

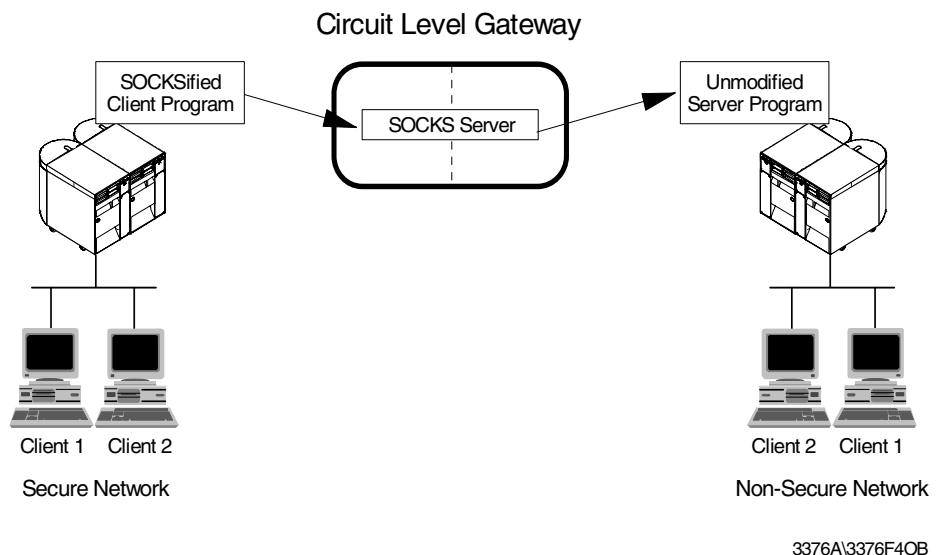


Figure 44. Circuit level gateway

SOCKS is a standard for circuit level gateways. It does not require the overhead of a more conventional proxy server where a user has to consciously connect to the firewall first before requesting the second connection to the destination. The user starts a client application with the destination server IP address. Instead of directly starting a session with the destination server, the client initiates a session to the SOCKS server on the firewall. The SOCKS server then validates that the source address and user ID are permitted to establish onward connection into the nonsecure network, and then creates the second session.

SOCKS needs to have new versions of the client code (called SOCKSified clients) and a separate set of configuration profiles on the firewall. However, the server machine does not need modification; indeed it is unaware that the session is being relayed by the SOCKS server. Both the client and the SOCKS server need to have SOCKS code. The SOCKS server acts as an application level router between the client and the real application server. SOCKSv4 is for outbound TCP sessions only. It is simpler for the private network user, but does not have secure password delivery so it is not intended for sessions between public network users and private network applications. SOCKSv5 provides for several authentication methods and can therefore be used for inbound connections as well, though these should be used with caution. SOCKSv5 also supports UDP-based applications and protocols.

The majority of Web browsers are SOCKSified and you can get SOCKSified TCP/IP stacks for most platforms.

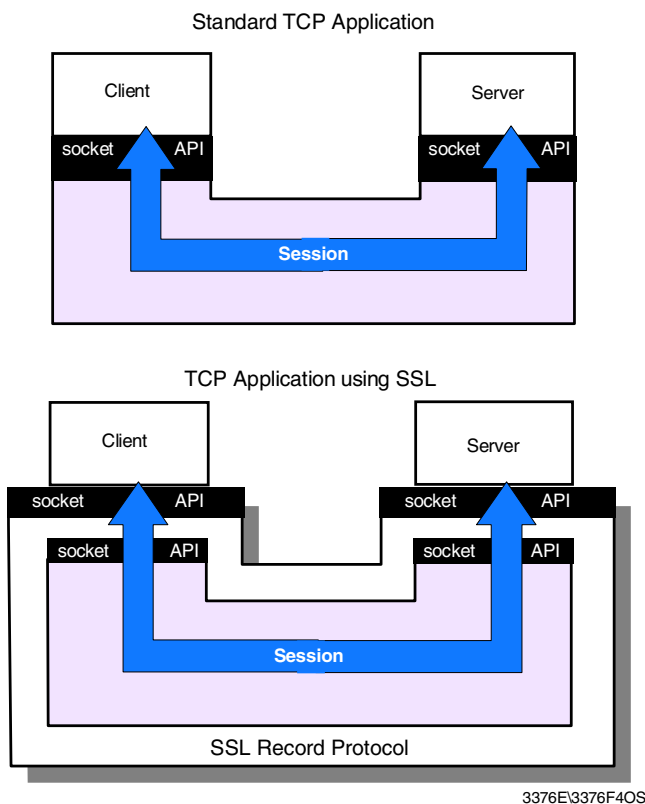
5.4 Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

SSL is a security protocol that was developed by Netscape Communications Corporation, along with RSA Data Security, Inc. The primary goal of the SSL protocol is to provide a private channel between communicating applications, which ensures privacy of data, authentication of the partners and integrity.

SSL provides an alternative to the standard TCP/IP socket API that has security implemented within it. Hence, in theory it is possible to run any TCP/IP application in a secure way without changing the application. In practice, SSL is only widely implemented for HTTP connections, but Netscape Communications Corporation has stated an intention to employ it for other application types, such as Network News Transfer Protocol (NNTP) and Telnet, and there are several such implementations freely available on the Internet. IBM, for example, is using SSL to enhance security for TN3270 sessions in its Host On-Demand, Personal Communications and Communications Server products, as well as securing configuration access to firewalls.

SSL is composed of two layers:

1. At the lower layer, there is a protocol for transferring data using a variety of predefined cipher and authentication combinations, called the SSL Record Protocol. Figure 45 on page 93 illustrates this, and contrasts it with a standard HTTP socket connection. Note that this diagram shows SSL as providing a simple socket interface, on which other applications can be layered. In reality, current implementations have the socket interface embedded within the application and do not expose an API that other applications can use.
2. At the upper layer, there is a protocol for the initial authentication and transfer of encryption keys, called the SSL Handshake Protocol.



3376E3376F40S

Figure 45. SSL - comparison of standard and SSL sessions

An SSL session is initiated as follows:

- On the client (browser) the user requests a document with a special URL that begins https: instead of http:, either by typing it into the URL input field, or by clicking a link.
- The client code recognizes the SSL request and establishes a connection through TCP port 443 to the SSL code on the server.
- The client then initiates the SSL handshake phase, using the SSL Record Protocol as a carrier. At this point there is no encryption or integrity checking built in to the connection.

The SSL protocol addresses the following security issues:

- Privacy:** After the symmetric key is established in the initial handshake, the messages are encrypted using this key.
- Integrity:** Messages contain a message authentication code (MAC) ensuring the message integrity.
- Authentication:** During the handshake, the client authenticates the server using an asymmetric or public key. It can also be based on certificates.

SSL requires each message to be encrypted and decrypted and therefore, has a high performance and resource overhead.

5.5 Comparing IPsec to SSL

As described in Chapter 3, “Layer-3 VPN protocols” on page 37, IPsec provides cryptographically strong authentication and encryption for IP traffic and also provides for secure and certificate-based key exchange and refresh using IKE. By deliberately jumping to conclusions, you might suggest that this is essentially the same functionality that SSL and TLS provide as well. In this section we point out the similarities and fundamental differences between IPsec and SSL and explain which are the main areas of use for both protocols.

Both are similar:

- IPsec (via IKE) and SSL provide client and server authentication.
- IPsec and SSL provide data authentication and secrecy, even though on different levels of the protocol stack.
- IPsec and SSL can use cryptographically strong algorithms for encryption and hashing operations and can use certificate-based authentication (IPsec via IKE).
- IPsec (via IKE) and SSL provide key generation and refresh without transmitting any keys in the clear or out of band.

Both are different:

- SSL is implemented as an API between the application and transport layers; IPsec is implemented as a framework at the internetwork layer.
- SSL provides application-to-application security (for instance, Web browser to Web server), IPsec provides device-to-device security
- SSL does not protect IP headers. This can be an exposure to spoofing and session hijacking attacks. IPsec does protect IP headers.
- SSL does not protect UDP traffic, IPsec does.
- SSL operates end-to-end and has no concept of tunneling. This can be a problem when traffic needs to be examined by content inspection and virus scanning systems before it is delivered to the final destination. IPsec can operate both ways, end-to-end and as a tunnel.
- SSL can traverse NAT or SOCKS which provides for hiding internal addressing structures or to avoid private IP address conflicts. IPsec in transport mode (end-to-end) cannot use NAT for that purpose but it can use an IPsec tunnel to achieve the same goal and provide even more security than NAT because that tunnel can also be encrypted.
- Applications need to be modified to use SSL (become SSL aware). This can be a problem when you do not have access to the application source code, or you do not have the time or expertise to change the application. IPsec is transparent to applications.

Usually, SSL is fine when you have only one application to be secured and that is already available in an SSL-aware version. This is the case with a variety of standard applications nowadays, not only with Web browsers and servers. Also, if you have the option of implementing 3-tier concepts by employing Web application gateways at the perimeter of the network, SSL is a good choice.

If you have a great number of applications to secure you may be better off securing the whole network instead of dealing with each application in turn. In this

case, IPSec is truly the better choice. Unless you develop your own applications, IPSec is much more flexible than SSL to implement a security policy that requires different levels and combinations of authentication, encryption and tunneling.

Last but not least, the choice of a proper security technology also depends on the business model. If the purpose of your application servers is to be accessible to the public, then a Web-based design and security technology based on SSL may be the right choice. SSL is available on any standard Web browser and that will be the only tool used and required by the users. In this case, everybody is your potential customer.

If, however, the circle of users who should be given access to your application servers or networks is more restrictive, then a VPN based on IPSec and maybe some layer-2 tunneling technologies is more likely the way to go. In this case, the participants and their roles in the data interchange are predefined.

Chapter 6. Directory-assisted policy management

Networks grow rapidly and the complexity of networks increases. The management of networks is a big issue from the viewpoint of scalability and security. To enable cost-effective administration of distributed networks and enforce security policy in a virtual private network (VPN), directory-assisted policy management is a must.

One of the possible alternatives is Lightweight Directory Access Protocol (LDAP), which was developed to provide standards for accessing the data in network directories. As the use of LDAP grew and its benefits became apparent, the stand-alone LDAP server can build directories that could be accessed by the LDAP client. A common directory infrastructure encourages new uses. The Directory Enabled Networks (DEN) specification allows information about network configuration, protocol information, router characteristics, and so on to be stored in an LDAP directory.

LDAP can be used to deploy IPsec security policy to distributed network devices through the Internet.

6.1 The benefits of directory-assisted policy management

An advantage of using a directory server to store policy information as opposed to more traditional methods of locally stored configurations is the ability to make a change in one place and have that change applied across all the devices in the extended network. This includes devices in the local administrative domain as well as devices across public boundaries. Take for example, an IPsec transform definition that resides in the directory. To change the corporate policy for encryption from DES to 3DES normally would require a change in the configuration of each device in the extended network. If the directory server is used to deploy the policies, then one IPsec transform would need to be changed in the LDAP server and then each policy-enabled device in the network would need to rebuild the internal policy database. Another good example would be if a DiffServ action named "GoldService" needed to be changed from 40% of bandwidth to 45% of bandwidth. The LDAP server and policy infrastructure allows these types of configuration changes to scale much better and reduce configuration mismatches.

This section is excerpted from the document "Configuration and Setup Instructions for Reading Policies from a LDAP Server" on the IBM Networking Web site. For more information, visit the following URL:

<http://www.networking.ibm.com/support/code.nsf>

then select either 2210, 2212 or 2216. Next click **LDAP Server Configuration Information**.

6.2 Directory client and servers

The network devices that support LDAP can be an LDAP client and can access required information from LDAP server. The information needed to configure the VPN tunnel is stored in a central LDAP server. The router or security gateway can

be an LDAP client. To take advantage of this feature an LDAP server operating at RFC Version 2 or 3 is required.

6.2.1 LDAP schema

An LDAP schema is the set of rules and information that comprise the class and attribute definitions that define the entries that ultimately exist in the directory. LDAP schema is typically written in ASN1 syntax similar to SNMP MIBs.

6.2.2 Directory security

Directories are likely to contain sensitive information that needs to be protected from unauthorized access and modification. When sending data over networks, sensitive information may also need to be protected against eavesdropping and modification during transportation. LDAP supports both basic client authentication using a distinguished name and password and Secure Sockets Layer (SSL), which provides mutual authentication between clients and servers as well as data security through encryption. LDAP Version 3 supports the Simple Authentication and Security Layer (SASL), a framework for adding additional authentication mechanisms.

More information on LDAP can be found in the following redbooks:

- *Understanding LDAP*, SG24-4986
- *LDAP Implementation Cookbook*, SG24-5110

6.3 Nways router policy administration with LDAP

In this scenario, an LDAP server is installed on an AIX system (AIXSRV1) and two routers (2216 center and 2216 branch) are used as LDAP clients. The network diagram for the test is shown in Figure 46 on page 99:

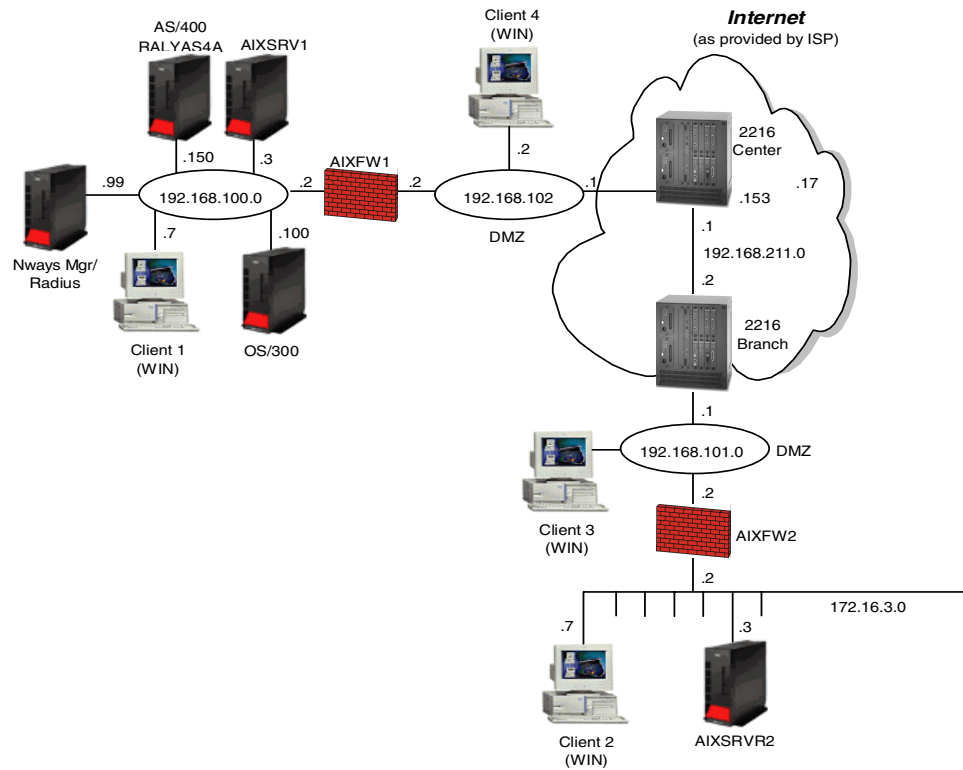


Figure 46. Router-to-router tunnel using LDAP

6.3.1 LDAP server configuration

IBM eNetwork LDAP Directory Server V2.1 is used as an LDAP server on AIXSRV1 (AIX V4.3.2). The LDAP server provides a native, scalable directory based on the IETF LDAP Version 2 (RFC 1777) plus some extensions for IETF LDAP Version 3. IBM Universal Database Version 5 is packaged with the LDAP server and used as the directory storage facility. Lotus Domino Go V4.6.2 is used for LDAP server configuration and administration.

LDAP Directory Server V2.1 is bundled in AIX V4.3.2 CD (CD #2). The required components are as follows:

- ldap.client: LDAP No-ssl Client
- ldap.html.lang: LDAP HTML Installation/Configuration Guide
- ldap.server: LDAP No-ssl Server

DB2 will be installed automatically during LDAP server installation.

For SSL Version 3 support, the following components that are in AIX V4.3.2 Bonus Pack must be installed after LDAP client and server installation:

- gskru301: 128-bit encryption for LDAP
- gskrf301: 40-bit encryption for LDAP

Note

For security reasons, SSL is needed to protect information transferred between LDAP client and server. The SSL feature is added by installing IBM GSKit packages. The GSKit packages include Secure Sockets Layer (SSL) Version 3 support and associated RSA technology. There are two GSKit packages available: U.S. and Export. They come with different encryption strength. For AIX, the appropriate GSKit packages are included in the AIX 4.3.2 Bonus Pack.

6.3.1.1 Obtaining and installing LDAP server configuration files

To communicate with IBM 221x router using LDAP, the following files which define attributes, object class and security policies for 221x router are required. The IBM networking Web site <http://www.networking.ibm.com> provides these file sets.

Visit the Web site mentioned above and select **Support** and choose 2216, 2210, or 2212 from the Product list, then select **Downloads**. From the Download page, select **LDAP Server Configuration Information** and then download the files from the LDAP Server Configuration Files menu.

Files in the LDAP server configuration are listed below:

| | |
|--|---|
| <code>policyTemplates.ldif</code> | Pre-defined policy objects |
| <code>policyExamples.ldif</code> | Some examples of security policies |
| <code>ibmPolicySchema.txt</code> | Description file for IBM's Policy Classes |
| <code>policySchema_oc.conf</code> | The objectclass file for the LDAP server |
| <code>policySchema_netscape_at.conf</code> | The attribute file for the Netscape LDAP server |
| <code>policySchema_ibm_at.conf</code> | The attribute file for the IBM LDAP server |
| <code>policySchema_openLdap_at.conf</code> | The attribute file for the OpenLdap server |

To apply these configurations to the LDAP server, perform the following configuration steps:

The first two steps include the Objectclass file (`policySchema_oc.conf`) and Attributes file (`policySchema_ibm_at.conf`) in the LDAP server.

1. Locate the LDAP server configuration file. This typically is the `slapd.conf` file. On AIX this is in the `/etc` directory.
2. Edit the `slapd.conf` file and add the following lines (these lines should be added after any other include statements in the config file):

```
include <path>/policySchema_ibm_at.conf
include <path>/policySchema_oc.conf
```

The next step is adding and modifying policy entries to the LDAP server. The LDAP server parses the LDAP Data Interchange Format (LDIF) file to translate into the format necessary to use the LDAP protocol, and then handle the request(s) with the directory server.

3. Add the policy templates first:

- Remove comments from the file using the following command:

```
grep -v '^#' policyTemplates.ldif > out.ldif
```

- Add the entries in the new out.ldif file using the ldapmodify client:

```
ldapmodify -h <hostname> -D <user dn> -w <password> -rac -f out.ldif
```

4. Make any modifications to the example policies supplied and then perform the following steps. Modification of the policy file is explained in 6.3.1.2, “Modifying LDAP server policy files for 221x router” on page 101.

- Remove comments from the file using the following command:

```
grep -v '^#' policyExamples.ldif > out.ldif
```

- Add the entries in the new out.ldif file using the ldapmodify client:

```
ldapmodify -h <hostname> -D <user dn> -w <password> -rac -f out.ldif
```

6.3.1.2 Modifying LDAP server policy files for 221x router

The policy class structure is shown in Figure 47 on page 102 and the policy search agent in the IBM 221x Router will retrieve all the policy information in the directory server that is intended for that device. The starting point for the policy search is DeviceProfile.

Two key objects in the Policy schema that allow the Policy Search Agent to search for and find the necessary policies for the device are the DeviceProfile and the DevicePolicyRules. The DeviceProfile has information about the device's mandatory DevicePolicyRules reference. Devices can be grouped together into one DeviceProfile or each device in the network can have its own DeviceProfile. This really will depend on whether more than one box in the network needs to fetch the same set of rules. Typically for security gateways this will not be true since every gateway will have a different tunnel endpoint. For QoS-only boxes, it would be conceivable that a group of devices would all read the same set of policies. The DevicePolicyRules object will be retrieved based on the value in the DeviceProfile that is fetched for the device. Once the DevicePolicyRules object has been retrieved, then the list of PolicyRules for that device can be retrieved. If any of the objectclass is not found or if an error is detected during a consistency check on an object, then the search is aborted and messages will be displayed for the PLCY ELS subsystem denoting the error detected.

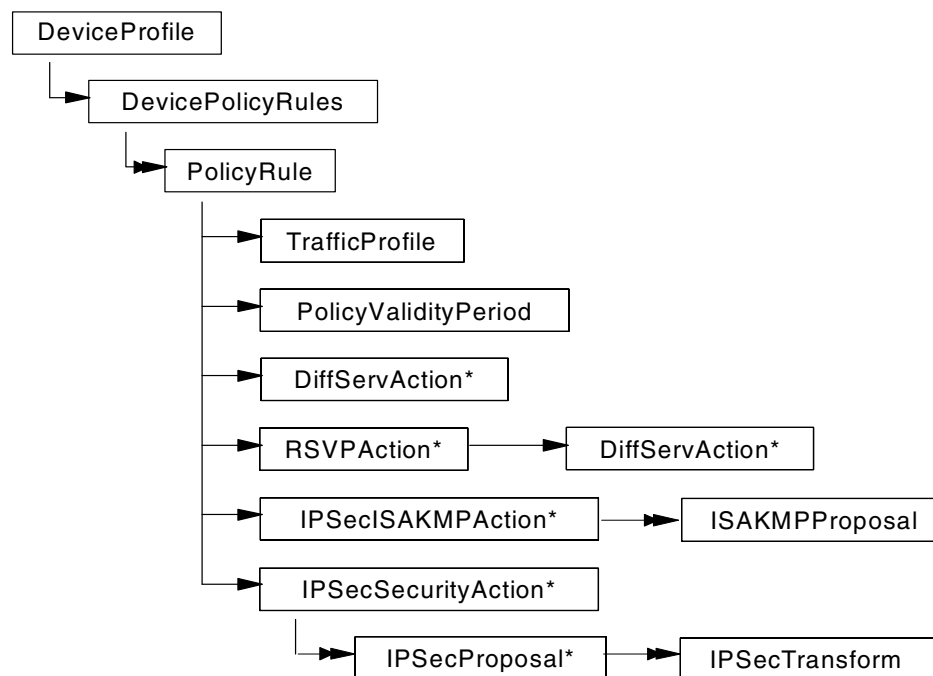


Figure 47. Policy class structure of LDAP configuration for 221x router

Modified policyExamples.ldif is shown below:

```

#####
###
### securing traffic between branch offices
###
### The policies in this file assume that the directory has been
### loaded with the pre-defined templates in "policyTemplates.ldif".
###
#####
### Branch office policy for securing traffic from 192.168.211.1 to
### 192.168.211.2. This policy consists of the information needed to
### setup the security association for the Security Gateway (2216CTR
### - public IP Address = 192.168.211.1) protecting the 192.168.102.0
### network and the information needed for the Security Gateway (2216BR
### - public IP Address = 192.168.211.2) protecting the 192.168.101.0
### network.
#####

# Profile for 2216CTR
dn: cn=G1toG2, o=ibm, c=us
objectclass: trafficprofile
cn: G1toG2
sourceaddressrange: 1:192.168.102.0-255.255.255.0
destinationaddressrange: 1:192.168.101.0-255.255.255.0

#IPSEC Action for 2216CTR
dn: cn=secureG1toG2, o=ibm, c=us
objectclass: IPsecSecurityAction
cn: secureG1toG2
securityaction: permit
ipsectunnelstart: 192.168.211.1
ipsectunnelend: 192.168.211.2
ipsecproposalreference: 1: cn=strongP2EspProp, o=ibm, c=us
ipsecproposalreference: 2: cn=strongP2EspAhProp, o=ibm, c=us
ipsecproposalreference: 3: cn=veryStrongP2EspProp, o=ibm, c=us
ipsecproposalreference: 4: cn=veryStrongP2EspAhProp, o=ibm, c=us

#Policy for 2216CTR
dn: cn=policySecureG1toG2, o=ibm, c=us

```

```

objectclass: policyrule
cn: policySecureG1toG2
rulepriority: 20
policyscope: isakmp
policyscope: ipsec
trafficprofilereference: cn=G1toG2, o=ibm, c=us
policyvalidityperiodreference: cn=allTheTime, o=ibm, c=us
ipsecsecurityactionreference: cn=secureG1toG2, o=ibm, c=us
ipsecisakmpactionreference: cn=generalPhase1Action, o=ibm, c=us

# Profile for 2216BR
dn: cn=G2toG1, o=ibm, c=us
objectclass: trafficprofile
cn: G2toG1
sourceaddressrange: 1:192.168.101.0-255.255.255.0
destinationaddressrange: 1:192.168.102.0-255.255.255.0

#IPSEC Action for 2216BR
dn: cn=secureG2toG1, o=ibm, c=us
objectclass: IPSecSecurityAction
cn: secureG2toG1
securityaction: permit
ipsectunnelstart: 192.168.211.2
ipsectunnelend: 192.168.211.1
ipsecproposalreference: 1: cn=strongP2EspProp, o=ibm, c=us
ipsecproposalreference: 2: cn=strongP2EspAhProp, o=ibm, c=us
ipsecproposalreference: 3: cn=veryStrongP2EspProp, o=ibm, c=us
ipsecproposalreference: 4: cn=veryStrongP2EspAhProp, o=ibm, c=us

#Policy for 2216BR
dn: cn=policySecureG2toG1, o=ibm, c=us
objectclass: policyrule
cn: policySecureG2toG1
rulepriority: 20
policyscope: isakmp
policyscope: ipsec
trafficprofilereference: cn=G2toG1, o=ibm, c=us
policyvalidityperiodreference: cn=allTheTime, o=ibm, c=us
ipsecsecurityactionreference: cn=secureG2toG1, o=ibm, c=us
ipsecisakmpactionreference: cn=generalPhase1Action, o=ibm, c=us

# DEVICEPOLICYRULES LIST for 2216CTR
dn: cn=rulesFor2216CTR, o=ibm, c=us
objectclass: devicepolicyrules
cn: rulesFor2216CTR
policyrulereference: cn=policySecureG1toG2, o=ibm, c=us

# DEVICEPROFILE for 2216CTR
dn: cn=deviceProfileFor2216CTR, o=ibm, c=us
objectclass: deviceprofile
cn: deviceProfileFor2216CTR
devicerulesreference: cn=rulesFor2216CTR, o=ibm, c=us

# DEVICEPOLICYRULES LIST for 2216BR
dn: cn=rulesFor2216BR, o=ibm, c=us
objectclass: devicepolicyrules
cn: rulesFor2216BR
policyrulereference: cn=policySecureG2toG1, o=ibm, c=us

# DEVICEPROFILE for 2216BR
dn: cn=deviceProfileFor2216BR, o=ibm, c=us
objectclass: deviceprofile
cn: deviceProfileFor2216BR
devicerulesreference: cn=rulesFor2216BR, o=ibm, c=us

```

In this scenario, pre-shared key mode is used on two 221x routers. It means that the certificate-based IKE Phase 1 negotiation definition should be removed or move down in ISAKMP proposal reference. To do this modify generalPhase1Action in the policyTemplates.ldif file like this:

```
dn: cn=generalPhase1Action, o=ibm, c=us
```

```
objectclass: ipsecisakmpaction
cn: generalPhase1Action
isakmpexchangemode: 2
isakmpproposalreference: 1: cn=veryStrongP1PropSharedKey, o=ibm, c=us
isakmpproposalreference: 2: cn=strongP1PropSharedKey, o=ibm, c=us
isakmpconnectionlifetime: 30000
isakmpconnectionlifetimekbytes: 5000
isakmpautostartflag: 0
```

LDAP server configuration for the 221x router is done and ready to access from routers.

6.3.2 LDAP client configuration on the IBM NWay 221x routers

The 221x family of routers (with V3.3 or greater) allow the repository of policy information to be a Lightweight Directory Access Protocol (LDAP) server. The routers support the ability to search (not modify) for information in the directory server. The policy search agent in the router will retrieve all the policy information in the directory server that is intended for that device.

When the policy exists in the LDAP server you should enable the routers to retrieve their policy from the LDAP server. You have to do the following steps:

- Set the default policy.
- Define the IP address of the LDAP server.
- Set the bind parameters to authenticate to the LDAP server.
- Configure the name of the DeviceProfile in the LDAP server.
- Enable retrieving policy from the LDAP server.
- List the LDAP configuration.
- Activate the LDAP configuration.

These bullets will be explained in more detail in the following sections.

6.3.2.1 Set default policy

We have to consider the time frame when the router is working but has not yet built its policy database. When a router boots it looks at the default rule. The default rule describes what a router should do with traffic while it is building its database. The options are forward all traffic or drop all traffic except LDAP traffic, or drop all traffic and secure LDAP traffic. The default is to forward all traffic.

If you are defining security policies you will probably wish to drop the traffic until the policy database is built; if not, the data would be forwarded without security. If you are retrieving you are also retrieving those policies using LDAP which you also want to use to forward your LDAP traffic. Therefore, you can define that LDAP should be secured. This default action is defined using the `set default` command. If you choose to secure your LDAP traffic you will be guided through creating an IPsec and ISAKMP action.

6.3.2.2 Define the IP address of the LDAP server

In `talk 6` and `feature policy` you have to define the IP address of the (primary) LDAP server. You could also define the IP address of a secondary LDAP server.

If the LDAP client gets no response from the primary LDAP server after the “retry interval” it will contact the secondary server. If the secondary server is available, it will retrieve the policies. If the secondary is unavailable, the router will then contact the primary again. The primary and then the secondary server will continue trying at the time interval specified in the “retry interval” until the router manages to retrieve the policies. The interval can be configured from `talk 6`, `feature policy`. While the router is trying other servers, it needs to know what to do with traffic. This is described in the default error handling procedure which is also configured using the `set default` command. The options are flush the whole database and apply the default rule or flush any LDAP rules and apply the local rules. This error handling also describes what happens if there is an error reading the rules.

If you are using LDAP and also define local rules, it is advisable to choose to apply the local rules if for any reason you cannot read the LDAP rules.

See Figure 48 for the configuration of the primary LDAP server:

```
Center *TALK 6
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>SET LDAP PRIMARY-SERVER 192.168.100.3
Center Policy config>
```

Figure 48. Set IP address of LDAP server

6.3.2.3 Set the bind parameters

LDAP defines that LDAP clients can either bind to the server without any authentication or with a user ID and password. Without authentication it is known as anonymous. Note that by default not all servers will support anonymous binds.

If you want to define authentication then set the bind parameters. First enable the sending of authentication parameters by issuing the following command (these parameters must match a user defined in your authentication server):

```
Center Policy config>
Center Policy config>SET LDAP ANONYMOUS-BIND
Do you wish to bind to the LDAP server anonymously? [Yes]: no
Center Policy config>SET LDAP BIND-NAME cn=root
Center Policy config>SET LDAP BIND-PW byte2eat
Center Policy config>
```

Figure 49. Set the LDAP bind parameters

6.3.2.4 Configure the name of the DeviceProfile in the LDAP server

When the router has bound with the LDAP server, it then performs its search for its policies. It identifies where it starts by sending in a start point. This value should be the distinguished name of the router as configured in the DeviceProfile.

Figure 51 on page 106 shows the configuration of the distinguished name of the DeviceProfile object in the LDAP server for this device.

```
Center Policy config>
Center Policy config>SET LDAP POLICY-BASE cn=DeviceProfileFor2216ctr, o=ibm, c=us
Center Policy config>
```

Figure 50. Configure the name of the DeviceProfile in the LDAP server

6.3.2.5 Enable retrieving policy from the LDAP server

To enable the retrieve function use the following command:

```
Center Policy config>
Center Policy config>ENABLE LDAP POLICY-SEARCH
Center Policy config>
```

Figure 51. Enable retrieving policy from the LDAP server

6.3.2.6 List LDAP configuration

The command `list ldap` lists the LDAP configuration (see Figure 52):

```
Center Policy config>
Center Policy config>LIST LDAP
LDAP CONFIGURATION information:
    Primary Server Address:          192.168.100.3
    Secondary Server Address:        0.0.0.0
    Search timeout value:            3 sec(s)
    Retry interval on search failures: 1 min(s)
    Server TCP port number:          389
    Server Version number:           2
    Bind Information:
    Bind Anonymously:                No
    Device Distinguished Name:        cn=root
    Base DN for this device's policies: cn=DeviceProfileFor2216ctr, o=ibm,
    Search policies from LDAP Directory: Enabled
Center Policy config>
```

Figure 52. Listing LDAP configuration

6.3.2.7 Activate the LDAP configuration

For the changes made above to take effect, the user must either restart/reload the router or go into talk 5 and use the dynamic reconfiguration feature of the router to activate the changes.

This procedure is shown in Figure 53:

```
Center *TALK 5
Center Policy console>RESET LDAP-CONFIG
LDAP Policy Configuration reset successfully
Center Policy console>
Center Policy console>RESET DATABASE
Policy Database reset successful
Center Policy console>
```

Figure 53. Activating the LDAP configuration

6.3.2.8 Support from IBM networking home page

Check the networking home page for LDAP server configuration information. It can be found at

<http://www.networking.ibm.com/support/code.nsf/22101dap?OpenView>

In "Configuration and Setup Instructions for Reading Policies from a LDAP Server" you can find further hints for troubleshooting LDAP.

6.3.3 Secure transmission of LDAP traffic using tunnels

LDAP traffic flows through the Internet, and is therefore assumed to be nonsecure. Because of this, from a security point of view, secure transmission of LDAP data between client and server is needed.

The best way to make LDAP traffic secure is using Secure Sockets Layer (SSL) between LDAP client and LDAP server. If the network devices do not support Secure Sockets Layer, other secure channels between them are needed.

We consider IKE tunnel or manual tunnel between LDAP client and server only for LDAP traffic.

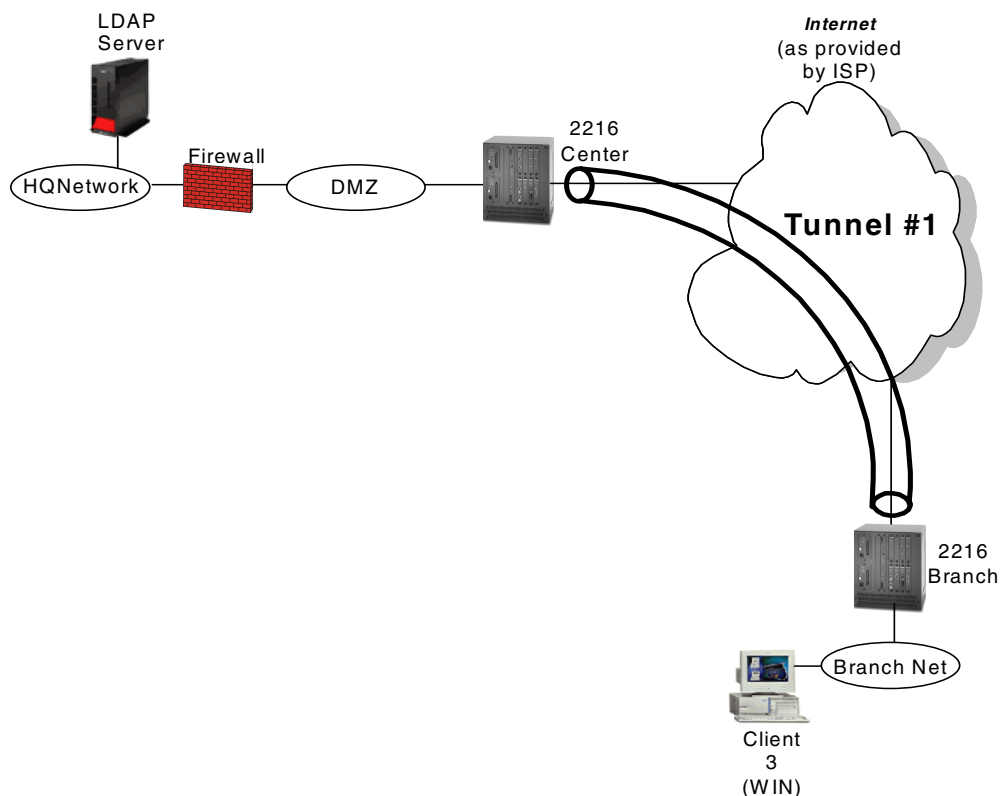


Figure 54. Initial tunnel for LDAP traffic

The following steps explain the procedure for securing LDAP information using a tunnel:

1. Before installing the 2216 branch router, IKE tunnel or manual tunnel definition that only allows IPsec and LDAP traffic (see Tunnel #1 in Figure 54) must be

in place in the 2216 branch router and the corresponding tunnel definition must be in place in the 2216 center router.

2. The 2216 branch router will initiate a predefined tunnel to the 2216 center router and establish a tunnel for a secure LDAP data transfer at boot-up.
3. The 2216 branch router will request tunnel configuration information to the LDAP server through a predefined tunnel.
4. The 2216 branch router makes tunnels according to the configuration information from LDAP server for normal data traffic.
5. The 2216 branch router may release a predefined tunnel if possible.

The predefined tunnel can be established directly between the LDAP server and 2216 branch router if there is no Network Address Translation (NAT) issue.

This method may be useful and efficient for a service provider to deploy an Internet VPN solution without human error.

Chapter 7. Network management for VPNs

With the growth of a network the complexity increases and the ability to manage it decreases. Therefore, everybody who is responsible for running a network should pay attention to this aspect of management. The network management function should enable the support functions to maintain the network effectively and efficiently.

In this section we describe the general concept of network management and design considerations specific to the Internet VPN.

7.1 Systems management

The management requirements are categorized into disciplines. A discipline is a broad category of systems management tasks and the functions that address those tasks. The disciplines, therefore, are categories for systems management processes. You can, for example, formalize this into the following six systems management disciplines:

Business management

The business management discipline focuses on managing the tasks that support a wide range of enterprise-wide business and administrative functions to improve control of information system assets and provide efficient and effective administrative processes.

Change management

The change management discipline focuses on managing the introduction of change into an information system environment.

Configuration management

The configuration management discipline focuses on managing the set of resources (hardware and software) and connectivity that provide the exchange of business information within an enterprise and with external customers.

Operations management

The operations management discipline focuses on managing the use of systems and resources to support the workloads of the enterprise's information systems.

Problem management

The problem management discipline focuses on managing problems and potential problems from their detection to their resolution.

Performance management

The performance management discipline focuses on managing the effectiveness with which information systems deliver services to their users.

In general, from the network management viewpoint, the above six disciplines can be applied to the Internet VPN management. Comparing traditional network

management, the Internet VPN has distinct characteristics that will be discussed in this chapter.

- For change management, the gateways (for example, routers) are physically connected through the Internet and the VPNs are logically controlled by tunnel definition on the gateways. The management of changes in VPN is logical rather than physical.
- For configuration management, the topology, tunnel definition, and applied security policy are maintained centrally in addition to traditional network configuration. The remote access user information must be maintained. The secure key distribution including certification and directory-based policy management will be the critical part of the configuration management.
- For problem management, there are two aspects of connectivity problems in VPN. One is the IP connectivity to the Internet and another is the secure VPN tunnel connectivity over IP connectivity. The VPN tunnel establishment and status monitoring in addition to IP connectivity monitoring must be done to identify the problem.
- For performance management, the normal IP traffic and secure VPN traffic through a tunnel is transferred using one physical line. And normally the performance degradation will occur to VPN traffic. The performance for each tunnel may also be measured as physical line traffic.

7.2 Design considerations

There are two topology viewpoints, physical topology and logical topology. From the point of view of an Internet VPN service provider, both physical topology and logical topology must be maintained and monitored. In other words, companies that use Internet VPN from a service provider only need logical topology management.

The topology of the traditional IP network is a star or tree from the physical and logical viewpoint. But for Internet VPN, the physical network topology is mesh. From the network management viewpoint, the physical network is considered a network cloud such as a frame relay network and each router is connected to that network cloud. Logical topology is more important than physical topology.

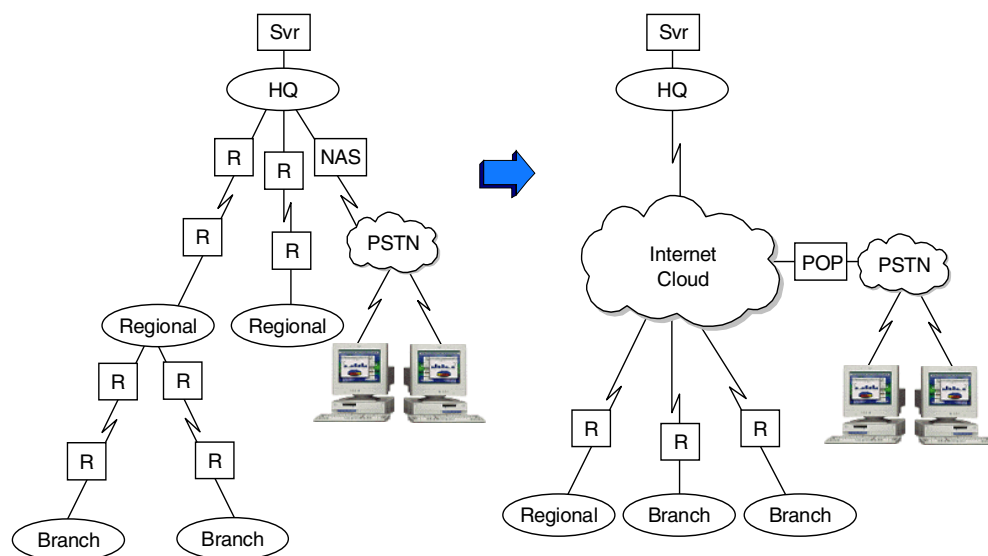


Figure 55. Comparison of conceptual topology

7.3 SNMP management

The network management system uses the following protocols:

- Simple Network Management Protocol (SNMP)
- ICMP echo/reply

SNMP is based on a manager-agent interaction. The network elements, such as gateways, routers, bridges, and hosts, contain SNMP agents that act as servers and perform the network management functions requested by the network managers. The network managers act as clients; they run the management applications that monitor and control the agents.

SNMP uses request/response processing as a means of communicating between the network managers and the agents in the network elements to send and receive information about network resources. This information can be status information, counters, identifiers, and more. Request/response processing involves the exchange of information among different entities through requests that are received by an entity for processing, after which it generates a response to be sent back to the originator of the request. SNMP uses this type of protocol to transfer data between managers and agents. The SNMP manager can send a request to the SNMP agent, which in return will send a response. The SNMP request/response process is shown in Figure 56 on page 112.

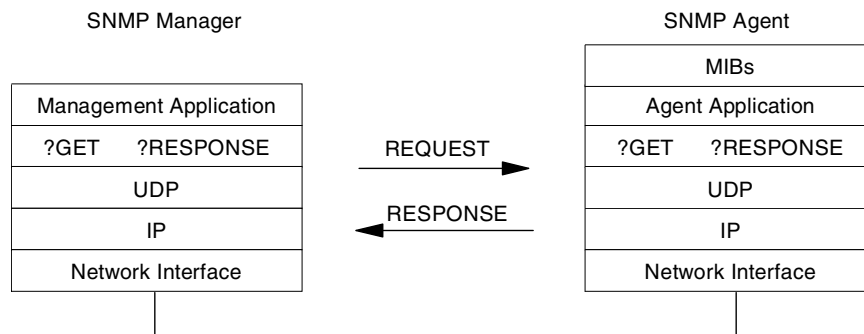


Figure 56. SNMP request/response process

An agent system can also generate SNMP messages called traps without a prior request from the managing system. The purpose of a trap message is to inform the managing system of an extraordinary event that has occurred at the agent system. The SNMP trap process is shown in Figure 57.

An SNMP protocol entity receives messages at UDP port 161 on the system with which it is associated, except for those that report traps. Messages that report traps should be received on UDP port 162.

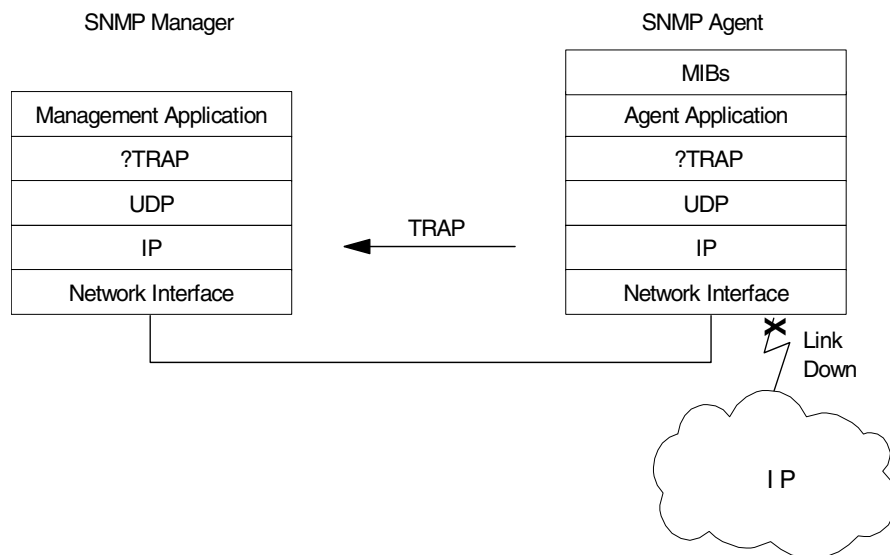


Figure 57. SNMP trap process

An SNMP community is an administrative relationship between an SNMP agent and one or more SNMP managers. Each community consists of a community name, an object access specification, and a list of SNMP managers' IP addresses. The SNMP manager needs to provide a valid community name to the SNMP agent before the agent will honor any requests from that manager. In this manner, the community acts as a password.

Even though SNMP uses community to authenticate a requested party, SNMP traffic flows in cleartext and can be sniffed easily and the critical network information is included in SNMP traffic. The secure SNMP data transmission

through the Internet is required. The management tunnels must be used for securing SNMP traffic. The data tunnel can also be used as the management tunnel. If a dedicated management tunnel is used, proper filter rules for SNMP and ICMP should be implemented to ensure security.

7.4 SNMP management and VPNs

We describe network design consideration for network management function, especially management tunnels. From the network management viewpoint, the Internet VPN is categorized below.

Figure 58 and Figure 59 on page 114 show typical network configurations for VPNs.

The general design consideration for Internet VPN is limiting the automatic network discovery function using a seed file when NMS discovers a network. For a normal IP network, NMS can discover as many network nodes as the network has. But in case of Internet VPN, specific IP addresses for each node must be defined before discovery. Sometimes, intermediate routers cannot provide IP address and interface information at the NMS's request.

The network management system can also use a data tunnel between the center gateway and the remote gateway to transfer management traffic between NMS and managed gateways. In this case, no special design considerations exist.

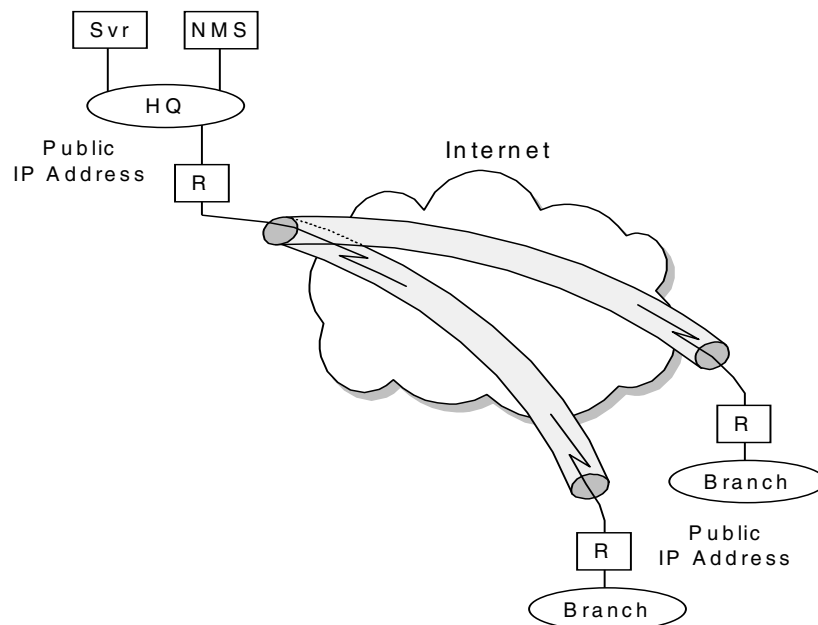


Figure 58. Gateway-to-gateway network connection with public IP addresses

For gateway-to-gateway tunnel connections these subnetworks use public IP addresses; NMS displays public addresses.

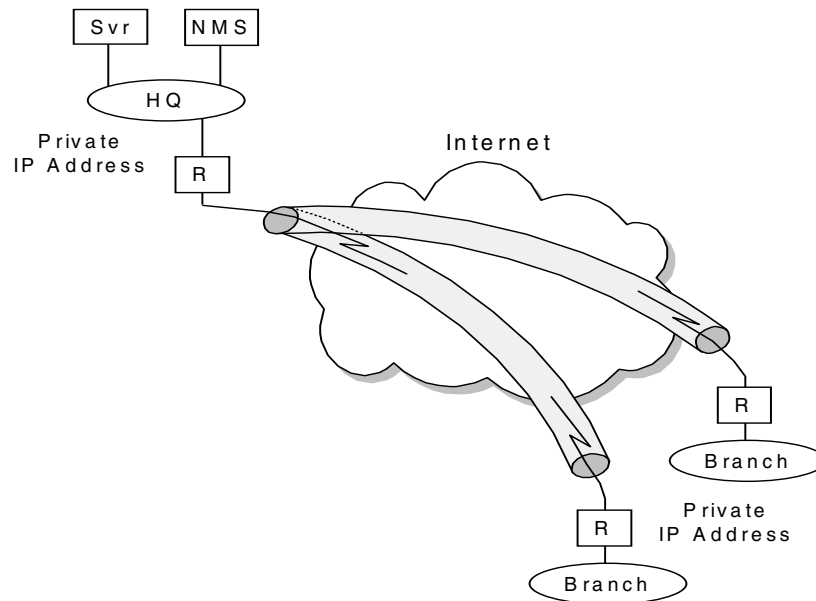


Figure 59. Gateway-to-gateway network connection with private IP addresses

For gateway-to-gateway tunnel connections these subnetworks use private IP addresses; NMS displays public IP addresses for Internet-connected interfaces and private IP addresses for subnets connected to a LAN interface. The tunnels provide a transparent view to NMS and NMS can recognize private IP addresses of the subnet on a remote site. The design consideration for these cases is the scope of managed objects. For example, for simple network management, the management scope may be the network between gateways. The management scope may include network, gateways, and LAN in remote sites. Before designing NMS, it is necessary to determine the management scope.

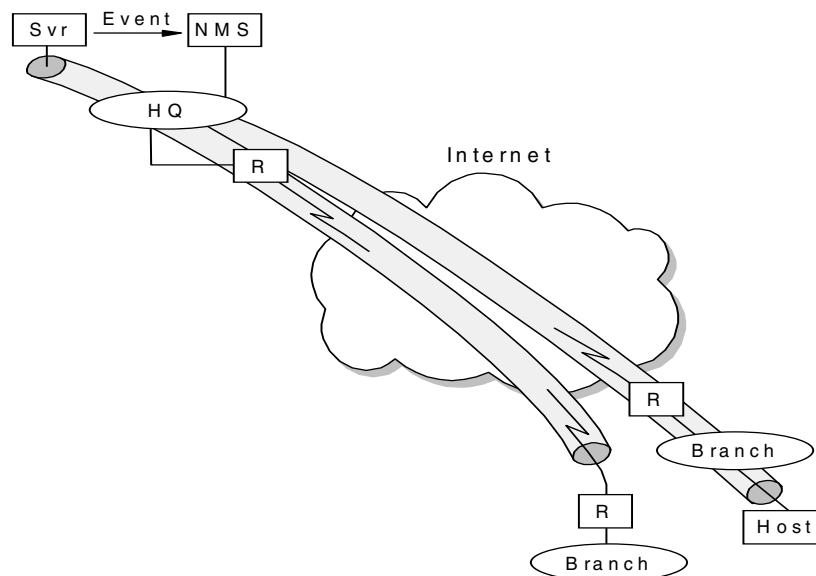


Figure 60. Gateway-to-host network connection and host-to-host network connection

For the gateway-to-host network connection, the NMS can monitor these types of tunnel connections through gateways. But if the NMS is located in a central site and the gateway is located in a remote site, it is not easy to monitor a gateway from NMS when the tunnel or physical line has a problem.

For the host-to-host network connection, the NMS cannot monitor host-to-host tunnel connections. In this case, special design consideration is required. One of the possible solutions is using a system management tool such as Tivoli Distributed Monitor to detect changes in the host and integrate an event to NMS. Before considering the above solution, checking if the host supports IPsec MIB may be needed.

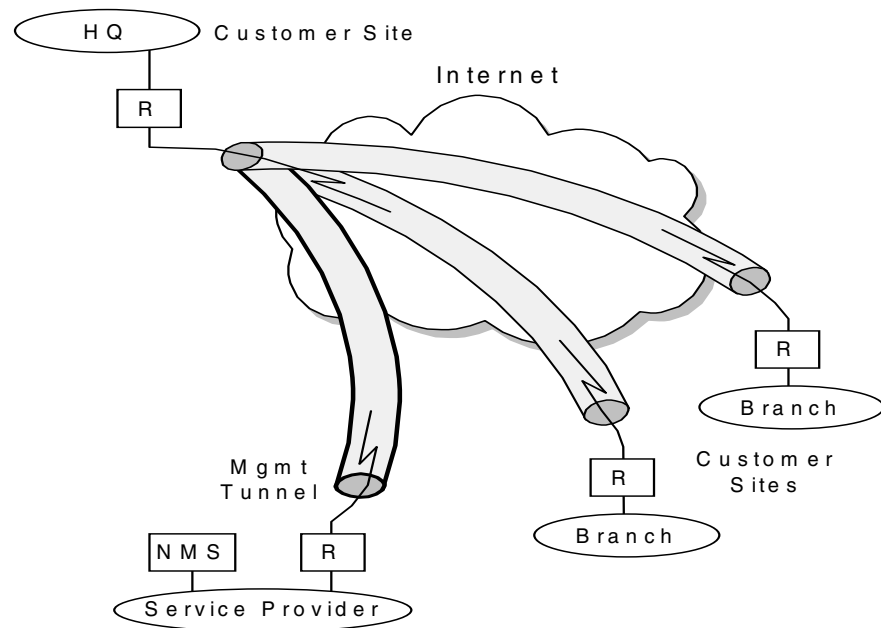


Figure 61. Internet VPN service provider

From the Internet VPN service provider viewpoint, an additional tunnel for management traffic between a service provider's network to the gateway in a customer's center site must be implemented to monitor a customer's VPNs. In this case, the filtering to protect traffic flow among a customer's network must be implemented and assured. The physical topology and IP connectivity should be monitored and maintained on behalf of the customer.

7.4.1 Management objects for Internet VPN

The physical and logical characteristics of a system make up a collection of information that can be managed through SNMP. The individual pieces of information make up Management Information Base (MIB) objects. A MIB is comprised of MIB objects, and they reside on the agent system, where they can be accessed and changed by the agent at the manager's request.

The MIBs that may be used for IPsec are categorized below:

- Monitoring and status MIBs for IPsec
- Configuring IPsec implementation
- Policy information

Currently, only monitoring and status MIBs for IPsec is in draft, `draft-ietf-ipsec-mib-03.txt`. These MIBs provide capabilities to determine operating conditions, perform system operational level monitoring of the IPsec portion of a network and statistics.

The IPsec MIB provides information related to both Phase 1 (or IKE) SAs and Phase 2 (or IPsec) SAs. SA configuration is provided as are statistics related to the SAs. A number of aggregate totals is provided for taking snapshots of system behavior or traffic trend without excessive SNMP traffic. This statistics MIB is useful to VPN service providers.

Four tables are used to define IPsec:

- The IKE control channel
- The IKE SAs
- The IPsec virtual tunnel
- The IPsec protection suite

Some information about SAs is left out for security considerations if SNMP traffic becomes compromised.

The SNMP traps are used to notify error condition and status changes from IPsec function. A transient tunnel such as a dial-in connection will go up and down frequently and notification from this tunnel is not necessary for system administration. A permanent tunnel such as a gateway-to-gateway connection is considered a significant resource and the notifications from this tunnel should be monitored and handled properly.

The traps are forwarded from an IPsec-enabled device when the Phase 1 or 2 negotiation fails, the packets with an invalid sequence number or selector are received, or ESP or AH packets with unknown SPIs are detected.

7.4.2 Integration into other management tools

For proactive management and system-network combined management, the network management system may cooperate with other management tools or directory server.

The Lightweight Directory Access Protocol (LDAP) server contains network configuration information centrally and NMS can be notified when configuration information in the LDAP server for certain network nodes is changed or NMS can issue configuration refresh action to a network node.

Normally NMS can monitor a gateway-to-gateway tunnel, but NMS cannot monitor host-to-host tunnel connection. In this case, the system management tool that provides system resource monitoring functions, such as Tivoli Distributed Monitor, can detect the status changes of the VPN tunnel between two hosts and forward the event to NMS. This seamless event integration can be helpful to network and system administrators to identify a problem cause and isolate a problem source.

7.5 Network management objects for IBM Nways routers

For Nways routers, two MIBs are defined for VPNs:

- ibmipsec.mib: IP Security MIB
- ibmvpnpolicy.mib: VPN Policy MIB

These two MIBs can be found under the IBM Enterprise Specific MIB tree.

The IP Security MIB has the following object groups:

- IPsec Levels Group:
Describes the level of the IBM IPsec MIB used.
- IPsec Phase-1 Group:
Consists of an Internet Key Exchange (IKE) tunnel table that has IKE tunnel configuration information.
- IPsec Phase-2 Group:
Consists of Phase-2 tunnel statistics, tunnel information, client information related to Phase-2 tunnel, and security protection suite.
- IPsec History Group:
Consists of previous Phase-2 tunnel history and failure records.
- IPsec TRAP Control Group:
Consists of objects that control the sending of IPsec TRAPs.

The VPN Policy MIB has the following object groups:

- The System Group: Consists of global system parameters such as policy source and LDAP configuration information.
- The Policy Group: Consists of policies, policy rules such as priorities, and correlations to VPN policies with VPN policy rules.
- The Conditions Group: Consists of a traffic profile and traffic interface which controls traffic, remote identification methods such as authentication, and validity period.
- The Actions Group: Consists of actions for RSVP, Differential Services, ISAKMP, which includes ISAKMP proposal, and Security, which includes security proposals and AH and ESP transforms.
- The Test Group: Consists of table for policy test.

The supported IP Security related traps are list in Figure 62 on page 118. These traps are defined in IP Security MIB and the enterprise value is ibmIROCroutingIpSec (1.3.6.1.4.1.2.6.119.4.9).

| Trap name | Trap no. | Description |
|------------------|----------|---|
| ikeTunnelStart | 1 | Generation of this trap occurs each time an IPSec IKE Phase-1 tunnel is created. |
| ikeTunnelStop | 2 | Generation of this trap occurs each time an IPSec IKE Phase-1 tunnel is terminated. |
| ipSecTunnelStart | 3 | Generation of this trap occurs each time an IPSec Phase-2 tunnel is created. |
| ipSecTunnelStop | 4 | Generation of this trap occurs each time an IPSec Phase-2 tunnel is terminated. |
| ipSecAuthFail | 5 | Generation of this trap occurs each time an IPSec Phase-2 authentication failure is detected. |
| ipSecDecryptFail | 6 | Generation of this trap occurs each time an IPSec Phase-2 decryption failure is detected. |

Figure 62. Traps defined in IP Security MIB

IBM provides VPN management function of the 221x router, status monitoring and policy management. To manage VPN networks that consist of IBM 221x routers, the following components are required:

- Tivoli TME 10 NetView
- Nways VPN Manager

In addition to traditional management functions, topology management and device management, the Nways VPN manager provides VPN specific functions:

- Supporting layer-2 and layer-3 VPNs, including IKE tunnel
- Validating VPN policies and tunnels
- Policy test simulating traffic against VPN policies in the router
- Layer-2 test for dial-in users to replicate dial-in response time and connectivity
- Forwarding of VPN events to the network management console such as Tivoli TME 10 NetView
- Operational control to prompt policy refresh from the LDAP server

You can find more details on Nways VPN manager in the redbook *A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions*, SG24-5234.

Part 2. IBM VPN platforms with IKE support

Chapter 8. Introduction to IBM VPN solutions

This chapter presents a detailed discussion of the VPN functions provided by various IBM platform implementations. Even though this redbook is almost entirely focused on IKE and VPN platforms that implement it, we have included in this chapter an overview of IBM VPN products that do not support it. This is because some of these products are still current and may fulfill a customer's VPN requirements for the time being even without IKE. However, scenarios based upon such products are not included in this redbook. For the benefit of customers who are planning on migrating from non-IKE-enabled VPN platforms to new implementations that support IKE, we have included a compatibility table between new and previous IBM VPN platforms in this chapter.

To learn more about IBM VPN products that do not support IKE, please refer to the redbook *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions*, SG24-5201.

Apart from software and operating system products that implement VPN technologies, IBM also offers network and security consultancy, design and implementation services for VPN, which are not subjects of this redbook. Your IBM representative will provide you with more information on additional VPN solutions from IBM, and you can also use the URLs below for further reference:

www.ibm.com/services/portfolios/

www.software.ibm.com/secureway/services/

8.1 IBM VPN platforms - IPSec and IKE feature summary

Table 16 illustrates the VPN capabilities of IBM platforms that support both IPSec and IKE. These are the platforms used to build the VPN scenarios in the following chapters of this redbook.

Table 16. IBM VPN solutions - VPN support using IPSec and IKE

| Feature | | Comm. Server V2R8 for OS/390 | OS/400 V4R4 Native VPN Support | Nways Routers MRS/AIS/MAS V3.3 | AIX 4.3.2 and AIX 4.3.3 |
|---|-----------------|------------------------------|--------------------------------|--------------------------------|-------------------------|
| Tunnel Type | Manual | √ | √ | √ | √ |
| | IKE | √ | √ | √ | √ |
| IPSec Header Format | RFCs 24xx | √ | √ | √ | √ |
| | RFCs 18xx | | | | √ |
| Internet Key Exchange (IKE) Protocol | | | | | |
| Key Management Tunnel (Phase 1) | | | | | |
| Negotiation Mode | Main Mode | √ | √ | √ | √ |
| | Aggressive Mode | √ | √ | √ | √ |
| Role | Initiator | √ | √ | √ | √ |
| | Responder | √ | √ | √ | √ |

| Feature | | Comm. Server V2R8 for OS/390 | OS/400 V4R4 Native VPN Support | Nways Routers MRS/AIS/MAS V3.3 | AIX 4.3.2 and AIX 4.3.3 |
|---|-----------------|------------------------------|--------------------------------|--------------------------------|-------------------------|
| Encryption Algorithm | DES | √ | √ | √ | √ |
| | Triple DES | √ | √ | √ | √ |
| Authentication Method | Pre-Shared Keys | √ | √ | √ | √ |
| | RSA Signatures | √ | | √ | (planned PTF for 4.3.3) |
| Hash Algorithm | HMAC-MD5 | √ | √ | √ | √ |
| | HMAC-SHA | √ | √ | √ | √ |
| Diffie-Hellman Group | Group 1 | √ | √ | √ | √ |
| | Group 2 | √ | √ | √ | √ |
| Phase 1 ID | IP Address | √ | √ | √ | √ |
| | FQDN | √ | √ | √ | √ |
| | other | √ | √ | √ | √ |
| Send Multiple SA Proposals | | | | √ | √ |
| Receive Multiple SA Proposals | | | | √ | √ |
| Send phase 1 delete | | √ | √ | √ | √ |
| On-demand Outbound Tunnels | | | | √ | √ (4.3.3) |
| Data Management Tunnel (Phase 2) - IPsec | | | | | |
| Encapsulation Mode | Tunnel Mode | √ | √ | √ | √ |
| | Transport Mode | √ | √ | √ | √ |
| Security Protocol ^a | AH | √ | √ | √ | √ |
| | ESP | √ | √ | √ | √ |
| AH Authentication Algorithm | HMAC-MD5 | √ | √ | √ | √ |
| | HMAC-SHA | √ | √ | √ | √ |
| ESP Encryption ^b Algorithm | CDMF | √ | | √ | |
| | DES | √ | √ | √ | √ |
| | Triple DES | √ | √ | √ | √ |
| | NULL | √ | √ | √ | √ |
| ESP Authentication ^b Algorithm | HMAC-MD5 | √ | √ | √ | √ |
| | HMAC-SHA | √ | √ | √ | √ |
| | NULL | √ | √ | √ | √ |
| Send Multiple SA Proposals | | | | √ | √ |
| Receive Multiple SA Proposals | | | | √ | √ |

| Feature | | Comm. Server V2R8 for OS/390 | OS/400 V4R4 Native VPN Support | Nways Routers MRS/AIS/MAS V3.3 | AIX 4.3.2 and AIX 4.3.3 |
|---|---------------------------|------------------------------|--------------------------------|--------------------------------|-------------------------|
| Perfect Forward Secrecy (PFS) | Group 1 | √ | √ | √ | √ (4.3.3) |
| | Group 2 | √ | √ | √ | √ (4.3.3) |
| Replay Protection Selectable ^c | | √ | | √ | √ |
| Other | Packet Filtering | √ | √ | √ | √ |
| | Logging | √ | √ | √ | √ |
| | IP Version 6 ^d | √ | | √ | √ |

a. Both AH and ESP are implicitly supported

b. Null is not supported for both

c. Supported on all IBM platforms but on OS/400 you cannot choose not to use it

d. IPSec for IPv6

8.2 IBM VPN platforms - layer-2 tunneling feature summary

Table 17 illustrates the VPN capabilities of IBM platforms that support layer-2 tunneling. These are the platforms used to build the VPN scenarios in the following chapters of this redbook.

Table 17. IBM VPN solutions - VPN support using layer-2 tunneling

| Feature | | OS/400 V4R4 Native VPN Support | Nways Routers MRS/AIS/MAS V3.3 |
|------------------------------|---------|--------------------------------|--------------------------------|
| Layer-2 tunneling | | | |
| Voluntary L2TP | | √ | √ |
| Compulsory L2TP | | LNS only | √ |
| L2TP Dial-out | | LAC only | √ |
| L2F | | | √ |
| PPTP | | | √ |
| PPP Authentication | PAP | √ | √ |
| | CHAP | √ | √ |
| | MS-CHAP | | √ |
| | SPAP | | √ |
| PPP Encryption | ECP | | √ |
| | MPPE | | √ |
| Tunnel Authentication | Local | √ | √ |
| | RADIUS | | √ |
| PPP Multilink Support | | | √ |

| Feature | OS/400 V4R4 Native VPN Support | Nways Routers MRS/AIS/ MAS V3.3 |
|----------------------------------|---|--|
| Multiprotocol Support | IP only | √ |
| IPSec Protection for L2TP Tunnel | √ | √ |

8.3 IBM VPN platforms - interoperability matrix for IKE

Table 18 provides an overview of possible compatibility scenarios between IBM VPN platforms that support IKE and IPSec. The combinations that we have used and tested in this or other redbooks are highlighted in bold.

Some of the combinations listed below are of academic interest only because they are unlikely or impractical, or both, in a customer environment. We have indicated such combinations by placing parentheses around them.

Table 18. IBM VPN solutions - IKE interoperability matrix

| Platform | Comm. Server V2R8 for OS/390 | OS/400 V4R4 Native VPN Support | Nways Routers MRS/MAS V3.3 | AIX 4.3.2 and AIX 4.3.3 |
|--|--|--|--|--|
| Comm. Server V2R8 for OS/390 | H - H (G - G) (H - G) (G - H) | H - H H - G (G - G) (G - H) | H - G (H - H) (G - G) (G - H) | H - H H - G (G - G) (G - H) |
| OS/400 V4R4 Native VPN Support | H - H G - H (G - G) (H - G) | H - H G - G H - G G - H | H - G G - G (G - H) (H - H) | H - H G - H H - G G - G |
| Nways Routers MRS/AIS/ MAS V3.3 | G - H (H - H) (G - G) (H - G) | G - G G - H (H - G) (H - H) | G - G H - H (G - H) (H - G) | G - H G - G (H - H) (H - G) |
| AIX 4.3.2 and AIX 4.3.3 | H - H G - H (H - G) (G - G) | H - H H - G G - H G - G | H - G G - G (H - H) (G - H) | H - H G - G H - G G - H |

Note: H - G does not imply that the reverse direction, G - H, is also possible. It is only possible where explicitly specified.

8.4 IBM VPN platforms supporting IPSec but not IKE

In this section we describe VPN capabilities of older IBM VPN products that do not have IKE capabilities but are still widely deployed and are not to be replaced

with new versions immediately because they perform their duties and customers have more important issues at hand for the time being.

Table 19. IBM VPN solutions - VPN support by products without IKE

| Feature | | Comm. Server V2R7 for OS/390 | OS/400 V4R3 Firewall | Nways Routers MRS/MAS V3.2 | AIX 4.3.1 | eNetwork Firewall V4.1 for AIX | eNetwork Firewall V3.3 for Windows NT |
|---------------------------------|---------------------------|------------------------------|----------------------|----------------------------|-----------|--------------------------------|---------------------------------------|
| Tunnel Type | IBM | | √ | | √ | | |
| | Manual | √ | √ | √ | √ | √ | √ |
| IPSec Header Format | RFCs 24xx | √ | | √ | √ | √ | √ |
| | RFCs 18xx | √ | √ | | √ | | |
| IPSec manual/IBM tunnels | | | | | | | |
| Encapsulation Mode | Tunnel Mode | √ | √ | √ | √ | √ | √ |
| | Transport Mode | √ | √ | √ | √ | √ | √ |
| Security Protocol | AH | √ | √ | √ | √ | √ | √ |
| | ESP | √ | √ | √ | √ | √ | √ |
| AH Authentication Algorithm | HMAC-MD5 | √ | √ | √ | √ | √ | √ |
| | HMAC-SHA | √ | √ | √ | √ | √ | √ |
| | Keyed MD5 | √ | √ | | √ | | |
| ESP Encryption Algorithm | CDMF | √ | √ | √ | ? | √ | √ |
| | DES 32-bit IV | √ | √ | √ | √ | | |
| | DES 64-bit IV | √ | √ | √ | √ | √ | √ |
| | Triple DES | √ | | √ | √ | √ | √ |
| | NULL | √ | | √ | √ | √ | √ |
| ESP Authentication Algorithm | HMAC-MD5 | √ | √ | √ | √ | √ | √ |
| | HMAC-SHA | √ | √ | √ | √ | √ | √ |
| | NULL | √ | | √ | √ | √ | √ |
| Other | Packet Filtering | √ | √ | √ | √ | √ | √ |
| | Logging | √ | √ | √ | √ | √ | √ |
| | IP Version 6 ^a | | | | √ | | |
| L2TP | | | | √ | | | |

a. IPSec for IPv6

8.5 IBM VPN platforms - interoperability matrix for IPSec without IKE

Table 20 on page 126 provides an overview of possible compatibility scenarios between IBM VPN platforms that support IKE and IPSec and those that only support IPSec with manual or IBM tunnels. None of these combinations has been

used and tested in this redbook because it focuses entirely on IKE. However, combinations between platforms supporting manual tunnels have been tested by IBM development.

Table 20. IBM VPN solutions - interoperability matrix between IKE-enabled and non-IKE-enabled IBM VPN platforms

| Platform | Comm. Server V2R7 for OS/390 | OS/400 V4R3 Firewall | Nways Routers MRS/MAS V3.1 | AIX 4.3.1 | eNetwork Firewall V4.1 for AIX | eNetwork Firewall V3.3 for NT |
|--------------------------------|------------------------------|----------------------|----------------------------|-----------------|--------------------------------|-------------------------------|
| Comm. Server V2R8 for OS/390 | manual RFC 24xx | | manual RFC 24xx | manual RFC 24xx | manual RFC 24xx | manual RFC 24xx |
| OS/400 V4R4 Native VPN Support | manual RFC 24xx | | manual RFC 24xx | manual RFC 24xx | manual RFC 24xx | manual RFC 24xx |
| Nways Routers MRS/MAS V3.3 | manual RFC 24xx | | manual RFC 24xx | manual RFC 24xx | manual RFC 24xx | manual RFC 24xx |
| AIX 4.3.2 and AIX 4.3.3 | manual RFC 24xx | manual RFC 18xx | manual RFC 24xx | manual RFC 24xx | manual RFC 24xx | manual RFC 24xx |

8.6 IBM and OEM VPN platforms - interoperability matrix

Table 21 provides an overview of possible compatibility scenarios between IBM and OEM VPN platforms that support IKE and IPSec. The combinations that we have used and tested in this or other redbooks are highlighted in bold.

Some of the combinations listed below are of academic interest only because they are unlikely, impractical or both in a customer environment. We have indicated such combinations by placing parentheses around them.

Table 21. IBM VPN solutions - OEM interoperability matrix

| Platform | Comm. Server V2R8 for OS/390 | OS/400 V4R4 Native VPN Support | Nways Routers MRS/MAS V3.3 | AIX 4.3.2 and AIX 4.3.3 |
|-----------------------------------|--|---|---|---|
| Cisco routers, IOS 12.0(5) | G - H (G - G) (H - G) (G - H) | G - G G - H (H - H) (H - G) | G - G H - H (G - H) (H - G) | G - G G - H (H - H) (H - G) |
| Windows 2000 server | H - H G - H (G - G) (H - G) | H - H G - G H - G G - H | H - G G - G (G - H) (H - H) | H - H G - H H - G G - G |
| IRE SafeNet 2.0.7b18 | H - H (H - G) | H - H H - G | H - G (H - H) | H - H H - G |

| Platform | Comm. Server V2R8 for OS/390 | OS/400 V4R4 Native VPN Support | Nways Routers MRS/MAS V3.3 | AIX 4.3.2 and AIX 4.3.3 |
|-----------------------------------|---|---|---|--|
| WRN WinVPN 1.2 | | H - G (H - H) | H - G (H - H) | |
| NTS Tunnel Builder 1.0 | | H - G (H - H) | H - G (H - H) | |

Note: H - G does not imply that the reverse direction, G - H, is also possible. It is only possible where explicitly specified.

Chapter 9. AIX V4.3.2 and V4.3.3

This section describes the VPN feature of AIX V4.3.2 and AIX V4.3.3. This includes VPN feature summary, installation, basic configuration, and advanced configuration of the Internet Key Exchange (IKE) feature. Manual tunnel configuration, which is inherited from previous AIX versions, is also described.

9.1 AIX V4.3.2

AIX V4.3.2 offers a rich set of VPN features. With its included packet filtering and logging functionality it could even be used as an entry firewall. In addition, the Internet Key Exchange (IKE) feature is added for easy and secure tunnel establishment.

9.1.1 IPSec and Internet Key Exchange (IKE) VPN features

AIX V4.3.2 offers an Internet Key Exchange feature that supports automated negotiation of security associations, and automated generation and refresh of cryptographic keys. The ability to perform these functions with little or no manual configuration of machines will be a critical element as a VPN grows in size.

IKE uses a two-phased approach, Phase 1 for key management tunnel establishment and Phase 2 for data management tunnel establishment.

Table 22. IBM SecureWay VPN Client - VPN features

| Feature | |
|----------------------------------|--|
| Tunnel Type | manual, IKE |
| IPSec Header Format | RFCs 24xx, RFC 18xx |
| IKE | |
| Key Management Tunnel (Phase 1) | |
| Role | Initiator, Responder |
| Negotiation Mode | Main Mode, Aggressive Mode |
| Encryption Algorithm | DES, Triple DES |
| Authentication Method | Pre-Shared Key |
| Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| Diffie-Hellman Group | Group 1, Group 2 |
| Send Phase 1 Delete | Yes |
| Multiple Proposals | Yes |
| Data Management Tunnel (Phase 2) | |
| Encapsulation Mode | Tunnel Mode, Transport Mode |
| Security Protocol | AH, ESP |
| AH Authentication Algorithm | HMAC-MD5, HMAC-SHA (keyed MD5 for manual) |

| Feature | |
|-------------------------------|--|
| ESP Encryption Algorithm | DES, Triple DES, NULL (CDMF for manual) |
| ESP Authentication Algorithm | HMAC-MD5, HMAC-SHA, NULL |
| Multiple Proposals | Yes |
| Perfect Forward Secrecy (PFS) | No |
| Other | IPv6, Logging |

9.1.2 VPN feature installation on AIX V4.3.2

The installation of additional features on AIX V4.3.2 are required, which are not installed through the standard AIX installation process. Web-based System Manager must be installed before the IPSec installation because Web-based System Manager is used to configuring and controlling the IKE feature of VPN.

Installation of the following components is needed from the AIX CD-ROM:

| Fileset | Level | State | Description |
|-------------------------|---------|-------|-------------------------------------|
| ----- | ----- | ----- | ----- |
| bos.msg.en_US.net.ipsec | 4.3.1.0 | C | IP Security Messages - U.S. English |
| bos.net.ipsec.rte | 4.3.2.0 | C | IP Security |

IP Security provides the means for verifying the authenticity and integrity of IP packets and providing privacy of data through the use of encryption. This is accomplished by applying keyed authentication and encryption algorithms to the data and using the Authentication Header (AH) protocol or the Encapsulating Security Payload (ESP) protocol.

The crypto packages are available on the AIX Bonus Pack CD-ROM. These crypto packages support the following algorithms:

- bos.crypto - 40-bit Encryption for IP Security (CDMF)
- bos.crypto-us - 56-bit Encryption for IP Security (DES)
- bos.crypto-priv - Triple DES Encryption for IP Security (3DES)

| Fileset | Level | State | Description |
|-----------------|---------|-------|---------------------------------------|
| ----- | ----- | ----- | ----- |
| bos.crypto | 4.3.2.0 | C | 40 Bit Encryption for IP Security |
| bos.crypto-priv | 4.3.2.0 | C | Triple DES Encryption for IP Security |
| bos.crypto-us | 4.3.2.0 | C | 56 bit Encryption for IP Security |

After installing IPsec, reboot the system. The IPsec feature included in AIX 4.3.2 provides manual tunnel support only. To also get IKE support, you must apply the PTFs listed below. These PTFs implement IKE and the configuration interface via WebSM and update IPsec. The PTFs mentioned are current as of the writing of this redbook:

| fileset | version | ptf | apars |
|----------------------|---------|---------|---------------------------------|
| ----- | ----- | ----- | ----- |
| bos.net.ipsec.rte | 4.3.2.5 | U465168 | IY01461 IY00768 |
| bos.net.ipsec.keymgt | 4.3.2.7 | U465245 | IY01963 IY00539 |
| bos.net.ipsec.websm | 4.3.2.1 | U461479 | IX86450 IX86277 IX86269 IX86265 |

To obtain these PTFs visit the RS/6000 support Web site at:

<http://techsupport.services.ibm.com/rs6k/fixdb.html>

On this page, select **AIX Version 4** and **PTF number**, then continue and enter the PTF numbers you want when prompted.

After completion of all IPsec and IKE components, check that all components are installed correctly using the "List installed software and related information" menu from SMIT. The components are shown in this output:

| Fileset | Level | State | Description |
|-------------------------|---------|-------|---------------------------------------|
| ----- | ----- | ----- | ----- |
| bos.msg.en_US.net.ipsec | 4.3.1.0 | C | IP Security Messages - U.S. English |
| bos.net.ipsec.keymgt | 4.3.2.7 | C | IP Security Key Management |
| bos.net.ipsec.rte | 4.3.2.5 | C | IP Security |
| bos.net.ipsec.websm | 4.3.2.1 | C | IP Security WebSM |
| bos.crypto | 4.3.2.0 | C | 40 Bit Encryption for IP Security |
| bos.crypto-priv | 4.3.2.0 | C | Triple DES Encryption for IP Security |
| bos.crypto-us | 4.3.2.0 | C | 56 bit Encryption for IP Security |

Reboot the system again before using IPsec and IKE.

9.1.3 AIX V4.3.2 IP Security: IKE tunnel basic setup

In AIX V4.3.2, there are two ways to set up IP Security. For manual tunnel and IBM tunnel mode setup, SMIT is used the same as AIX V4.3. For IKE tunnel mode setup, the Web-based System Manager is used.

9.1.3.1 Loading IP Security

After the installation of the IPsec filesets IP Security has to be loaded. On the Web-based System Manager double-click the **Network** icon and the Network configuration window is displayed (see Figure 63 on page 132).

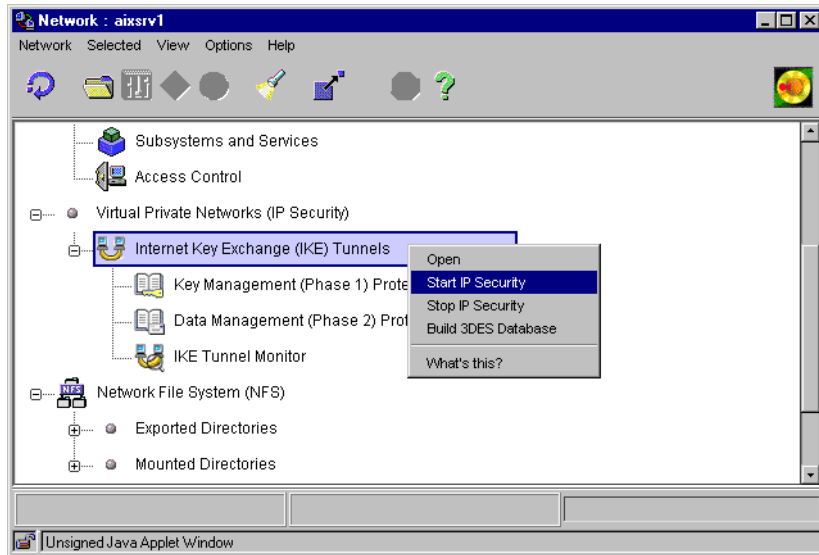


Figure 63. AIX - VPN menu in the Network panel

Right-click **Internet Key Exchange (IKE) Tunnels** and hold down the mouse button then select **Start IP Security** to enable the IPsec stack.

The **Stop IP Security** menu is used in the same manner to disable the IPsec stack.

Important note

There are two ways to load the IP Security network kernel. One is using **Start IP Security** in the Configure IP Security menu in SMIT, which is designed for IBM or manual tunnel. Another is using the **Start IP Security** menu in Web-based System Manager shown above. If manual or IBM tunnel and IKE tunnel are needed at the same time, use Web-based System Manager. The second method enables the IP Security network kernel, ipsec_v4 and v6 and additional daemon for IKE, tunnel manager daemon (/usr/sbin/tmd) and ISAKMP daemon (/usr/sbin/isakmpd).

IKE uses two phases for tunnel establishment. Phase 1, the key management tunnel, is used to establish an authenticated key exchange. Phase 2, the data management tunnel, is used to derive keying material and negotiate a shared policy for non-ISAKMP SAs.

Two main tasks are required to complete IKE configuration:

- Key management tunnel configuration
 1. Define the key management tunnel name and local and remote endpoints for the tunnel.
 2. Associate the key management policy to the tunnel.
 3. Define a pre-shared key.
- Data management tunnel configuration

1. Define the data management tunnel name and associate it to the key management tunnel.
2. Define the type and ID of the local and remote endpoints.
3. Associate the data management policy to the tunnel.

9.1.3.2 Key management tunnel configuration

1. Double-click **Internet Key Exchange (IKE) Tunnels** on the Network panel to open the Internet Key Management (IKE) Tunnel configuration panel.

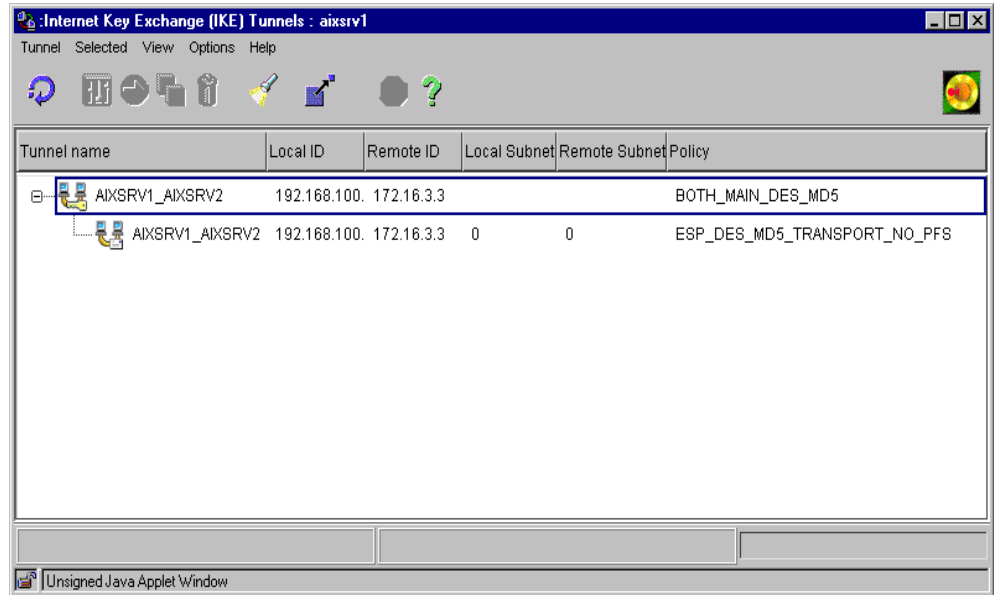


Figure 64. AIX - Internet Key Exchange (IKE) Tunnel configuration panel

2. Select **Tunnel -> New Key Management Tunnel** to open the Key Management (Phase 1) Tunnel Properties window.

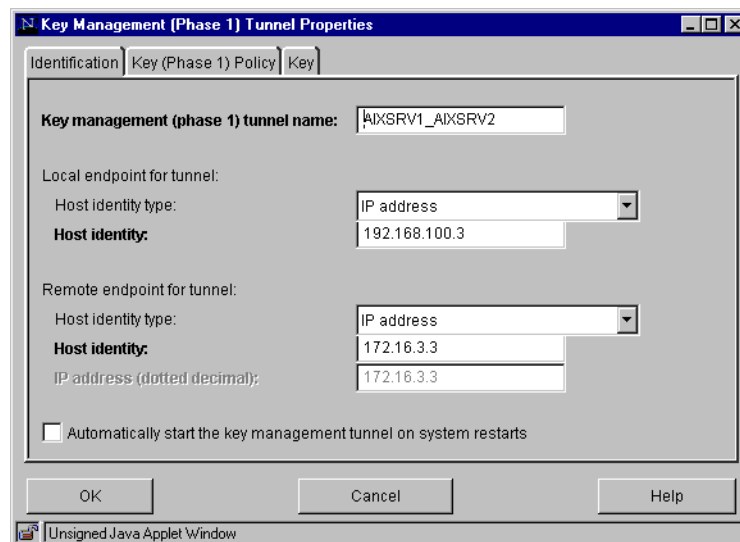


Figure 65. AIX - Key Management (Phase 1) Tunnel Properties: Identification

3. On the Identification panel, enter the key management tunnel name which can be distinguished easily, for example, local-hostname_remote-hostname.
4. Select Host identity type and enter appropriate Host identity.

Host identity type can be one of the following:

 - IP address: Fixed IP addresses are assigned to two endpoint nodes
 - Fully qualified domain name
 - user@fully qualified domain name
5. Mark the automatic key management tunnel starting option properly.

This option is used when your side will be the initiator and you want to reinitiate the key management tunnel to the remote node at system restart.
6. Click the **Key (Phase 1) Policy** tab.

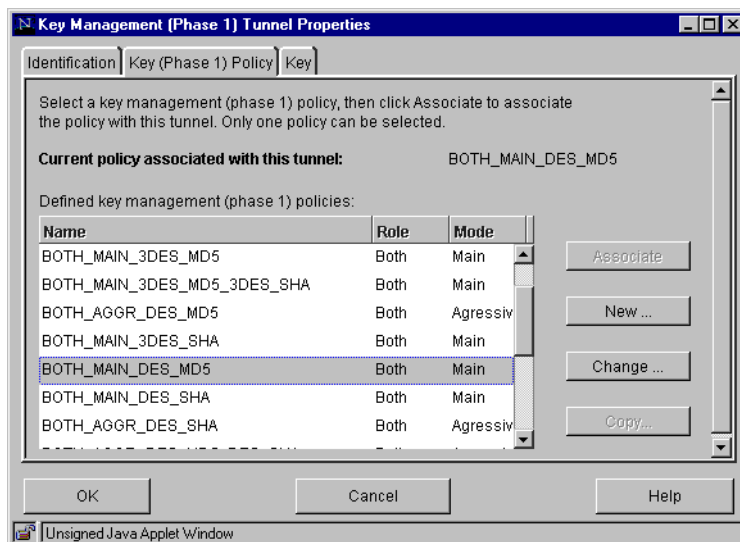


Figure 66. AIX - Key Management (Phase 1) Tunnel Properties: Key (Phase 1) Policy

7. Select the key management policy from the defined key management (phase 1) policies window and associate the selected policy to the key management tunnel by clicking the **Associate** button.

The notation of the key management policy has meaning in itself. For example, BOTH_MAIN_DES_MD5 means:

- BOTH: Allow initiator and responder negotiations.
- MAIN: Use Oakley main mode for identity protection.
- DES: Applied encryption algorithm is DES.
- MD5: Applied hash algorithm is HMAC-MD5.

If the predefined key management policy does not meet your requirement, you can create or customize your own key management policy using the Key Management (Phase 1) Protection Policies menu from the Network panel. Refer to 9.1.4.1, "Key management tunnel policy creation/customization" on page 142 for more detail.

8. Click the **Key** tab.

Predefined key management policies starting IBM are listed in Table 23:

Table 23. Predefined key management policies

| Key management policy | Low | Medium | High |
|-----------------------|----------------|----------------|-----------------|
| Policy Name | IBM_low_prekey | IBM_med_prekey | IBM_high_prekey |
| Mode | Aggressive | Aggressive | Main |
| Auth Method | Pre-shared Key | Pre-shared Key | Pre-shared Key |
| Encryption Algo | DES | DES | Triple DES |
| Hash | MD5 | MD5 | SHA |
| SA Lifetime | 24 Hours | 24 Hours | 1 Hours |
| Group number | 1 | 1 | 1 |

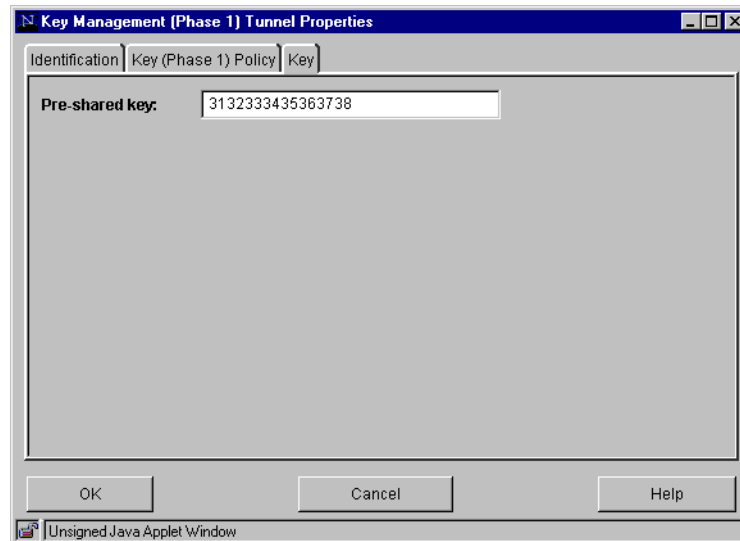


Figure 67. AIX - Key Management (Phase 1) Tunnel Properties: Key

9. Enter the pre-shared key. The hexadecimal notation may be used in the pre-shared key field for interoperability reasons when AIX is used to communicate with other devices such as S/390, AS/400 or SecureWay VPN Client.

For example, Hex 31, 32 is equivalent to Decimal 1, 2 respectively.

10. Click **OK**.

Now that the key management tunnel has been configured, next we configure the data management tunnel associated with the key management tunnel.

9.1.3.3 Data Management Tunnel Configuration

1. Select **Tunnel -> New Data Management Tunnel** on the Internet Key Exchange (IKE) Tunnel configuration panel (see Figure 64 on page 133) to open the Data Management (Phase 2) Tunnel Properties window.

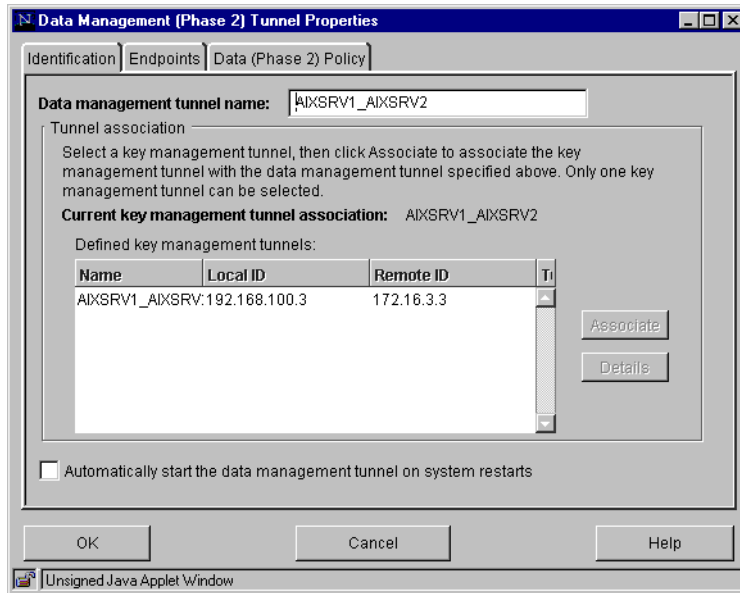


Figure 68. AIX - Data Management (Phase 2) Tunnel Properties: Identification

2. On the Identification panel, enter the data management tunnel name that can be distinguished easily, for example, local-hostname_remote-hostname. Multiple data management tunnels can be associated to one key management tunnel. In this case, the data management tunnel name should be distinguishable among data management tunnels associated to the key management tunnel.
3. Choose the key management tunnel name to be associated from the defined key management tunnel and associate the chosen key management tunnel to the data management tunnel by clicking the **Associate** button.
4. Mark the automatic data management tunnel starting option properly.
This option is used when your side will be initiator and you want to reinitiate the data management tunnel to the remote node at system restart. Matching this option to the automatic key management tunnel starting option is preferable.
5. Click **Endpoints**.

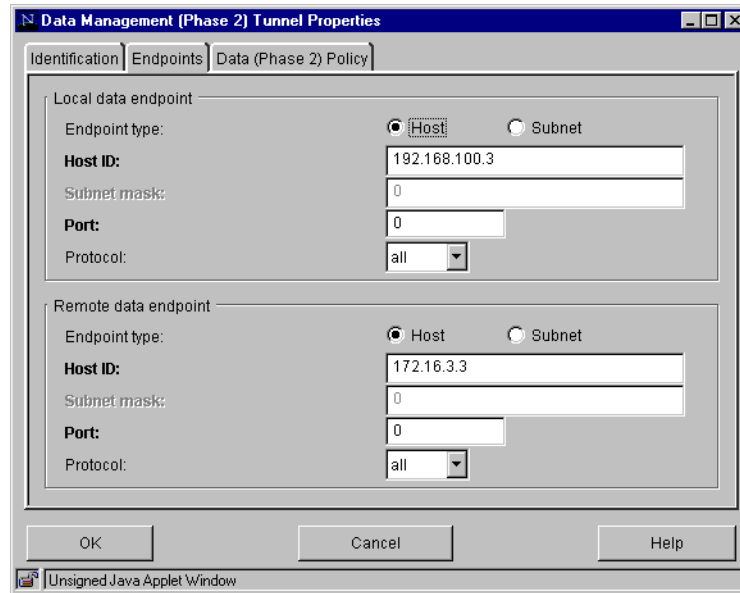


Figure 69. AIX - Data Management (Phase 2) Tunnel Properties: Endpoints

6. Select the Endpoint type and enter the related information for local and remote endpoint.

The endpoint type can be one of the following:

- Host: Used to define one host node. In this case, the IP address is required in the Host ID field.
- Subnet: Used to define the subnet. In this case, the IP address and subnet mask of the network are required in the Host ID and Subnet mask fields respectively.

7. Define filter rule if needed. The default is permitting all traffic.

If filtering is required, specify the port number and protocol for the local data endpoint and remote data endpoint. The filter rule investigates incoming traffic from the remote data endpoint to the local data endpoint and only accepts when the condition is satisfied.

The Protocol field can be set to one of following values:

- all, TCP, TCP/ACK, UDP, ICMP, or OSPF

For example, the local data endpoint only permits a Telnet connection from the remote data endpoint; the filter rule setting is as shown in Figure 70 on page 138:

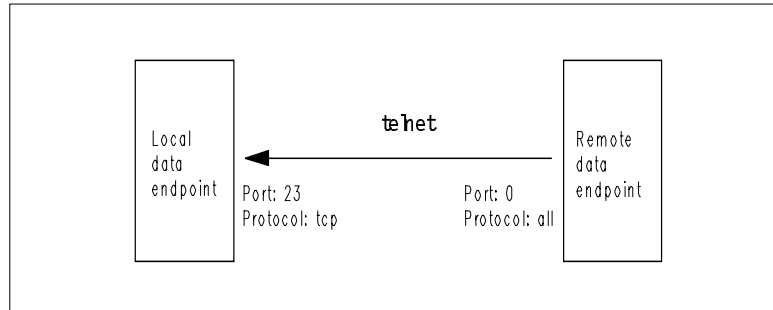


Figure 70. Filter rule example for IKE Data Management Tunnel

8. Click **Data (Phase 2) Policy**.

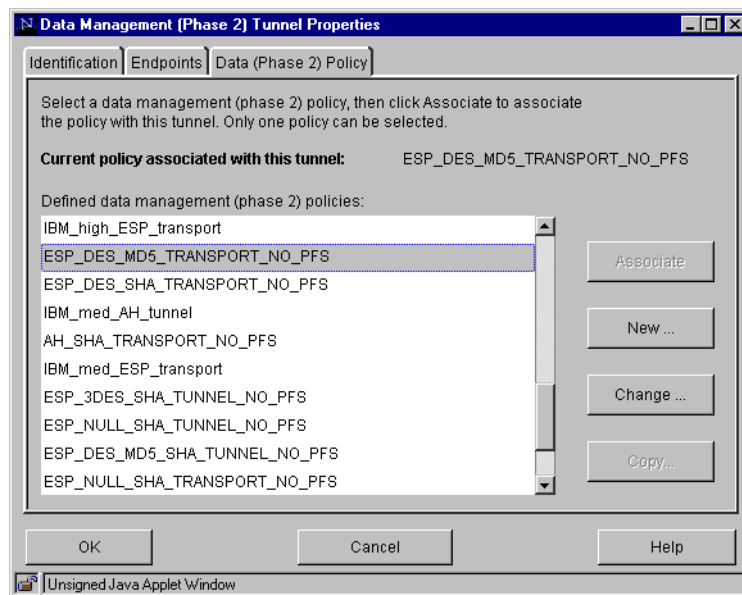


Figure 71. AIX - Data Management (Phase 2) Tunnel Properties: Data (Phase 2) Policy

9. Select the data management policy from the defined data management (phase 2) policies window and associate the selected policy to the data management tunnel by clicking **Associate**.

The notation of the data management policy has meaning in itself. For example, ESP_DES_MD5_TRANSPORT_NO_PFS means:

- ESP: Encapsulation Security Payload (ESP) is used as protocol.
- DES: DES is used as ESP encryption algorithm.
- MD5: HMAC-MD5 is used as ESP authentication algorithm.
- TRANSPORT: Encapsulation mode is transport mode.
- NO_PFS: Perfect Forward Secrecy (PFS) is not applied.

If the predefined data management policy does not meet your requirement, you can create or customize your own data management policy using the Data Management (Phase 2) Protection Policies menu from the Network panel.

Refer to 9.1.4.2, “Data management tunnel policy creation/customization” on page 145 for more details.

10. Click **OK**.

The predefined data management policies starting IBM are listed in Table 24 on page 139 to Table 27 on page 140. The policies are categorized by mode (tunnel or transport) and transform (AH or ESP):

Table 24. Predefined data management policies (ESP, tunnel mode)

| Data management policy | Low | Medium | High |
|------------------------|--------------------|--------------------|---------------------|
| Name | IBM_low_ESP_tunnel | IBM_med_ESP_tunnel | IBM_high_ESP_tunnel |
| Transform | ESP | ESP | ESP |
| Encryption Algo | DES | DES | Triple DES |
| Auth Algorithm | MD5 | MD5 | SHA |
| PFS | No | No | No |
| Encap Mode | Tunnel | Tunnel | Tunnel |
| SA Lifetime | 30 min | 20 min | 10 min |

Table 25. Predefined data management policies (ESP, transport mode)

| Data management policy | Low | Medium | High |
|------------------------|-----------------------|-----------------------|------------------------|
| Name | IBM_low_ESP_transport | IBM_med_ESP_transport | IBM_high_ESP_transport |
| Transform | ESP | ESP | ESP |
| Encryption Algo | DES | DES | Triple DES |
| Auth Algorithm | MD5 | MD5 | SHA |
| PFS | No | No | No |
| Encap Mode | Transport | Transport | Transport |
| SA Lifetime | 30 min | 20 min | 10 min |

Table 26. Predefined data management policies (AH, tunnel mode)

| Data management policy | Low | Medium | High |
|------------------------|-------------------|-------------------|--------------------|
| Name | IBM_low_AH_tunnel | IBM_med_AH_tunnel | IBM_high_AH_tunnel |
| Transform | AH | AH | AH |
| Auth Algorithm | MD5 | MD5 | SHA |
| PFS | No | No | No |

| Data management policy | Low | Medium | High |
|------------------------|--------|--------|--------|
| Encap Mode | Tunnel | Tunnel | Tunnel |
| SA Lifetime | 30 min | 20 min | 10 min |

Table 27. Predefined data management policies (AH, transport mode)

| Data management policy | Low | Medium | High |
|------------------------|----------------------|----------------------|-----------------------|
| Name | IBM_low_AH_transport | IBM_med_AH_transport | IBM_high_AH_transport |
| Transform | AH | AH | AH |
| Auth Algorithm | MD5 | MD5 | SHA |
| PFS | No | No | No |
| Encap Mode | Transport | Transport | Transport |
| SA Lifetime | 30 min | 20 min | 10 min |

Now the data management tunnel is configured. The configured system can act as initiator or responder. If the system acts as initiator, the system must activate the key management tunnel and data management tunnel.

9.1.3.4 IKE tunnel activation and deactivation

The system that acts as initiator must activate the key management tunnel and data management tunnel to make a secure communication path with the remote system. The initiator or responder can deactivate the data management tunnel and key management tunnel.

1. To activate the tunnel, select the tunnel name that you want to activate. Click **Selected** on the menu bar and hold down the mouse button then select **Activate** from the AIX - Internet Key Exchange (IKE) Tunnel configuration panel (see Figure 64 on page 133).

The task processing window will be displayed and the task processing result will be shown.

The IKE Tunnel Monitor is used to check the status of IKE tunnels and to deactivate the IKE tunnel.

Double-click the **IKE Tunnel Monitor** menu on the AIX - VPN menu in the Network panel (see Figure 63 on page 132).

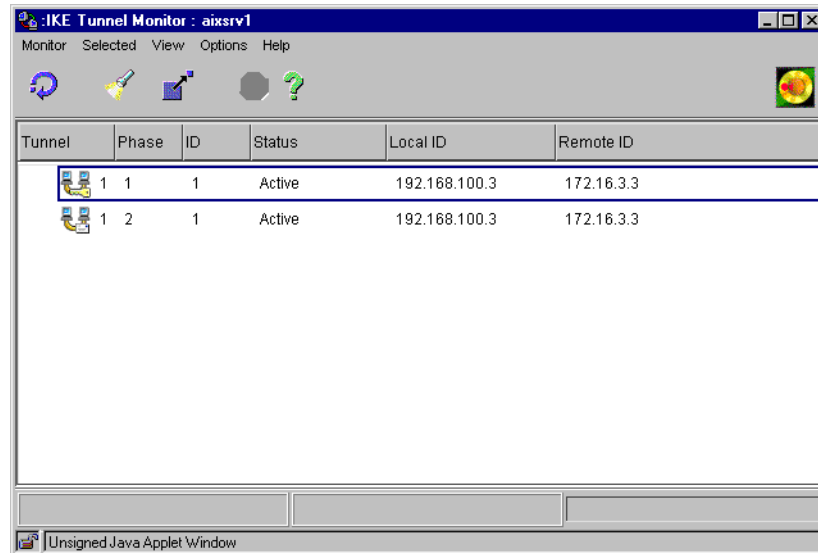


Figure 72. AIX - IKE Tunnel Monitor

- To deactivate the tunnel, select the tunnel name you want to deactivate. Click **Selected** on the menu bar and hold down the mouse button then select **Deactivate** from the AIX - IKE Tunnel Monitor.

The task processing window will be displayed and the task processing result will be shown.

The tunnel status is one of the following:

- Active: Tunnel is active.
- Negotiating: The system is still negotiating with the remote system.
- SA expired: The security association is expired. This status can be seen when the system receives a tunnel release request from the remote system.
- Tun expired: The tunnel is expired. This status can be seen when the tunnel lifetime is over.

Note

When activating the tunnel, activate the key management tunnel and check the status of the key management tunnel before activating the data management tunnel.

9.1.4 AIX V4.3.2 IP Security IKE advanced setup

There are plenty of predefined policies for the key management tunnel and data management tunnel. But sometimes it does not meet your requirement or some parameters need to change because of interoperability or security. You can create or customize your own key management policy using the Key Management (Phase 1) Protection Policies menu from the Network panel or can create or customize your own data management policy using the Data Management (Phase 2) Protection Policies menu from the Network panel.

9.1.4.1 Key management tunnel policy creation/customization

The key management tunnel configuration is associated to the key management policy. The policy consists of a policy role, proposal and tunnel lifetime. The proposal consists of the identity protection mode and transforms used.

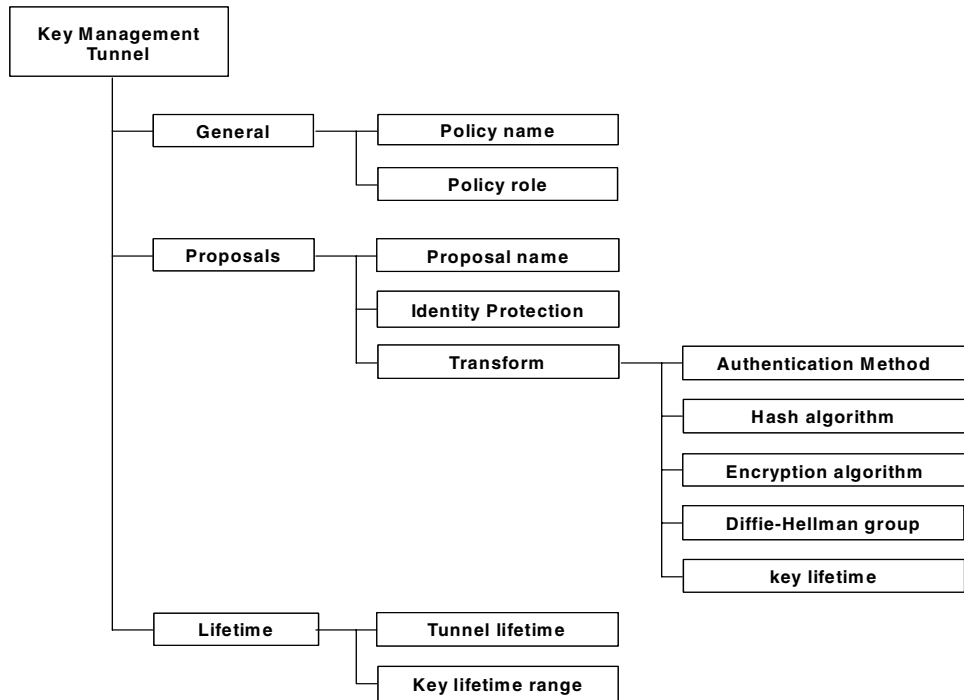


Figure 73. Key management protection policy hierarchy

1. Double-click **Key Management (Phase 1) Protection Policies** in the AIX - VPN menu in the Network panel (see Figure 63 on page 132) to open the AIX - Key Management (Phase 1) Protection Policies window.

| Policy Name | Proposal Name | Role | Tunnel Lifetime | Tunnel Lifesize | Key Overlap |
|----------------------|-------------------|------|-----------------|-----------------|-------------|
| BOTH_AGGR_3DES_MD5 | AGGR_3DES_MD5 | Both | 43200 | 0 | 5 |
| IBM_med_prekey | IBM_med_prekey | Both | 43200 | 0 | 5 |
| BOTH_MAIN_3DES_MD5 | MAIN_3DES_MD5 | Both | 43200 | 0 | 5 |
| BOTH_MAIN_3DES_MD5_3 | MAIN_3DES_MD5_3Df | Both | 43200 | 0 | 5 |
| BOTH_AGGR_DES_MD5 | AGGR_DES_MD5 | Both | 43200 | 0 | 5 |
| BOTH_MAIN_3DES_SHA | MAIN_3DES_SHA | Both | 43200 | 0 | 5 |
| BOTH_MAIN_DES_MD5 | MAIN_DES_MD5 | Both | 43200 | 0 | 5 |
| BOTH_MAIN_DES_SHA | MAIN_DES_SHA | Both | 43200 | 0 | 5 |
| BOTH_AGGR_DES_SHA | AGGR_DES_SHA | Both | 43200 | 0 | 5 |

Figure 74. AIX - Key Management (Phase 1) Protection Policies

2. Select **Key Policy -> New Key Management Policy** to open the AIX - Key Management (Phase 1) Policy Properties window.

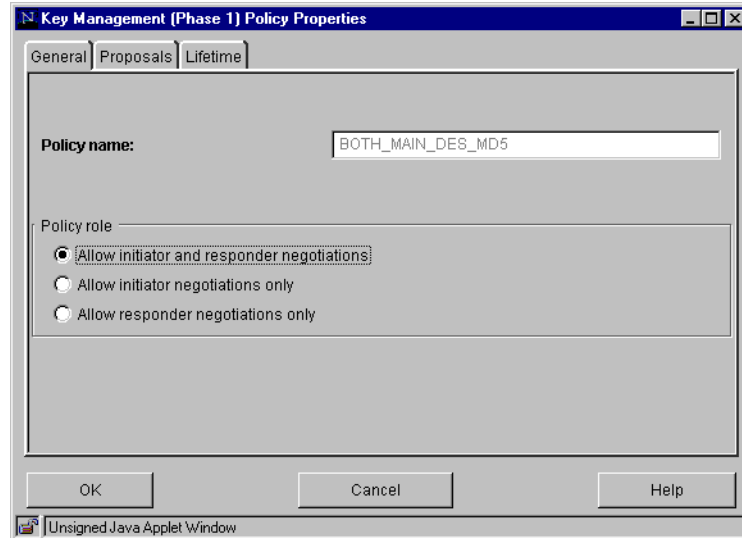


Figure 75. AIX - Key Management (Phase 1) Policy Properties window

3. Enter the policy name and choose the policy role. The policy role can be initiator, responder, or both.
4. Click the **Proposals** tab.

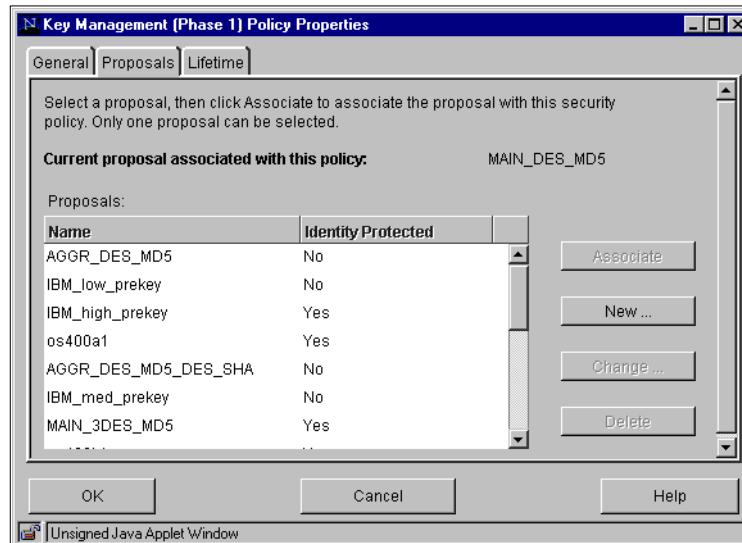


Figure 76. AIX - Key Management (Phase 1) Policy Properties: General

5. Select the key management proposal from the proposal window and associate the selected proposal to the key management policy by clicking the **Associate** button if the appropriate proposal exists. Click the **Lifetime** tab to set a tunnel lifetime.

If a new proposal is required, click **New** to create your own proposal.

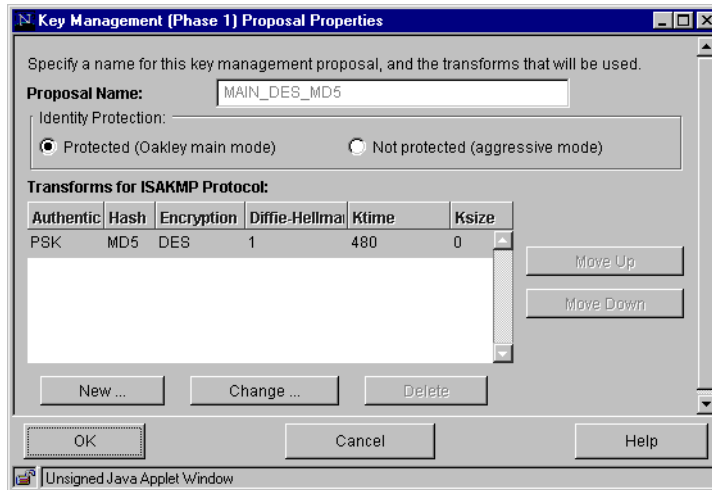


Figure 77. AIX - Key Management (Phase 1) Proposal Properties

6. Enter the proposal name and choose an identity protection mode.

The identity protection mode can be one of the following values:

- Protected (Oakley main mode)
- Not protected (aggressive mode)

7. Click **New** to create a new transform for the ISAKMP protocol.

Note

The proposal can have more than one transform. The precedence is top to bottom.

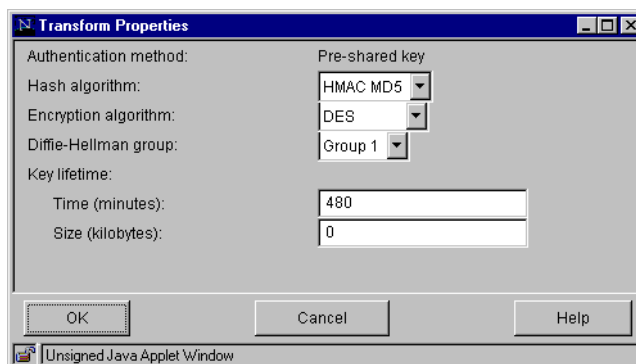


Figure 78. AIX - Transform Properties window for key management tunnel proposal

8. You will choose values for the Hash algorithm, Encryption algorithm, and Diffie-Hellman group.

The hash algorithm can be one of the following values:

- HMAC D5
- HMAC SHA

The encryption algorithm can be one of the following values:

- DES
- Triple DES

The Diffie-Hellman group can be one of the following values:

- Group 1
- Group 2

9. Enter the Key lifetime.

The key lifetime can be set from two aspects. One is elapsed time from the key creation in minutes and another is size of traffic transferred in KB. When slow speed media is used in between, the Key lifetime should be set long enough to establish the key management tunnel successfully. The default time is 480 minutes and the default size is 0, which means no limit.

10. Click **OK**.

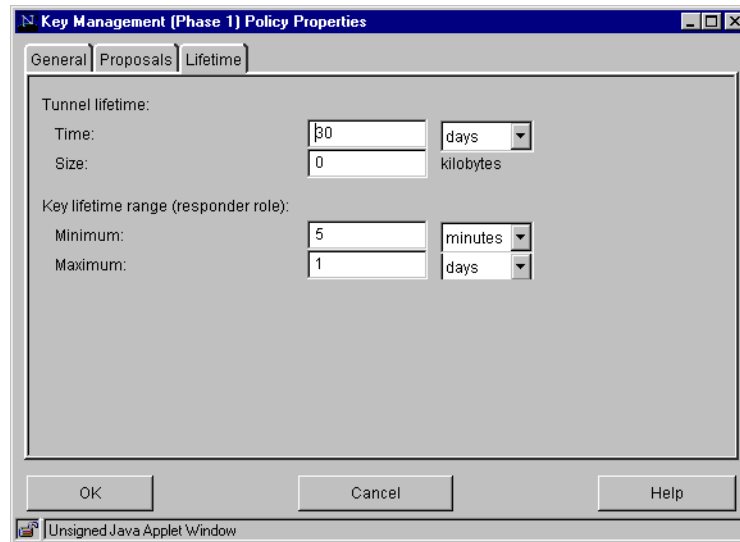


Figure 79. AIX - Key Management (Phase 1) Policy Properties: Lifetime

11. Enter the Tunnel lifetime.

12. Enter the Key lifetime range.

These values are used only if this system is the responder. During negotiation, the initiator proposes the key lifetime and the responder accepts the initiator's value if the key lifetime value from the initiator comes within this range.

Note

The key lifetime and/or tunnel lifetime may be set according to security policy. Short key lifetime is better from the point of security, but it requires frequent key refresh.

9.1.4.2 Data management tunnel policy creation/customization

The data management tunnel configuration is associated to the data management policy. The policy consists of policy role, proposal, and tunnel lifetime. The proposal consists of protocol and transforms used.

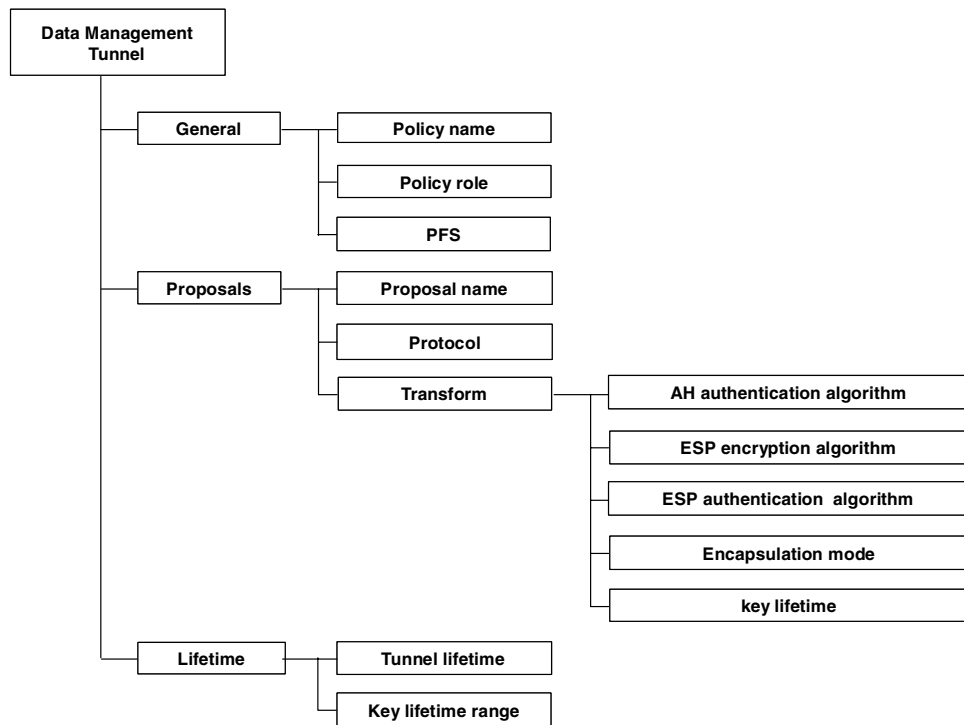


Figure 80. AIX - data management protection policy hierarchy

1. Double-click **Data Management (Phase 2) Protection Policies** in the AIX - VPN menu in the Network panel (see Figure 63 on page 132) to open the AIX - Data Management (Phase 2) Protection Policies.

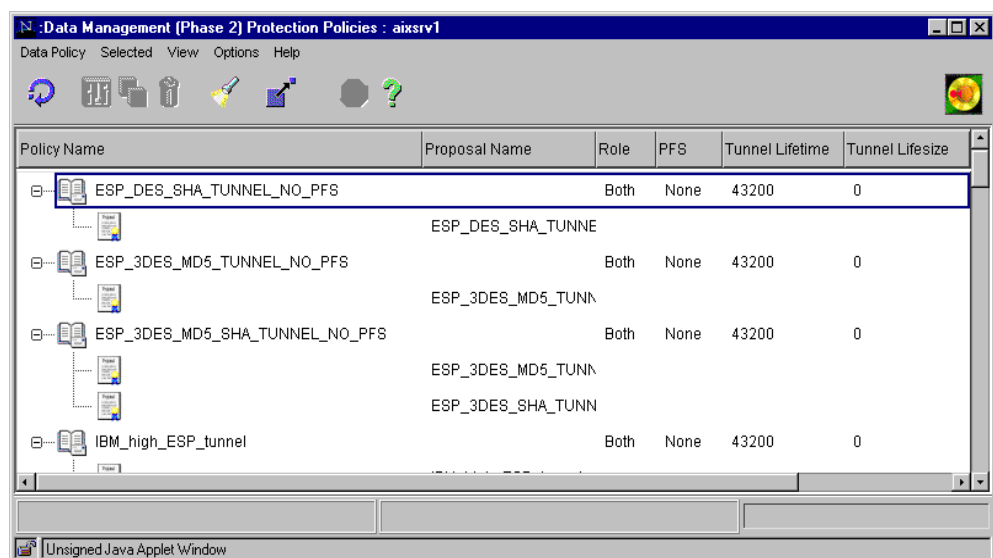


Figure 81. AIX - Data Management (Phase 2) Protection Policies

2. Select **Data Policy -> New Data Management Policy** to open the AIX - Data Management (Phase 2) Policy Properties: General window.

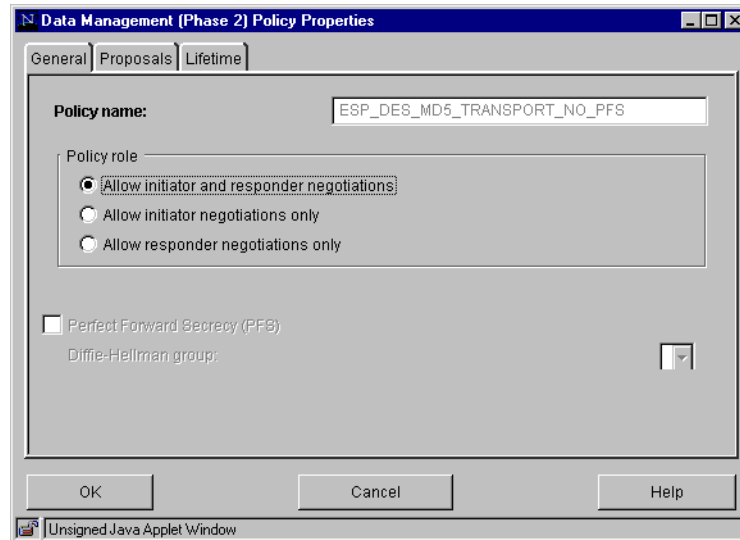


Figure 82. AIX - Data Management (Phase 2) Policy Properties: General

3. Enter the policy name and choose a policy role. The policy role can be initiator, responder, or both.
4. Click the **Proposals** tab.

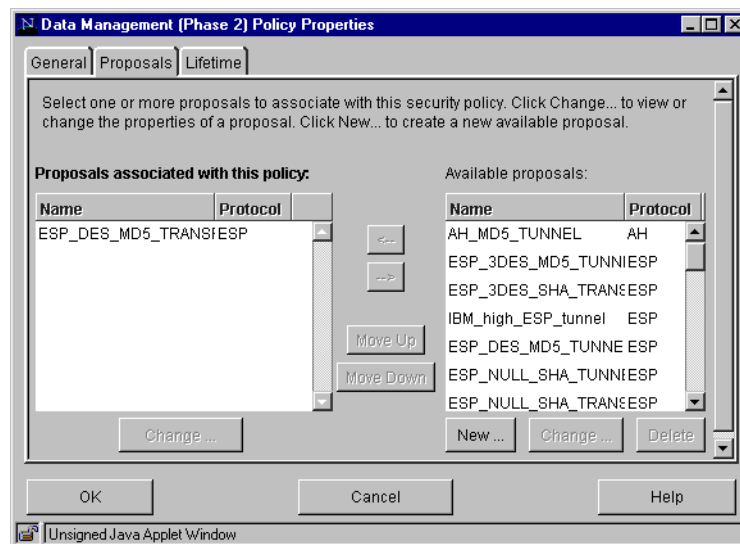


Figure 83. AIX - Data Management (Phase 2) Policy Properties: Proposals

5. Select the data management proposal from the Available proposals window and move to the left window to associate the selected proposal to the data management policy if the appropriate proposal exists. Click the **Lifetime** tab to set the tunnel lifetime.

More than one proposal can be selected and associated to a single data management policy. The precedence of proposals in the left proposal window is top to bottom. Use the **Move Up** and **Move Down** buttons to change the precedence of the proposal.

If a new proposal is required, click **New** to create your own proposal.

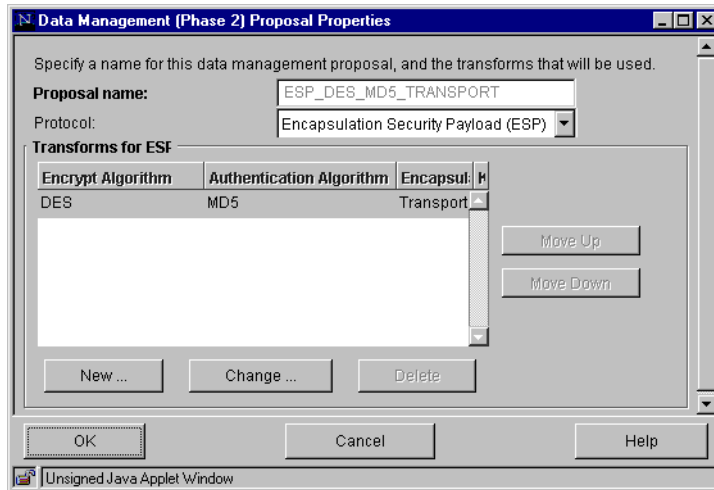


Figure 84. AIX - Data Management (Phase 2) Proposal Properties

6. Enter the proposal name and choose a protocol applied to this proposal.

The protocol can be one of the following values:

- Encapsulation Security Payload (ESP)
- Authentication Header (AH)

7. Click **New** to create a new transform for ESP or AH.

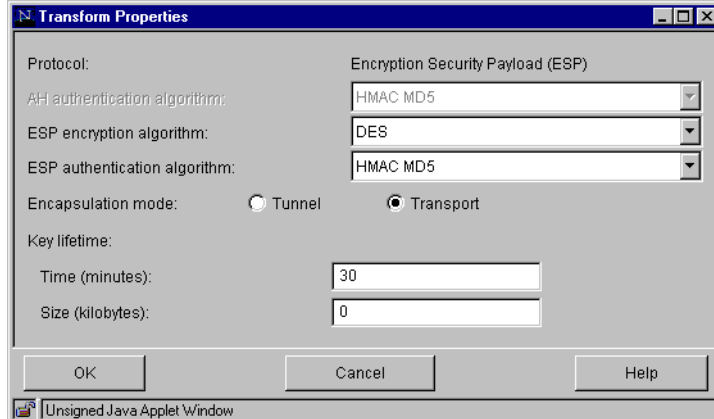


Figure 85. AIX - Transform Properties for data management tunnel

The applied protocol is displayed according to the protocol selected in the previous window. And some fields in this window are displayed in gray indicating an unused field.

8. Select algorithms for AH or ESP and the Encapsulation mode.

The AH authentication algorithm can be one of the following values:

- HMAC MD5
- HMAC SHA

The ESP encryption algorithm can be one of the following values:

- DES

- Triple DES
- NULL

The encapsulation mode can be set to one of the following values:

- Tunnel
- Transport

9. Enter the Key lifetime.

The key lifetime can be set from two aspects. One is the elapsed time from the key creation in minutes and another is the size of traffic transferred in KB. The default time is 30 minutes and the default size is 0, which means no limit.

10. Click **OK**.

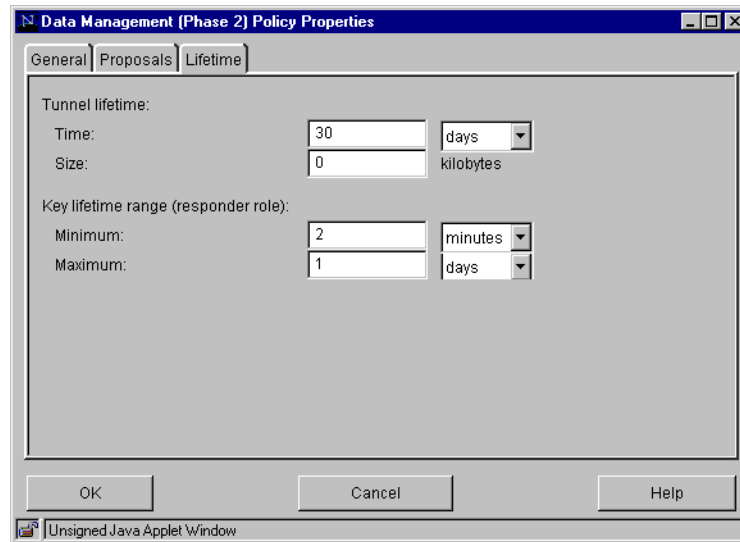


Figure 86. AIX - Data Management (Phase 2) Policy Properties: Lifetime

11. Enter the Tunnel lifetime in time and size.

12. Enter the Key lifetime range.

These values are used only if this system is a responder. During negotiation initiator proposes the key lifetime and responder accepts initiator's value if the key lifetime value from initiator is within this range.

Note

The key lifetime and/or tunnel lifetime may be set according to security policy. Short key lifetime is better from the point of security, but it requires frequent key refresh.

9.1.5 Use tunnel lifetime and lifesize

There are several locations for setting tunnel and SA lifetimes and lifesizes. The actual design of the IKE database is like this:

1. The policy will control the following:
 - Tunnel lifetime and lifesize.

- When acting as the responder, it will specify the bounds for the SA lifetime.
2. The transform will have/control the following:
- When acting as the initiator, SA lifesize and lifetime.
 - When acting as the responder, SA lifesize only.

This means when AIX is the initiator, the values in the transform will be offered. When acting as the responder, the SA attributes in the initiator_offered_proposal will be matched against the AIX proposal/transform except for the lifetime attribute, which is in the policy.

9.1.6 Packet filtering

Filtering can also be used without tunnels, to deny or permit any traffic on specific criteria such as source and destination IP addresses and masks. Packet filtering conditions include:

- Protocol
- Port number
- Direction
- Fragmentation control
- Routing
- Tunnel
- Interface

In addition you can specify on a per rule basis whether logging should be done.

If you define a tunnel, AIX will automatically configure the filter rules needed to allow any traffic through the tunnel. Of course the filters can be changed afterward if there are specific needs to be met. Go to the SMIT IPsec main panel (smit ipsec4), then select **Advanced IP Security Configuration** and **Configure IP Security Filter Rules**. Modifications done within this series of menus have to be activated by choosing **Activate/Update/Deactivate IP Security Filter Rule**.

You can check the contents of your rule base via the SMIT path **List Active IP Security Filter Rules** or the `lsfilt` command. You can find some sample filter rules in the file `/usr/samples/ipsec/filter.sample`. For our scenario we do not need to touch the filters at all, because the auto-generated filter rules have allowed any traffic through the tunnel already.

Activating the IKE tunnel will cause filter rules for the new tunnel to be inserted into the dynamic filter table. These entries can be viewed using the `lsfilt` command with the `-d` option for dynamic filter rules. Following are the filter rules generated automatically when the IKE tunnel is activated:

```
Rule 1:
Rule action      : permit
Source Address   : 0.0.0.0
Source Mask      : 0.0.0.0
Destination Address : 0.0.0.0
Destination Mask : 0.0.0.0
Source Routing   : no
Protocol         : udp
Source Port      : eq 4001
Destination Port : eq 4001
Scope            : both
```

Direction : both
Logging control : no
Fragment control : all packets
Tunnel ID number : 0
Interface : all
Auto-Generated : yes

Rule 2:

*** Dynamic filter placement rule for IKE tunnels ***
Logging control : no

Rule 0:

Rule action : permit
Source Address : 0.0.0.0
Source Mask : 0.0.0.0
Destination Address : 0.0.0.0
Destination Mask : 0.0.0.0
Source Routing : yes
Protocol : all
Source Port : any 0
Destination Port : any 0
Scope : both
Direction : both
Logging control : no
Fragment control : all packets
Tunnel ID number : 0
Interface : all
Auto-Generated : no

End of IPv4 filter rules.

Dynamic rule 0:

Rule action : permit
Source Address : 0.0.0.0
Source Mask : 0.0.0.0
Destination Address : 0.0.0.0
Destination Mask : 0.0.0.0
Source Routing : no
Protocol : udp
Source Port : eq 500
Destination Port : eq 500
Scope : local
Direction : both
Fragment control : all packets
Tunnel ID number : 0

Dynamic rule 1:

Rule action : permit
Source Address : 0.0.0.0
Source Mask : 0.0.0.0
Destination Address : 0.0.0.0
Destination Mask : 0.0.0.0
Source Routing : no
Protocol : ah
Source Port : any 0
Destination Port : any 0
Scope : both
Direction : inbound

```
Fragment control : all packets
Tunnel ID number : 0
```

Dynamic rule 2:

```
Rule action      : permit
Source Address   : 0.0.0.0
Source Mask      : 0.0.0.0
Destination Address : 0.0.0.0
Destination Mask : 0.0.0.0
Source Routing   : no
Protocol         : esp
Source Port      : any 0
Destination Port : any 0
Scope           : both
Direction       : inbound
Fragment control : all packets
Tunnel ID number : 0
```

Dynamic rule 3:

```
Rule action      : permit
Source Address   : 192.168.100.3
Source Mask      : 255.255.255.255
Destination Address : 172.16.3.3
Destination Mask : 255.255.255.255
Source Routing   : no
Protocol         : all
Source Port      : any 0
Destination Port : any 0
Scope           : both
Direction       : outbound
Fragment control : all packets
Tunnel ID number : 2
```

Dynamic rule 4:

```
Rule action      : permit
Source Address   : 192.168.100.3
Source Mask      : 255.255.255.255
Destination Address : 172.16.3.3
Destination Mask : 255.255.255.255
Source Routing   : no
Protocol         : all
Source Port      : any 0
Destination Port : any 0
Scope           : both
Direction       : inbound
Fragment control : all packets
Tunnel ID number : 2
```

9.1.7 Manual tunnel setup

Manual tunnels provide backward compatibility and will interoperate with machines that do not support IKE key management protocols. The disadvantage of manual tunnels is that the key values are static. In other words, the encryption and authentication keys are the same for the life of the tunnel and must be manually updated.

From the SMIT main IPSec panel choose **Basic IP Security Configuration->Add IP Security Tunnel->Use Manual Session Key Refresh Method (Manual Tunnel)**, then select one of the following:

- Host-Host (manual tunnel)
- Host-Firewall-Host (manual tunnel)

In each configuration panel, encryption and authentication method combination using AH and/or ESP can be selected:

- Authentication Only (AH)
- Authentication with AH, Encryption with ESP
- Encryption and Authentication with ESP

In this section Host-Host (manual tunnel) and then Authentication with AH, Encryption with ESP case will be explained.

```

                                Authentication with AH, Encryption with ESP

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                [Entry Fields]
* Source Address                      [192.168.100.3]      +
* Destination Address                 [172.16.3.3]        +
  Encapsulation Mode                 [Transport]         +
  Policy                             [encr/auth]         +
  Authentication Algorithm            [HMAC_MD5]          +
  Encryption Algorithm               [DES_CBC_8]         +
  Source Authentication Key           []                   X
  Source Encryption Key               []                   X
  Destination Authentication Key      []                   X
  Destination Encryption Key          []                   X
  Source SPI for AH                   []                   #
  Source SPI for ESP                  []                   #
  Destination SPI for AH              []                   #
* Destination SPI for ESP             [259]               #
  Tunnel Lifetime (in minutes)        [0]                  #
  Replay Prevention                   [no]                 +
[BOTTOM]

F1=Help          F2=Refresh      F3=Cancel      F4=List
Esc+5=Reset      Esc+6=Command   Esc+7=Edit     Esc+8=Image
Esc+9=Shell      Esc+0=Exit      Enter=Do

```

Input the necessary information in the tunnel definition panel.

A tunnel lifetime of zero (unlimited) is good from an administration point of view, because there is no key distribution problem. Unfortunately, it is not a valid solution from our point of view, because there is a security problem if you do not refresh/change the keys from time to time. We strongly recommend you change your keys on a regular basis.

To change the policy of this tunnel, such as key changes, from the Basic IP Security Configuration panel choose **Change IP Security Tunnel->Use Manual Session Key Refresh Method (Manual Tunnel)->Host-Host**. Then select the tunnel that you just created. Change the desired fields.

The necessary packet filters were created automatically when you defined the tunnel. You can list the filters by issuing a `lsfilt` command.

9.2 AIX V4.3.3

In this section we describe newly added VPN features in AIX V4.3.3 and its installation and setup. We will focus on the changes from AIX V4.3.2.

9.2.1 VPN features and improvements in AIX V4.3.3

We describe VPN features in AIX V4.3.3, and focus on the changes from AIX V4.3.2. The newly added functions or improvements are summarized below:

- Basic tunnel setup has been simplified by the addition of a quick configuration feature.
- The manual tunnel configuration menu is added in the Web-based System Manager.
- The static filter rule configuration for manual tunnels and the dynamic filter rule for IKE tunnels menu are added in the Web-based System Manager.
- The filtering of traffic by the interface is added in addition to filtering by a variety of IP characteristics.
- Extensive use of system traces and statistics for problem determination.
- User-defined default action allows the user to specify whether traffic that does not match defined tunnels should be allowed or denied.
- The Perfect Forward Secrecy (PFS) is supported in IKE.
- The IP address range option is added in addition to Host and Subnet on the endpoint type field for the IKE data management tunnel.
- The value for an IKE pre-shared key can be entered in ASCII and hexadecimal format.
- Support for on-demand outbound connections has been added so that tunnels only become active when there is traffic that is supposed to flow through them.

The authentication and encryption algorithms for the IKE tunnel and the manual tunnel are listed in Figure 28 and Figure 29:

Table 28. IKE tunnel support

| Algorithm | AH IP Version 4 | ESP IP Version 4 |
|-----------|-----------------|------------------|
| HMAC MD5 | X | X |
| HMAC SHA1 | X | X |
| DES CBC 8 | | X |
| 3DES CBC | | X |
| ESP Null | | X |

Table 29. Manual tunnel support

| Algorithm | AH IP Version 4 | AH IP Version 6 | ESP IP Version 4 | ESP IP Version 6 |
|-----------|-----------------|-----------------|------------------|------------------|
| HMAC MD5 | X | X | X | X |
| HMAC SHA1 | | | | |
| DES CBC 8 | | | X | X |
| DES CBC 4 | | | X | X |
| CDMF | | | X | X |
| 3DES CBC | | | X | X |

9.2.2 AIX V4.3.3 VPN feature installation

The IP Security feature in AIX can be installed and loaded separately. The filesets that need to be installed are:

- bos.net.ipsec.rte - The run-time environment for the kernel IP Security environment and commands
- bos.net.ipsec.keymgt - the tunnel manager and IKE daemons that perform key management
- bos.net.ipsec.websm - the IP Security configuration GUI
- bos.msg.LANG.net.ipsec where LANG is the desired language, such as en_US

And either:

- bos.crypto for CDMF support (40-bit key Commercial Data Masking Facility) available on the World Trade Accessory Pack

or

- bos.crypto-wt for DES (56-bit Data Encryption Standard) available on the U.S. Accessory Pack
- bos.crypto-priv for Triple DES support (available in U.S. and Canada only)

Once installed, IP Security can be separately loaded for IP Version 4 and IP Version 6. This is accomplished by issuing `mkdev` commands, through the IP Security SMIT panels, or the Web-based System Manager.

Important

The version of AIX V4.3.3 that we used in this chapter and scenarios in other chapters of this redbook was a development pre-release. Features and screenshots of the final version may be different from what is described and illustrated in this redbook.

9.2.2.1 Loading IP Security

If using SMIT or Web-based System Manager, the IP Security modules will be automatically loaded when IPSec security is started. This is the preferred method

to ensure that the kernel extensions and IKE daemon are loaded in the proper order.

On the Web-based System Manager double-click the **Network** icon and the Network configuration window is displayed (see Figure 87):

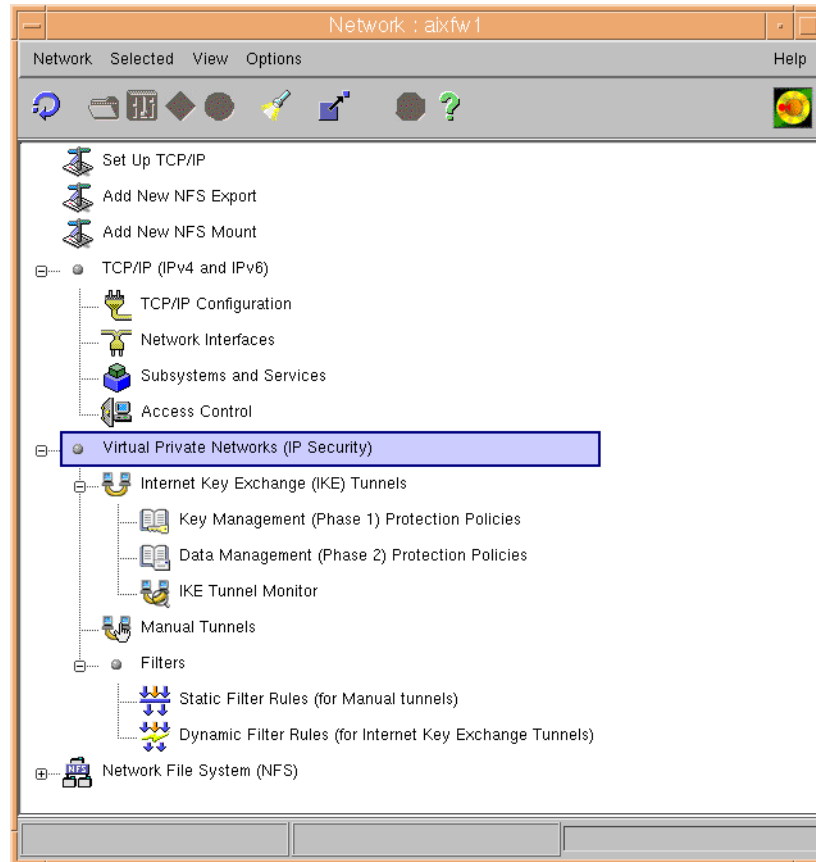


Figure 87. AIX V4.3.3 - VPN menu in the Network panel

Right-click **Internet Key Exchange (IKE) Tunnels** and hold down the mouse button then select **Start IP Security** to enable the IPsec stack. The Start options window will be displayed (see Figure 88):

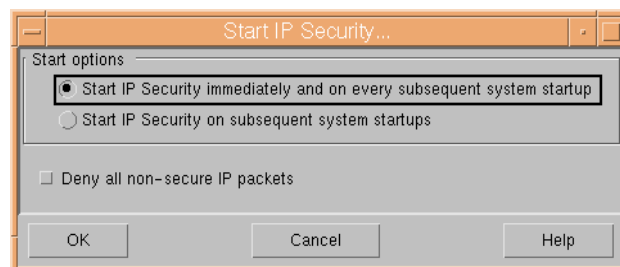


Figure 88. AIX V4.3.3 - IP Security Start options window

You can deny or permit nonsecure IP packets in this options window.

If the loading completed successfully, the `lsdev` command will show the IPsec devices as Available:

```
lsdev -C -c ipsec
ipsec_v4 Available IP Version 4 Security Extension
ipsec_v6 Available IP Version 6 Security Extension
```

Once the IP Security kernel extension has been loaded, tunnels and filters are ready to be configured.

Important note

Loading IP Security will enable the filtering function. Therefore, before loading, it is important to ensure the correct filter rules are created, or all outside communication may be blocked.

9.2.3 IP Security IKE tunnel basic setup using quick configuration

IKE uses two phases for tunnel establishment. Phase 1, the key management tunnel, is used to establish an authenticated key exchange. Phase 2, the data management tunnel, is used to derive keying material and negotiate a shared policy for non-ISAKMP SAs.

To simplify the configuration of IKE and IPsec tunnels, AIX 4.3.3 offers a quick configuration path that creates a host-to-host VPN connection using IKE main mode for negotiations. To start quick configuration, open the Internet Key Exchange (IKE) Tunnels window and click **Tunnel -> New Tunnel -> Basic Configuration**, as shown in Figure 89:

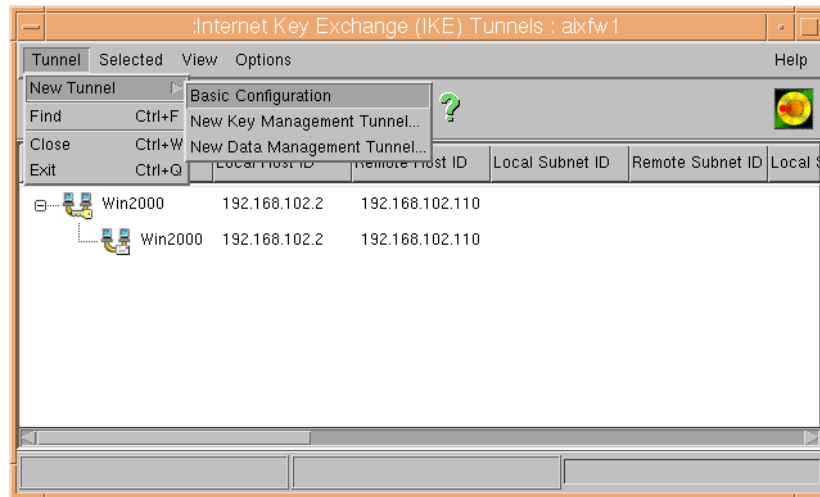


Figure 89. AIX 4.3.3 - Starting quick configuration

On the first panel, enter a tunnel name and the IP addresses and subnet masks for the tunnel endpoints, as shown in Figure 90 on page 158. Irrespective of the subnet masks, a host-to-host tunnel will be created.

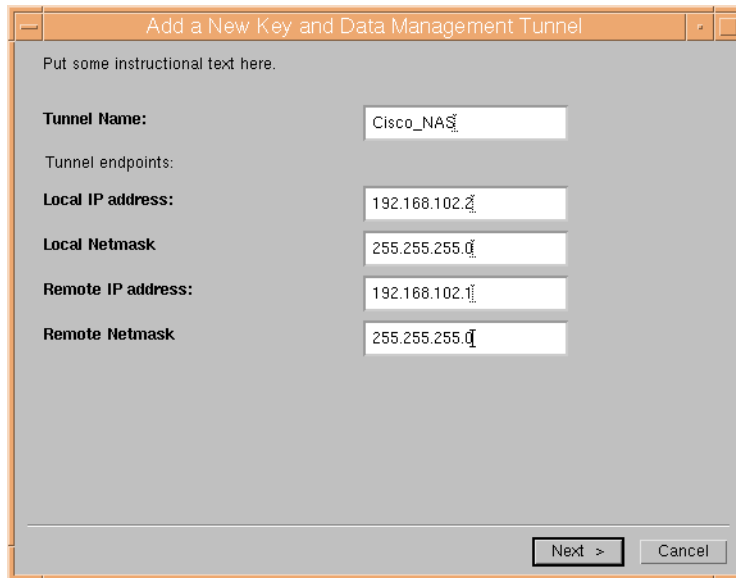


Figure 90. AIX 4.3.3 - quick configuration - tunnel names and addresses

The second panel allows you to specify the IKE authentication method, pre-shared key and Diffie-Hellman group for the Phase 1 (key management) tunnel. It also allows you to select the IPSec protocol (erroneously listed as Transform for the ISAKMP protocol) and encapsulation mode for the Phase 2 (data management) tunnel. The options for encryption and hash algorithm that you can select in this panel are used for both the key and data management tunnel. This panel is shown in Figure 91:

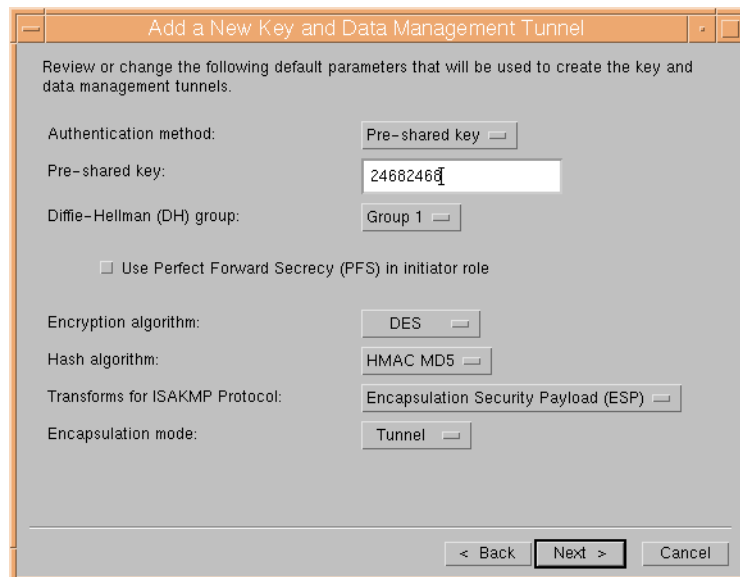


Figure 91. AIX 4.3.3 - quick configuration - tunnel mode and transform parameters

When you have entered all the configuration parameters, click **Next** and then click **Finish** on the panel shown in Figure 92 on page 159.

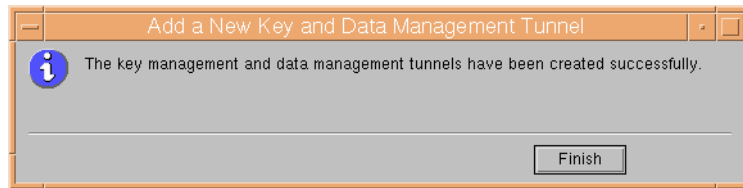


Figure 92. AIX 4.3.3 - quick configuration - finishing the configuration

The key and data management tunnels for the connection that have been created are listed in the Internet Key Exchange (IKE) Tunnels window as shown in Figure 93. To make adjustments, highlight the tunnel and then double-click it to invoke the detailed configuration panels.

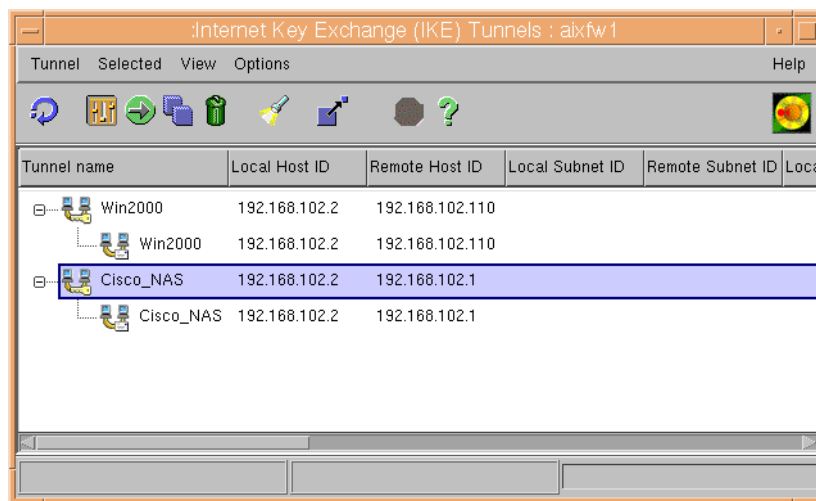


Figure 93. AIX 4.3.3 - Internet Key Exchange (IKE) Tunnels window

Important

The quick configuration path only supports the pre-shared key authentication method but allows you to enter the key in hexadecimal or in ASCII format.

For interoperability reasons, we suggest that you enter the pre-shared key in ASCII format, unless your VPN partner supports hexadecimal format for pre-shared keys.

The quick configuration path only creates host-to-host VPN connections. If you need to create a gateway-to-gateway or host-to-gateway connection, you have to edit the data management tunnel definition that has been created. This is shown in Figure 94 on page 160.

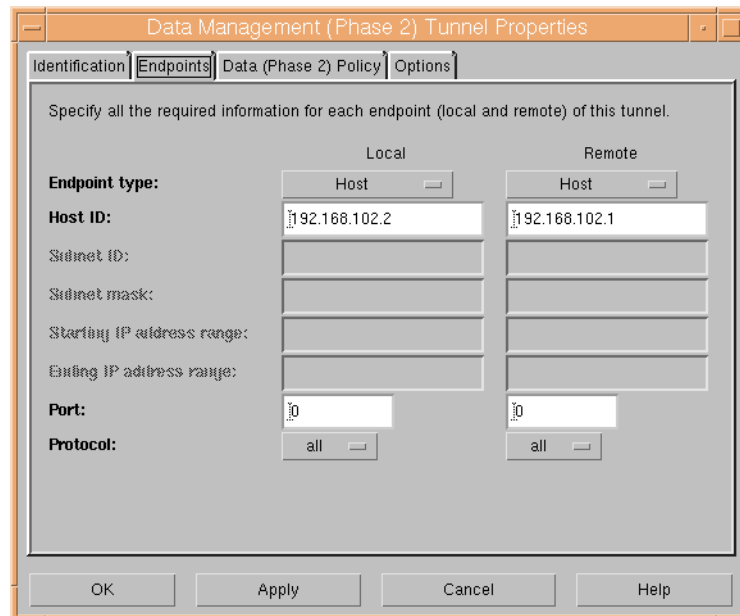


Figure 94. AIX 4.3.3 - Phase 2 endpoint type panel

9.2.4 IP Security IKE tunnel advanced setup

In AIX V4.3.3, the key management tunnel configuration panels are the same as AIX V4.3.2 with the exception of the configuration of the pre-shared key value, which cannot optionally be entered in ASCII as well as hexadecimal format. This new panel is shown in Figure 94.

The data management tunnel configuration has changed. We will show these changes in this section. Refer to 9.1.3.2, “Key management tunnel configuration” on page 133 for the key management tunnel configuration.

- Data management tunnel configuration
 1. Define the data management tunnel name and associate it to the key management tunnel.
 2. Define the type and ID of the local and remote endpoints.
 3. Associate the data management policy to the tunnel.
- 1. Select **Tunnel -> New Data Management Tunnel** on the Internet Key Exchange (IKE) Tunnel configuration panel (see Figure 64 on page 133) to open the Data Management (Phase 2) Tunnel Properties window.

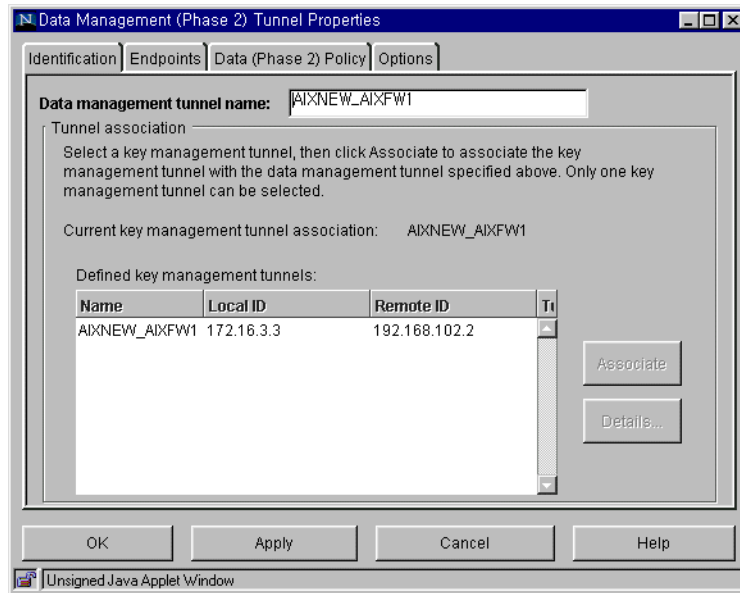


Figure 95. AIX V4.3.3 - Data Management (Phase 2) Tunnel Properties: Identification

2. On the Identification panel, enter a data management tunnel name that can be distinguished easily, for example, local-hostname_remote-hostname. Multiple data management tunnels can be associated to one key management tunnel. In this case, the data management tunnel name should be distinguishable among data management tunnels associated to the key management tunnel.
3. Choose the key management tunnel name to be associated from the defined key management tunnel and associate the chosen key management tunnel to the data management tunnel by clicking the **Associate** button.
4. Click **Endpoints**.

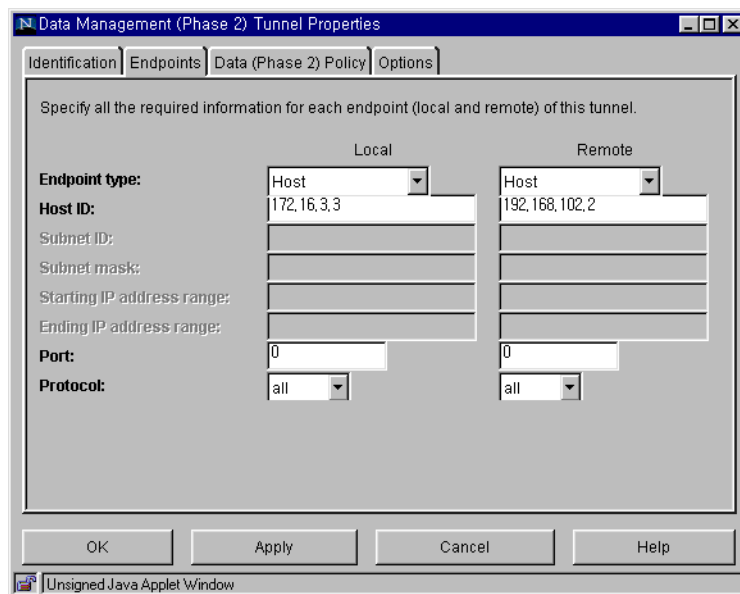


Figure 96. AIX V4.3.3 - Data Management (Phase 2) Tunnel Properties: Endpoints

5. Select the endpoint type and enter the related information for local and remote endpoints.

The endpoint type can be one of the following:

- Host: Used to define one host node. In this case, the IP address is required in the Host ID field.
 - Subnet: Used to define the subnet. In this case, the IP address and subnet mask of the network are required in the Host ID and Subnet mask fields respectively.
 - IP Address Range: Used to define range of the IP addresses that will be using the tunnel. The starting and ending IP addresses are required.
6. Define filter rule if needed. The default is permitting all traffic.

If filtering is required, specify the port number and protocol for the local data endpoint and remote data endpoint. The filter rule investigates incoming traffic from the remote data endpoint to the local data endpoint and only accepts when the condition is satisfied.

The protocol field can be set to one of following values:

- all, TCP, TCP/ACK, UDP, ICMP, or OSPF

For example, the local data endpoint only permits a Telnet connection from the remote data endpoint, the filter rule setting is as shown in Figure 97:

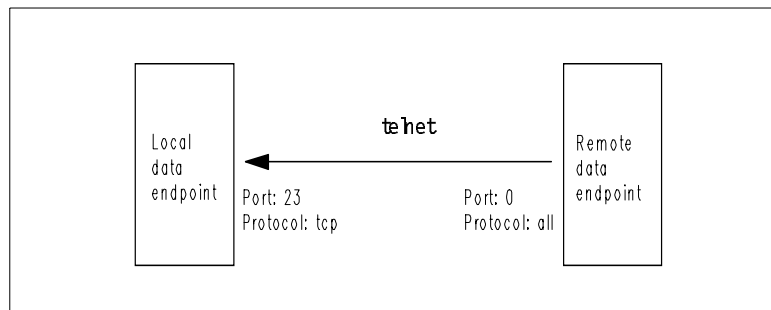


Figure 97. Filter rule example for IKE data management tunnel

7. Click **Data (Phase 2) Policy**.

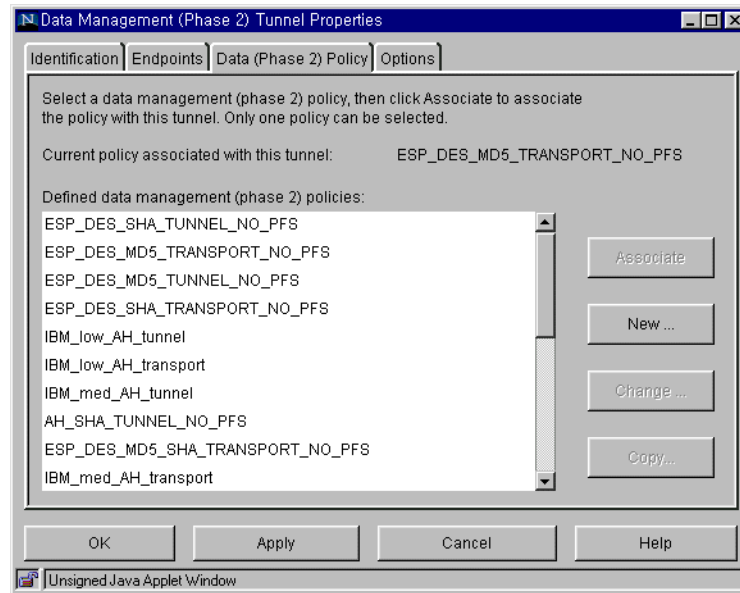


Figure 98. AIX V4.3.3 - Data Management (Phase 2) Tunnel Properties: Data (Phase 2) Policy

8. Select the data management policy from the defined data management (phase 2) policies window and associate the selected policy to the data management tunnel by clicking **Associate**.

The notation of the data management policy has meaning in itself. For example, ESP_DES_MD5_TRANSPORT_NO_PFS means:

- ESP: Encapsulation Security Payload (ESP) is used as a protocol.
- DES: DES is used as an ESP encryption algorithm.
- MD5: HMAC-MD5 is used as an ESP authentication algorithm.
- TRANSPORT: Encapsulation mode is a transport mode.
- NO_PFS: Perfect Forward Secrecy (PFS) is not applied.

If the predefined data management policy does not meet your requirement, you can create or customize your own data management policy using the Data Management (Phase 2) Protection Policies menu from the Network panel.

Refer to 9.1.4.2, “Data management tunnel policy creation/customization” on page 145 for more details.

9. Click **Options**.

The predefined data management policies starting IBM are listed in Table 30 and Table 31:

Table 30. Predefined data management policies (ESP, tunnel mode)

| Data management policy | Low | Medium | High |
|------------------------|--------------------|--------------------|---------------------|
| Name | IBM_low_ESP_tunnel | IBM_med_ESP_tunnel | IBM_high_ESP_tunnel |
| Transform | ESP | ESP | ESP |
| Encryption Algo | DES | DES | Triple DES |

| Data management policy | Low | Medium | High |
|------------------------|---------|-------------|--------------|
| Auth Algorithm | MD5 | MD5 | SHA |
| PFS | No | Yes | Yes |
| Encap Mode | Tunnel | Tunnel | Tunnel |
| SA Lifetime | 8 hours | 8 hours | 1 hour |
| Group Number | N/A | 1 (768 bit) | 2 (1024 bit) |

Table 31. Predefined data management policies (ESP, transport mode)

| Data management policy | Low | Medium | High |
|------------------------|-----------------------|-----------------------|------------------------|
| Name | IBM_low_ESP_transport | IBM_med_ESP_transport | IBM_high_ESP_transport |
| Transform | ESP | ESP | ESP |
| Encryption Algo | DES | DES | Triple DES |
| Auth Algorithm | MD5 | MD5 | SHA |
| PFS | No | Yes | Yes |
| Encap Mode | Transport | Transport | Transport |
| SA Lifetime | 30 min | 20 min | 10 min |
| Group Number | N/A | 1 (768 bit) | 2 (1024 bit) |

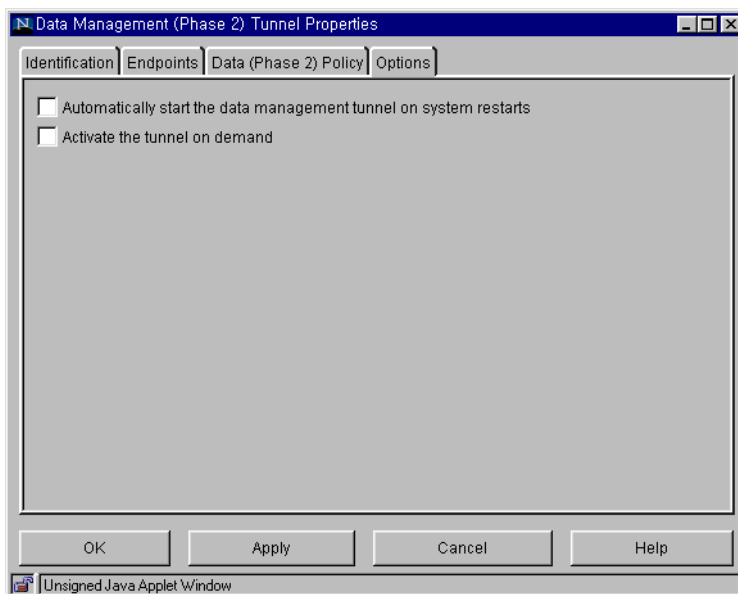


Figure 99. AIX V4.3.3 - Data Management (Phase 2) Tunnel Properties: Options

10. Set the automatic data management tunnel starting option properly.

This option is used when your side will be the initiator and you want to reinitiate the data management tunnel to the remote node at system restart. Matching this option to the automatic key management tunnel starting option is preferable.

Now the data management tunnel is configured. The configured system can act as initiator or responder. If the system acts as initiator, the system must activate the key management tunnel and data management tunnel.

11. Mark the activation on the demand option properly.

If it is desired to have only the negotiation protocol active when data traffic requires it, select the Activate the tunnel on demand option. This will prepare the tunnel parameters for the tunnel, but the negotiation will actually be started once a packet matching the tunnel characteristics are sent or received. In this case, the tunnel information is to be inserted into the kernel, waiting for a packet to match. Once an incoming or outgoing packet matches the tunnel characteristics, the IKE protocol message will flow to cause the tunnel to be set up.

12. Click **OK**.

There are plenty of predefined policies for the key management tunnel and data management tunnel. But sometimes it does not meet your requirement or some parameters need to change because of interoperability or security. You can create or customize your own key management policy using the Key Management (Phase 1) Protection Policies menu from the Network panel or can create or customize your own data management policy using the Data Management (Phase 2) Protection Policies menu from the Network panel. In AIX V4.3.3, the key management policy configuration panel is the same as AIX V4.3.2. The data management policy configuration has changed. We will show these changes in this section. Refer to 9.1.4.1, "Key management tunnel policy creation/customization" on page 142 for the key management policy configuration.

1. Double-click **Data Management (Phase 2) Protection Policies** in the AIX V4.3.3 - VPN menu in the Network panel (see Figure 87 on page 156) to open the AIX - Data Management (Phase 2) Protection Policies.
2. From the Data Management (Phase 2) Protection Policies window (see Figure 81 on page 146), Select **Data Policy -> New Data Management Policy** to open the AIX V4.3.3 - Data Management (Phase 2) Policy Properties: General window.

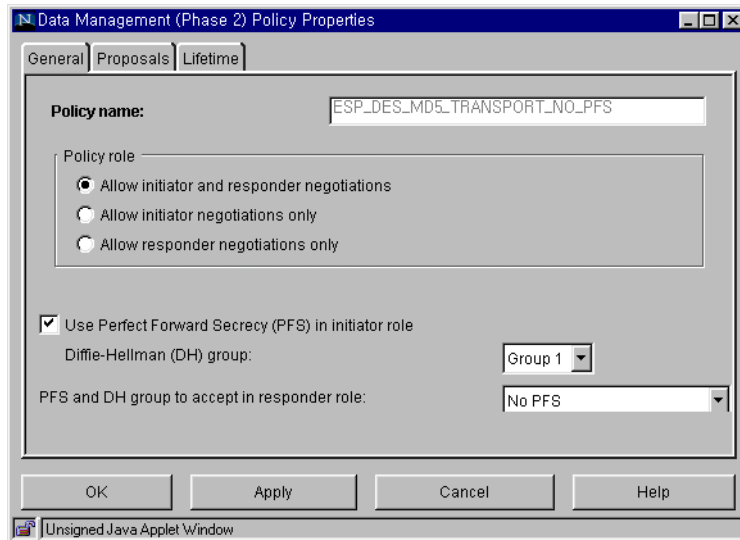


Figure 100. AIX V4.3.3 - Data Management (Phase 2) Policy Properties: General

The only difference in AIX V4.3.2 is the Perfect Forward Secrecy (PFS) option is added in the data management policy definition.

The Perfect Forward Secrecy (PFS) means that each key uses fresh keying material, that information on new keys cannot be derived from knowing the values of the old keys. If using PFS, the Diffie-Hellman group needs to be specified. This describes the group in which exponentiation will occur for exchanging Diffie-Hellman values. This group must match the group selected at the remote end. Group 1 is sufficient for most uses. Group 2 is more secure but requires more computational resources. All transforms in the suite must use the same group number. For Phase 2, this is used when Perfect Forward Secrecy is required and another Diffie-Hellman exchange is performed to get new keying material. This operation is computationally expensive and will consume CPU resources, therefore, if it is not needed, it is more efficient not to use it.

3. Select PFS in the initiator role, then choose appropriate values for the Diffie-Hellman (DH) group. The DH group can be one of the following values:
 - Group 1
 - Group 2
4. Choose an acceptable PFS and Diffie-Hellman group in the responder role. This can be one of the following values:
 - No PFS
 - DH Group 1
 - DH Group 2
 - DH Group 1 or 2
 - No PFS, or DH Group 1 or 2

9.2.5 Manual tunnel configuration using WebSM

In AIX V4.3.3, the manual tunnel configuration panel is added in the Web-based System Manager. For the simplest case, setting up a manual tunnel, defining the

tunnel parameters and filter rules are done in one step. As long as all traffic goes through the tunnel, the necessary filter rules will be automatically generated. The process for setting up a tunnel includes defining the tunnel on one end, creating a matching definition on the other end, and activating the tunnel on both ends. Then the tunnel is ready to be used for securing communication between the hosts. If information about the tunnel is not explicitly supplied, values will be defaulted and automatically generated. These values will then be specified in the export file that can be imported on the remote side. For instance, the encryption and authentication keys specified for the source will be used for the destination if the destination values are not specified. The source and destination addresses will be automatically swapped. This makes creating the tunnel much simpler.

A client configuration matching the manual tunnel example shown in this section is described in 19.1.6, “Configuring manual IPsec tunnels” on page 608.

9.2.5.1 Configure manual tunnels

For basic manual IPsec tunnel configuration, follow the steps below:

1. Double-click **Manual Tunnels** in the AIX V4.3.3 - VPN menu in the Network panel (see Figure 87 on page 156) to open the AIX V4.3.3 - Manual Tunnels configuration window window.

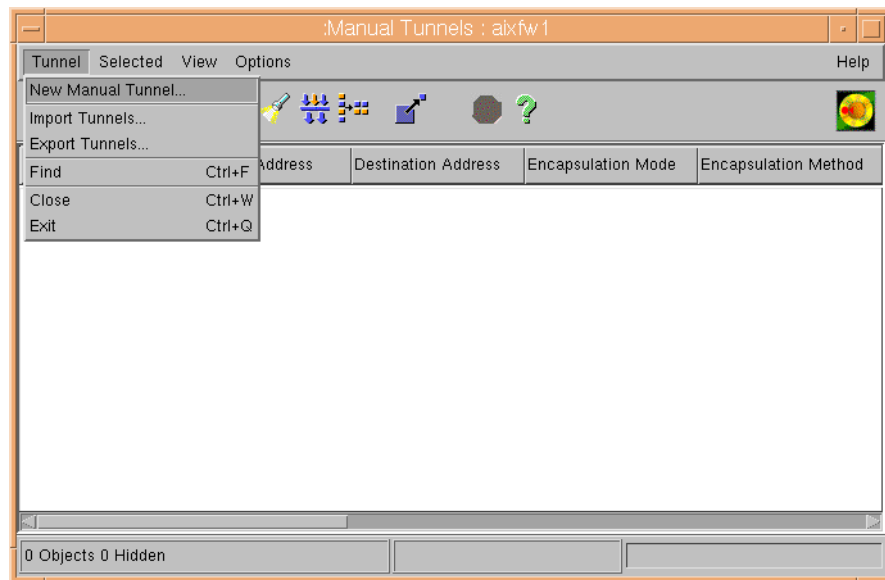


Figure 101. AIX V4.3.3 - Manual Tunnels configuration window

2. From the Manual Tunnels configuration window (see Figure 101), Select **Tunnel -> New Manual Tunnel** to open the AIX V4.3.3 - Manual Tunnel Properties: General window.

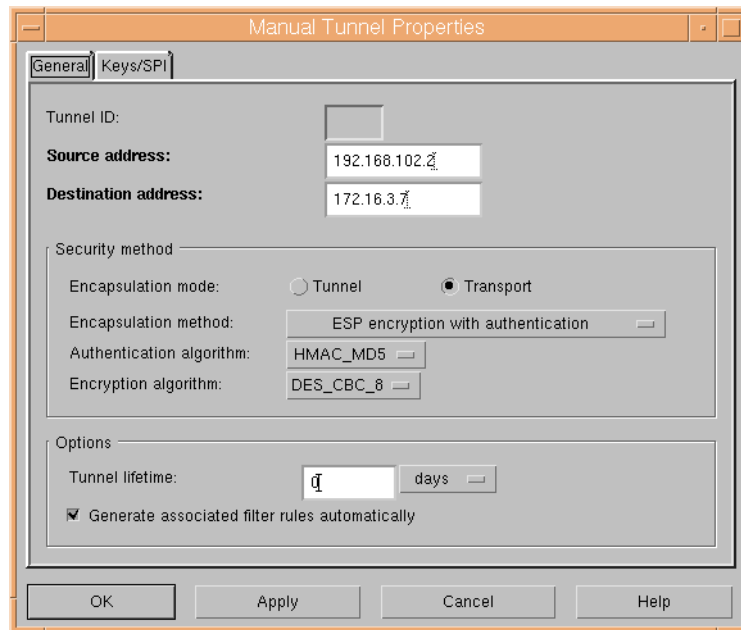


Figure 102. AIX V4.3.3 - Manual Tunnel Properties: General

3. Enter the Source and Destination IP address.
4. Select the Security method. The Encapsulation method can be one of following values:
 - AH authentication
 - AH authentication followed by ESP encryption
 - ESP encryption with authentication

The possible authentication and encryption algorithm is listed in Table 29 on page 155.

5. Select options. The automatic filter rules generation is recommended to ensure security and make it simple.
6. Click the **Keys/SPI** tab.

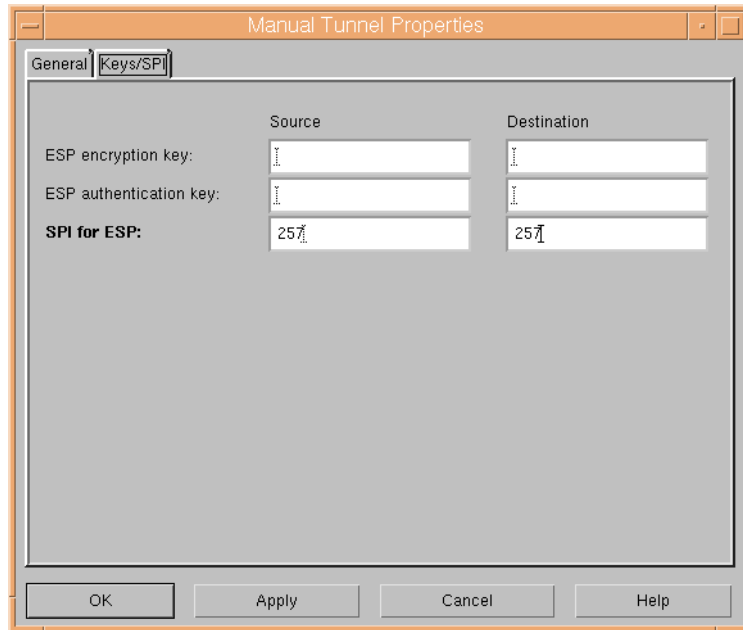


Figure 103. AIX V4.3.3 - Manual Tunnel Properties: Keys/SPI

7. Enter the authentication and encryption keys and specify SPI values (see Figure 103).

Important

Any key values you leave empty will be automatically generated by AIX. This method is simple and guarantees a fair amount of randomness and security for the keys.

Key values are entered in hexadecimal form.

SPI values must be entered at all times and are not automatically generated.

SPI values are entered in decimal form.

8. Click **OK**.

9.2.5.2 Transfer manual tunnel definitions

To set up the other side, if the other host is an AIX 4.3 IPSec machine, the tunnel definition can be exported on host A, then imported to host B. Before you do that, check the configuration again, especially if you let AIX generate the keys. An example is shown in Figure 104 on page 170.

Note: The SPI values shown in Figure 104 on page 170 are different from those in Figure 103 in order to match a client configuration as described in 19.1.6, “Configuring manual IPSec tunnels” on page 608.

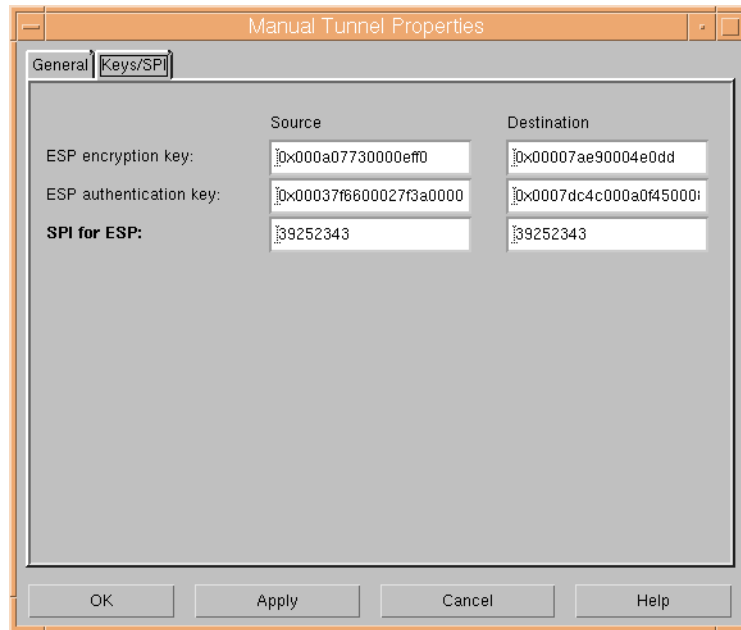


Figure 104. AIX V4.3.3 - check manual keys and SPIs

To export, you can use the **Tunnel -> Export Tunnels** pull-down menu in AIX V4.3.3 - Manual Tunnels configuration window (see Figure 101 on page 167) or the command line:

```
exptun -v4 -f /tmp
```

This will export the tunnel definition into a file named `ipsec_tun_manu.exp` and any associated filter rules to the file `ipsec_fltr_rule.exp`, in the directory indicated by the `-f` flag.

Figure 105 shows the manual tunnel export panel:

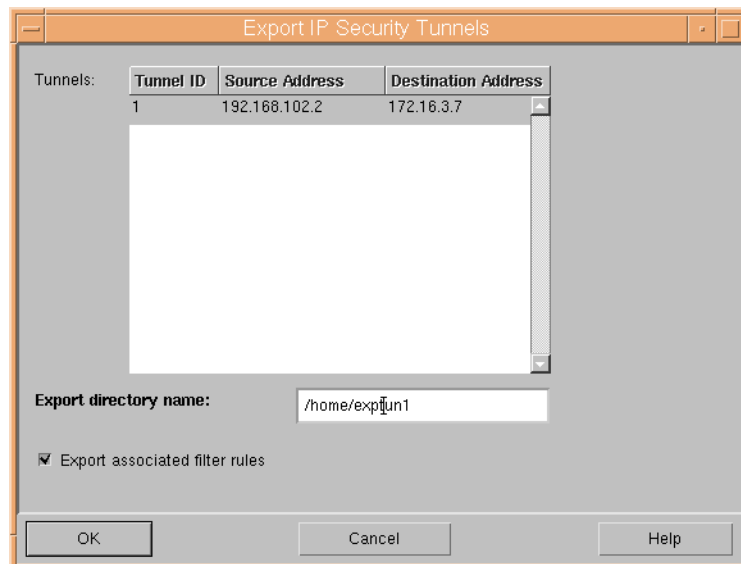


Figure 105. AIX V4.3.3 - manual tunnel export panel

Figure 106 shows an example of an AIX manual tunnel export file:

```
#-----  
4  
192.168.102.2  
172.16.3.7  
1  
257  
257  
257  
257  
DES_CBC_8  
8  
0x00007ae90004e0dd  
DES_CBC_8  
8  
0x000a07730000eff0  
NONE  
0  
0x  
NONE  
0  
0x  
0  
0  
tunnel  
tunnel  
exex  
1  
1  
HMAC_MD5  
16  
0x0007dc4c000a0f4500084019000766ec  
HMAC_MD5  
16  
0x00037f6600027f3a0000c045000a1ff6  
0  
-  
-
```

Figure 106. AIX V4.3.3 - manual tunnel export file

To create the matching end of the tunnel, the export files are copied to the remote side and imported into that remote AIX 4.3 machine by using the **Tunnel -> Import Tunnels** pull-down menu in AIX V4.3.3 - Manual Tunnels configuration window (see Figure 101 on page 167) or the command line:

```
imptun -v4 -t 1 -f /tmp
```

where 1 is the tunnel to be imported and /tmp is the directory where the import files reside. This tunnel number is system generated, and must be referenced from the output of the gentun command, or by using the lstun command to list the tunnels and determine the correct tunnel number to import. If there is only one tunnel in the import file, or if all the tunnels are to be imported, then the -t option is not needed.

9.2.5.3 Activating manual IPSec tunnels

Once the tunnel definitions are in place on both ends, the manual IPSec tunnel must be activated on both ends before it can be used to protect traffic. To do that,

highlight a tunnel in the Manual Tunnels window and click the green **Activate** button. An example of the result is shown in Figure 107:

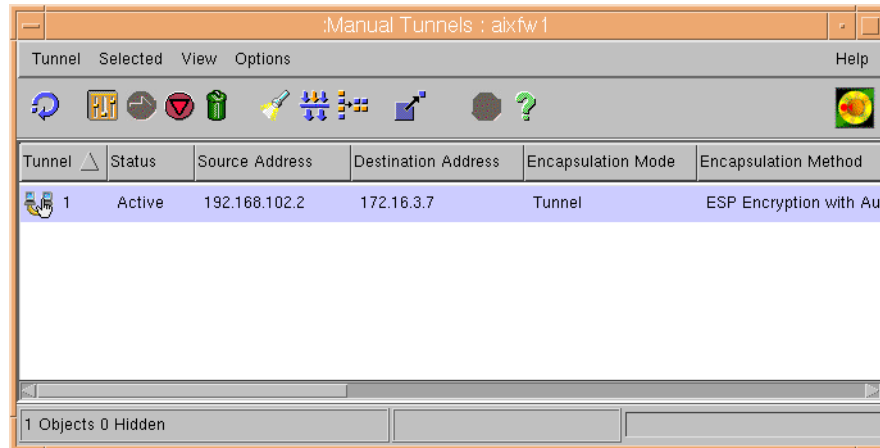


Figure 107. AIX V4.3.3 - activate manual IPSec tunnel

9.2.6 Filtering capability

Filtering is a basic function in which incoming and outgoing packets can be accepted or denied based on a variety of characteristics. This allows a user or system administrator to configure the host to control the traffic between this host and other hosts. Filtering is done on a variety of packet properties, such as source and destination addresses, IP Version (4 or 6), subnet masks, protocol, port, routing characteristics, fragmentation, interface, and tunnel definition. Rules known as “filter rules” are used to associate certain kinds of traffic with a particular tunnel.

When the tunnel is modified or deleted, the filter rules for that tunnel are automatically deleted. This greatly simplifies IP Security configuration and helps reduce human error. Tunnel definitions can be propagated and shared among AIX machines and AIX firewalls using import and export utilities. This is especially helpful in the administration of a large number of machines.

Filter rules are necessary to associate particular types of traffic with a tunnel, but data being filtered does not necessarily need to travel in a tunnel. This allows AIX to provide a base firewall function for users who want to restrict the flow of certain types of traffic to or from their machine. This is especially useful for the administration of machines in an intranet that do not have the protection of a firewall. This can be part of setting up a DMZ around a group of machines to provide a second barrier in case of a compromise.

Once the filter rules are generated, they are stored in a table and loaded into the kernel. When packets are ready to be sent or received from the network, the filter rules are checked in the list from top to bottom to determine whether the packet should be permitted, denied, or sent through a tunnel. The criteria of the rule is compared to the packet characteristics until a match is found or the default rule is reached.

The IP Security function also implements filtering of nonsecure packets based on very granular user-defined criteria. This is a useful function to allow the control of

IP traffic between networks and machines that do not require the authentication or encryption properties of IP Security.

To view or define filter rules for the manual tunnel, double-click **Static Filter Rules (for Manual tunnels)** in Figure 108:

| Filter Rule | Action | Source Address | Source Mask | Destination Address | Destination Mask | Source Routing | Protocol | Source |
|-------------|--------|----------------|-----------------|---------------------|------------------|----------------|----------|--------|
| 1 | permit | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | no | udp | eq |
| 2 | *** | Dynamic | filter | placement | rule | for | IKE | tunne |
| 3 | permit | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | yes | ah | any |
| 4 | permit | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | yes | esp | any |
| 5 | permit | 192.168.102.2 | 255.255.255.255 | 172.16.3.7 | 255.255.255.255 | yes | all | any |
| 6 | permit | 172.16.3.7 | 255.255.255.255 | 192.168.102.2 | 255.255.255.255 | yes | all | any |
| 0 | permit | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | yes | all | any |

Figure 108. AIX V4.3.3 - static IP filters for manual IPsec tunnel

For manual tunnels, when a user defines a host-to-host tunnel, filter rules are auto-generated to direct all traffic from that host through the secure tunnel. If more specific types of traffic are desired (for instance, subnet-to-subnet), the filter rules can be edited or replaced to allow precise control of the traffic using a particular tunnel.

1. Click **Filter Rule -> New Filter Rule** to open Figure 109:

Filter Rule Properties

General | Match Criteria

Specify the filter rule attributes.

Filter rule number:

Action taken when rule is matched: Permit Deny

Network interface for filter rule:

Tunnel ID:

Apply rule to the following:

IP packet type:

IP packet direction:

IP packet fragmentation:

Source routing

Create log entry when IP packet matches rule

OK Apply Cancel Help

Unsigned Java Applet Window

Figure 109. AIX V4.3.3 - Filter Rule Properties: General

2. Define the action, permit or deny, when the rule is matched.
3. Specify the interface. In the Network Interface field, you can choose a specific interface or all of the interfaces.
4. Specify the Tunnel ID if this filter rule is associated to a certain manual tunnel. The default value, 0, means that this filter rule is not associated to a tunnel and will be applied to all traffic.
5. Select the characteristics of the IP packet you want to apply.

The IP packet type can be one of the following values:

 - both, local, route

The IP packet direction can be one of the following values:

 - both, inbound, outbound

The IP packet fragmentation can be one of the following values:

 - all packets
 - fragment headers and unfragmented packets only
 - fragments and fragment headers only
 - unfragmented packets only
6. Click the **Match Criteria** tab.

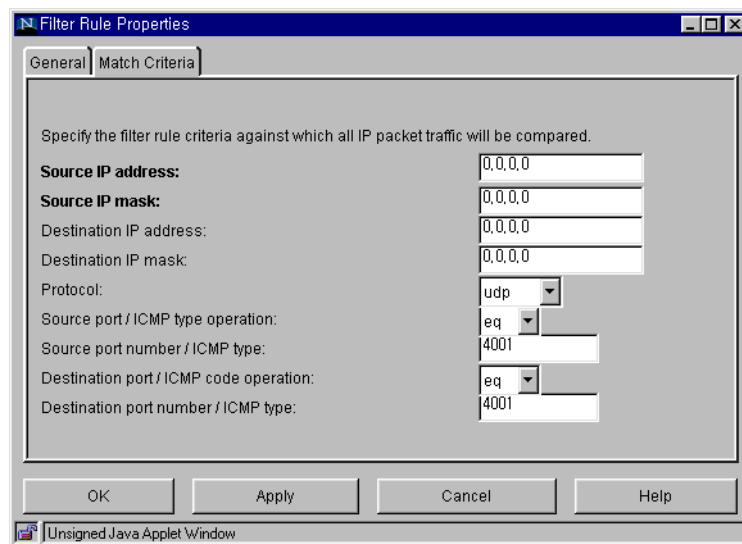


Figure 110. AIX V4.3.3 - Filter Rule Properties: Match Criteria

7. Enter the IP address and mask for the source and destination.
8. Select the protocol and port number for the source and destination.

The protocol can be one of the following values:

 - all, TCP, TCP/ACK, UDP, ICMP, OSPF, IPIP, ESP, or AH
9. Click **OK**.

To view filter rules for the IKE tunnel, double-click **Dynamic Filter Rules (for Internet Key Exchange Tunnels)** in AIX V4.3.3 - VPN menu in the Network panel (see Figure 87 on page 156).

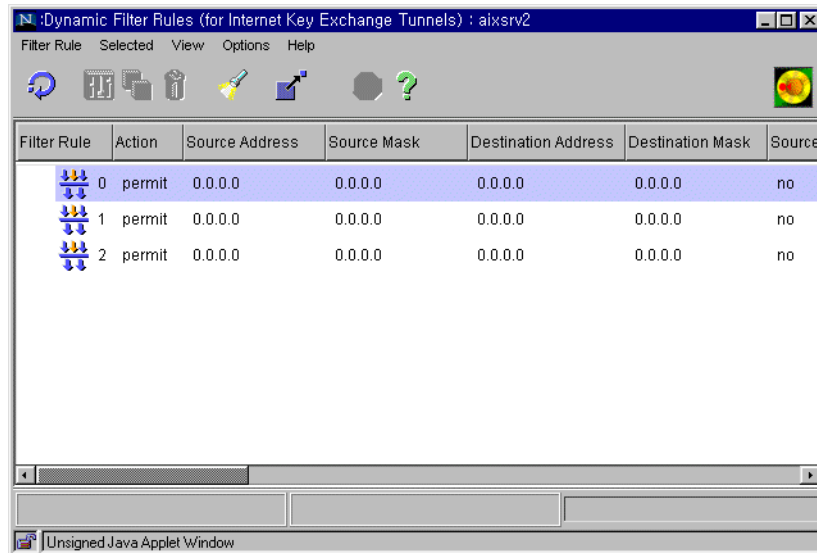


Figure 111. AIX V4.3.3 - Dynamic Filter Rules (for IKE Tunnels)

For IKE tunnels, the filter rules are also automatically generated and inserted in the filter table once the tunnel is activated.

IKE filter rules are also auto-generated and will be kept in a separate table. The IKE negotiation has support to specify protocol and port numbers; they will be set accordingly in the filter rules. The IKE filter rules will be searched after the static filter rules and before the auto-generated rules. The position in the static filter table where IKE filter rules will be inserted will be defaulted but can be moved by the user. Since the auto-generated rules permit all traffic over the tunnel, user-defined rules may be necessary to place restrictions on certain types of traffic. These user-defined rules should be placed before the auto-generated rules because the first rule that applies to the packet will be used.

9.2.7 IKE setup for digital certificate support

By adding a PTF to AIX 4.3.3, you can enable IKE to use digital signature authentication mode.

9.2.7.1 Installing required filesets and PTFs

To enable this feature, you need to install a key and certificate management tool called `gskit.rte` from the AIX Bonus Pack CD-ROM. (This will automatically install the required fileset `gskrf301.base`.)

| Fileset | Level | State | Description |
|----------------------------|----------|-------|--------------------------------------|
| <code>gskit.rte</code> | 4.0.1.12 | C | AIX Certificate and SSL Base Runtime |
| <code>gskrf301.base</code> | 3.0.1.84 | C | <code>gskrf301</code> for AIX |

After installing `gskit`, you have to apply the following PTFs. Be aware that the PTFs mentioned are not yet publicly available at the time of writing this redbook.

The planned release date is November 1999; please verify that the indicated PTF numbers are okay.

The PTFs contain the IKE daemons and configuration panels to support signature mode authentication:

| fileset | version | ptf | apars |
|----------------------|---------|---------|---------|
| bos.net.ipsec.keymgt | 4.3.3.1 | U467160 | IY02769 |
| bos.net.ipsec.websm | 4.3.3.1 | U467254 | IY02769 |

To obtain these PTFs visit the RS/6000 support Web site at:

<http://techsupport.services.ibm.com/rs6k/fixdb.html>

On this page, select **AIX Version 4** and **PTF number**, then continue and enter the PTF numbers you want when prompted.

9.2.7.2 Using keys and certificates

To generate key pairs and to request and receive client and CA certificates, use the gsk4ikm application that can be launched by entering its name on a command line.

Note: Before you start gsk4ikm, properly set the JAVA_HOME environment variable, for example, `JAVA_HOME=/usr/jdk_base`.

Follow the steps below to request and load certificates for IKE.

1. Enter `gsk4ikm` from a command shell to start the certificate manager. This application takes a while to load so please be patient.
2. Select **Key Database File -> New** to create a new database for storing keys and certificates used with IKE. Select **CMS key database file** as the database type. Name the database `ikekey.kdb` and place it in the `/etc/security` directory.

Important

You must enter the name and location of the new key database exactly as shown in Figure 112 or else it cannot be used with IKE. The reason is that these names are hard-coded into the new cpsd daemon that parses and loads certificates.

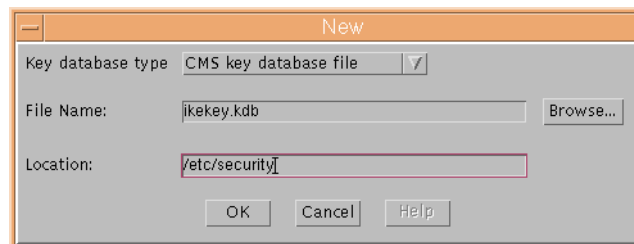


Figure 112. AIX 4.3.3 - create new key database

3. Click **OK**.

- On the following panel, enter a password for the key database and check the Stash password box. The key fields in Figure 113 indicate the relative strength of the password you have selected.

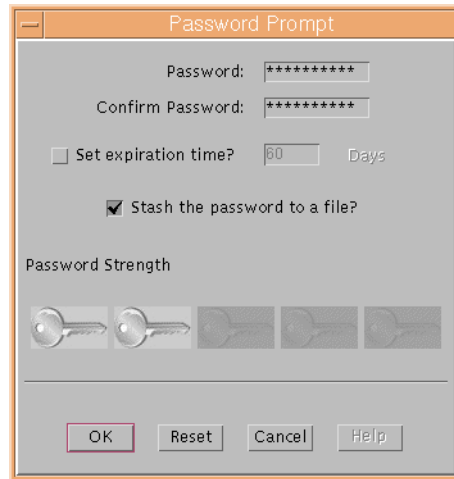


Figure 113. AIX 4.3.3 - password for key database

Note: You can also use the certificate manager to create self-signed certificates, but you cannot use those certificates for IKE.

- Click **OK**.
- Once the new key database has been created, a list of preloaded CA certificates is shown in the key database content pane (see Figure 114):

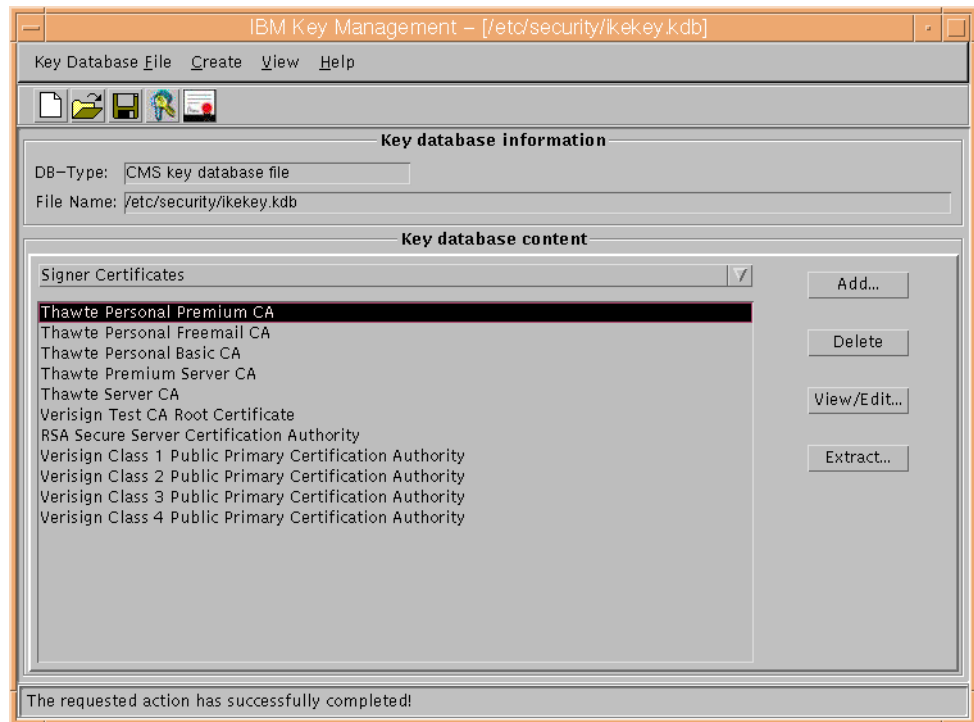


Figure 114. AIX 4.3.3 - preloaded CA certificates

7. Select **Create -> New certificate request** from the menu bar and fill in at least the required fields in the certificate request form. An example is shown in Figure 115:

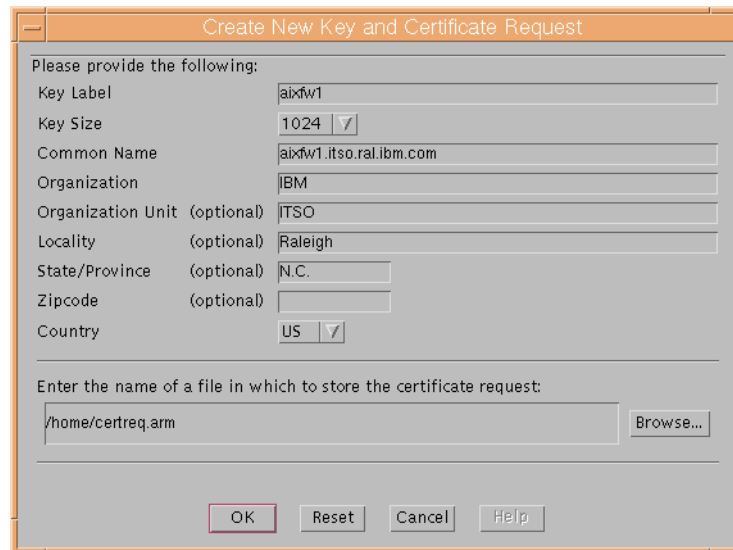


Figure 115. AIX 4.3.3 - certificate request form

8. Click **OK**. A private and public key pair, the certificate request file, and the default name certreq.arm, are created by the system. The certificate manager will display a list of pending certificate requests in the key database content pane.
9. Send the certificate to a CA by means of whatever infrastructure you are using, for example, file transfer, e-mail, copy and paste into a Web browser, mail a diskette.
10. Retrieve a CA certificate and a device certificate for your system. You must now first load the CA certificate, then the device certificate, into the key database.
11. From the pull-down list in the key database content pane, select **Signer Certificates**, then click **Add**.
12. Select the file that holds the CA certificate you have just received and choose the proper format (binary DER or base64 ASCII). Click **OK**.
13. Enter a name for this CA in the label field and click **OK**. The new CA certificate is added to the list.
14. From the pull-down list in the key database content pane, select **Personal Certificates**, then click **Receive**.
15. Select the file that holds the device certificate you have just received; choose the proper format (binary DER or base64 ASCII) and enter a name for the device in the label field (see Figure 116 on page 179). Click **OK**.

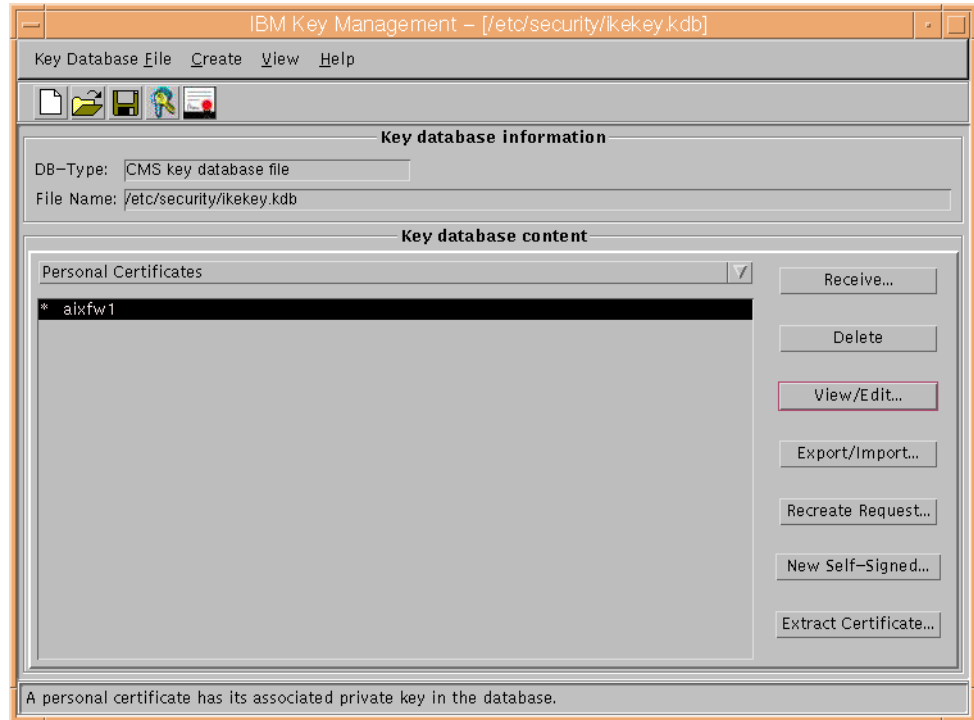


Figure 116. AIX 4.3.3 - load device certificate

16. The new device certificate is added to the list which completes this part of the configuration. You may now exit the certificate manager.

If IP Security has not yet been started, you can start it from WebSM. At that time, the cpsd daemon will parse all certificates and load them for use with IKE if successful.

If IP Security is already active, the cpsd daemon will parse and load certificates when a new tunnel configuration is performed.

Output of the cpsd daemon can be directed to the /var/security/isakmpd.log file.

9.2.7.3 Configuring IKE for digital signature mode

To use signature authentication mode with IKE, you can either create a new key management tunnel or change an existing one from a pre-shared key to digital signature mode. The updated configuration panel is shown in Figure 117 on page 180.

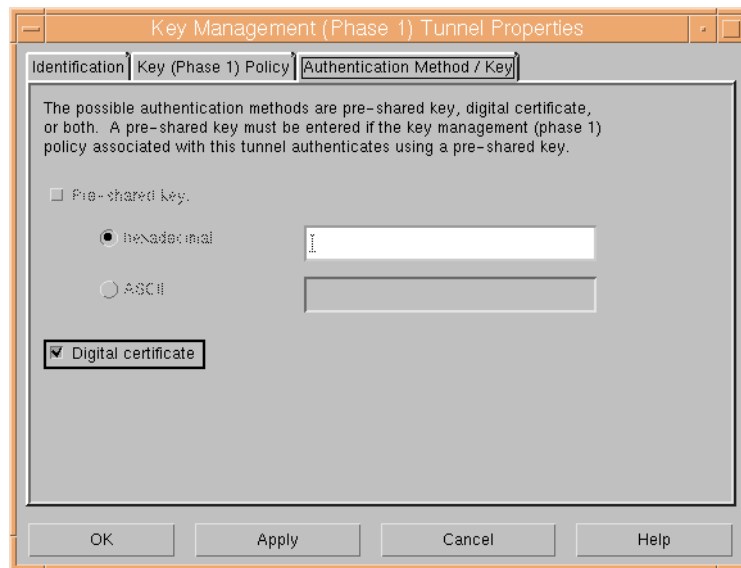


Figure 117. AIX 4.3.3 - configure key management tunnel authentication mode

For local and remote identifiers for the key management tunnel endpoints, you must use the type that is supplied in the `subject_alternate_name` fields of the VPN device certificates. This can be one of the following:

- IP address
- Fully qualified domain name (FQDN)
- E-mail address
- User name

You can also use the subject DN as an ID.

Note: According to the current draft, a VPN device certificate supports multiple `subject_alternate_name` entries as long as they are of different types.

We have successfully tested IKE signature authentication with AIX in conjunction with an IRE SafeNet VPN client.

9.3 Creating a VPN host-to-host connection

Virtual private network features in AIX V4.3.2 provide secure communication between two AIX servers. AIX V4.3.2 offers two types of tunneling, transport mode, and tunnel mode. In this host-to-host scenario, transport mode is used to make the VPN tunnel.

In this host-to-host connection we describe parameters or values applied to the key management and data management tunnels. Refer to 9.1.3, “AIX V4.3.2 IP Security: IKE tunnel basic setup” on page 131 for more details.

For IKE configuration in AIX, two tunnel configurations are needed:

- Key management tunnel configuration
 1. Define the key management tunnel name and local and remote endpoints for the tunnel.

2. Associate the key management policy to the tunnel.
 3. Define the pre-shared key.
- Data management tunnel configuration
 1. Define the data management tunnel name and associate to the key management tunnel.
 2. Define the local and remote endpoints type and ID.
 3. Associate the data management policy to the tunnel.

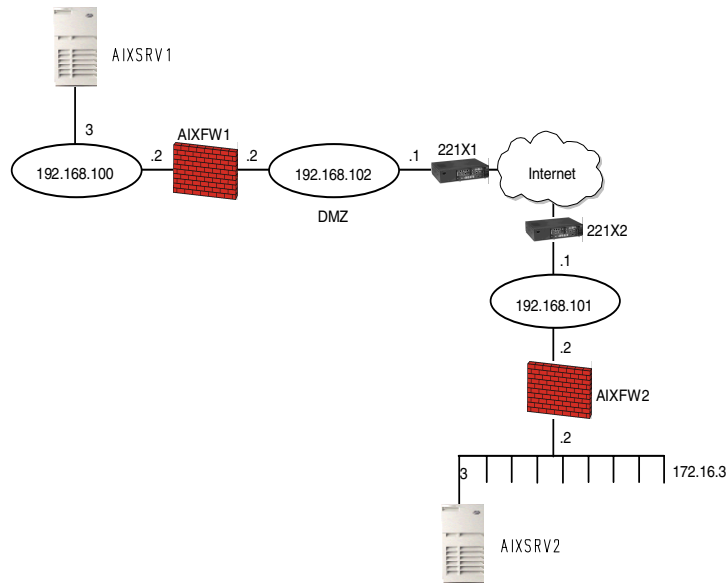


Figure 118. AIX - host-to-host connection

In this host-to-host case, we use two AIX systems named AIXSRV1 and AIXSRV2. Both can be the initiator and responder in this scenario.

In this section, we only describe the configuration on AIXSRV1 even though the configuration on AIXSRV2 is needed. The only difference is setting the endpoint IP address in reverse. The local endpoint IP address in AIXSRV1 should be put into the remote endpoint IP address in AIXSRV2 and vice versa.

The parameters used in this scenario are shown in Table 32:

Table 32. AIX - host-to-host VPN connection IPSec parameters

| IPSec parameters and some pertinent information on the other party | |
|--|---------------|
| Local | |
| Hostname | AIXSRV1 |
| IP Address | 192.168.100.3 |
| Role | Initiator |
| Remote | |
| Hostname | AIXSRV2 |

| IPSec parameters and some pertinent information on the other party | | |
|---|----------------------|-----|
| 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 Life Time | 480 min (default) | |
| Negotiation ID | IP Address | |
| Pre-Shared Key | 3132333435363738 | |
| 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 | |
| SA Lifetime | 30 min (default) | |

Perform the following steps to configure a host-to-host VPN on AIXSRV1.

We start from the Internet Key Exchange (IKE) Tunnels configuration panel.

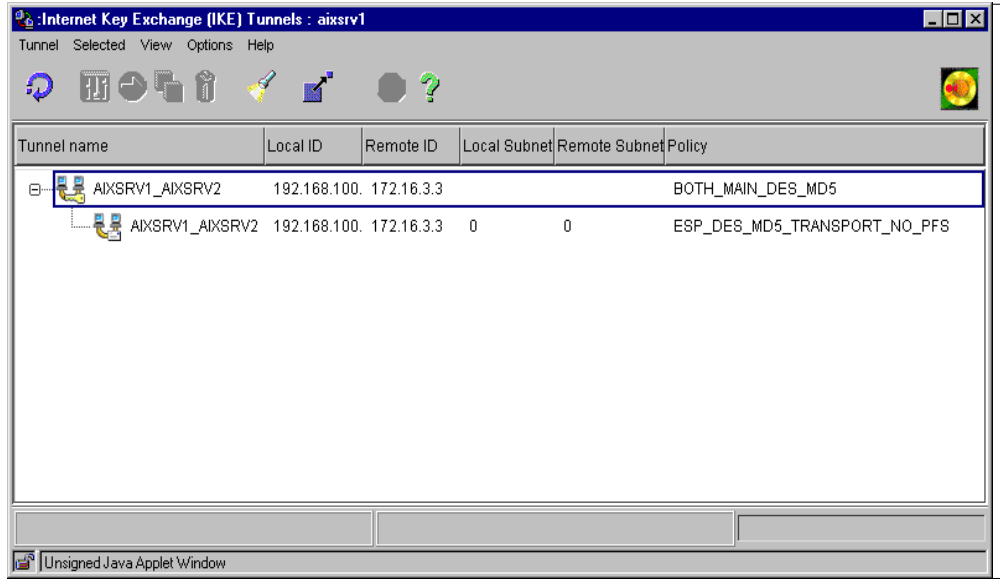


Figure 119. AIX - Internet Key Exchange (IKE) Tunnel s configuration panel

17. Select **Tunnel -> New Key Management Tunnel** to open the Key Management (Phase 1) Tunnel Properties window.

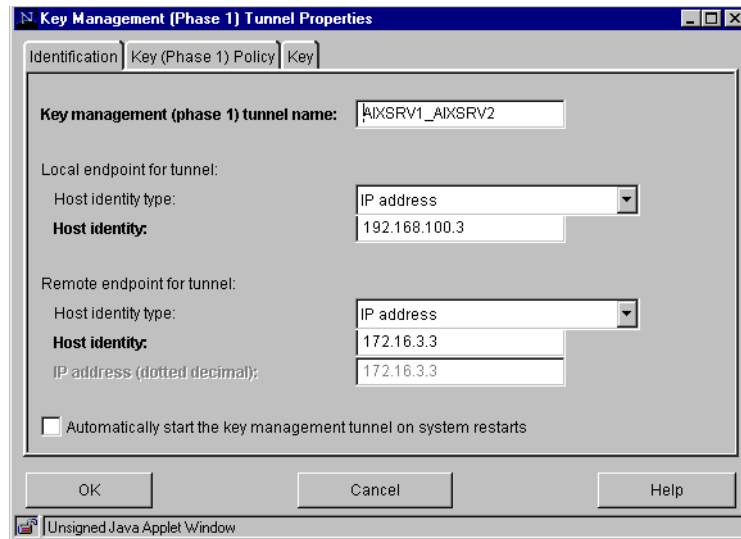


Figure 120. AIX - Key Management (Phase 1) Tunnel Properties: Identification

18. On the Identification panel, enter the key management tunnel name. In this case, AIXSRV1_AIXSRV2.
19. Select **IP address** as the Host Identity type for the local and remote endpoint for the tunnel and enter the IP addresses of the local and remote hosts.
20. Click the **Key (Phase 1) Policy** tab.

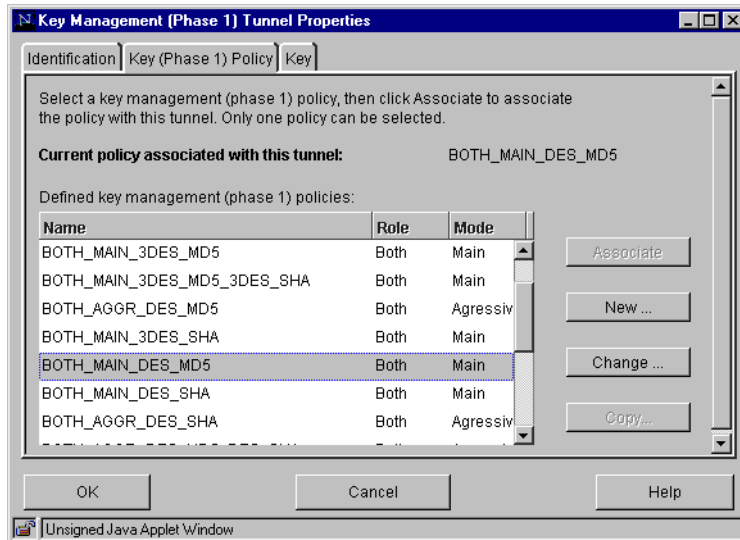


Figure 121. AIX - Key Management (Phase 1) Tunnel Properties: Key (Phase 1) Policy

21. Select **BOTH_MAIN_DES_MD5** policy from the defined key management (phase 1) policies and click **Associate**.

22. Click the **Key** tab.

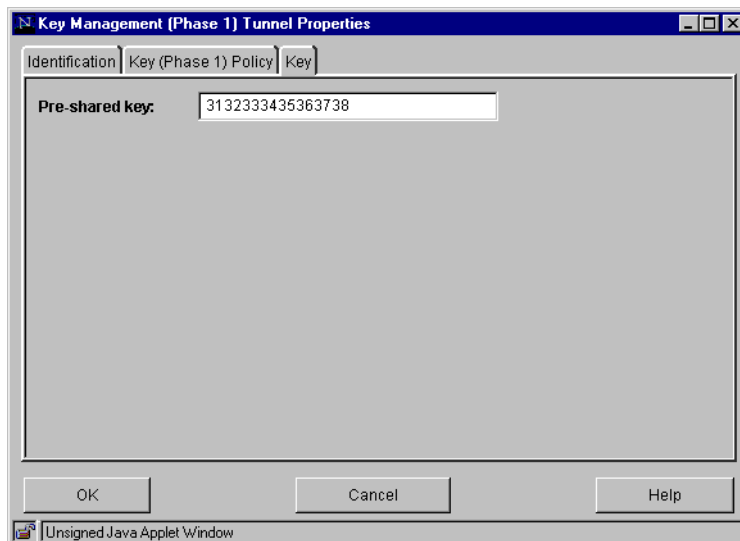


Figure 122. AIX - Key Management (Phase 1) Tunnel Properties: Key

23. Enter the pre-shared key. Use the hexadecimal notation, for example, Hex 31, 32 is equivalent to Decimal 1, 2 respectively.

24. Click **OK**.

The key management tunnel has been configured. Next we configure the data management tunnel associated to the key management tunnel.

25. Select **Tunnel -> New Data Management Tunnel** on the Internet Key Exchange (IKE) Tunnels configuration panel to open the Data Management (Phase 2) Tunnel Properties window.

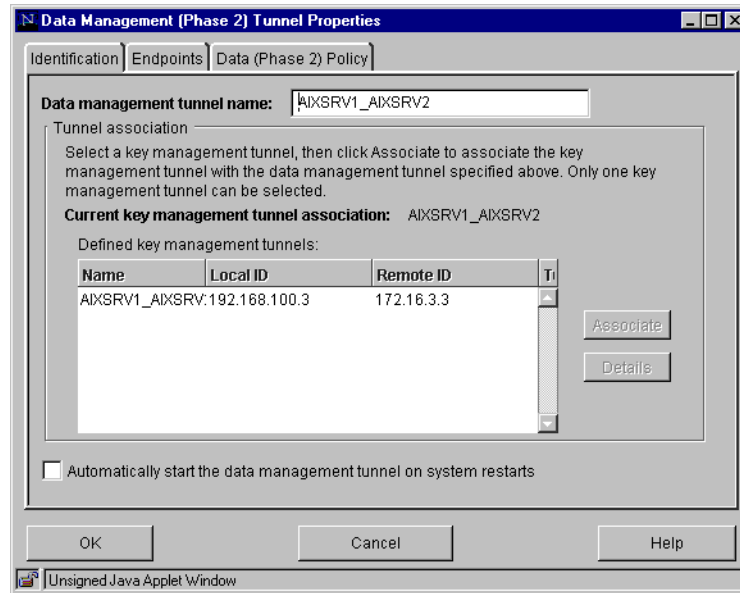


Figure 123. AIX - Data Management (Phase 2) Tunnel Properties: Identification

26. On the Identification panel, enter the data management tunnel name. In this case, AIXSRV1_AIXSRV2.

27. Choose the key management tunnel name you want to be associated, in this case, AIXSRV1_AIXSRV2, and click the **Associate** button.

Note

Unmark the Automatically start the data management tunnel on system restarts button if your side will be the responder or you do not want to establish data management tunnel at system restart.

28. Click the **Endpoints** tab.

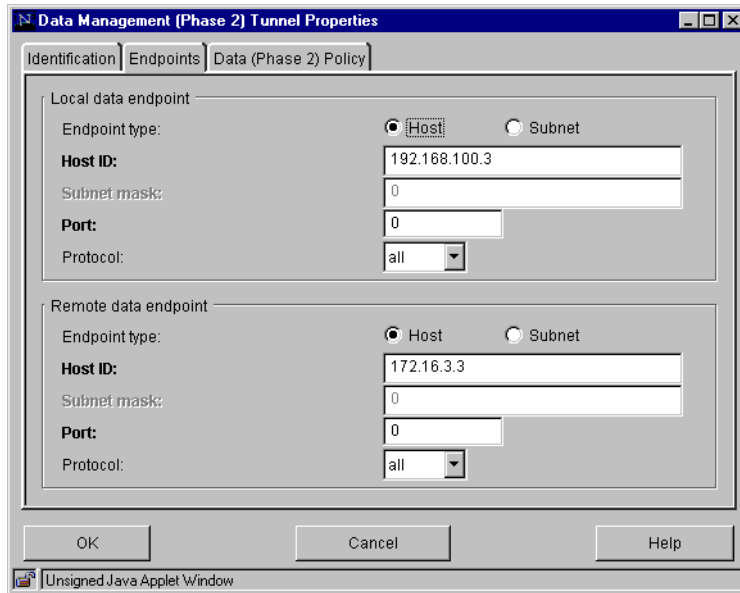


Figure 124. AIX - Data Management (Phase 2) Tunnel Properties: Endpoints

29. Select **Host** as the endpoint type for the local and remote data endpoint.
30. Enter the local and remote IP address in the Host ID field.
31. Click the **Data (Phase 2) Policy** tab.

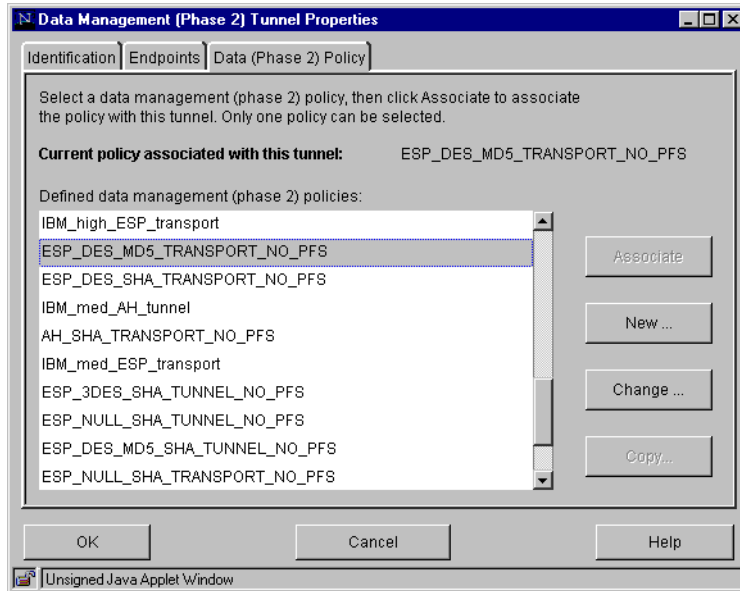


Figure 125. AIX - Data Management (Phase 2) Tunnel Properties: Data (Phase 2) Policy

32. Select the **ESP_DES_MD5_TRANSPORT_NO_PFS** policy from the defined data management (phase 2) policies and click the **Associate** button.
33. Click **OK**.

Now the data management tunnel is configured successfully.

After the IPSec IKE configuration, AIXSRV2 needs to be configured as described above.

After completion of IKE on AIXSRV1 and AIXSRV2, AIXSRV1 activates the key management tunnel and data management tunnel as an initiator. Then check if the tunnel is active using the IKE tunnel monitor (see 9.1.3.4, “IKE tunnel activation and deactivation” on page 140).

Chapter 10. OS/400 V4R4 native VPN support

This chapter describes VPN implementation on the AS/400 system.

10.1 Overview

AS/400 VPN technologies are based on the latest Internet Engineering Task Force's (IETF) IPsec standards. The following are available in the AS/400 V4R4 VPN implementation:

1. Manual VPN connections
 - Each endpoint is configured manually
 - Cryptographic keys are predefined
2. Dynamic key connections
 - Internet Key Exchange (IKE) protocol for dynamic key exchange
 - Cryptographic keys are negotiated
3. Dynamic IP connections
 - Remote client IP address not fixed
4. L2TP (Layer 2 Tunneling Protocol) connections
 - Provides a virtual PPP tunnel across a public network allowing a private corporate address space to be extended out to a remote client
5. Virtual Private Network Address Translation (VPNAT)
 - AS/400 unique solution
 - Resolves IP address conflicts

10.2 VPN software prerequisites

The VPN support on the AS/400 system in V4R4 requires the following products:

- 5769-SS1 V4R4 OS/400
- 5769-TC1 TCP/IP Connectivity Utilities for AS/400
- 5769-AC2 or 5769AC3 Cryptographic Access Provider for AS/400
- 5769-SS1 option 34 OS/400 - Digital Certificate Manager
- 5769-XE1 Client Access/400 Express for Windows (with Operations Navigator - Network component installed)

Because AS/400 VPN uses strong cryptography in its implementation, you must install the Cryptographic Access Provider (5769-AC2 or AC3). 5769-AC1 is not supported by AS/400 VPN. 5769-AC3 is permitted for use within the U.S. and Canada. At the time of writing, 5769-AC3 is also available outside of North America with the following conditions:

- For use by U.S.-affiliated banks or medical institutions
- Permission is granted by the U.S. Department of Commerce

5769-AC2 can be ordered outside of North America without the above conditions.

5769-AC2 and 5769-AC3 are free of charge. They will be shipped automatically if Internet Connection Secure Server (5769-NC1 or 5769-NCE V4R2) or previous

versions of 5769-AC2 or 5769-AC3 were installed on the system. Otherwise, Cryptographic Access Provider must be ordered even when it is free of charge.

Note

OS/400 VPN support is able to dynamically determine the cryptographic capabilities of the system and only use currently supported algorithms. What this means is, if 5769-AC2 is installed, the highest security available is 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. So, for a 5769-AC2 system to 5769-AC3 system negotiation, the key and data policy transforms must be modified so that they match.

In V4R4, although AS/400 VPN does not use digital signatures and certificates for authentication, Digital Certificate Manager (5769-SS1 option 34) must be installed because there are several APIs provided by DCM that AS/400 VPN requires. DCM is included with OS/400 but may not be loaded on all systems.

AS/400 Client Access Express for Windows client is shipped with OS/400 V4R4 and installed as licensed program 5769-XE1. All functions of the Express client, with the exception of PC5250 Display and Print Emulation and Data Transfer, can be used without acquiring a license for the AS/400 Client Access Family for Windows product (5769-XW1). AS/400 Client Access Express for Windows client is also included with the Client Access Family for Windows product (5769-XW1) along with the other client members.

10.3 AS/400 VPN components

AS/400 VPN support consists of these components:

- AS/400 Operations Navigator
- VPN New Connection Wizard
- VPN server and VPN policy database
- IP packet filtering with ACTION = IPSEC

The next sections briefly introduce each of these components.

10.3.1 AS/400 Operations Navigator

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

AS/400 VPN requires the AS/400 Operations Navigator's Network component. This component provides the Virtual Private Networking Configuration GUI for you to configure and manage VPN connections.

There are no "green screen" commands available for VPN configuration or management.

10.3.2 New Connection Wizard

The New Connection Wizard is initiated from the Virtual Private Networking Configuration GUI. It provides an easy-to-use, step-by-step graphical user interface for creating VPNs for the following combination of hosts and gateways: host-to-host, gateway-to-host, host-to-gateway, gateway-to-gateway. Dynamic IP user-to-host and dynamic IP user-to-gateway connections can also be created using the wizard. Other types of connections must be manually defined using the Virtual Private Networking Configuration GUI.

Based on the specific security needs and the network configuration, a minimum of parameters is required for input by the New Connection Wizard to create VPN connections.

Since the manual configuration of VPN connections is a complicated task, it is advisable to use the New Connection Wizard to create the VPN objects first and then to manually customize the parameters in those VPN objects.

10.3.3 VPN server jobs

The VPN server jobs must be started before VPN connections can be initiated. The VPN server jobs run in the QSYSWRK subsystem and they are:

- 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.

10.3.4 VPN policy database

Once you create your VPN, the associated configuration objects are stored in the VPN policy database. The VPN policy database consists of the following objects in QUSRSYS:

Table 33. OS/400 - VPN policy database objects

| Object | Type | Library | Attribute |
|-------------|-------|---------|-----------|
| QATOVDAAH | *FILE | QUSRSYS | PF |
| QATOVDCCDEF | *FILE | QUSRSYS | PF |
| QATOVDDEF | *FILE | QUSRSYS | PF |
| QATOVDDESEL | *FILE | QUSRSYS | PF |
| QATOVDDESP | *FILE | QUSRSYS | PF |
| QATOVDIID | *FILE | QUSRSYS | PF |
| QATOVDIPAD | *FILE | QUSRSYS | PF |
| QATOVDLID | *FILE | QUSRSYS | PF |
| QATOVDMCOL | *FILE | QUSRSYS | PF |
| QATOVDNATP | *FILE | QUSRSYS | PF |
| QATOVDN1 | *FILE | QUSRSYS | PF |

| Object | Type | Library | Attribute |
|------------|-------|---------|-----------|
| QATOVDPKEY | *FILE | QUSRSYS | PF |
| QATOVDGRGP | *FILE | QUSRSYS | PF |
| QATOVD1 | *FILE | QUSRSYS | PF |
| QATOVDSRVR | *FILE | QUSRSYS | PF |
| QATOVDUCP | *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 | |

10.3.5 IP packet filtering

IP packet filtering is an integrated feature of OS/400 that was first introduced in V4R3. Filtering allows you to implement basic IP packet filtering rules to control traffic flowing into and out of your AS/400 system. Initially, packet filtering supported either DENY or PERMIT as an action type. However, in V4R4, the action type IPSEC was added to support VPN specific traffic.

Filter rules are a very important part of the VPN implementation process. Filter rules are required to direct traffic through the VPN connection as well as allow IKE negotiations to occur. The New Connection Wizard does not create the filter rules necessary for VPN connections to work. This must be done manually by using Operations Navigator's IP packet filtering configuration GUI.

For most basic dynamic key connections, three IP packet filter rules are required (see Figure 126):

- 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

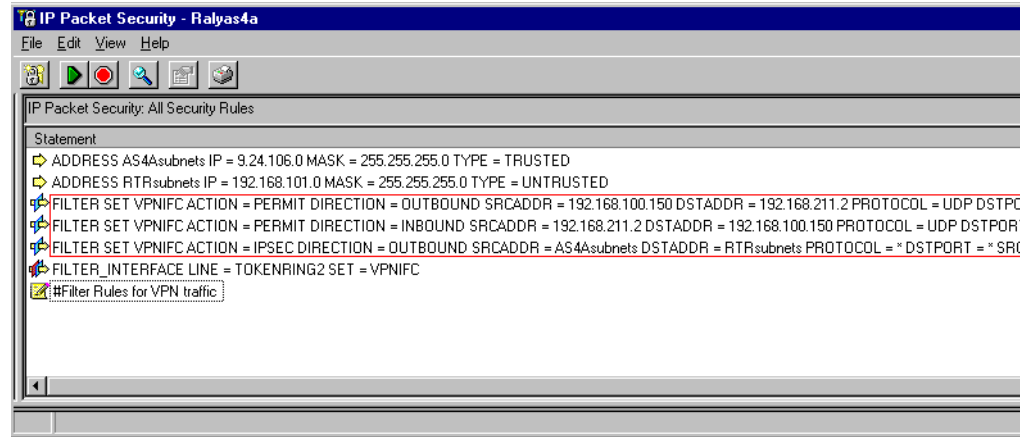


Figure 126. OS/400 - Example of dynamic key connection IP filter rules

For manual key connections only one IPSEC filter rule is required.

IP packet filtering can also be used to limit services on VPN connections. For example, there may be requirements to allow only Telnet on a VPN connection and deny other services such as FTP, SMTP, POP, LPD, and so on.

10.4 Basic planning

To simplify the planning process, the following planning worksheets can be used to gather the necessary information before the actual implementation.

10.4.0.1 Prerequisite checklist

The prerequisite checklist planning worksheet ensures that the software components required for VPN support are installed, the QRETSVRSEC system value is set correctly and that TCP/IP routing is configured and tested before attempting to implement a VPN connection. If normal TCP/IP communications cannot be established between the required endpoints then 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.

The checklist also ensures that if there are any firewalls or routers between the VPN partners, the firewalls and routers are configured to permit IKE (UDP port 500), AH and ESP protocols. The firewalls must also be configured to perform IP forwarding.

All the answers in the prerequisite checklist (Table 34) must be *yes* before proceeding with the VPN connection implementation.

Table 34. OS/400 - 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? | |
| Is Cryptographic Access Provider (5769-AC2 or AC3) installed? | |

| Prerequisite checklist | Answers (Yes/No) |
|---|------------------|
| Is 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 *SEC) 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)? | |
| If the VPN tunnel traverses firewalls or routers that implement IP packet filtering, do the firewall and/or router filter rules support AH and ESP protocols? | |
| Have the firewalls or routers been configured to permit IKE (UDP port 500), AH and ESP protocols? | |
| Have the firewalls been configured to enable IP forwarding? | |

10.4.0.2 New Connection Wizard planning worksheet

The New Connection Wizard can be used to configure dynamic key (IKE) or dynamic IP connections. If the New Connection Wizard is used to create these connections, use the planning worksheet in Table 38.

First, the level of security must be determined. The level of security determines the algorithms used to protect keys and data as they travel across the network. Take note that specifying maximum security for VPN may affect system performance.

Based on the level of security specified, the New Connection Wizard uses the corresponding default algorithms for key and data protection (Table 35 and Table 36):

Table 35. OS/400 - system delivered default algorithms for key protection

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

Table 36. OS/400 - system delivered default algorithms for data protection

| Field | Value |
|---|----------------|
| Data Protection Transform for Minimum Security, Highest Performance (HP) | |
| Protocol | AH |
| Authentication Algorithm | HMAC-MD5 |
| Encryption Algorithm | Not applicable |
| Diffie-Hellman Perfect Forward Secrecy (PFS) | Not selected |
| Data Protection Transform for Balanced Security and Performance (BS) | |
| Protocol | ESP |
| Authentication Algorithm | HMAC-MD5 |
| Encryption Algorithm | DEC-CBC |
| Diffie-Hellman perfect forward secrecy (PFS) | Not selected |
| Data Protection Transform for Highest Security, Lowest Performance (HS) | |
| Protocol | ESP |
| Authentication Algorithm | HMAC-SHA |
| Encryption Algorithm | 3DEC-CBC |
| Diffie-Hellman Perfect Forward Secrecy (PFS) | Not selected |

The New Connection Wizard also uses the following system delivered default values to create policies and connections. Refer to 10.5.3, “Changing the New Connection Wizard default values” on page 204 on how these default values can be changed.

Table 37. OS/400 - system delivered default values used by New Connection Wizard

| Field | Value |
|--|--------------------------------------|
| IP security level | Highest security, lowest performance |
| Use identity protection (ISAKMP main mode) when negotiating key policies | Not selected |
| Diffie-Hellman Perfect Forward Secrecy (PFS) when protecting data | Not selected |
| Key Management | |
| - Maximum key lifetime | 60 minutes |
| - Maximum size limit | No size limit |
| Key expiration | |
| - Expire after | 1440 minutes |
| - Expire at size limit | No size limit |
| Connection lifetime | Never expires |

Finally, a plan should be developed for implementing the VPN connection that includes information such as source and destination IP addresses (or some other means to identify the communicating systems), a mutually agreed upon pre-shared key, authentication and encryption strategy, and various other factors.

Based on this plan, complete the New Connection Wizard planning worksheet (Table 38) from the perspective of the local AS/400 VPN partner:

Table 38. OS/400 - New Connection Wizard planning worksheet

| This is the information needed to create VPN with the New Connection Wizard | 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 | |
| What is the name of the connection group? | |
| 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 | |
| How is the local VPN server identified? | |
| What is the local VPN server's identifier? | |
| How is the remote VPN server identified? | |
| What is the remote VPN server's identifier? | |
| What is the pre-shared key? | |
| 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 | |

10.4.0.3 IP filtering planning worksheet

In IP filtering planning, it is important to consider the existing network connections and to understand the impact of introducing the new filter rules required for VPN connections. Improper planning may result in connection failures when IP filtering is activated.

Whenever any filter rules are added for an AS/400 line description, the system automatically adds a default DENY ALL for that line. This means that any traffic not explicitly permitted will be denied. This rule cannot be seen nor changed. From a security viewpoint, default DENY is a sound policy, particularly if the AS/400 is directly connected to the Internet. In the worst case, access may be accidentally denied on the line that is used for AS/400 Operations Navigator, preventing its use to turn off IP filtering. To fix this problem, use the `RMVTCPTBL *ALL` command from a green screen to deactivate all filter rules.

Other filter rules implicitly defined by the AS/400 system include AH, ESP and inbound IKE (UDP port 500) traffic between the VPN partners.

When either of the VPN partners is a gateway, defined addresses must be created for subnets that are allowed to use the VPN gateway.

The IP filter rules planning worksheet (Table 39) must be completed from the perspective of the local AS/400 system. In the example worksheet in Table 39, the filter rules allow VPN traffic between the local AS/400 system and the remote VPN partner. Non-VPN traffic from other systems in the 192.168.100.0 subnet is also permitted. A filter set name, VPNIFC, groups all the rules together and applies them to an interface. The interface is TOKENRING2; this is the token-ring line description used to connect out to the 192.168.100.0 network. When these filter rules were activated, they allowed the VPN host-to-host traffic from the remote VPN partner as well as general traffic from other systems in the 192.168.100.0 subnet through TOKENRING2.

Table 39. OS/400 - 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/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 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 address(es)? Use this name as the <i>source address</i> on IPSEC filter | Not applicable |
| If the remote 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 address(es)? Use this name as the <i>destination address</i> on 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 for the <i>source address</i> on 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 for the <i>destination address</i> on IPSEC filter if the remote server is acting as a host | 192.168.101.100 |
| What is the name of the interface (for example, the token-ring or Ethernet line) to which these filters will be applied? | TOKENRING2 |

| 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. | host |
| Is the remote 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? | Not applicable |
| What is the name for these address(es)? Use this name as the <i>source address</i> on IPSEC filter | |
| If the remote 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? | Not applicable |
| What is the name for these address(es)? Use this name as the <i>destination address</i> on IPSEC filter | |
| 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> . | General traffic from the 192.168.100.0 subnet |

10.5 VPN configuration

The AS/400 Operations Navigator is used as a starting point to create VPN configurations.

10.5.1 AS/400 Operations Navigator

As mentioned in 10.5.1, "AS/400 Operations Navigator" on page 199, AS/400 Operations Navigator's Network component provides the Virtual Private Networking Configuration GUI for you to configure and manage VPN connections.

This section described the AS/400 V4R4 implementation of VPN.

The basic objects required to define a VPN connection are:

- Key policies
- Data policies
- Key connection groups
- Data connections

The common components that are independent of the connection type are:

- Key policies

- Data policies
- Key connection groups

10.5.1.1 Key policies

- Can be used by multiple key connection groups
- Govern IKE Phase 1 negotiations
- A key policy contains a single key protection proposal that is offered to the remote VPN key server
- A proposal, in turn, is a collection of transforms that defines how to use the IKE protocol
- Phase 1 transforms include:
 - Authentication method
 - Is used to identify a message sender
 - Pre-shared key is the only authentication method available in OS/400 V4R4
 - Digital certification will be available as an authentication method in a future release of OS/400
 - Hash algorithm
 - Converts variable length input data into fixed length output data, or a hash
 - MD5 and SHA are supported
 - Encryption algorithm
 - Is an algorithm that scrambles data to make it unreadable to someone who intercepts it
 - DES-CBC and 3DES-CBC are supported
 - Diffie-Hellman group
 - Defines the characteristics of how key information is derived
 - Default 768-bit MODP(Group1) and Default 1024-bit MODP(Group 2) are supported
 - Key management
 - Specifies how long your protection suite remains valid
 - If the AS/400 system is the VPN connection initiator, the key management values are proposed to the remote key server
 - If the AS/400 system is the VPN connection responder, it accepts and uses the lower of these values
 - The values that can be defined are maximum key lifetime and maximum size limit
 - Maximum key lifetime specifies the length of time your protection suite remains valid
 - Maximum size limit specifies the amount of IKE Phase 2 traffic that is allowed to use the current protection suite
 - The AS/400 system AS/400 system reinitiates IKE Phase 1 negotiations when it reaches 75% of the key management values in order to establish a new protection suite before the current one expires
- Other fields that can be defined in the key policies include:
 - Initiator negotiation
 - Specifies if identity protection is used to encrypt identities during the negotiation of key policies
 - If identity protection is selected, then IKE main mode negotiation is used
 - If identity protection is not selected, then IKE aggressive mode is used
 - Aggressive mode negotiation is faster than main mode negotiation because aggressive mode negotiation does not encrypt identities
 - Responder negotiation

- Specifies the level of identity protection the AS/400 system requires of the remote VPN key server that initiates a connection
- Possible values are *require identity protection*, *allow identity protection* and *do not allow identity protection*
- *Require identity protection* specifies that the AS/400 system can only establish a connection if the remote VPN key server requests main mode negotiation
- *Allow identity protection* specifies that the AS/400 system can establish a connection regardless of whether the remote VPN key server requests main mode or aggressive mode negotiation
- *Do not allow identity protection* specifies that the AS/400 system can establish a connection only if the remote VPN key server requests aggressive mode negotiation

10.5.1.2 Data policies

- Can be used by multiple key connection groups
- Governs IKE Phase 2 negotiations
- Define how your data is protected
- Allows the selection of Diffie-Hellman perfect forward secrecy to prevent someone who intercepts your key from deducing future keys based on the intercepted key. If Diffie-Hellman perfect forward secrecy is selected, a Diffie-Hellman group must be specified to define the characteristics of how the AS/400 system derives its key information. The possible values are *default 768-bit MODP* (Diffie-Hellman Group 1) and *default 1024-bit MODP* (Diffie-Hellman Group 2).
- A data policy contains one or more data protection proposals
- A data protection proposal is a collection of data protection transforms
- A data protection transform is a collection of protocols
- A protocol, in turn, is a collection of ports
- A data policy can have more than one data protection proposal

10.5.2 Using the New Connection Wizard

To start the New Connection Wizard perform the following steps:

1. Activate AS/400 Operations Navigator for your AS/400.
2. Sign on when prompted.
3. Expand **Network**.
4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking.
5. Double-click **Virtual Private Networking** to start the VPN configuration GUI interface.
6. Click **File** from the menu bar.
7. Select **New Connection**.
8. Select, for example, **Gateway to Gateway**, from the pull-down menu. This starts the New Connection Wizard for a gateway-to-gateway connection.

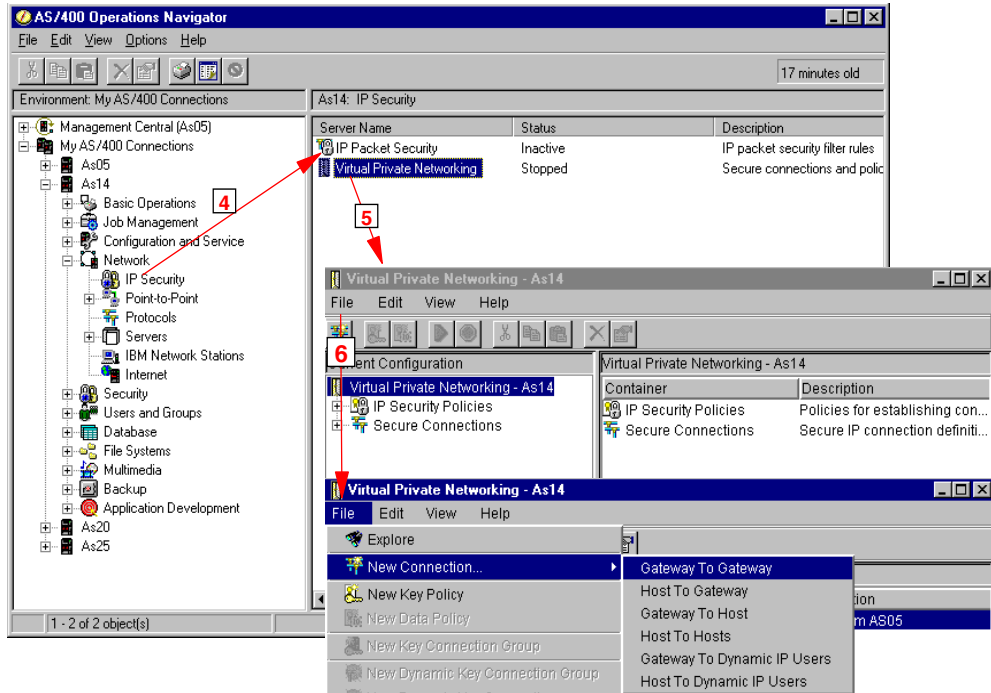


Figure 127. OS/400 - Starting the New Connection Wizard

Figure 128 shows the New Connection Wizard welcome window:

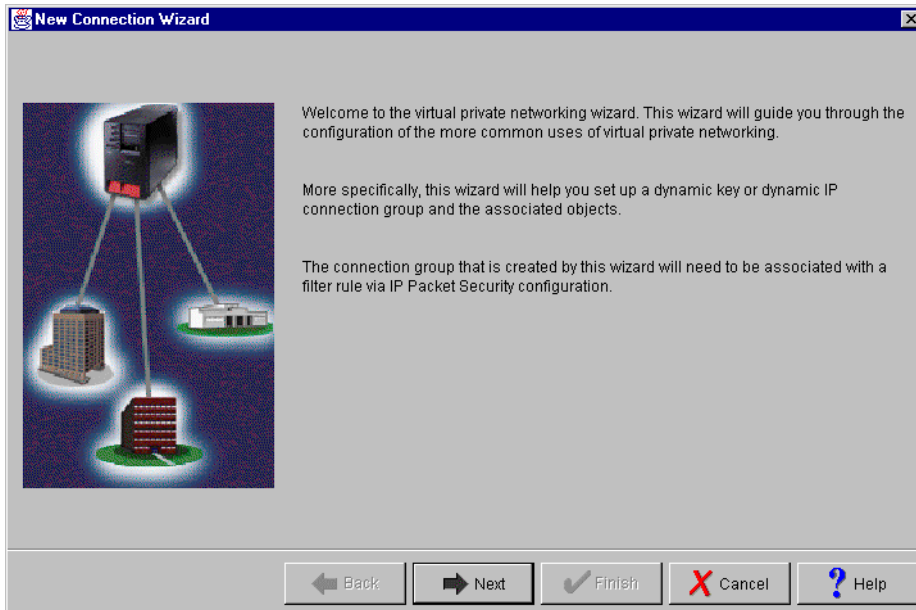


Figure 128. OS/400 - New Connection Wizard welcome window

The wizard prompts for parameters as detailed in Table 38 on page 197. The last window presented by the New Connection Wizard shows the parameters as entered by the user for final confirmation before the relevant VPN configuration objects are created.

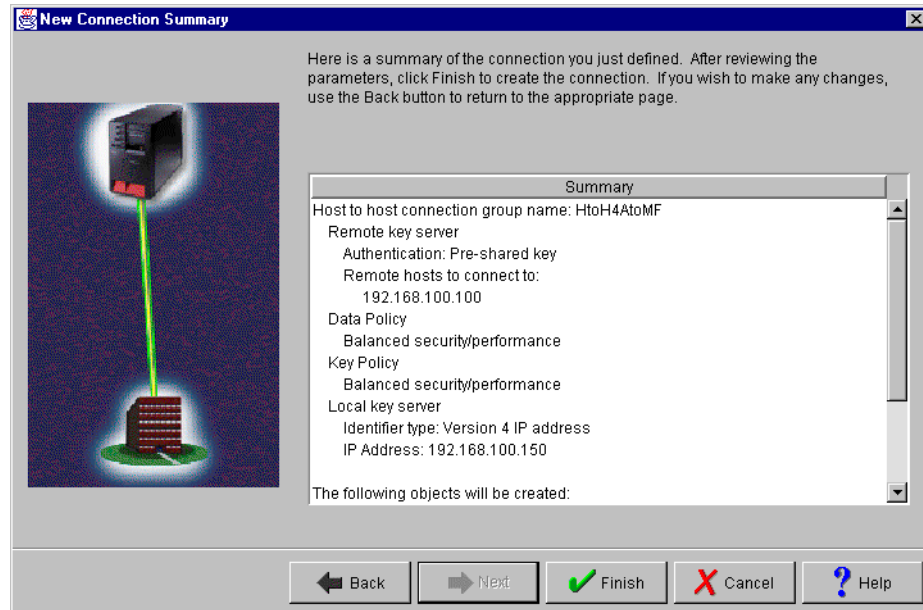


Figure 129. OS/400 - Wizard, parameters summary

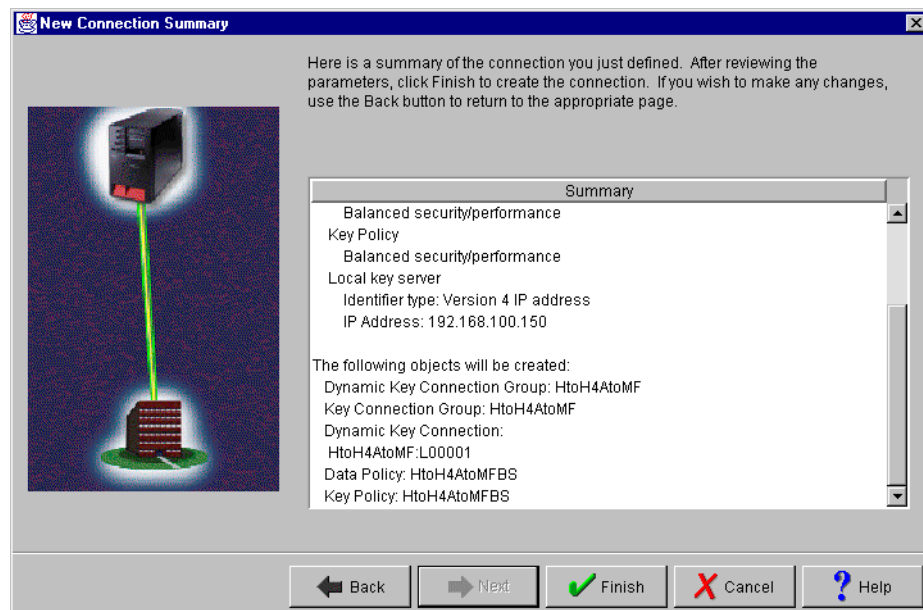


Figure 130. OS/400 - Wizard, objects to be created

For the VPN connections that cannot be created by the New Connection Wizard, refer to the relevant sections in this redbook.

Filter rules must then be manually created to allow the VPN traffic into and out of the network.

10.5.3 Changing the New Connection Wizard default values

The New Connection Wizard uses a few default values (refer to Table 37 on page 196) when creating policies and connections. These default values can be changed by following these steps:

1. Activate AS/400 Operations Navigator for your AS/400.
2. Sign on when prompted.
3. Expand **Network**.
4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking.
5. Double-click **Virtual Private Networking** to start the VPN configuration GUI interface.
6. From the menu bar, click **Edit -> Defaults**.

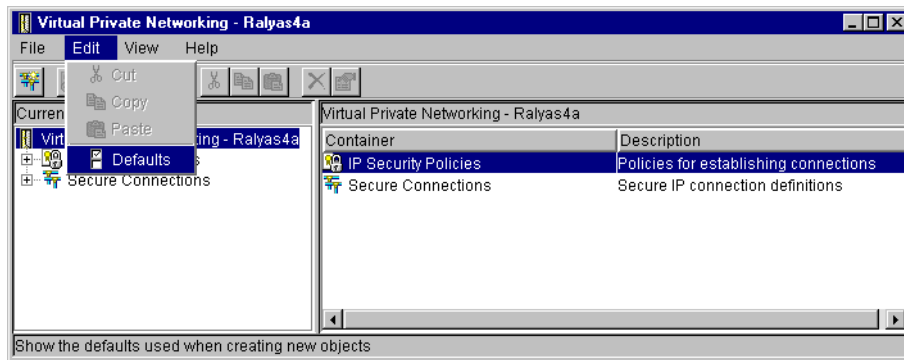


Figure 131. OS/400 - Initiating Virtual Private Networking defaults

7. At the Virtual Private Networking Defaults window, select the relevant page to change the New Connection Wizard default values.

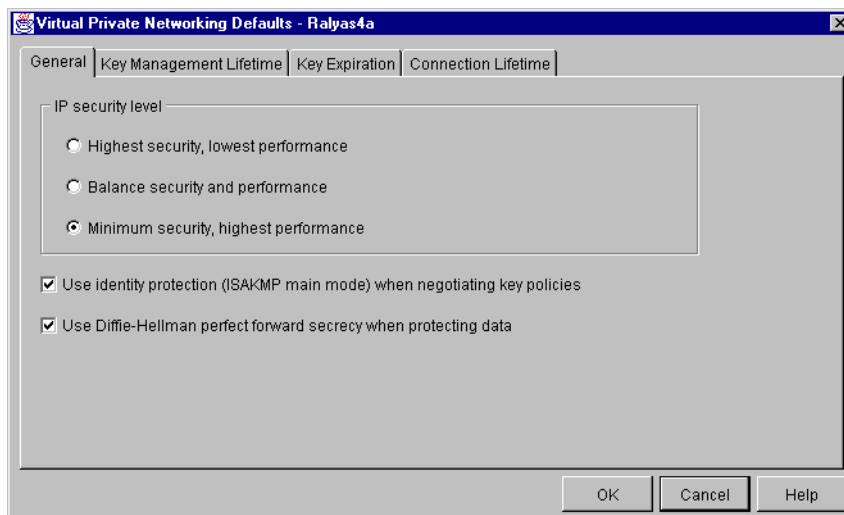


Figure 132. OS/400 - Virtual Private Networking Defaults window

10.5.4 Objects created by the wizard

Figure 133 shows a summary of objects created by the New Connection Wizard:

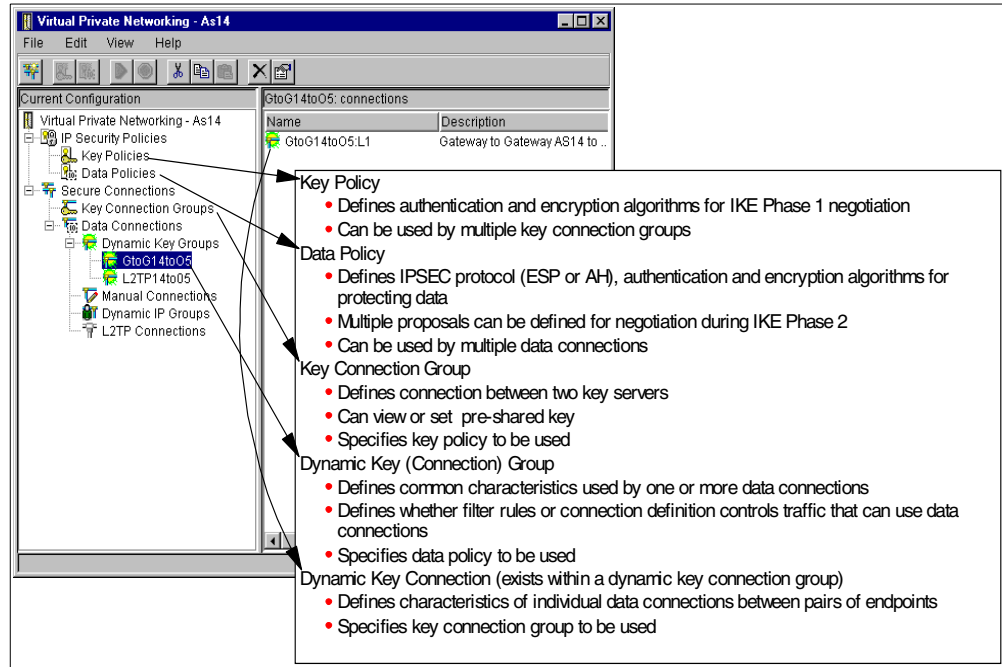


Figure 133. OS/400 - Summary of object created by wizard

10.5.5 Configuring IP filters

IP filters must be added for VPN connections (refer to Table 39 on page 198).

10.5.5.1 Checking the existing IP filter rules file

Before creating the IP filter rules needed for a new VPN connection, check if IP packet security is already configured on the AS/400 system. The IP filters for the new VPN connection must be merged into the existing IP filter rules file.

There is no means of determining the previously active IP filter rules file after IP packet security is deactivated. IP packet security must be deactivated before it can be configured.

If IP packet security is already configured and active on the AS/400 system, follow these steps to confirm the name of the active IP filter rules file before deactivating IP packet security.

1. Activate AS/400 Operations Navigator for your AS/400.
2. Sign on when prompted.
3. Expand **Network**.
4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking.
5. Double-click **IP Packet Security**.
6. The full IFS directory path of the active IP filter rules file is displayed at the top of the left panel of the IP Packet Security window. In the example in Figure 134, the active IP filter rules file is \QIBM\VPNRB\HTOH_ASTOMF.I3P.

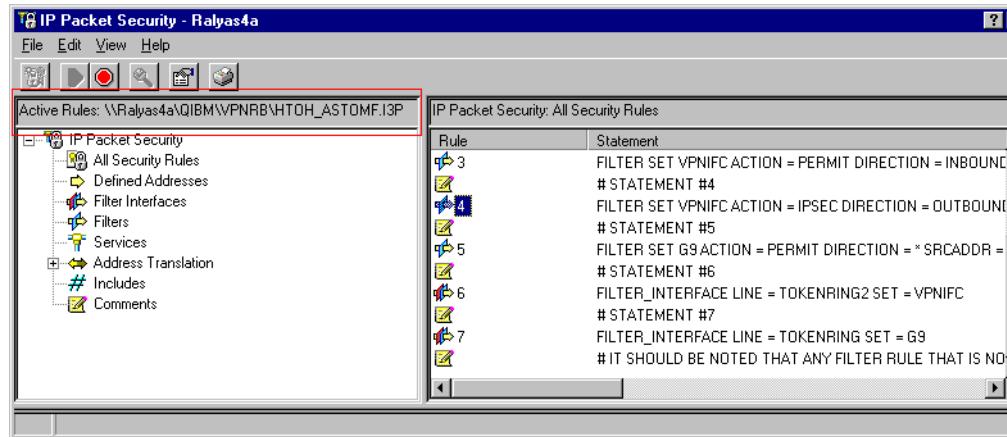


Figure 134. OS/400 - IP Packet Security window

10.5.5.2 Merging IP filter rules

Place *all* the IKE negotiation filter rule pairs ahead of the IPSec filter rules. When an outbound IPSec filter rule is created, OS/400 implicitly adds an inbound IPSec filter rule. Careful planning is required when merging VPN-related IP filter rules with other non-VPN-related IP filter rules. Placing rules wrongly can cause problems.

10.5.5.3 Automatically starting IP packet security at IPL

If IP packet filtering is active when the AS/400 system is shut down, IP packet filtering will automatically restart at the next IPL with the same IP filter rules file that was in use prior to the shutdown. There is no other method available to automatically start IP packet security at IPL.

10.5.6 Object relationships

Object relationships summarizes the type of information held in each configuration object and its relationships. The objects above the dotted line can be customized through the AS/400 Operations Navigator Virtual Private Networking configuration GUI. The objects below this line can be customized through the AS/400 Operations Navigator IP Packet Security configuration GUI. See Figure 135 on page 207.

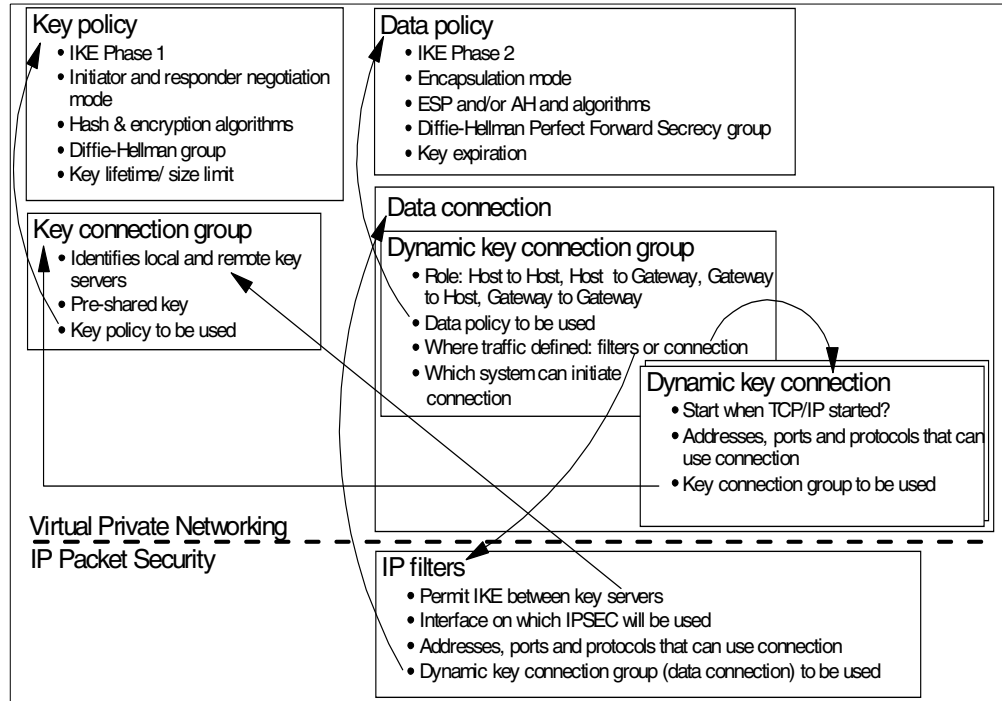


Figure 135. OS/400 - Object relationships for dynamic key connections

10.6 VPN management

VPN connections are managed using the AS/400 Operations Navigator. The following sections describe how to manage VPN connections.

10.6.1 IP packet security

In the following sections we describe tasks related to managing IP packet security. IP packet security must be activated before VPN connections can be established.

10.6.1.1 Checking IP packet security status

AS/400 Operations Navigator can also be used to check IP packet security status by following these steps:

1. Activate AS/400 Operations Navigator for your AS/400.
2. Sign on when prompted.
3. Expand **Network**.
4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking.
5. The status of the IP Packet Security server should be active before attempting to start VPN connections.

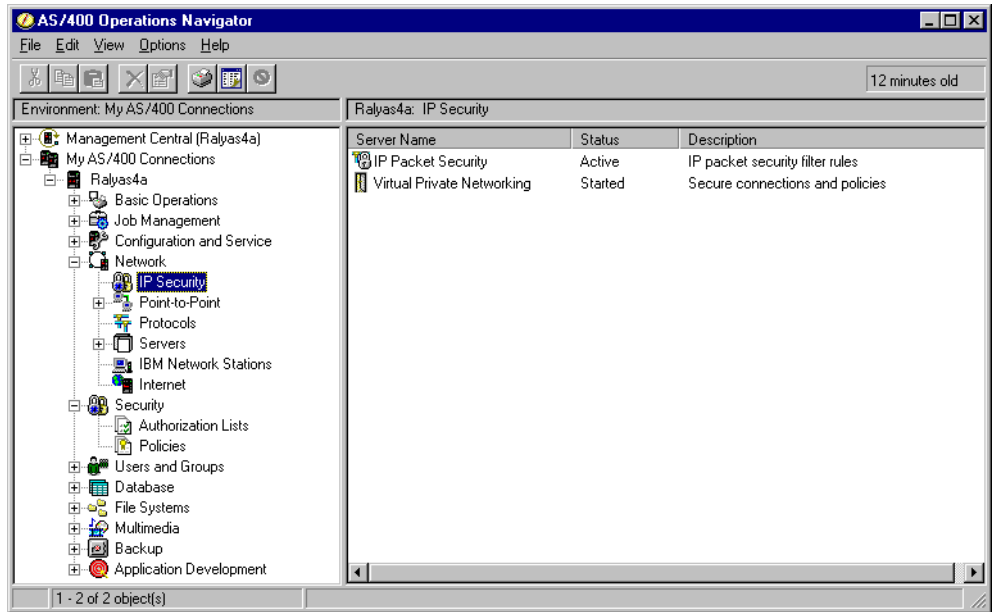


Figure 136. OS/400 - IP security servers' status

10.6.1.2 Deactivating IP packet security

IP packet security cannot be ended if there are active VPN connections. However IP packet security can be ended if there are no active VPN connections but with VPN server jobs still active.

Note

As an added precaution for situations where the AS/400 system's VPN connection physical interface is connected directly to the Internet without firewall protection, disable that TCP/IP interface first by using the OS/400 command `ENDTCPIFC` before deactivating IP packet security.

Note

If an AS/400 TCP/IP interface that has VPN connections defined, is accidentally ended, the VPN connection may still appear to be active at the VPN active connections window. However, this is not true.

In order to restart the VPN connection, firstly restart the AS/400 TCP/IP interface by running the command `STRTCPIFC` and then restart the VPN connection again.

Perform the following steps to deactivate IP packet security. If you do not know the currently active IP packet filter rule's file name, remember to check for it (refer to 10.5.5.1, "Checking the existing IP filter rules file" on page 205) before deactivating IP packet security.

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

4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking.
5. Double-click **IP Packet Security**.
6. At the IP Packet Security window, click the red dot icon to deactivate IP packet security. (Refer to Figure 134 on page 206.)

10.6.1.3 Activating IP packet security

Perform the following steps to activate IP packet security:

1. Activate AS/400 Operations Navigator for your AS/400.
2. Sign on when prompted.
3. Expand **Network**.
4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking.
5. Double-click **IP Packet Security**.
6. At the IP Packet Security window menu bar, click **File -> Open**.
7. At the Open Rules File window, select the IP filters rule file to activate.
8. Back at the IP Packet Security window menu bar, click the green triangle icon to activate IP packet security.

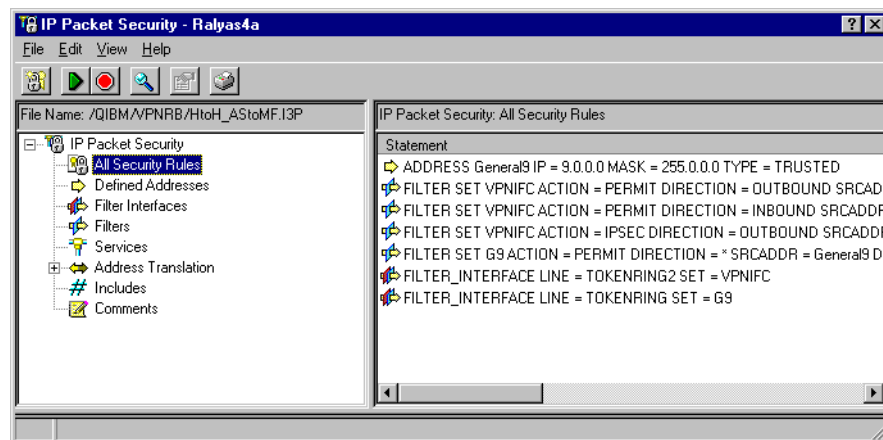


Figure 137. OS/400 - Activating IP packet security

10.6.2 VPN server jobs

The following sections describe tasks related to managing VPN server jobs. The VPN server jobs must be active before VPN connections can be established.

10.6.2.1 Checking VPN server jobs status

The VPN server jobs status can be checked by running the OS/400 command `WRKSBSJOB QSYSWRK` and making sure that the two jobs, QTOKVPNIKE and QTOVMAN, are active.

Alternatively, the AS/400 Operations Navigator can also be used by following these steps:

1. Activate AS/400 Operations Navigator for your AS/400.
2. Sign on when prompted.

3. Expand **Network**.
4. Click **IP Security** to reveal two server names: IP Packet Security and Virtual Private Networking.
5. If the status of the Virtual Private Networking server is Started, that means the VPN server jobs are active.

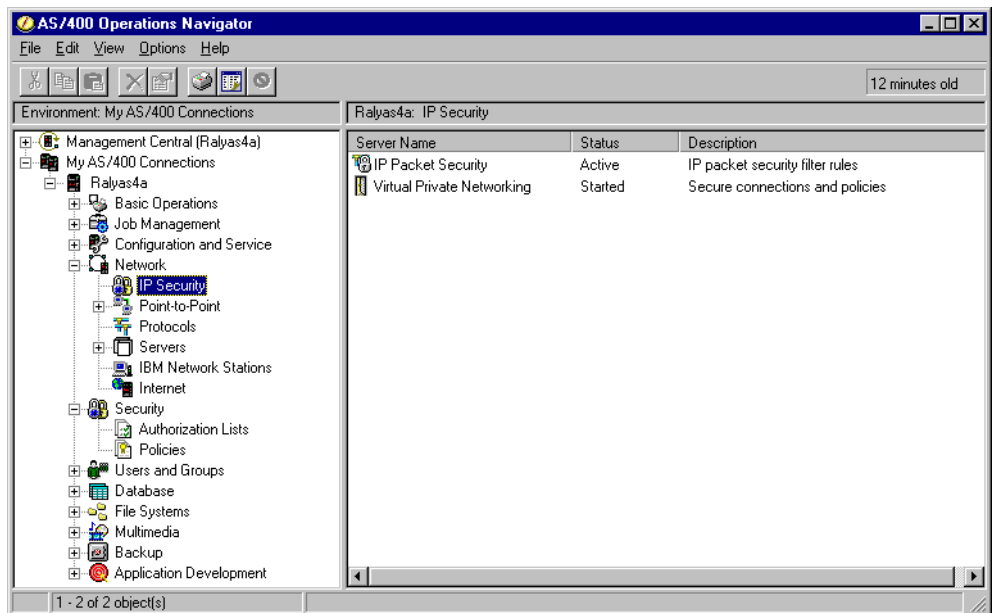


Figure 138. OS/400 - IP security server status

10.6.2.2 Manually starting the VPN server jobs

The VPN server jobs can be started by either running the OS/400 command `STRTCPSVR *VPN` or AS/400 Operations Navigator:

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

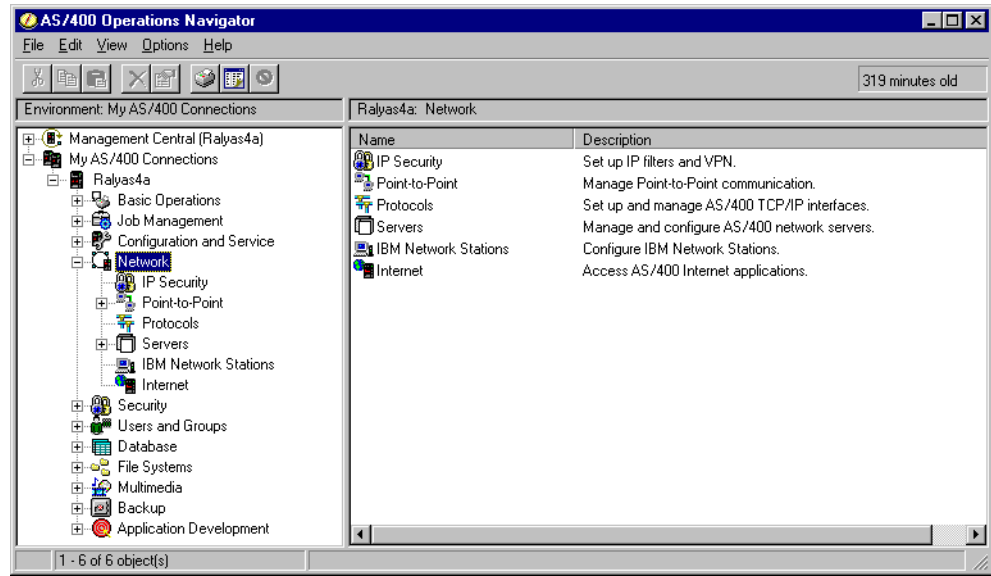


Figure 139. OS/400 - expanding network

4. Click **IP Security** to reveal two server names in the right panel: IP Packet Security and Virtual Private Networking.

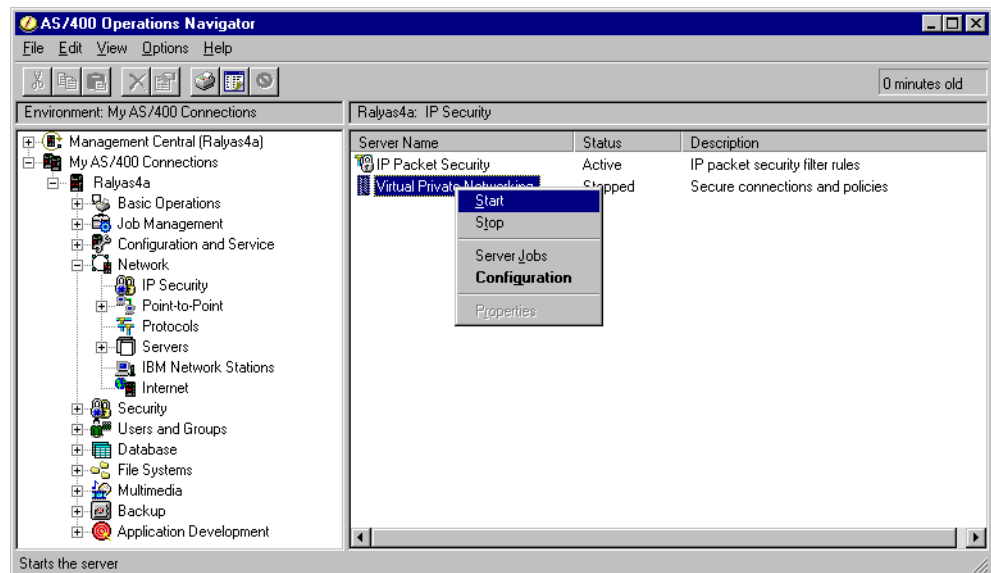


Figure 140. OS/400 - Starting the VPN jobs manually

5. Right-click **Virtual Private Networking**.
6. Click **Start**.

10.6.2.3 Automatically starting VPN server jobs at IPL

The VPN server jobs can be configured to automatically start at IPL by performing the following steps using AS/400 Operations Navigator. There are no green screen commands available for this.

1. Start AS/400 Operations Navigator from the desktop.

2. Click **Network -> Protocols -> TCP/IP**.
3. Select the **Servers to Start** tab and enable **Virtual private networking**. See Figure 141.
4. Click **OK**.

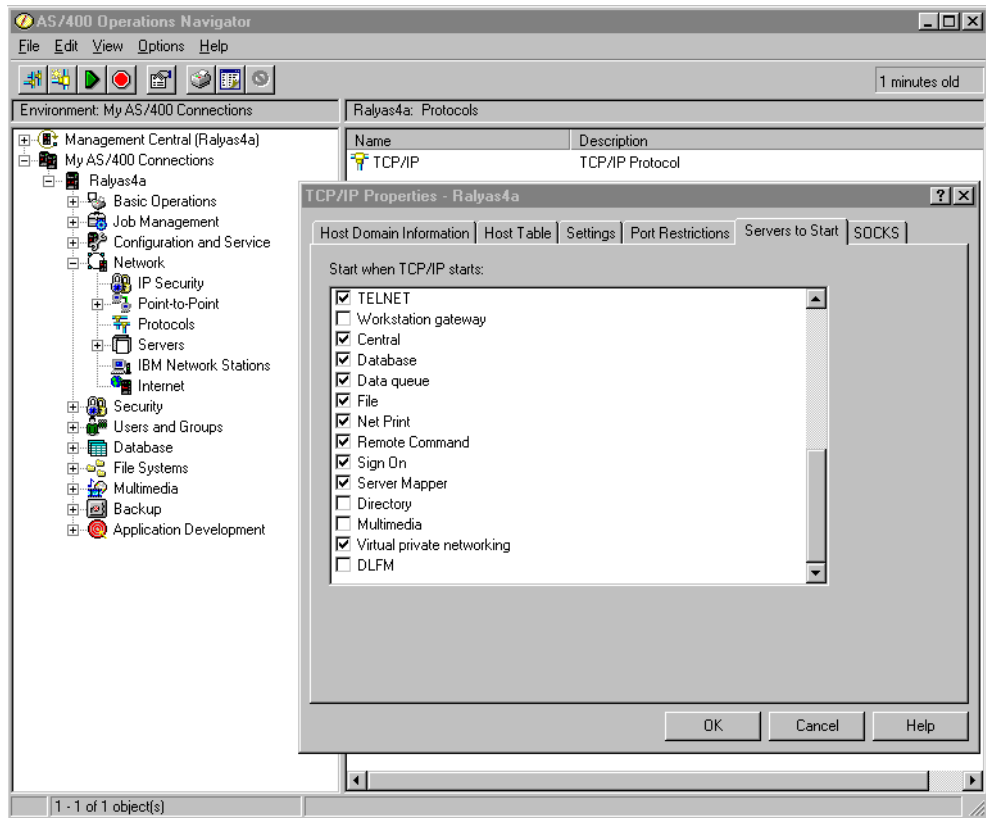


Figure 141. OS/400 - Automatically starting VPN server jobs at IPL

10.6.2.4 Manually ending VPN server jobs

The VPN server jobs can be ended even if there are active VPN connections. Precautions should be taken to prevent accidentally disrupting VPN connections that are still in use.

The VPN server jobs can be ended by either running the OS/400 command `ENDTCPSVR *VPN` or AS/400 Operations Navigator. To stop the VPN server jobs using Operations Navigator, perform steps 1 through 5 of 10.6.2.2, “Manually starting the VPN server jobs” on page 210. For step 6, click **Stop** instead.

10.6.3 Starting VPN connections

VPN connections can be started in the following ways.

10.6.3.1 Manually starting dynamic key connections

Make sure that the remote VPN partner is ready to accept VPN connection requests before performing these steps:

1. Start AS/400 Operations Navigator from the desktop.

2. Expand the AS/400 system, for example, **RALYAS4A**. Sign on when prompted.
3. Expand **Network**.

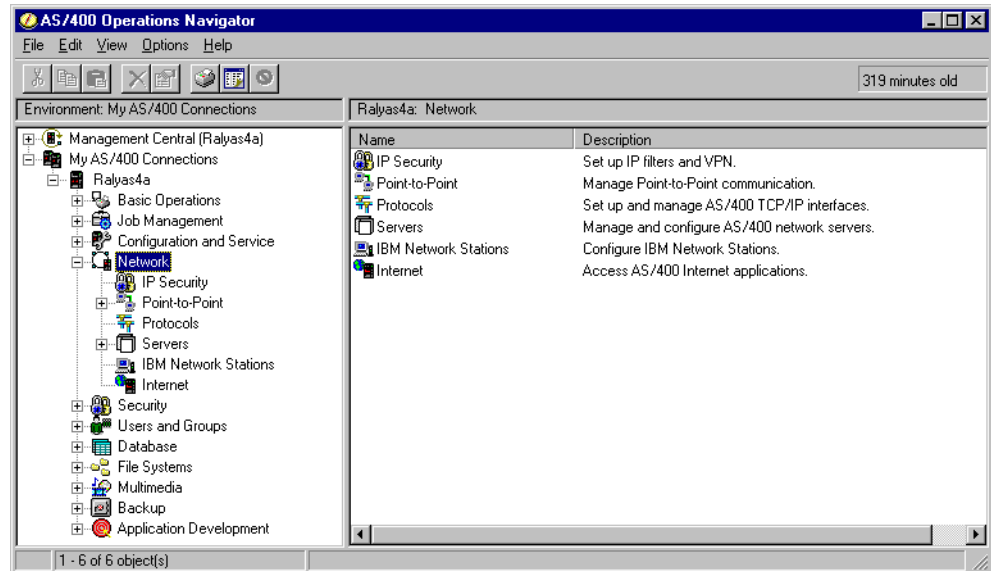


Figure 142. OS/400 - expanding network

4. Click **IP Security** to reveal two server names in the right panel: IP Packet Security and Virtual Private Networking.

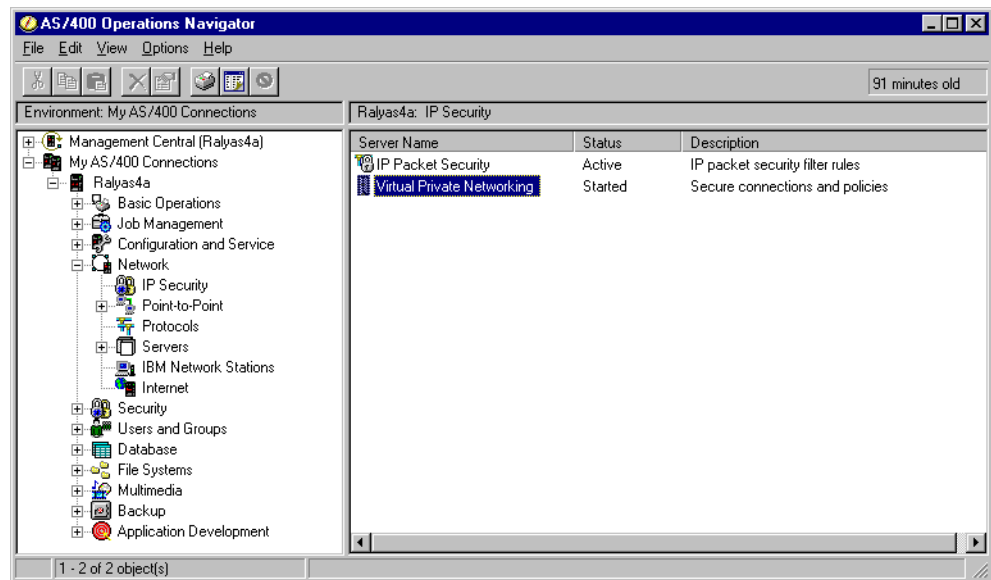


Figure 143. OS/400 - Starting the VPN configuration GUI

5. Double-click **Virtual Private Networking**.
6. Expand **Secure Connections**.
7. Expand **Data Connections**.
8. Expand **Dynamic Key Groups**.

9. Click the dynamic key group for the VPN connection that you wish to start.
10. Right-click the VPN connection you wish to start on the right panel.
11. Click the green triangle **Start** icon.

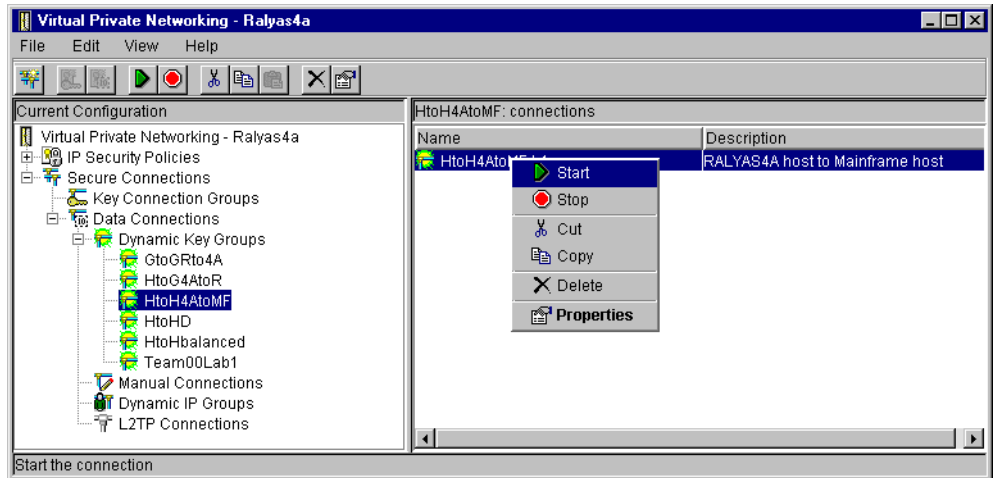


Figure 144. OS/400 - starting a dynamic key VPN connection

10.6.3.2 Automatically starting dynamic key connections

Dynamic key VPN connections can be started automatically when TCP/IP is started by performing the following steps:

1. Perform steps 1 to 10 in 10.6.3.1, “Manually starting dynamic key connections” on page 212.
2. Click **Properties** (refer to Figure 144).
3. Select **Start when TCP/IP is started**.

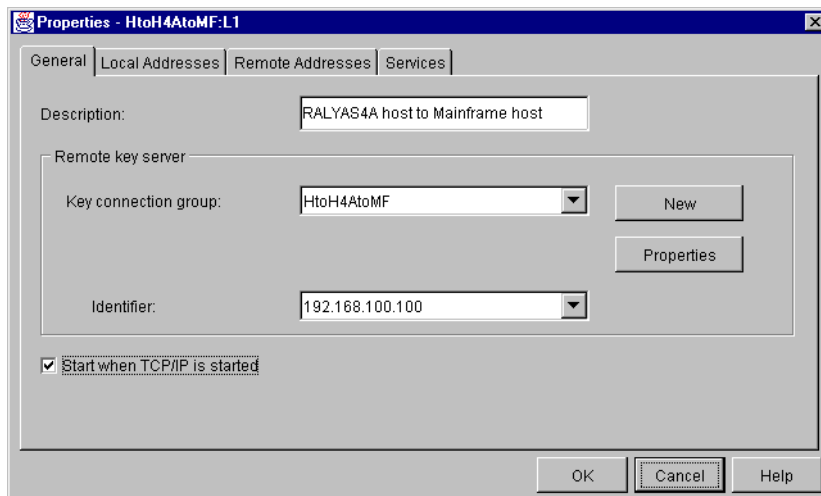


Figure 145. OS/400 - automatically starting a dynamic key connection

4. Click **OK**.

10.7 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 there are changes to the VPN configuration or IP packet filter configuration.

- Use the OS/400 `SAVOBJ` commands to back up the VPN configuration objects individually from the QUSRSYS library. Refer to Table 33 on page 191 for a list of the VPN configuration object.
Since the VPN configuration objects reside in the QUSRSYS library, they are also saved when a full system save is performed or by running the OS/400 commands `SAVLIB QUSRSYS`, `SAVLIB *NONSYS` or `SAVLIB *ALLUSR`.
- Use the `SAV` command to back up the filter rules file from the IFS.

10.7.1 Creating a VPN host-to-host connection

Virtual private networking, as implemented in V4R4, uses the IP Security Architecture (IPSec) to provide a secured connection between two IP-based entities. We will create a VPN to connect two hosts residing at two different locations, over the Internet. Using the configuration wizard is the easiest way to set up a host-to-host connection. Within the wizard, you provide the minimum information required to establish a VPN connection. Based on the configuration values provided, the wizard creates the required objects. In the case of a host-to-host connection the following objects are created:

- A key policy
- A data policy
- A key connection group
- A dynamic key connection group
- A dynamic key connection

For more information about the various configuration objects, refer to 10.7.4, “Relationship between the wizard and the configuration objects” on page 235.

Figure 146 on page 216 illustrates the network environment we use for this scenario. We will now configure a host-to-host connection between RALYAS4A and RALYAS4C using the IPSec protocol, Encapsulated Security Payload (ESP). Perform the following steps:

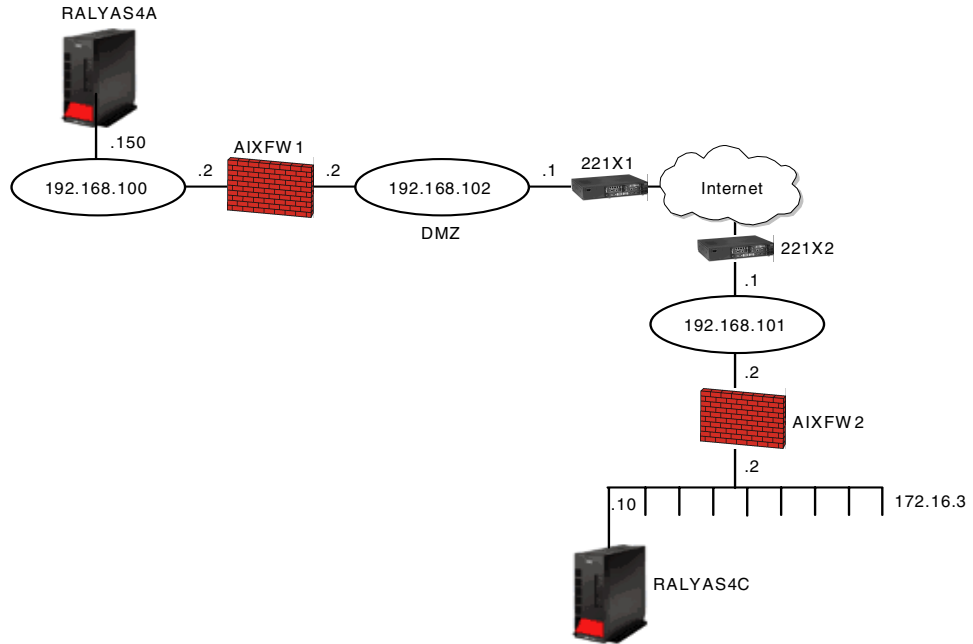


Figure 146. AS/400 - host-to-host connection

1. Start **AS/400 Operations Navigator** from your desktop.

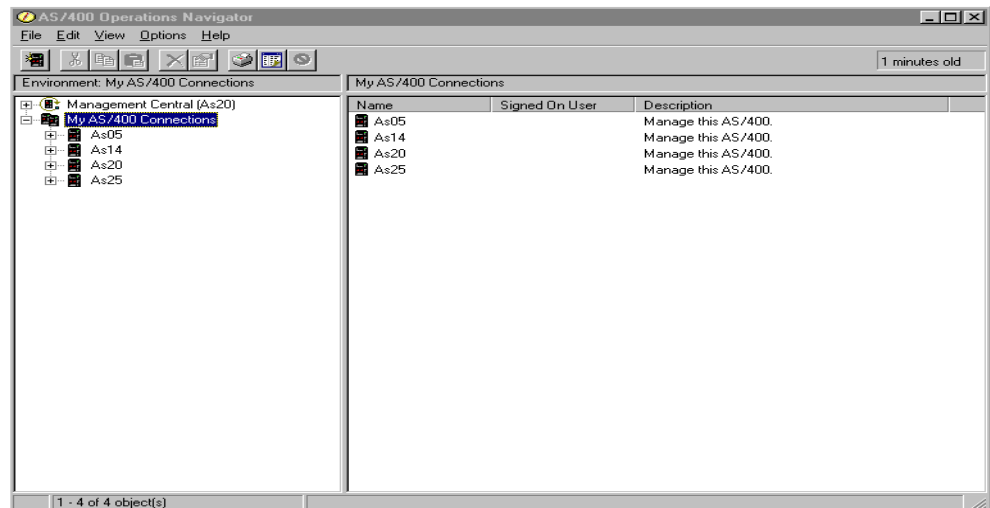


Figure 147. AS/400 - AS/400 Operations Navigator

2. Click the plus sign (+) next to the AS/400 connection. We will use (RALYAS4A) to expand AS/400 Operations Navigator. Sign on when prompted:

User name: **User ID**
 Password: **Password**

3. Expand **Network** and click **IP Security**.

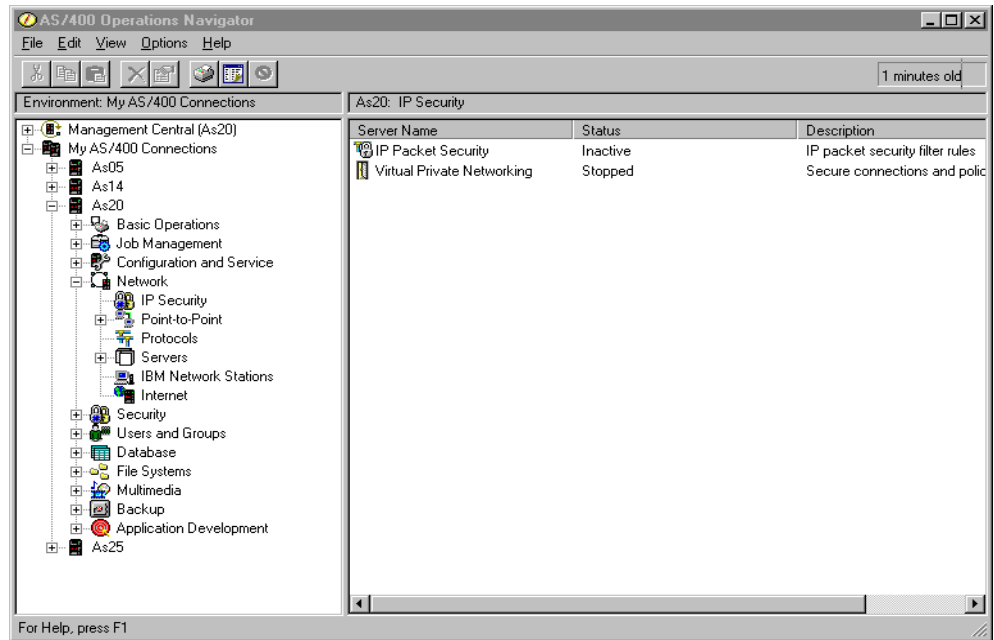


Figure 148. AS/400 - AS/400 Operations Navigator expanded to IP Security

4. Double-click **Virtual Private Networking**.

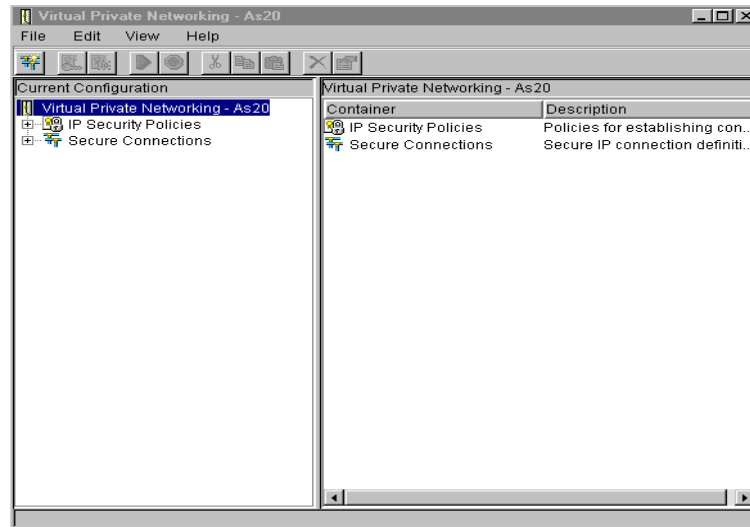


Figure 149. AS/400 - Virtual Private Networking

5. Select **File** from the main menu, and then select **New Connection**.

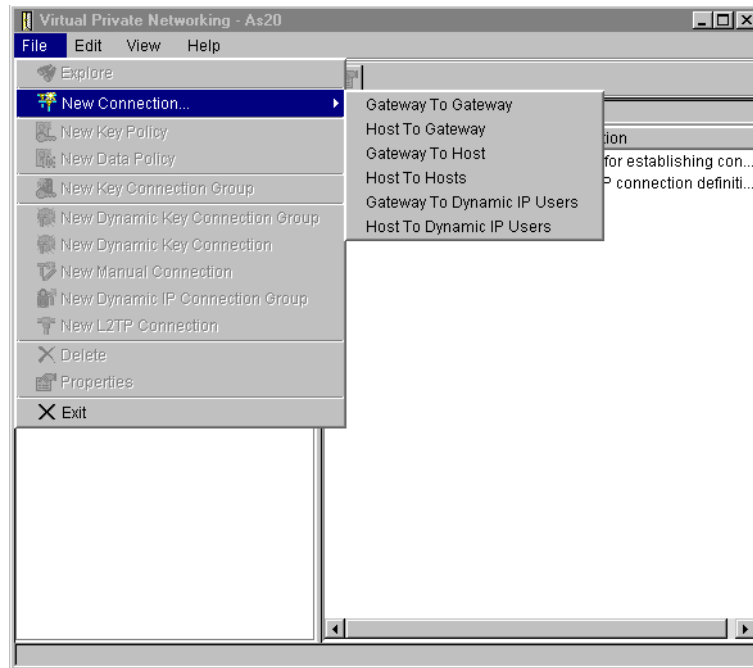


Figure 150. AS/400 - Selecting the New Connection Wizard

6. Select **Host To Hosts** from the drop-down menu.

This starts the *New Connection Wizard* for a host-to-host connection as shown in Figure 151 on page 219.

Note: The wizard can only configure dynamic key or dynamic IP connections. You must create a *manual* connection if, for example, you are connecting to a remote system that does not support the Internet Key Exchange (IKE) protocol.

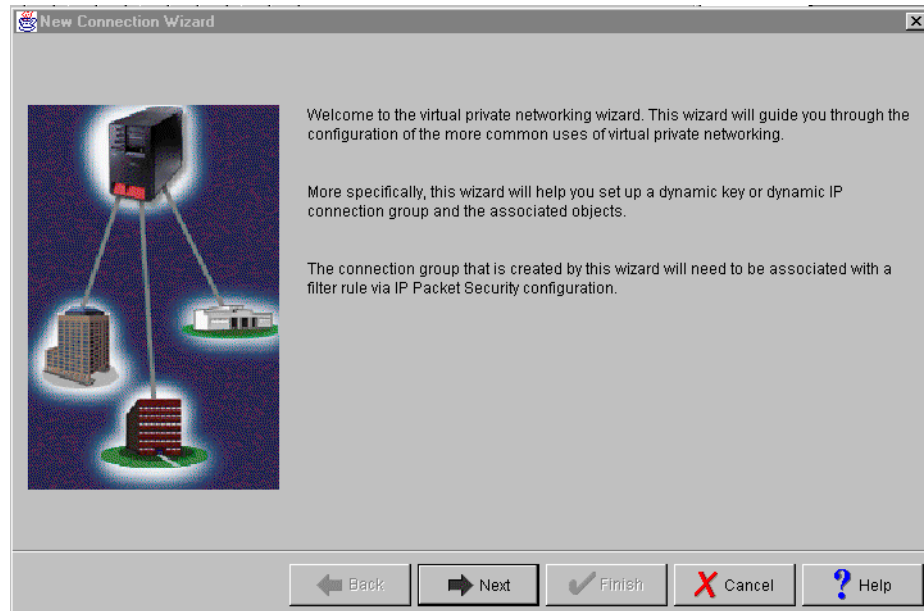


Figure 151. OS/400 - New Connection Wizard welcome window

7. Click **Next**.

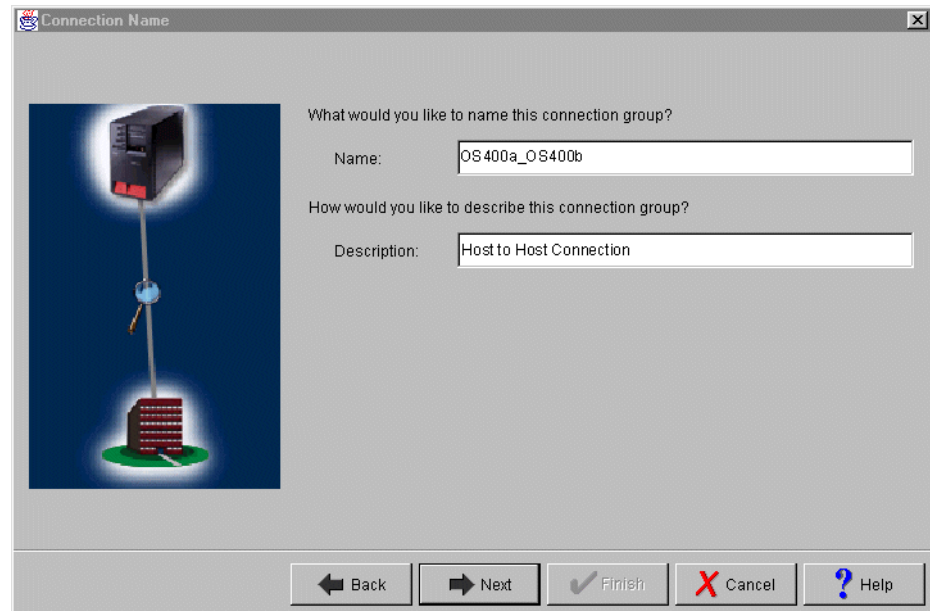


Figure 152. OS/400 - Connection Name Window

8. Enter the connection name and a description. The connection name is the name for all objects that the wizard creates for this particular connection:

Connection Name: RALYAS4A_RALYAS4C

Description: host-to-host Connection

9. Click **Next**.

Note

The *Name* field is case-sensitive. Be sure to enter the connection name exactly as shown above (RALYAS4A_RALYAS4C).

10. Click **Next**.

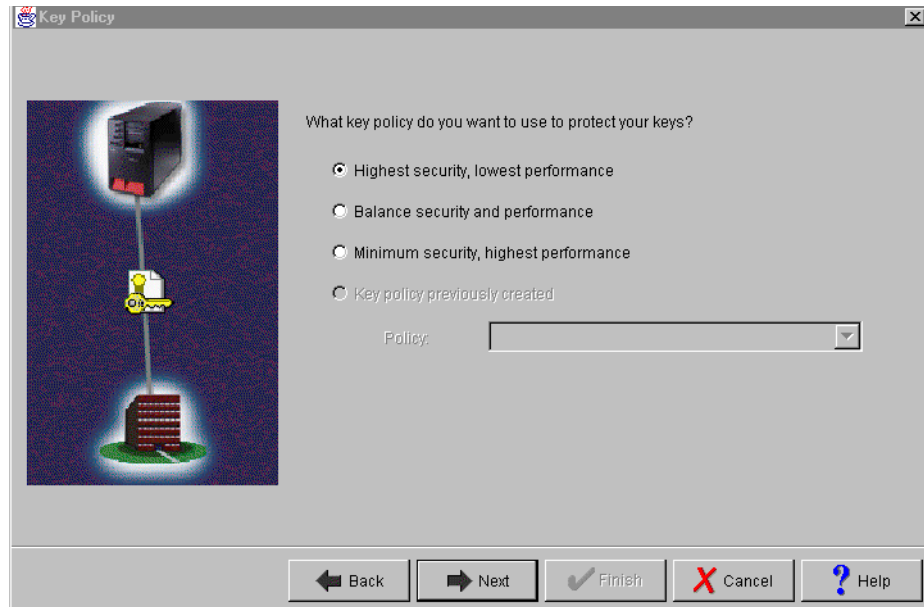


Figure 153. OS/400 - Key Policy selection window

11. Select **Highest security, lowest performance** on the Key Policy window.

The *Key Policy* specifies what level of protection IKE uses during Phase 1 negotiations. Based on the selection you make in the window shown in Figure 153, the wizard selects the appropriate authentication and encryption algorithms.

12. Click **Next**.

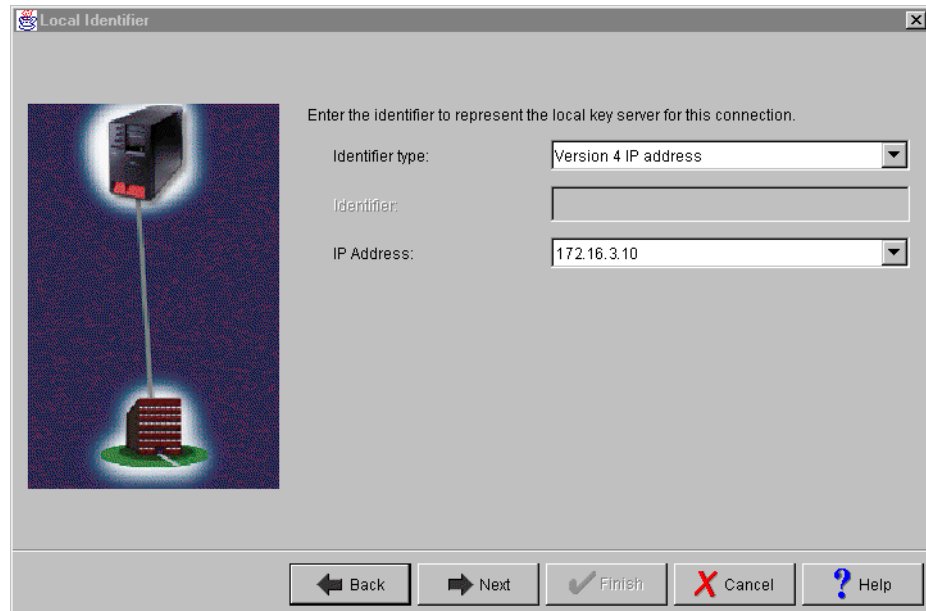


Figure 154. OS/400 - Local Identifier window

13. Select the Identifier type and IP address of the local key server.

Identifier type: **Version 4 IP address**

IP Address: **172.16.3.10**

14. Click **Next**.

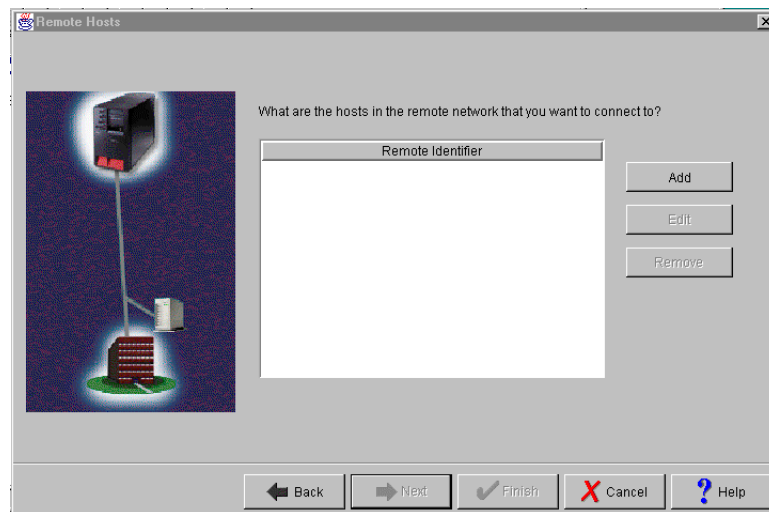


Figure 155. OS/400 - Remote Hosts

On the *Remote Hosts* window, you specify the hosts you want to communicate with over the VPN.

15. Click **Add** to add the remote host definitions.

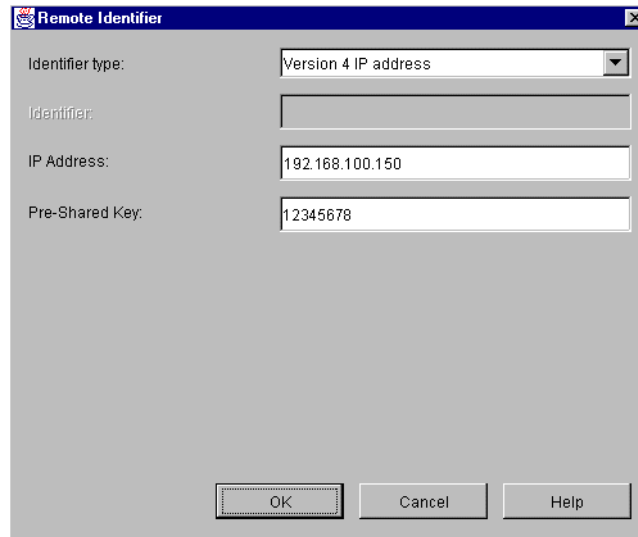


Figure 156. OS/400 - Remote Identifier

16. In the Remote Identifier window, you define the appropriate parameters for one particular remote system. Select the following values:

Identifier type: **Version 4 IP address**

IP Address: 192.168.100.150

Pre-Shared Key: 12345678

17. Click **OK**.

18. Click **Next**.

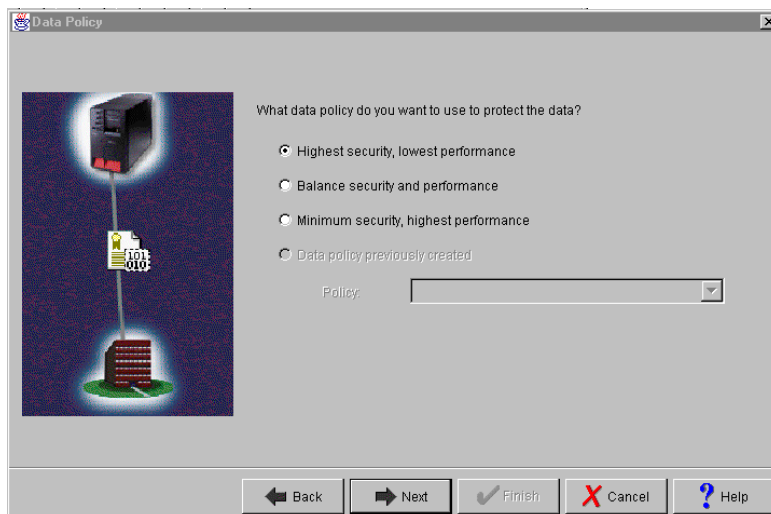


Figure 157. OS/400 - Data Policy

19.) Select **Highest security, lowest performance** on the Data Policy window.

Based on the selection you make on the Data Policy window, the wizard selects the appropriate encryption and authentication algorithms, and the IPsec protocol for the user data traffic.

20. Click **Next**.

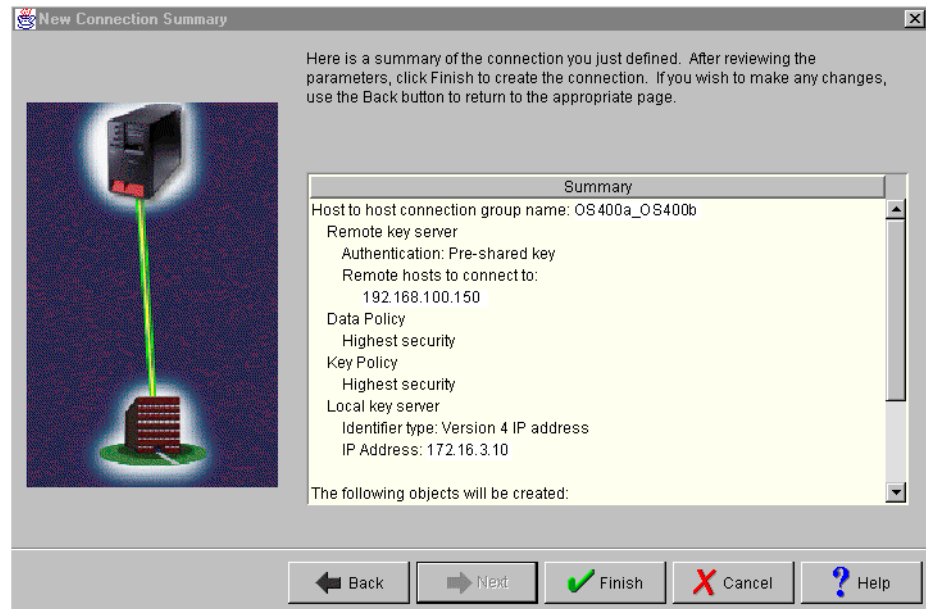


Figure 158. OS/400 - Wizard summary page

This window summarizes the selections you made during the wizard configuration. It also provides information about the objects the wizards creates when you click **Finish**.

21. Click **Finish**.

22. Select **File** from the main menu and then select **Exit** to close the Virtual Private Networking window.

10.7.2 Configuring IP packet security

You may have noticed that the configuration wizard explained that you also need to configure *IP Packet Filters* to allow VPN to work properly. The *IP Packet Filters* direct outbound traffic through the IP Security Architecture (IPSec) protocols and allow Internet Key Exchange (IKE) negotiations.

AS/400 introduced *IP Packet Filtering* in V4R3. When configuring *IP Packet Filters* you must 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.

You only need to configure the filter rules that are necessary to establish the VPN connection you configured in 10.7.1, “Creating a VPN host-to-host connection” on page 215.

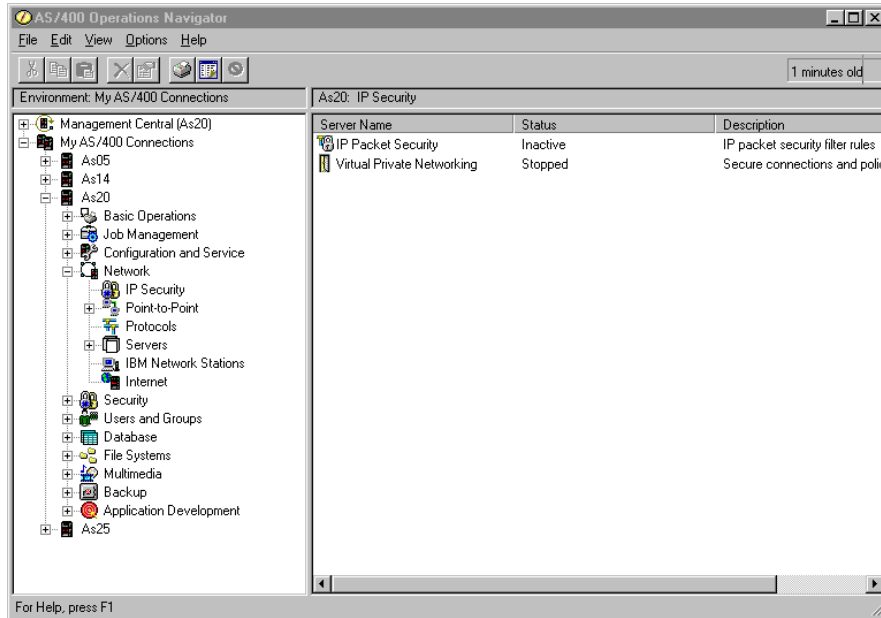


Figure 159. OS/400 - Operations Navigator IP security

1. Double-click **IP Packet Security**.

Note that *IP Packet Security* and *Virtual Private Networking* are still inactive or stopped.

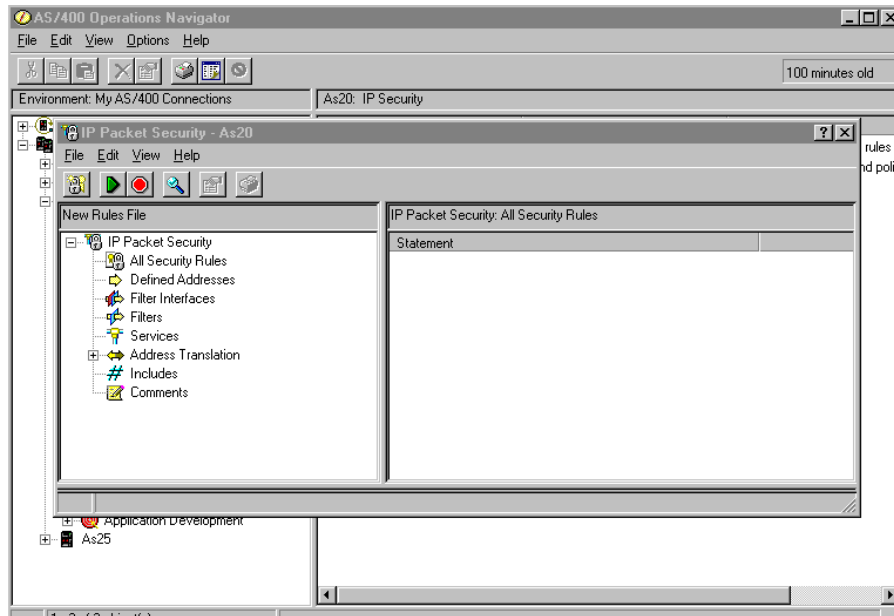


Figure 160. IP packet security initial window

2. Right-click **Filters**, and select **New Filter**.

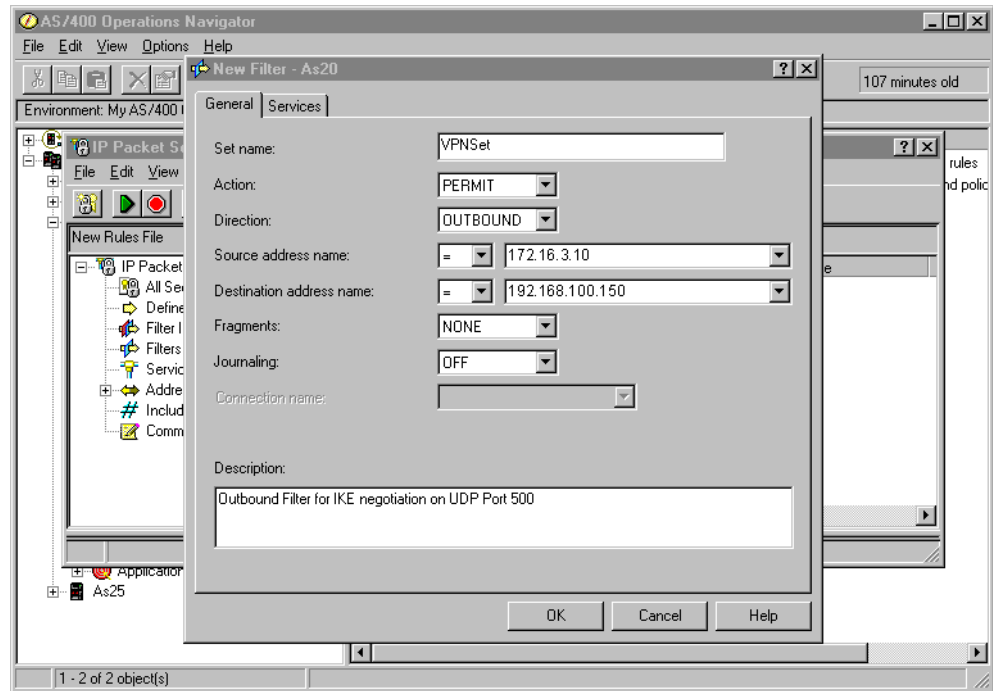


Figure 161. OS/400 - outbound filter rule for IKE General page

3. Complete the New Filter General page.

Table 40 shows you the fields for the outbound IKE filter rule and the values we used in our lab:

Table 40. OS/400 - values for outbound IKE filter rule

| Field | Value |
|--------------------------|---|
| General Page | |
| Set name | VPNSet |
| Action | PERMIT |
| Direction | OUTBOUND |
| Source address name | = 172.16.3.10 |
| Destination address name | = 192.168.100.150 |
| Fragments | NONE |
| Journaling | OFF |
| Description | Outbound Filter for IKE negotiation on UDP port 500 |
| Services Page | |
| Protocol | UDP |
| Source port | = 500 |
| Destination port | = 500 |

4. Click the **Services** tab.

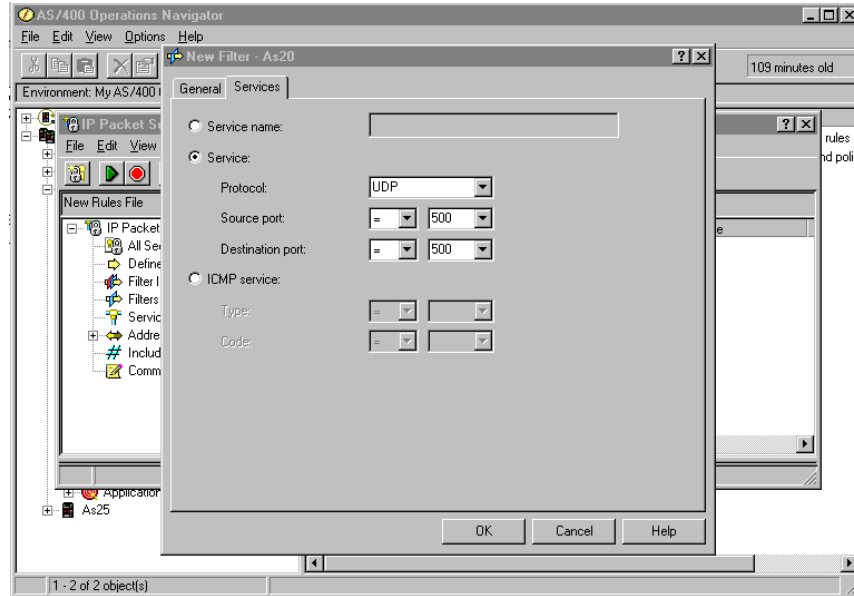


Figure 162. Outbound filter rule for IKE Services page

5. Complete the *New Filter Services* page based on the values provided in Table 40.

The UDP port 500 is reserved as a well-known port number for the Internet Key Exchange (IKE) protocol, which is the same port that is also used by the Internet Security Association Key Management Protocol (ISAKMP). Click **OK**.

6. Create the second filter rule by right-clicking **Filters** and selecting **New Filter**. The second filter rule is used for the IKE inbound traffic.

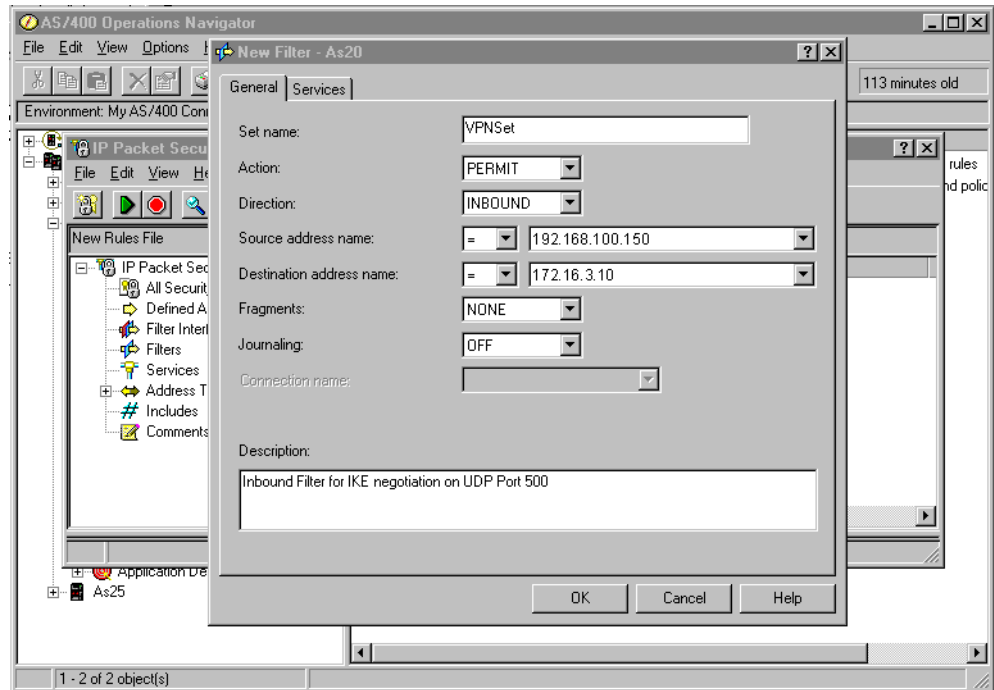


Figure 163. OS/400 - inbound filter rule for IKE General page

7. Complete the General page with the values shown in the following table:

Table 41. OS/400 - values for inbound IKE filter rule

| Field | Value |
|--------------------------|--|
| General Page | |
| Set name | VPNSet |
| Action | PERMIT |
| Direction | INBOUND |
| Source address name | = 192.168.100.150 |
| Destination address name | = 172.16.3.10 |
| Fragments | NONE |
| Journaling | OFF |
| Description | Inbound Filter for IKE negotiation on UDP port 500 |
| Services Page | |
| Protocol | UDP |
| Source port | = 500 |
| Destination port | = 500 |

8. Click the **Services** tab.
9. Complete the Services page for the inbound filter rule with the values shown in Table 41.

10. Click **OK**.

The inbound and outbound filter rules defined for UDP port 500 are used during the IKE negotiation process. We recommend that you define an explicit address pair for both ends of the VPN connection, as we did for this lab. 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 wildcard 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.

Tip

Place all the IKE negotiation filter rule pairs on top of the IPSEC filter rules. When you create an OUTBOUND IPSEC filter rule, OS/400 adds the implicit INBOUND IPSEC rule. Placing this rule wrongly causes problems. Any inbound filter should *always* be placed in front of the IPsec filters to avoid these problems.

11. 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. At the AS/400 system IP Packet Security window, right-click **Filters** and select **New Filter** to define the third and last filter used for the VPN connection. This filter is used for the data connection.

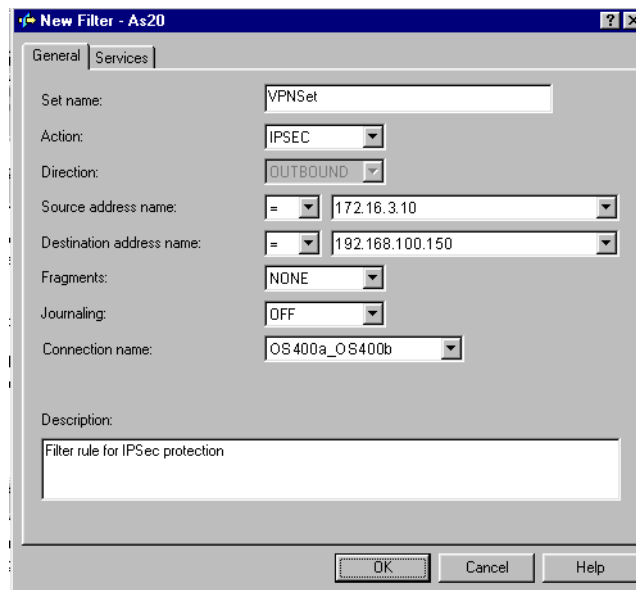


Figure 164. OS/400 - IPsec filter rule General page

Table 42 shows you the values used in the IPSec filter rule:

Table 42. OS/400 - values for IPSec filter rule

| Field | Value |
|--------------------------|---------------------------------------|
| General Page | |
| Set name | VPNSet |
| Action | IPSEC |
| Direction | OUTBOUND (grayed out) |
| Source address name | = 172.16.3.10 |
| Destination address name | = 192.168.100.150 |
| Fragments | NONE |
| Journaling | OFF |
| Connection name | RALYAS4A_RALYAS4C |
| Description | Filter rule for IPSec data protection |
| Services Page | |
| Protocol | * |
| Source port | = * |
| Destination port | = * |

12. Click the **Services** tab.

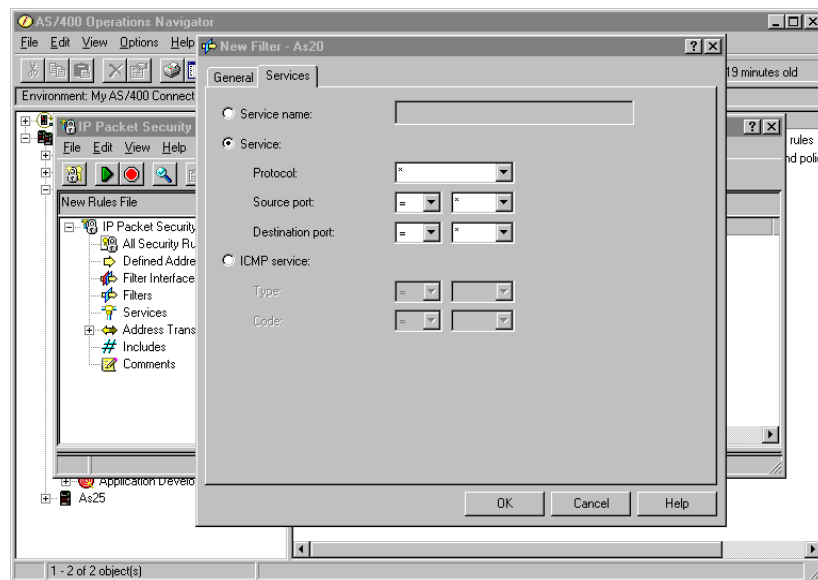


Figure 165. OS/400 - IPSec filter rule Services page

13. Complete the Services page with the values shown in Table 42 on page 229.

14. Click **OK**.

Note

You might be wondering why there is no filter rule specified for the secured inbound traffic. This is done implicitly by the AS/400 system.

10.7.3 Starting the VPN connection

After we configure the VPN connection and activate the filter rules, we can now start the VPN connection. By default, each host within the host-to-host configuration can initiate a VPN connection. The host that starts the connection request is known as the *initiator*. The host that answers the connection request is known as the *responder*. In a host-to-host connection, each host is both the connection endpoint and the data endpoint. The connection endpoint is responsible for authentication and encryption/decryption, while the data endpoint is the origin or destination of the data.

Important note

To establish a successful connection, you must start the VPN server prior to initiating or responding to a connection request. Since the server jobs exist only once on a system, the first team to finish the VPN configuration and that is ready to activate its connection, performs step 1.

If the virtual private networking servers are already started, go to step 2.

1. Right-click **Virtual Private Networking** and select **Start** to begin the VPN server jobs on the AS/400 system.

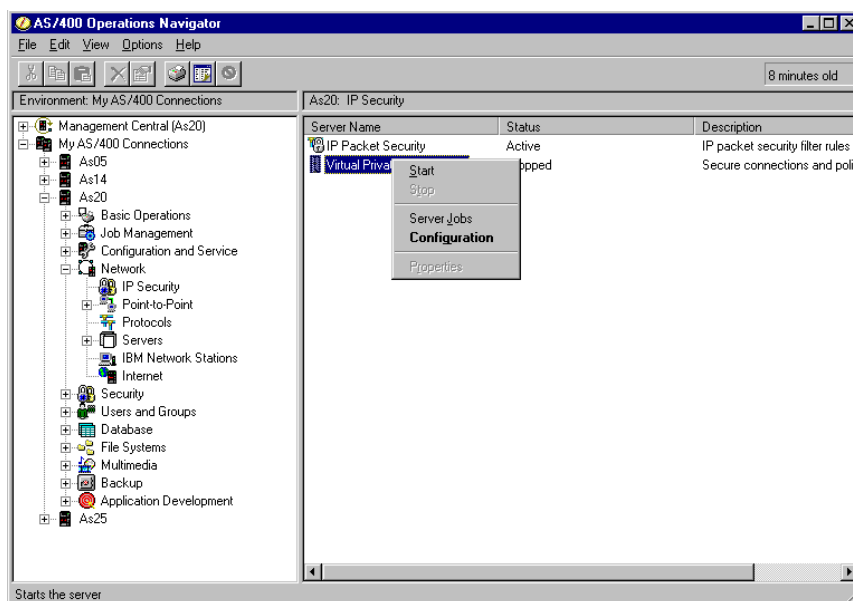


Figure 166. OS/400 - Starting VPN server jobs

After we start the VPN server jobs, the IP Security window displays IP Packet Security as *Active* and Virtual Private Networking as *Started*.

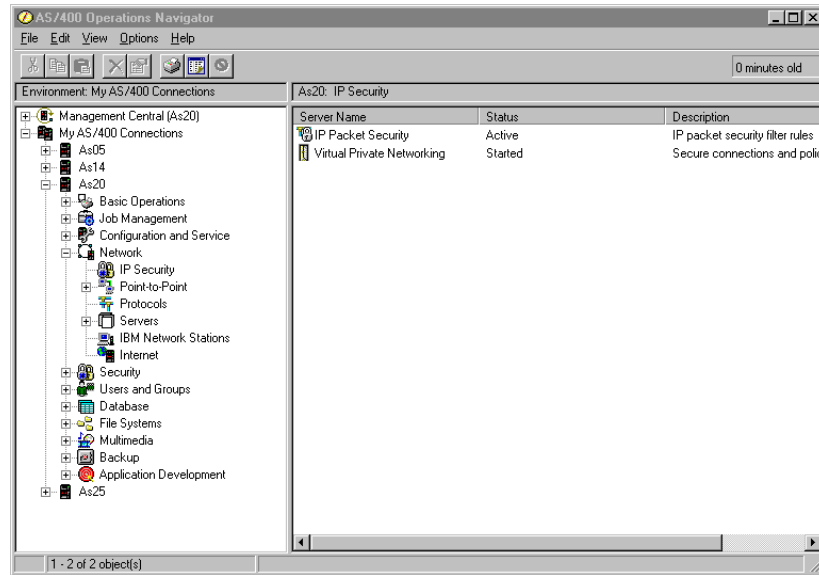


Figure 167. OS/400 - VPN server status

2. Only the *initiator* will perform the actions listed within this step:

Note

Before continuing any further make sure that the remote VPN server has also been started.

- a. Double-click **Virtual Private Networking**.
- b. Expand **Secure Connections** and then expand **Data Connections** and **Dynamic Key Groups**.
- c. Click Dynamic Key Group **RALYAS4A_RALYAS4C**.

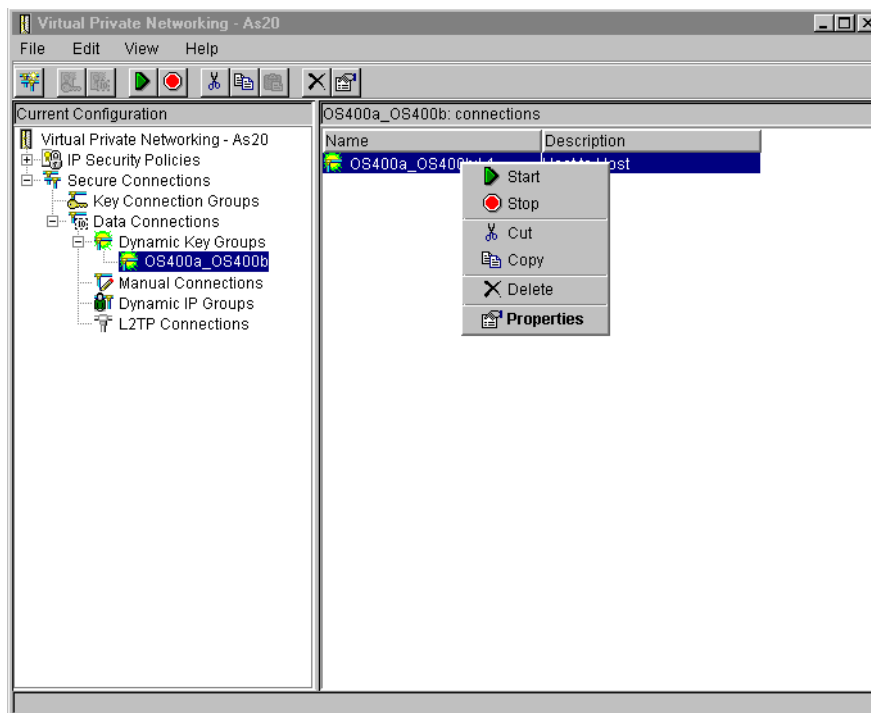


Figure 168. OS/400 - Starting the VPN connection

- d. Right-click your connection, **RALYAS4A_RALYAS4C**, in the right pane and select **Start** to initiate a VPN connection to the remote host.

If your configuration is correct and the VPN connection started successfully, you will receive no messages at all. This usually indicates that the connection works. If the remote VPN servers are not running, an error message will pop up after a certain time. For most other error conditions you will receive an error message immediately.

3. Use the Active Connections window to verify that your VPN connection is working. To do so, select **View** from the main menu and then select **Active Connections**.

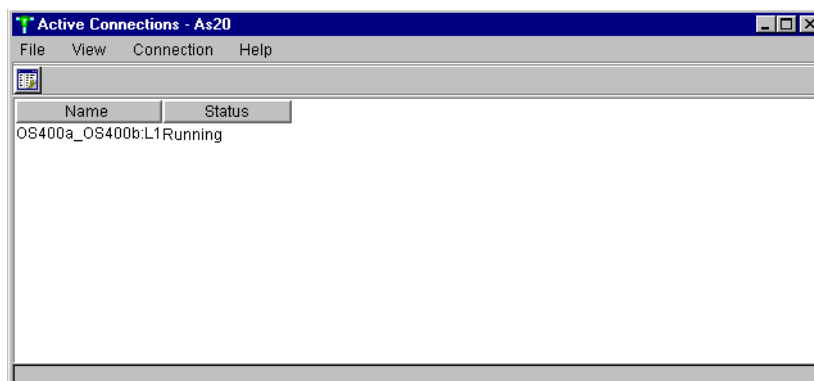


Figure 169. OS/400 - Active Connections window

The Active Connections window displays information about each VPN connection that is currently running. The window also displays information about where errors may have occurred. By default, you see only the *Name*

and the *Status* of the connection. To get more information about error information, security associations, encryption methods, and so on, you can customize the Active Connections window.

Note

A common error that occurs when the VPN connection fails to start, is a pre-shared key mismatch. If this happens, you must check the pre-shared key for the other party. To check and change the pre-shared key, go into the *Key Connection Group*. On the *General* page, select the remote server identifier and click **Set Pre-shared Key**. Do not attempt to change the pre-shared key from the key policy. This may cause problems when more than one user tries to update the pre-shared keys at the same time.

If your connection is not running, deactivate the tunnel and verify native IP connectivity.

- 4. Select **File** from the main menu and then select **Exit** to close the Active Connections window.

The following steps prove the active connection at user level. Use the PC 5250 emulator to establish a session over the secured connection.

- 5. In AS/400 Operations Navigator, right-click the AS/400 connection we used before (RALYAS4A) and select **Display Emulator** to open a 5250 session.

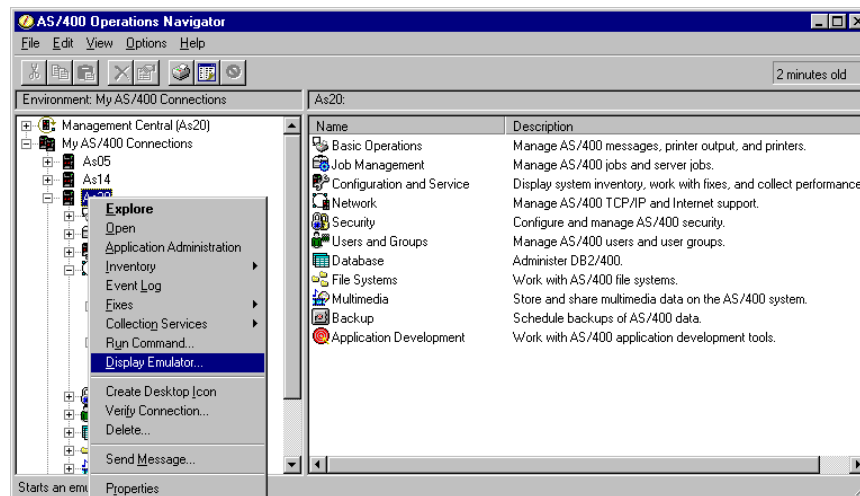


Figure 170. OS/400 - open 5250 display

A PC 5250 emulator session starts.

```

                                Sign On
                                System . . . . . : RALYAS4A
                                Subsystem . . . . . : QINTER
                                Display . . . . . : QPADEV000P

                                User . . . . . VPN01
                                Password . . . . .
                                Program/procedure . . . . .
                                Menu . . . . .
                                Current library . . . . .

                                (C) COPYRIGHT IBM CORP. 1980, 1999.

```

6. Sign on to the **AS/400** system using:

Userid: **User ID**
 Password: **Password**

7. Start a Telnet session to the remote host.

```

MAIN                                AS/400 Main Menu                                System:  RALYAS4A

Select one of the following:

    1. User tasks
    2. Office tasks
    3. General system tasks
    4. Files, libraries, and folders
    5. Programming
    6. Communications
    7. Define or change the system
    8. Problem handling
    9. Display a menu
   10. Information Assistant options
   11. Client Access/400 tasks

   90. Sign off

Selection or command
===> telnet '192.168.100.150'

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 1999.

```

8. Use the following AS/400 command to telnet to the remote system:

```

TELNET '192.168.100.150'
(Refer to the Lab Environment Conversion Table)

```

```

                                Sign On
                                System . . . . . : AS25
                                Subsystem . . . . . : QINTER
                                Display . . . . . : QPADEV000M

                                User . . . . .
                                Password . . . . .
                                Program/procedure . . . . .
                                Menu . . . . .
                                Current library . . . . .

(C) COPYRIGHT IBM CORP. 1980, 1999.

```

If you get the AS/400 system sign-on display, you have successfully configured and established a VPN host-to-host connection.

- 9. Press the **Esc** key and take option 99 to end the Telnet connection and return to your local system.
- 10. Minimize the AS/400 5250 session window.

10.7.4 Relationship between the wizard and the configuration objects

You can configure a virtual private network (VPN) connection on your AS/400 system by using the configuration wizard or by creating all the required objects manually. If your network administrator does not have an in-depth knowledge of virtual private networking, we recommend that you use the configuration wizard. The wizard creates all the objects automatically based on information provided by your administrator and the default values of the system.

For an AS/400-to-AS/400 connection, the wizard is the best choice to perform basic configuration. However, in some cases you may want to change a parameter, for example, the key lifetime, the authentication algorithm, or the encryption method. In these cases, you need to understand the relationship between the input provided to the wizard and the objects it creates.

The following chart illustrates the relationship between the configuration wizard and the objects it creates:

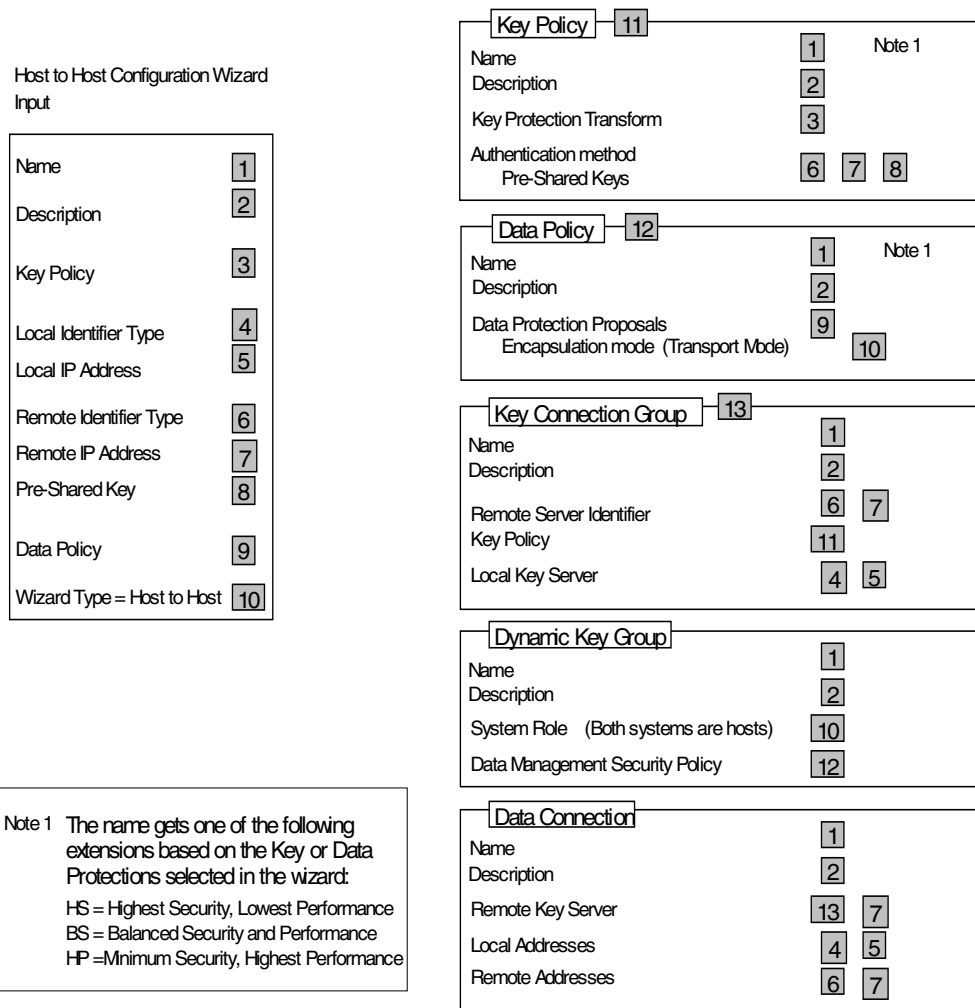


Figure 171. Relationship wizard - configuration objects

The Key Policy window of the host-to-host configuration wizard sets up the security options that the Internet Key Exchange (IKE) protocols use for processing. The wizard configures values for the Key Protection Transform based on the selection you make on the Key Policy window, for example, *highest security, lowest performance*. The following table shows the different key protection transforms the wizard creates based on the various parameters you can specify for the key policy:

Table 43. Security options for key policies

| Field | Value |
|--|------------------------------------|
| Key Protection Transform for Minimum Security, Highest Performance (HP) | |
| Hash algorithm | MD5 (Message Digest 5) |
| Encryption algorithm | DES-CBC (Data Encryption Standard) |
| Diffie-Hellman Group | Group 1 = Default 768-bit MODP |
| Key Protection Transform for Balanced Security and Performance (BS) | |

| Field | Value |
|---|--|
| 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 (Secure Hash Algorithm) |
| Encryption algorithm | 5769-AC3: 3DES-CBC (Triple DES) 5769-AC2: DES-CBS |
| Diffie-Hellman Group | Group 1 = Default 768-bit MODP |

The Data Policy window of the host-to-host configuration wizard sets up the security options that protect user data. The wizard configures values for the Data Protection Proposal based on the selection you make on the Data Policy window, for example, *highest security, lowest performance*. The following table shows the different data protection proposals the wizard creates based on the various parameters you can specify for the key policy.

Table 44. Security options for data policies

| Field | Value |
|--|--|
| Data Protection Proposal for Minimum Security, Highest Performance (HP) | |
| Protocol | AH (Authentication Header) |
| Authentication Algorithm | HMAC-MD5 (Hashed Message Authentication Code - Message Digest 5) |
| Encryption algorithm | |
| Diffie-Hellman Perfect Forward Secrecy (PFS) | Not selected |
| Data Protection Proposal for Balanced Security and Performance (BS) | |
| Protocol | ESP (Encapsulated Security Payload) |
| Authentication algorithm | HMAC-MD5 |
| Encryption algorithm | DES-CBC |
| Diffie-Hellman Perfect Forward Secrecy (PFS) | Not selected |
| Data Protection Proposal for Highest Security, Lowest Performance (HS) | |
| Protocol | ESP |
| Authentication algorithm | HMAC-SHA |
| Encryption algorithm | 5769-AC3: 3DES-CBC 5769-AC2: DES-CBC |
| Diffie-Hellman Perfect Forward Secrecy (PFS) | Not selected |

Chapter 11. Communications Server V2R8 for OS/390

This section describes the VPN feature of OS/390, especially the IKE tunnel configuration. This includes customization of SecureWay Communications Server components and the IKE tunnel configuration using GUI and command line.

In OS/390 V2R8, we have the dynamic tunnels support based on the Internet Security Association and Key Management Protocol (ISAKMP) standards developed by the Internet Engineering Task Force (IETF). The dynamic tunnels provide a more reliable and secure connection than the manually configured tunnels because the key exchange is done automatically. The secure key negotiation and key refreshment is done in an industry-standard way.

The ISAKMP support is based on the following RFC standards:

- RFC 2407 - The Internet IP Domain of Interpretation for ISAKMP
- RFC 2408 - The Internet Security Association and Key Management Protocol
- RFC 2409 - The Internet Key Exchange

11.1 Firewall technologies for OS/390

The OS/390 Firewall Technologies is a collection of programs that provide the firewall functions on OS/390 including support for virtual private networks (VPNs). The virtual private network further enhances the level of security of the system by providing a mechanism for data to be encrypted and/or authenticated between endpoints. The OS/390 Firewall Technologies provides the facilities to manually or dynamically define a virtual private network according to standards defined by IETF.

In essence, the OS/390 firewall consists of traditional firewall functions and support for VPNs. The OS/390 Firewall Technologies provides for:

- **IPSec, virtual private network, or tunneling**
 - Key management either manually or dynamically. Dynamic VPN support has been introduced by OS/390 V2R8. The Internet Key Exchange (IKE) authentication is done using either pre-shared keys or RSA signatures.
 - S/390 hardware cryptographic facility will be used if available.
- **Application gateways (proxies)**
 - FTP proxy
- **Transparent gateways (SOCKS)**
 - SOCKS V4 server
- **Packet filtering**
 - Filter rules
- **Network Address Translation (NAT)**
 - Administrator-defined address mapping
 - Address translation in IP headers only
- **Logging**
 - Enhanced syslog server

- SMF records
- **Configuration and administration**
 - Compatible with AIX and Windows NT (command line and GUI)
 - Commands are valid in OE only, not from TSO
 - Commands create intermediate files, which are used to update the online configuration
 - An external security manager such as RACF is used to control authorization to maintain network security profiles. This is in line with general security concepts on the OS/390 servers.

The above features may be used in any combination.

Although OS/390 Firewall Technologies provides various functions, in this chapter we will focus only on the dynamic VPN functions. For more information on the other firewall functions on OS/390, see *Stay Cool on OS/390: Installing Firewall Technology*, SG24-2046, *OS/390 Firewall Technologies Guide and Reference*, SC24-5835, and *Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements*, SG24-5631.

11.2 Installation and customization of VPN IKE feature

To implement dynamic tunnels in OS/390 you have to implement the firewall services in OS/390. Firewall services implements the IKE function in OS/390 in conjunction with SecureWay CS IP Services, Open Cryptographic Services Facility (OCSF), and Security Server.

The following high-level steps are required to define dynamic VPNs:

1. Define policies:
 - Key management
 - Data management
 - Dynamic tunnel
2. Define key server information
3. Define authentication data
4. Define anchor filter rules
5. Define locally activated dynamic connections

Each high-level step is comprised of a series of lower-level steps that will be covered in detail in this chapter.

11.2.1 OS/390 SecureWay CS IP services customization

To configure OS/390 IP to support IKE functions you need to complete the following steps. If you need more information see *OS/390 Firewall Technologies Guide and Reference*, SC24-5835. At ITSO Raleigh, we used the TCPIP stack in system RA03 to implement the firewall function.

11.2.1.1 Configure the TCP/IP profile

Add the device statements that you will use to connect the OS/390 with the networks. Refer to *OS/390 SecureWay Communications Server IP Configuration*, SC31-8513 for more information. Look at the example below:

```
DEVICE TR1B LCS      2020 AUTORESTART
LINK  TR1B  IBMTR    0    TR1B
```

If you want to start FWKERN automatically insert the following AUTOLOG statement:

```
AUTOLOG
      FWKERN          ; OS/390 Firewall
ENDAUTOLOG
```

Note: If you are running a system that will be connected to the Internet or to another nonsecure network you should remove any AUTOLOG statement for the standard TCP/IP servers. They should start only after FWKERN.

Add the following PORT statements:

```
500 UDD OMVS          ; OS/390 Firewall ISAKMP Server
514 UDP OMVS          ; OS/390 Firewall Syslogd Server
1014 TCP OMVS         ; OS/390 Firewall Configuration Client
```

Add the following definitions in the IPCONFIG block statement:

```
IPCONFIG
      FIREWALL
      DATAGRAMFWD
ENDIPCONFIG
```

The FIREWALL keyword cannot be dynamically activated using the VARY OBEY console command. To activate the firewall function, you have to restart the TCP/IP stack.

11.2.1.2 Configure /etc/services

Create the /etc/services file if it does not exist, then add the definitions for the SYSLOG server and ISAKMP server as follows:

```
syslog  514/udp
isakmp  500/udp
```

11.2.1.3 Checking TCP/IP configuration

During the TCP/IP stack initialization you can check if the following messages appear in the system log:

```
EZZ0641I IP FORWARDING NOFWMULTIPATH SUPPORT IS ENABLED
EZZ0349I FIREWALL SUPPORT IS ENABLED
```

Using the commands below you can check all the other configurations you made:

```

Display TCPIP,TCPIPB,N,CONFIG 1
EZZ2500I NETSTAT CS V2R8 TCPIPB
TCP CONFIGURATION TABLE:
DEFAULTRCVBUFSIZE: 00065536 DEFAULTSNDBUFSIZE: 00065536
DEFLTMAXRCVBUFSIZE: 00262144
MAXRETRANSMITTIME: 120.000 MINRETRANSMITTIME: 0.500
ROUNDTRIPGAIN: 0.125 VARIANCEGAIN: 0.250
VARIANCEMULTIPLIER: 2.000 MAXSEGLIFETIME: 60.000
DEFAULTKEEPALIVE: 0.120 LOGPROTOERR: 00
TCPFLAGS: 10
UDP CONFIGURATION TABLE:
DEFAULTRCVBUFSIZE: 00016384 DEFAULTSNDBUFSIZE: 00016384
CHECKSUM: 00000001 LOGPROTOERR: 01
UDPFLAGS: 23
IP CONFIGURATION TABLE:
FORWARDING: YES 2 TIMETOLIVE: 00060 RSMTIMEOUT: 00015
FIREWALL: 00001 3 ARPTIMEOUT: 01200 MAXRSMSSIZE: 65535

```

Figure 172. Report from Netstat CONFIG command

- 1** This command shows configuration information about the TCP/IP stack.
- 2** FORWARDING: YES means that TCP/IP will transfer data between networks. NO means that this stack will not transfer data between networks.
- 3** FIREWALL: 00001 means that the firewall function is active in this stack; 00000 means that this stack is not activated.

To check if the devices are well configured and ready issue the following command:

```

Display TCPIP,TCPIPB,N,DEvlinks 1
EZZ2500I NETSTAT CS V2R8 TCPIPB 757
DEVNAME: LOOPBACK          DEVTYPE: LOOPBACK  DEVNUM: 0000
LNKNAME: LOOPBACK         LNKTTYPE: LOOPBACK STATUS: READY
NETNUM: 0  QUESIZE: 0  BYTEIN: 0000308050  BYTEOUT: 0000308050
BSD ROUTING PARAMETERS:
MTU SIZE: 00000          METRIC: 00
DESTADDR: 0.0.0.0       SUBNETMASK: 0.0.0.0
MULTICAST SPECIFIC:
MULTICAST CAPABILITY: NO
DEVNAME: TR1B             DEVTYPE: LCS       DEVNUM: 2020
LNKNAME: TR1B            LNKTTYPE: TR       STATUS: READY 2
NETNUM: 0  QUESIZE: 0  BYTEIN: 0001000461  BYTEOUT: 0001722471
ARPMACADDRESS: NON-CANONICAL  SRBRIDGINGCAPABILITY: YES
BROADCASTCAPABILITY: YES      BROADCASTTYPE: ALL RINGS
BSD ROUTING PARAMETERS:
MTU SIZE: 00000          METRIC: 00
DESTADDR: 0.0.0.0       SUBNETMASK: 255.255.255.0
MULTICAST SPECIFIC:
MULTICAST CAPABILITY: YES

```

Figure 173. Report from Netstat DEvlinks command

- 1** This command displays information about devices and links defined in the TCP/IP stack.
- 2** STATUS: READY means that this device is ready and operational.

To check if the port statements are well configured, issue the following command:

```
Display TCPIP,TCPIPB,N,PORTList 1
EZZ2500I NETSTAT CS V2R8 TCPIPB 779
PORT# PROT USER      FLAGS RANGE
00007 TCP  MISC SERV A
00009 TCP  MISC SERV A
00019 TCP  MISC SERV A
00020 TCP  OMVS
00021 TCP  FTPD1  A
00021 TCP  FTPDB1 A
00025 TCP  SMTP  A
00053 TCP  OMVS  A
00080 TCP  OMVS  A
00111 TCP  OMVS  A
00443 TCP  OMVS  A
00500 UDP  OMVS  A 2
00514 UDP  OMVS  A 2
00515 TCP  T03ALPD A
00750 TCP  MVS KERB A
00751 TCP  ADM@SRV A
00760 TCP  IOASNMP A
01014 TCP  OMVS  A 2
```

Figure 174. Report from Netstat PORTList command

1 This command shows information about port reservation in the TCP/IP stack.

2 Ports 500 and 514 over protocol UDP, and 1014 over TCP are reserved for UNIX System Services application, that is FWKERN in this case.

11.2.2 UNIX System Services customization

There are some parameters in BPXPRMxx member in SYS1.PARMLIB that must be checked and changed if necessary. Check the following parameters:

- MAXPROCSYS: The firewall requires 11 processes to start its servers. The default is 200.
- MAXPROCUSER: The firewall requires 11 processes to start its servers. The default is 25.
- MAXFILEPROC: The firewall requires at least 25 open file descriptors for its servers, two for each concurrent connection to the SOCKS server and four for each concurrent connection to the FTP proxy server. The default is 64.
- MAXTHREADTASKS: The firewall requires approximately 10 threads for firewall servers, one thread for each concurrent connection to the SOCKS server, and one thread for each concurrent connection to the proxy FTP server. The default is 50.
- MAXTHREAD: The SOCKS and proxy FTP servers require one thread for each concurrent connection. The default is 200.
- MAXSOCKETS: The firewall requires approximately 25 sockets for firewall servers, two for each concurrent connection to the SOCKS server, and four for each concurrent connection to the FTP proxy server. ISAKMP requires one additional socket per interface defined to a firewall stack. The default is 64.

Check if you have AF_UNIX configured. If not, please add the following statements to the BPXPRMxx file:

```

NETWORK DOMAINNAME (AF_UNIX)
        DOMAINNUMBER (1)
        MAXSOCKETS (100)
        TYPE (IBMUDES)

```

For more information about the BPXPRMxx configuration, please see *OS/390 UNIX System Services Planning*, SC28-1890, and *OS/390 MVS Initialization and Tuning Reference*, SC28-1752.

11.2.3 OS/390 Security Server and cryptographic services customization

The following procedures assume that you are performing them from a RACF administration ID. The table below provides a brief description of the RACF profiles we are using here:

Table 45. RACF profile description

| Class | Profile | Description |
|----------|------------------|--|
| FACILITY | BPX.SMF | Checks if the caller attempting to cut an SMF record is allowed to write an SMF record or test if an SMF type or subtype is being recorded. |
| FACILITY | BPX.DAEMON | Restricts access to the following services: seteuid, setuid, setruid, setreuid, and spawn. The caller of this service must be a superuser. |
| FACILITY | BPX.SERVER | Restricts the use of the pthread_security_np service. A user with read or write access to the BPX.SERVER FACILITY class profile can use this service. It creates or deletes the security environment for the caller's thread. This profile is also used to restrict the use of the BPX1ACK service, which determines access authority to an OS/390 resource. |
| FACILITY | BPX.SUPERUSER | Users with access to the BPX.SUPERUSER FACILITY class profile can switch to superuser authority (effective UID of 0). |
| FACILITY | BPX.FILEATTR.APF | Controls that users are allowed to set the APF-authorized attribute in an HFS file. This authority allows the user to create a program that will run APF authorized. This is similar to the authority of allowing a programmer to update SYS1.LINKLIB or SYS1.LPALIB. |

| Class | Profile | Description |
|----------|-----------------------|---|
| FACILITY | BPX.FILEATTR.PROGCTL | Controls that users are allowed to set the program-controlled attribute in an HFS file. Programs marked with this attribute can execute in server address spaces that run with a high level of authority. |
| FACILITY | ICA.CFGSRV | Permits the access of the Firewall Configuration GUI. |
| FACILITY | IRR.DIGTCERT.ADD | Permission to add a certificate. |
| FACILITY | IRR.DIGTCERT.ADDRING | Permission to add a key ring. |
| FACILITY | IRR.DIGTCERT.CONNECT | Permission to connect to a key ring. |
| FACILITY | IRR.DIGTCERT.DELETE | Permission to delete a certificate. |
| FACILITY | IRR.DIGTCERT.DELRING | Permission to delete a key ring. |
| FACILITY | IRR.DIGTCERT.GENCERT | Permission to generate a certificate. |
| FACILITY | IRR.DIGTCERT.GENREQ | Permission to generate a certificate request. |
| FACILITY | IRR.DIGTCERT.LIST | Permission to list a certificate. |
| FACILITY | IRR.DIGTCERT.LISTRING | Permission to list a key ring. |
| FACILITY | CDS.CSSM.CRYPTO | Authorizes the daemon to call a Cryptographic Service Provider. |
| FACILITY | CDS.CSSM.DATALIB | Authorizes the daemon to call a Data Library (DL) Service Provider. |
| FACILITY | FWKERN.START.REQUEST | Permits FWKERN to issue the <code>START</code> console command and to start its servers. It also controls firewall administrator IDs that are allowed to issue the <code>fwdaemon</code> command to start and stop firewall servers. |
| STARTED | STC name | The STARTED class allows you to assign RACF identities to started procedures and jobs dynamically, using the <code>RDEFINE</code> and <code>RALTER</code> commands. Unlike the started procedures table, it does not require you to modify code or re-IPL in order to add or modify RACF identities for started procedures. It provides, in effect, a dynamic started procedures table. |
| CSFSERV | ICSF Services | Controlling use of Integrated Cryptographic Service Facility (ICSF) cryptographic services. |

11.2.3.1 Planning for group definition

Determine the current group definitions:

```
LISTGRP * OMVS NORACF
```

Note: Bear in mind that two groups, SYS1 (or equivalent) and FWGRP, are required for the OS/390 Firewall Technologies configuration. If these groups already exist, note their group identifiers. If not, note available group identifiers for use in the definition of the required group(s).

Determine if the SYS1 group (or a logically equivalent group to contain UID=0 users) exists:

```
LISTGRP SYS1 OMVS
```

If the SYS1 (or equivalent) group does not exist, create it:

```
ADDGROUP SYS1 OMVS(GID(nnn))
```

Note: The installation-defined group ID for the SYS1 group that was identified in the previous steps is *nnn*.

11.2.3.2 Defining users and groups

Define the firewall kernel address space to RACF or an equivalent security product.

- Define FWKERN user.
- Define the firewall kernel started procedure as a started task.

```
ADDGROUP FWGRP SUPGROUP(SYS1) OMVS(GID(nnn))
MKDIR '/u/fwkernel' MODE(7,5,5)
ADDUSER FWKERN OMVS(HOME('/u/fwkernel/') UID(0))
        DFLTGRP(FWGRP) AUTHORITY(CREATE) UACC(ALTER) PASSWORD(pw)
RDEFINE STARTED FWKERN STDATA(USER(FWKERN))
SETROPTS RACLIST(STARTED) REFRESH
```

Note: The installation-defined group ID for the FWGRP group that was identified in the previous steps is *nnn*; *pw* is the password for the FWKERN user ID. Choose this password with extreme care to avoid potential security exposure.

11.2.3.3 Granting users and groups authority to firewall objects

Create the FWKERN.START.REQUEST resource profile:

```
RDEFINE FACILITY FWKERN.START.REQUEST UACC(NONE)
PERMIT FWKERN.START.REQUEST CLASS(FACILITY) ID(FWKERN) ACCESS(UPDATE)
SETROPTS CLASSACT(FACILITY)
```

Permit FWKERN access to start the servers:

```
RDEFINE STARTED ICAPSLOG.** STDATA(USER(FWKERN) GROUP(FWGRP))
RDEFINE STARTED ICAPSOCK.** STDATA(USER(FWKERN) GROUP(FWGRP))
RDEFINE STARTED ICAPPFTP.** STDATA(USER(FWKERN) GROUP(FWGRP))
RDEFINE STARTED ICAPCFGS.** STDATA(USER(FWKERN) GROUP(FWGRP))
RDEFINE STARTED ICAPSTAK.** STDATA(USER(FWKERN) GROUP(FWGRP))
RDEFINE STARTED ICAPIKED.** STDATA(USER(FWKERN) GROUP(FWGRP))
SETROPTS RACLIST(STARTED) REFRESH
```

Permit FWKERN access to READ the TCP/IP data sets if necessary:

```
PERMIT 'TCPIP.**' ID(FWKERN) ACCESS(READ)
```

Permit FWKERN to read to the BPX.SMF facility (for logging):

```
RLIST FACILITY BPX.SMF ALL
RDEFINE FACILITY BPX.SMF UACC(NONE)
PERMIT BPX.SMF CLASS(FACILITY) ID(FWKERN) ACCESS(READ)
```

Permit FWKERN to read the BPX.DAEMON facility:

```
RLIST FACILITY BPX.DAEMON
RDEFINE FACILITY BPX.DAEMON UACC(NONE)
PERMIT BPX.DAEMON CLASS(FACILITY) ID(FWKERN) ACCESS(READ)
```

Once you activate the BPX.DAEMON facility, you have to turn on the program control using `SETOPTS WHEN(PROGRAM)`.

Program control

This command activates RACF program control, which includes both access control to load modules and program access to data sets. To set up access control to load modules, you must identify your controlled programs by creating a profile for each in the PROGRAM class. To set up program access to data sets, you must add a conditional access list to the profile of each program-accessed data set. Then, when program control is active, RACF ensures that each controlled load module is executed only by callers with the defined authority. RACF also ensures that each program-accessed data set is opened only by users who are listed in the conditional access list with the proper authority and who are executing the program specified in the conditional access list entry.

The firewall server programs must be marked as program controlled. It is also necessary to mark the SSL library SGSKLOAD as program controlled. This can be done by using the following commands:

```
RALTER PROGRAM * ADDMEM('ICA.SICALMOD'/'*****'/NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM('hlq.SGSKLOAD'/'*****'/NOPADCHK) UACC(READ)
SETOPTS WHEN(PROGRAM) REFRESH
```

Note: Program control is the concept of having trusted applications. When it is active, processes will be marked dirty if they attempt to load programs from libraries that are not trusted. OS/390 UNIX also has the concept of trusted applications. In the UNIX file system, executable files may be tagged with the program-controlled extended attribute. If a user issues an OS/390 shell command or runs a program that does not have the program-controlled extended attribute, the process becomes dirty; in either case, the process is never cleaned. That is, the dirty bit remains, which will cause certain services to fail as a result. For more information see *OS/390 UNIX System Services Planning*, SC28-1890.

To use the configuration server, some setup is required.

Note: All user IDs that will use the firewall configuration GUI must explicitly be given permission to update the configuration through the configuration server. This includes user IDs that have superuser privileges or are members of the firewall group.

```
RDEFINE FACILITY ICA.CFGSRV UACC(NONE)
PERMIT ICA.CFGSRV CLASS(FACILITY) ID(userid) ACCESS(UPDATE)
SETOPTS CLASSACT(FACILITY)
SETOPTS RACLIST(FACILITY) REFRESH
```

Adding firewall administrators to FWGRP:

If the user IDs that will administer the firewall are not superusers (UID=0), add them to the FWGRP group as follows:

```
CONNECT userid GROUP (FWGRP)
```

The ISAKMP server supports the ability to perform peer authentication using RSA signature mode. RSA signature mode requires that digital certificates be stored in RACF and connected onto a key ring. RACF provides digital certificate and key ring support using the `RACDCERT` command. The authorizations necessary to perform the basic `RACDCERT` actions are shown below:

```
RDEFINE FACILITY IRR.DIGTCERT.ADD UACC (NONE)
RDEFINE FACILITY IRR.DIGTCERT.ADDRING UACC (NONE)
RDEFINE FACILITY IRR.DIGTCERT.CONNECT UACC (NONE)
RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC (NONE)
RDEFINE FACILITY IRR.DIGTCERT.GENREQ UACC (NONE)
RDEFINE FACILITY IRR.DIGTCERT.LIST UACC (NONE)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC (NONE)
PERMIT IRR.DIGTCERT.ADD CLASS (FACILITY) ID(userid) ACC(CONTROL)
PERMIT IRR.DIGTCERT.ADDRING CLASS (FACILITY) ID(userid) ACC(UPDATE)
PERMIT IRR.DIGTCERT.CONNECT CLASS (FACILITY) ID(userid) ACC(CONTROL)
PERMIT IRR.DIGTCERT.GENCERT CLASS (FACILITY) ID(userid) ACC(CONTROL)
PERMIT IRR.DIGTCERT.GENREQ CLASS (FACILITY) ID(userid) ACC(CONTROL)
PERMIT IRR.DIGTCERT.LIST CLASS (FACILITY) ID(userid) ACC(CONTROL)
PERMIT IRR.DIGTCERT.LISTRING CLASS (FACILITY) ID(userid) ACC(UPDATE)
SETROPTS RACLIST (FACILITY) REFRESH
```

where `userid` is the ID of the person who will be executing the `RACDCERT` command to store digital certificates.

Authority to the `IRR.DIGTCERT` function resource in the `FACILITY` class allows a user to issue the `RACDCERT` command that is used to install and maintain digital certificates and key rings in RACF. To issue the `RACDCERT` command, users must have one of the following authorities:

- The `SPECIAL` attribute
- Sufficient authority to resource `IRR.DIGTCERT.function` in the `FACILITY` class.
 - `READ` access to `IRR.DIGTCERT.function` to issue the `RACDCERT` command for themselves.
 - `UPDATE` access to `IRR.DIGTCERT.function` to issue the `RACDCERT` command for others.
 - `CONTROL` access to `IRR.DIGTCERT.function` to issue the `RACDCERT` command for `SITE` and `CERTAUTH` certificates. This authority also has other uses.

Refer to the *OS/390 Security Server (RACF) Command Language Reference*, SC28-1919, for a complete description of the facilities and authorizations needed to create and modify digital certificates and key rings.

11.2.3.4 Installing Open Cryptographic Services Facility (OCSF) code

To perform the cryptographic functions needed by the IKE function, you have to install and configure Open Cryptographic Services Facility (OCSF). In this chapter we will show how to perform this configuration. For more information about OCSF, please see *Open Cryptographic Services Facility Application Developer's Guide and Reference*, SC24-5875.

OCSF consists of four different features. The installation method varies with the feature installed. The following are the OCSF features available on OS/390 V2R8. You can order only one of the four OCSF security features (OCSF France, OCSF Security Level 1, OCSF Security Level 2, or OCSF Security Level 3).

- OCSF France

In conjunction with the base element Cryptographic Services, this feature provides weak (40-bit) software cryptographic services, a data library service provider, certificate library service providers, trust policy service providers, and 40-bit hardware cryptographic services, and may be used in France.

- OCSF Security (Level 1)

OCSF Security Level 1, in conjunction with base element Cryptographic Services, provides weak (40-bit) software cryptographic services, a data library service provider, certificate library service providers, trust policy service providers, and hardware cryptographic services.

- OCSF Security (Level 2)

OCSF Security Level 2, in conjunction with base element Cryptographic Services, provides weak (40-bit) and strong (56-bit) software cryptographic services, a data library service provider, certificate library service providers, trust policy service providers, and hardware cryptographic services.

- OCSF Security (Level 3)

OCSF Security Level 3, in conjunction with base element Cryptographic Services, provides weak (40-bit) and strong (56-bit and greater) software cryptographic services, a data library service provider, certificate library service providers, trust policy service providers, and hardware cryptographic services. This feature may not be exported from the United States and Canada (with limited exceptions).

Table 46 lists the cryptographic features available in OS/390 V2R8:

Table 46. OS/390 V2R8 cryptographic features

| OCSF Feature | FMID | Subset ID |
|--------------------------------------|--------------------|-------------|
| Open Cryptographic Services Facility | HCRY280 HCPT280 | OCSF SSL |
| OCSF Security Level 3 | JCRY286 | OCSF |
| OCSF Base Crypto | JCRY282 | OCSF |
| OCSF Strong Crypto | JCRY281 | OCSF |
| Open Cryptographic Enhanced Plug-Ins | HRO6608 | OCEP |
| System SSL Security Level 3 | JCPT281 | SSL |

To use OCSF services the following administration must be done:

- OCSF-related RACF facility class profiles need to be defined and the FACILITY class made active if it is not already active.
- All of the programs, modules, and DLLs loaded into the OCSF application address space must be defined as program controlled. Programs or modules loaded from the traditional OS/390 search order (that is, STEPLIB, LINKLIST,

etc.) need to reside in program-controlled libraries. Programs loaded from the UNIX file system must have the program-controlled extended attribute.

- OCSF application user IDs must be defined to RACF and permitted to the OCSF facility class profiles. Depending on whether your system is operating with OS/390 UNIX security or UNIX security, these user IDs will also need to be permitted to the BPX.SERVER facility class profile (when OS/390 UNIX security is in effect), or the OCSF daemon application must run with an effective UID of 0 (when UNIX security is in effect).

If you use OCSF from APF-authorized applications, you will need to turn on the APF-authorized extended attribute for the OCSF DLLs in the `/usr/lpp/ocsf/lib` and `/usr/lpp/ocsf/addins` directories. The SMP/E installation of OCSF does not ordinarily turn on the APF-authorized extended attribute. You can turn on the APF-authorized extended attribute using the `extattr +a` command.

AFP authorization

The ISAKMP firewall (IKE function) runs as an APF-authorized application. So, we have to turn on the APF-authorized extended attribute for the OCSF and OCEP dynamically loaded libraries.

Mark the OCSF programs in the OCSF UNIX Library as APF authorized and program controlled using the `extattr` command. To issue the `extattr` command, the user ID has to have access to a specific RACF class profile:

```
RDEFINE FACILITY BPX.FILEATTR.APF ACC(NONE)
PERMIT BPX.FILEATTR.APF CLASS(FACILITY) USER(GIANCA) ACCESS(UPDATE)
RDEFINE FACILITY BPX.FILEATTR.PROGCTL ACC(NONE)
PERMIT BPX.FILEATTR.PROGCTL CLASS(FACILITY) USER(GIANCA) ACCESS(UPDATE)
SETROPTS CLASS(FACILITY) REFRESH
```

From the command prompt in the OS/390 UNIX shell, enter the following commands:

```

$ cd /usr/lpp/ocsf/lib
$ extattr +a *.dll 1
$ ls -E *.dll 2
-rwxr-xr-x  aps  2  OMVSKERN  SYS1      49152 May 11 21:20  cdserprt.dll
-rwxr-xr-x  aps  2  OMVSKERN  SYS1      86016 May 11 21:20  cdsibmut.dll
-rwxr-xr-x  aps  2  OMVSKERN  SYS1      86016 May 11 21:20  cdskwtf.dll
-rwxr-xr-x  aps  2  OMVSKERN  SYS1    4173824 May 11 21:20  cdsnspsp.dll
-rwxr-xr-x  aps  2  OMVSKERN  SYS1    192512 May 11 21:20  cdsport.dll
-rwxr-xr-x  aps  2  OMVSKERN  SYS1    188416 May 11 21:21  cdsrandm.dll
-rwxr-xr-x  aps  2  OMVSKERN  SYS1    823296 May 11 21:19  cssm32.dll
lrwxrwxrwx   1  OMVSKERN  SYS1         16 May 11 21:20  cssmanp.dll -> cssma
np_sl3.dll
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     36864 May 11 21:20  cssmanp_sl3.dll
lrwxrwxrwx   1  OMVSKERN  SYS1         16 May 11 21:20  cssmusep.dll -> cssmus
ep_sl3.dll
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     36864 May 11 21:20  cssmusep_sl3.dll

$ cd /usr/lpp/ocsf/addins
$ extattr +a *.so 1
$ ls -E *.so 2
-rwxr-xr-x  aps  2  OMVSKERN  SYS1    450560 May 11 21:20  ibmcca.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1    589824 May 11 21:20  ibmcl.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1   1474560 May 11 21:21  ibmcl2.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1   5701632 May 11 21:21  ibmdl2.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1   6856704 May 11 21:20  ibmocepd1.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1    425984 May 11 21:20  ibmoceptp.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1   1138688 May 11 21:20  ibmswcsp.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     57344 May 11 21:21  ibmtp.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1   3563520 May 11 21:21  ibmtp2.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1   1069056 May 11 21:21  ibmwkcsp.so

```

Figure 175. extattr shell command

1 Give the APF authorization attributes to all files with the dll suffix in the /usr/lpp/ocsf/lib directory and files with the so suffix in /usr/lpp/ocsf/addins.

2 Using the ls command with the -E option, you can see the extended attributes of the HFS files. The a and p flags in the second column indicate that the files do have the API-authorized and program-controlled attribute.

Define the following RACF facility class profiles:

```

DEFINE FACILITY CDS.CSSM UACC(NONE)
RDEFINE FACILITY CDS.CSSM.CRYPTO UACC(NONE)
RDEFINE FACILITY CDS.CSSM.DATALIB UACC(NONE)

```

Grant the permission to use OCSF services to the FWKERN user ID:

```

PERMIT CDS.CSSM CLASS(FACILITY) ID(FWKERN) ACC(READ)
PERMIT CDS.CSSM.CRYPTO CLASS(FACILITY) ID(FWKERN) ACC(READ)
PERMIT CDS.CSSM.DATALIB CLASS(FACILITY) ID(FWKERN) ACC(READ)

```

Permit FWKERN access to the BPX.SERVER:

```

PERMIT BPX.SERVER CLASS(FACILITY) ID(FWKERN) ACC(READ)

```

Refresh the FACILITY class and PROGRAM class profile:

```

SETROPTS CLASS(FACILITY) REFRESH

```

Run the installation script from the UNIX System Services shell. You have to use a user ID with a UID of 0 (superuser) or have permission to issue the su command

(BPX.SUPERUSER profile). This user ID must have access permission to the CDS.CSSM and the BPX.SERVER RACF facility class. Issue the following commands to give a user access permission:

```
PERMIT CDS.CSSM CLASS(FACILITY) ID(userid) ACC(READ)
PERMIT CDS.CSSM.CRYPTO CLASS(FACILITY) ID(userid) ACC(READ)
PERMIT CDS.CSSM.DATALIB CLASS(FACILITY) ID(userid) ACC(READ)
PERMIT BPX.SERVER CLASS(FACILITY) ID(userid) ACC(READ)
PERMIT BPX.SUPERUSER CLASS(FACILITY) ID(userid) ACC(READ)
SETROPTS CLASS(FACILITY) REFRESH
```

The installation scripts that you need to run are determined by which of the OCSF features you have installed. When you have the Security Level 3 feature or the Security Level 2 feature installed, you have to issue the installation scripts for the strong cryptographic facility in addition to scripts for the basic level feature.

If you have the Security Level 1, 2, or 3 feature or the French feature, perform the following steps:

```
$ su
$ cd /usr/lpp/ocsf/bin
$ ocsf_install_basic_crypto
Installing CSSM...
CSSM Framework successfully installed
Installing IBMTP...
Addin successfully installed.
Installing IBMTP2...
Addin successfully installed.
Installing IBMCL...
Addin successfully installed.
Installing IBMCL2...
Addin successfully installed.
Installing IBMDL2...
Addin successfully installed.
Installing IBMWKCSPP...
Addin successfully installed.
Installing IBMCCA...
Addin successfully installed.
```

Figure 176. *ocsf_install_basic_crypto* shell command

If the user does not have read access permission to the BPX.SERVER RACF facility class, the command will fail with the message shown in Figure 177. You will also see the RACF error message on the MVS console shown in Figure 178.

```
JRIVERA @ RA28:/usr/lpp/ocsf/bin>ocsf_install_basic_crypto
Installing CSSM...
CSSM Framework successfully installed
Installing IBMTP...
CSSM_Init failed
Exiting with bad rc = 65
Error: could not install IBMTP.
```

Figure 177. *Error message from the ocsf_install_basic_crypto* command

```
ICH408I USER(JRIVERA ) GROUP(WTCRES ) NAME(JORGE RIVERA )
BPX.SERVER CL(FACILITY)
INSUFFICIENT ACCESS AUTHORITY
ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )
```

Figure 178. Error message on MVS console

If you have Security Level 2 or 3 installed, perform the following step, too:

```
$ ocsf_install_strong_crypto
Installing IBMSWCSP...
Addin successfully installed.Installing CSSM...
```

Figure 179. ocsf_install_strong_crypto shell command

Now, run the installation verification procedures (IVP). This verifies that you have installed and configured correctly.

```

$ cd /usr/lpp/ocsf/ivp
$ ocsf_baseivp
Starting OCSF base addins ivp

Initializing CSSM
CSSM Initialized

Attaching ibmwkcsp

*****
* Portions of the IBM Software Cryptographic Service Provider or IBM *
* Weak Software Cryptographic Service Provider contain software *
* provided by RSA Data Security, Inc. Before use, see *
* /usr/lpp/ocsf/README.FIRST for required terms. *
*****
Attach successful, Detaching ibmwkcsp
Detach of ibmwkcsp successful

Attaching ibmcca
Attach successful, Detaching ibmcca
Detach of ibmcca successful

Attaching ibmcl
Attach successful, Detaching ibmcl
Detach of ibmcl successful

Attaching ibmcl2
Attach successful, Detaching ibmcl2
Detach of ibmcl2 successful

Attaching ibmdl2
Attach successful, Detaching ibmdl2
Detach of ibmdl2 successful

Attaching ibmtp
Attach successful, Detaching ibmtp
Detach of ibmtp successful

Attaching ibmtp2
Attach successful, Detaching ibmtp2
Detach of ibmtp2 successful

Completed OCSF base addins ivp

```

Figure 180. *ocsf_baseivp* shell command

If you have Security Level 2 or 3 installed, run the following script:

```

$ cd /usr/lpp/ocsf/ivp
$ ocsf_scivp
Starting OCSF strong crypto ivp

Initializing CSSM
CSSM initialized

Attaching ibmswmsp

*****
* Portions of the IBM Software Cryptographic Service Provider or IBM *
* Weak Software Cryptographic Service Provider contain software *
* provided by RSA Data Security, Inc. Before use, see *
* /usr/lpp/ocsf/README.FIRST for required terms. *
*****
Attach successful, Detaching ibmswmsp
Detach of ibmswmsp successful

Completed OCSF strong crypto ivp

```

Figure 181. ocsf_scivp shell command

11.2.3.5 Installing Open Cryptographic Enhanced Plug-Ins (OCEP)

Now we will install the OCSF plug-ins. For more information please see *OS/390 Security Server Open Cryptographic Enhanced Plug-ins Guide and Reference*, SA22-7429. Ensure that the installation process enables the OCEP code for program control.

If you have not defined the following RACF facility class profiles, issue the commands below to define them:

```

RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
SETROPTS CLASS(FACILITY) REFRESH

```

Give the FWKERN user ID permission to use the class profiles:

```

PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(FWKERN) ACC(READ)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(FWKERN) ACC(READ)
SETROPTS CLASS(FACILITY) REFRESH

```

Give permission to use the class profiles to the user ID that will install the code and run the IVP programs:

```

PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(userid) ACC(READ)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(userid) ACC(READ)
SETROPTS CLASS(FACILITY) REFRESH

```

Mark the OCSF enhanced plug-ins programs in the OCSF UNIX library as APF authorized and program controlled:

```

$ su
$ cd /usr/lpp/ocsf/addins
$ extattr +ap *.so
$ ls -E *.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1      450560  May 11 21:20  ibmcca.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1      589824  May 11 21:20  ibmc1.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     1474560  May 11 21:21  ibmc12.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     5701632  May 11 21:21  ibmdl2.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     6856704  May 11 21:20  ibmocepd1.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     425984  May 11 21:20  ibmoceptp.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     1138688  May 11 21:20  ibmswvsp.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1       57344  May 11 21:21  ibmtp2.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     3563520  May 11 21:21  ibmtp2.so
-rwxr-xr-x  aps  2  OMVSKERN  SYS1     1069056  May 11 21:21  ibmwkvsp.so

```

Figure 182. extattr shell command

Run the installation script from a UNIX System Services shell. To run this command, you must have superuser authority (UID=0).

```

$ cd /usr/lpp/ocsf/bin
$ ocep_install
Installing IBMOCEPTP...
Addin successfully installed.
Installing IBMOCEPDL...
Addin successfully installed.

```

Figure 183. ocep_install shell command

Now, run the Installation Verification Procedures (IVP). This verifies that you have installed and configured correctly.

```

$cd /usr/lpp/ocsf/ivp
$socep_ivp
Starting OCEP IVP

Initializing CSSM
CSSM Initialized

Attaching ibmocepd1
Attach successful, Detaching ibmocepd1
Detach of ibmocepd1 successful

Attaching ibmoceptp
Attach successful, Detaching ibmoceptp
Detach of ibmoceptp successful

Completed OCEP IVP

```

Figure 184. ocep_ivp shell command

11.2.3.6 ICSF/MVS authorization

OS/390 Firewall Technologies can take advantage of the encryption and decryption functions available in the new generation of System/390 processors. The firewall uses several of these functions in two ways:

- Encrypting and decrypting TCP/IP packet data in an IP tunnel.

- Encrypting signature data included as part of the ISAKMP message flows. This encryption is only performed when RSA signature mode authentication is requested and the associated certificate was defined using the `RACDCERT` command that specified the ICSF keyword.

This support is provided by the combination of the Integrated Cryptographic Feature (ICRF) on the processor and the Integrated Cryptographic Service Facility/MVS (ICSF/MVS) software product.

To use this support, ICSF/MVS must be started and running. It is preferable to do this prior to starting TCP/IP; however, it can also be done when TCP/IP is active.

Note: The remaining configuration is only applicable to the use of hardware crypto when encrypting and decrypting TCP/IP packet data in an IP tunnel.

If you plan to use this hardware crypto support and issue TCP/IP commands such as `OPING` from a user ID on the system where the firewall is running, this user ID must be permitted to access the ICSF/MVS cryptographic services (CSFSERV). This is because these are RACF controlled. Perform the following steps to set up profiles in the CSFSERV resource class and permit users to access these profiles:

Define the appropriate profiles in the CSFSERV class:

```
RDEFINE CSFSERV service-name UACC(NONE) other-optional-operands
```

The service names that the OS/390 Firewall Technologies uses are CSFCKI, CSFDEC1, CSFENC1, CSFRNG, CSFCKM, and CSFOWH1. Note that if triple DES hardware crypto support is not available on your S/390 processor, the CSFCKM service is not used.

Permit user access to these profiles:

```
PERMIT profile-name CLASS(CSFSERV) ID(yourid) ACCESS(READ)
```

Activate the CSFSERV class and refresh the in-storage RACF profiles. This is done by the RACF administrator.

```
SETROPTS CLASS(CSFSERV)
SETROPTS RACLIST(CSFSERV) REFRESH
```

The MAXLEN installation option for hardware crypto determines the maximum length that can be used to encrypt and decrypt data using ICSF/MVS. Set the MAXLEN ICSF/MVS installation option to greater than 65527 as this is the maximum TCP/IP packet size. For more information, refer to *Open Cryptographic Services Facility Application Developer's Guide and Reference*, SC24-5875.

11.2.4 OS/390 Firewall USS customization and starting

11.2.4.1 Copying shell scripts

OS/390 Firewall Technologies contains the following executable shell scripts:

```
fwlogmgmt
getmsg
```

Running shell scripts from locales that are not generated from code page IBM-1047 requires multiple copies of each shell script, one for each different locale's code page. You can use the `iconv` command to convert a shell script from

one code page to another. For example, to convert the fwlogmgmt script to the Da_DK.IBM-277 locale, enter the following command:

```
iconv -f IBM-1047 -t Da_DK.IBM-277 /usr/lpp/fw/bin/fwlogmgmt > /tmp/fwlogmgmt
```

For more information about the `iconv` command, see the *OS/390 UNIX System Services Command Reference*, SC28-1892.

For more information about customizing your locale, see the *OS/390 UNIX System Services User's Guide*, SC28-1891, and the *OS/390 UNIX System Services Planning*, SC28-1890.

11.2.4.2 Activate sample configuration files

It is important to preserve the owner, group, and mode settings when copying sample files. This can be done using the `-p` option of the `cp` command from a superuser (UID=0). For example:

```
cp -p /usr/lpp/fw/etc/security/fwrules.cfg /etc/security/fwrules.cfg
```

The following sample configuration files are shipped with OS/390 Firewall Technologies in `/usr/lpp/fw/etc`:

- `syslog.conf`: Logging server configuration file

To use this sample, copy it into the `/etc` directory.

If you do not install the sample `syslog.conf` file before IPLing your system and starting the firewall, an existing `syslog.conf` file will be used if one exists. If none exists, default logging will be in effect. Default logging sends all messages with a priority of error and above to the OS/390 operator console (to file `/dev/console`). You must create the special character file from a superuser by issuing:

```
mknod /dev/console c 9 0
```

See the *OS/390 UNIX System Services Command Reference*, SC28-1892, for further details on the `mknod` command.

In addition, the following files are shipped with OS/390 Firewall Technologies in `/usr/lpp/fw/etc/security`. They contain firewall default definitions:

- `fwaudio.cfg` - real audio configuration file
- `fwdaemon.cfg` - firewall servers configuration file
- `fwobjects.cfg` - Network objects configuration file
- `fwrules.cfg` - firewall configured filter rules configuration file
- `fwservices.cfg` - services configuration file
- `fwsocks.cfg` - SOCKS configuration file
- `logmgmt.cfg` - log management configuration file
- `fwahtran.cfg` - AH transform configuration file
- `fwesptran.cfg` - ESP transform configuration file
- `fwkeypol.cfg` - key policy configuration file
- `fwkeyprop.cfg` - key proposal configuration file
- `fwkeyring.cfg` - key ring configuration file
- `fwkeytran.cfg` - key transform configuration file

If you are not migrating from a previous release of OS/390 Firewall Technologies, you must copy these files into the /etc/security directory during installation, if they are not already there.

If you are migrating from a previous release, use the command `fwmigrate` to preserve your current configuration, and copy the following files into the /etc/security directory, if they are not already there. Also see *OS/390 Firewall Technologies Guide and Reference*, SC24-5835 for more information.

- fwahtran.cfg
- fwesptran.cfg
- fwkeypol.cfg
- fwkeyprop.cfg
- fwkeyring.cfg
- fwkeytran.cfg

Whether or not you are migrating from a previous release of OS/390 Firewall Technologies, you must copy the following files into the /etc/security directory during installation:

- fwguicmds.En_US
- fwguicmds.Ja_JP (if Japanese version is installed)

In our configuration we changed the file /etc/syslog.conf. Look at our configuration below:

```
BROWSE -- /etc/syslog.conf ----- Line 00000000 Col 001 034
Command ==>                               Scroll ==> CSR
***** Top of Data *****
#local0.* /tmp/firewall.local0.log
#local4.* /tmp/firewall.local4.log
#syslog.* /tmp/firewall.syslog.log
*.*      /tmp/firewall.all.log
***** Bottom of Data *****
```

Figure 185. SYSLOGD configuration file

Using this configuration all messages directed to the SYSLOGD server will be written in /tmp/firewall.all.log.

11.2.4.3 Defining firewall stack

To define the firewall stack we have to use the `fwstack` command in the UNIX System Services shell prompt:

```
$ fwstack cmd=add stack=tcpipb
```

Figure 186. Defining the TCPIPB stack to firewall kernel

In this release the firewall code can control many TCP/IP stacks in the same OS/390 image.

11.2.4.4 Configuring firewall servers

All the OS/390 Firewall Technologies servers run in their own address spaces. Servers are controlled by the control task running in the firewall kernel referred to as the FWKERN address space.

The FWKERN address space must be started before any of the servers are started. All requests to start, stop, or query the firewall servers (either collectively or individually) are made through the FWKERN control task through the `START`, `STOP`, or `MODIFY` commands, which you issue from the OS/390 operator console.

Use the `fwdaemon` command to list and change server configuration attributes, query server status, and start and stop servers.

At this time we only have to define four servers to the firewall stack. Go to the UNIX System Services shell prompt and use the `fwdaemon` command:

```
$ fwdaemon cmd=change daemon=syslogd started=yes
$ fwdaemon cmd=change daemon=fwstackd started=yes
$ fwdaemon cmd=change daemon=isakmpd started=yes
$ fwdaemon cmd=change daemon=cfgsrv started=yes \
  daemonopts="-f /etc/security/fwcfgsrv.kdb 1 -p 1014" 2
```

Figure 187. Defining firewall servers

1 Key database file for the SSL connection. When you create the key database for the firewall client, follow the steps in 11.2.4.6, “Firewall GUI configuration client” on page 263.

2 TCP/IP port number where the server will be listening.

11.2.4.5 Configuring filter rules for the configuration client

Now the firewall server has to be configured to support the configuration client connection. We have to define some filter rules to permit the connection to the secure interface. We have to create a filter rule to permit all connections through the secure interface or only permit some services, such as the configuration client service using port 1014. In our environment, we permit all types of traffic in the secure interface.

The following steps show how to customize a filter rule to permit all types of traffic to the secure interface(s). You have to go to the UNIX System Services shell environment using the authorized user ID defined previously and issue the following commands:

```

GIANCA @ RA03:/u/gianca>su ❶
GIANCA @ RA03:/u/gianca>fwfrule cmd=add name="R2612.Permit.All.Secure" \
  desc="Permit all in the Secure Interface" type=permit protocol=all \
  srcopcode=any srcport=0 destopcode=any destport=0 interface=secure \
  routing=local direction=both log=yes ❷
GIANCA @ RA03:/u/gianca>fwfrule cmd=list name="R2612.Permit.All.Secure"
  id = 529
  type = permit
  name = R2612.Permit.All.Secure
  desc = Permit all traffic in the secure interface
  protocol = all
  srcopcode = any
  srcport = 0 ❸
  destopcode = any
  destport = 0
  interface = secure
  routing = local
  direction = both
  log = yes
  tunnel =
  fragment =

```

Figure 188. Defining firewall configuration client rules

- ❶ To use the firewall commands you have to be in *superuser mode* or a member of the FWGRP group. Using the `su` command, you can change to the superuser mode.
- ❷ The `fwfrule` command creates a rule that allows any kind of traffic over the secure interface to the local host.
- ❸ List the rule you have created to get the ID. It will be used in the `fwservice` command.

```

GIANCA @ RA03:/u/gianca>fwservice cmd=create name="R2612.Permit.All.Secure" \
  desc="Permit all in the secure interface" rulelist=529/f,529/b ❹
GIANCA @ RA03:/u/gianca>fwservice cmd=list name="R2612.Permit.All.Secure"
  id = 509
  name = R2612.Permit.All.Secure
  desc = Permit all in the secure interface
  rulelist = 529/f,529/b
  log =
  fragment = ❺
  tunnel =
  time =
  month =
  day =
  weekday =
  timefilter =

```

Figure 189. Defining firewall configuration client services

- ❹ Create a service that contains the rule created previously.
- ❺ List the service you have created to get the ID. It will be used in the `fwconns` command.

```

GIANCA @ RA03:/u/gianca>fwnwobj cmd=add name="Network.9.0.0.0" \
  desc="IBM Intranet" type=network addr=9.0.0.0 mask=255.0.0.0 6
GIANCA @ RA03:/u/gianca>fwnwobj cmd=add name="Host.9.24.104.33" \
  desc="Host 9.24.104.33" type=host addr=9.24.104.33 mask=255.255.255.255 7
GIANCA @ RA03:/u/gianca>fwnwobj cmd=list name="Host.9.24.104.33"
  id = 501
  type = Host
  name = Host.9.24.104.33
  desc = Host 9.24.104.33
  addr = 9.24.104.33 8
  mask = 255.255.255.255
  startaddr =
  endaddr =

GIANCA @ RA03:/u/gianca>fwnwobj cmd=list name="Network.9.0.0.0"
  id = 502
  type = Network
  name = Network.9.0.0.0
  desc = IBM Intranet
  addr = 9.0.0.0
  mask = 255.0.0.0 9
  startaddr =
  endaddr =

```

Figure 190. Defining firewall configuration client Network objects

- 6 Create a Network object that represents your intranet. In this case, we used the IBM Intranet.
- 7 Create a Network object that represents the host where the firewall server is running.
- 8 List the Network object to get the ID. It will be used in the `fwconns` command.
- 9 List the Network object to get the ID. It will be used in the `fwconns` command.

```

GIANCA @ RA03:/u/gianca>fwconns cmd=create name="R2612.Permit.All.Secure" \
  desc="Permit all traffic over secure interface" source=502 \
  destination=501 servicelist=509 10
GIANCA @ RA03:/u/gianca>fwfilter cmd=update 11
ICAC1577i Processing firewall TCP/IP stack TCPIPB:

Filter support (level 2.80) initialized at 13:54:15 on Jul-06-1999

ICAC1531w Unable to inform the sock daemon to refresh configuration data. 12

```

Figure 191. Defining the connection for the firewall configuration client

- 10 Create a connection associating the two Network objects with the service.
- 11 Update the filter rules.
- 12 You will receive this warning message unless you have the SOCKS server running. If you do not need it, ignore this message.

Now you can start any type of connection with the host 9.24.104.33 using a workstation in the IBM Intranet.

All other configurations related to the IKE function will be made using the firewall configuration client GUI. For more information about the firewall command see *OS/390 Firewall Technologies Guide and Reference*, SC24-5835.

11.2.4.6 Firewall GUI configuration client

The firewall configuration server uses the Secure Sockets Layer (SSL) protocol of OS/390 for communication between the graphical user interface (GUI) clients and the server.

The administrator must run the GSKKYMAN utility to create a new key database, if one has not already been created. The administrator needs to use the Create a self-signed certificate option to create and store a Self-Signed Certificate Version 3, then use the store-encrypted database password option. See the *OS/390 Cryptographic Services System Secure Sockets Layer Programming Guide and Reference*, SC24-5877 for information on how to use the GSKKYMAN utility.

GSKKYMAN uses the DLLs that are installed with System SSL and must have access to these at run time. GSKKYMAN must also have access to the message catalogs; /bin includes a symbolic link to /usr/lpp/gskssl/bin/gskkyman, therefore, if your PATH environment variable contains this directory, you will find the GSKKYMAN utility. If your PATH environment variable does not contain this directory, add /usr/lpp/gskssl/bin to your PATH using the following command:

```
PATH=$PATH:/usr/lpp/gskssl/bin
```

/usr/lib/nls/msg/C and /usr/lib/nls/msg/En_US.IBM-1047 (and /usr/lib/nls/msg/Ja_JP for JCPT272 installations) include symbolic links to the message catalogs for gskkyman. If they do not include these links, add /usr/lpp/gskssl/lib/nls/msg to your NLSPATH using the following command:

```
export NLSPATH=$NLSPATH:/usr/lpp/gskssl/lib/nls/msg/%L/%N
```

This setting assumes that your environment has the LANG environment variable set to En_US.IBM-1047 (Ja_JP for JCPT272 installations that expect Japanese messages and prompts). If LANG is not set properly, set the NLSPATH environment variable using the following command:

```
export NLSPATH=$NLSPATH:/usr/lpp/gskssl/lib/nls/msg/En_US.IBM-1047/%N
```

Or for JCPT272 installations that expect Japanese messages and prompts, use the following command:

```
export NLSPATH=$NLSPATH:/usr/lpp/gskssl/lib/nls/msg/Ja_JP/%N
```

The DLLs for System SSL are installed into a partitioned data set (PDS). These DLLs are not installed into the LINKLIB or LPALIB by default. To access these DLLs, if they have not been placed in LINKLIB or LPALIB, you must set the STEPLIB environment variable to find the DLLs. Consult your system programmer for the high-level qualifier of the System SSL PDS. In the example below, the high-level qualifier for the System SSL PDS is GSK. In the following command, replace the value to match your installation:

```
export STEPLIB=GSK.SGSKLOAD
```

Use the GSKKYMAN utility to create a key database for the configuration server:

```
GIANCA @ RA03:/u/gianca/firewall>gskkyman

          IBM Key Management Utility

Choose one of the following options to proceed.

  1 - Create new key database
  2 - Open key database
  3 - Change database password

  0 - Exit program

Enter your option number: 1
Enter key database name or press ENTER for "key.kdb": fwcfgsrv.kdb
Enter password for the key database.....>
Enter password again for verification.....>
Should the password expire? (1 = yes, 0 = no) : 0

The database has been successfully created, do you want to continue to work with
the database now? (1 = yes, 0 = no) : 1                               Enter your
```

Figure 192. GSKKYMAN utility - main menu

Enter option 1 to create a new kdb file and press Enter. Type the key database name and press Enter. We used fwcfgsrv.kdb. Enter the password for the key database file twice (press Enter after you type the password). Do not forget this password because each time you have to access this kdb file you will be prompted to this particular password. Type 0 and press Enter to not use an expired password. Type 1 and press Enter to continue to work with this database.


```

Key database menu

Current key database is /u/gianca/firewall/os390/fwcfgsrv.kdb

1 - List/Manage keys and certificates
2 - List/Manage request keys
3 - Create new key pair and certificate request
4 - Receive a certificate issued for your request
5 - Create a self-signed certificate
6 - Store a CA certificate
7 - Show the default key
8 - Import keys
9 - Export keys
10 - List all trusted CAs
11 - Store encrypted database password

0 - Exit program

Enter option number (or press ENTER to return to the parent menu): 5
Enter version number of the certificate to be created (1, 2, or 3): 3
Enter a label for this key.....> Firewall GUI Key
Select desired key size from the following options (512):
1: 512
2: 1024
Enter the number corresponding to the key size you want: 1
Enter certificate subject name fields in the following.
Common Name (required).....> Firewall GUI Key
Organization (required).....> IBM
Organization Unit (optional).....> ITSO
City/Locality (optional).....> Cary
State/Province (optional).....> North Carolina
Country Name (required 2 characters)..> US
Enter number of valid days for the certificate : 365
Do you want to set the key as the default in your key database? (1 = yes, 0 = no
): 1
Do you want to save the certificate to a file? (1=yes, 0=no) : 0

Please wait while self-signed certificate is created...

Your request has completed successfully, exit gskkyman? (1=yes,0=no) : 0

```

Figure 193. GSKKYMAN: creating a self-signed certificate

Type 5 and press Enter to create a self-signed certificate. You can use another certificate importing a key into your database or creating a certificate request. For this case we used a self-signed certificate. Type 3 and press Enter to create a Version 3 certificate. The version number refers to the X.509 standard version number. Type a label for the key and press Enter. Type a common name and press Enter. Type an organization name and press Enter. All the other fields are optional. Then type the number of days this certificate should be valid and press Enter. We chose one year. Type 1 and press Enter to set this key as the default key in this database. Type 0 and press Enter to not save this certificate into a file. Type 0 and press Enter to return to the previous menu.

```
Key database menu

Current key database is /u/gianca/firewall/os390/fwcfgsrv.kdb

 1 - List/Manage keys and certificates
 2 - List/Manage request keys
 3 - Create new key pair and certificate request
 4 - Receive a certificate issued for your request
 5 - Create a self-signed certificate
 6 - Store a CA certificate
 7 - Show the default key
 8 - Import keys
 9 - Export keys
10 - List all trusted CAs
11 - Store encrypted database password

 0 - Exit program

Enter option number (or press ENTER to return to the parent menu): 11

The encrypted password has been stored in file /u/gianca/firewall/os390/fwcfgsrv
.sth

Your request has completed successfully, exit gskkyman? (1=yes, 0=no) >: 1
```

Figure 194. GSKKYMAN - storing an encrypted password

Type 11 and press Enter to store the encrypted database password in a stashed file. Finally, type 1 and press Enter to leave GSKKYMAN.

Now you have two files in the directory in which you were running GSKKYMAN: a kdb file and an sth file, whose file names in our example were fwcfgsrv.kdb and fwcfgsrv.sth respectively. The kdb file contains the keys and certificates you created and the sth file contains the database password. Copy these two files to the directory you specified in the fwdaemon daemonopts parameter for the CFGSRV server.

11.2.4.7 Start the firewall kernel

Before starting the firewall code you have to be sure that all previous configurations are available: the TCP/IP configuration, the BPXPRMxx configuration; ICA.SICALMOD and GSK.SGSKLOAD must be APF authorized and the firewall code at /usr/lpp/fw must be mounted and available. We insert both libraries in the LNKLSTxx to make them available to the firewall servers and to prevent updating many procedures.

You have to copy all members of the ICA.SICAPROC data set to a library in the JES concatenated started procedure libraries or concatenate this data set to JES.

How to start the firewall kernel is shown in Figure 195 on page 267:

```

S FWKERN
$HASP100 FWKERN ON STCINRDR
IEF695I START FWKERN WITH JOBNAME FWKERN IS ASSIGNED TO USER FWKERN
, GROUP OMVSGRP
$HASP373 FWKERN STARTED
IEF403I FWKERN - STARTED - TIME=16.16.38
ICAM1057i Release 2.8.0 Service Level 0000000. Created on Jun 22 1999.
$HASP100 ICAPSLOG ON STCINRDR
$HASP373 ICAPSLOG STARTED
IEF403I ICAPSLOG - STARTED - TIME=16.16.42
ICAM1069i Daemon SYSLOGD has been started.
$HASP100 ICAPCFGS ON STCINRDR
$HASP373 ICAPCFGS STARTED
IEF403I ICAPCFGS - STARTED - TIME=16.16.48
ICAM1069i Daemon CFGSRV has been started.
$HASP100 ICAPIKED ON STCINRDR
$HASP373 ICAPIKED STARTED
IEF403I ICAPIKED - STARTED - TIME=16.16.57
ICAM1069i Daemon ISAKMPD has been started.
$HASP100 ICAPSTAK ON STCINRDR
$HASP373 ICAPSTAK STARTED
IEF403I ICAPSTAK - STARTED - TIME=16.17.18
ICAM1069i Daemon FWSTACKD has been started.
ICAM1003i FWKERN initialization complete.

```

Figure 195. Starting FWKERN

To start the firewall kernel go to the OS/390 console and type `S FWKERN` and press Enter. FWKERN will start all the firewall servers configured previously. You have to check the message ICAM1003i to be sure that all servers were started successfully.

There are some console commands you can use to check the firewall status, to stop or start a firewall server, and to stop FWKERN.

Some examples are:

```

F FWKERN,QUERY ISAKMPD
ICAM1001i Firewall daemon ISAKMPD status is READY and process id is 145
335544366.
F FWKERN,QUERY SYSLOGD
ICAM1001i Firewall daemon SYSLOGD status is READY and process id is 147
33554455.
F FWKERN,QUERY FWSTACKD
ICAM1001i Firewall daemon FWSTACKD status is READY and process id is 149
50331695.
+JSX015 JESX SLU=RMT3 T011,RINCD=1000 LU NOT AVAILABLE
F FWKERN,QUERY CFGSRV
ICAM1001i Firewall daemon CFGSRV status is READY and process id is 152
67108917.
F FWKERN,QUERY LEVEL
ICAM1057i Release 2.8.0 Service Level 0000000. Created on Jun 22 1999.

```

Figure 196. Examples of FWKERN console commands

After starting the FWKERN check the socket connections that are open. You can use either the console command `Display TCPIP,TCPIPB,Netstat,SOCKETS` or the UNIX Shell command `netstat -p tcpipb -s`. We used the shell command:

```

GIANCA @ RA03:/u/gianca>netstat -p tcpipb -s
MVS TCP/IP onetstat CS V2R8          TCPIP Name: TCPIPB          14:36:43
Sockets interface status:
Type  Bound to          Connected to          State  Conn
====  =====          =====          =====  =====
Name: FTPD1      Subtask: 007E7390
Stream 0.0.0.0..21          0.0.0.0..0          Listen 00000048
Name: HODSRV3   Subtask: 007E4E78
Stream 0.0.0.0..8999          0.0.0.0..0          Listen 00000021
Name: HODSRV3   Subtask: 007E7390
Stream 0.0.0.0..8989          0.0.0.0..0          Listen 0000003C
Name: ICAPCFGS  Subtask: 007E7420
Stream 0.0.0.0..1014 1          0.0.0.0..0          Listen 0000014A
Name: ICAPIKED  Subtask: 007E7420
Dgram 9.24.104.33..500      *.*          UDP    0000014C
Dgram 192.168.100.100..500  *.* 2          UDP    0000014D
Dgram 172.16.233.4..500    *.*          UDP    0000014E
Name: ICAPSLOG  Subtask: 007E7420
Dgram 0.0.0.0..514 3          *.*          UDP    00000149
Name: TCPIPb    Subtask: 007D2AB0
Stream 0.0.0.0..9923          0.0.0.0..0          Listen 00000019
Name: TCPIPb    Subtask: 007D2CD0
Stream 0.0.0.0..8823          0.0.0.0..0          Listen 00000018
Name: TCPIPb    Subtask: 007D2E68
Stream 0.0.0.0..7723          0.0.0.0..0          Listen 00000017
Name: TCPIPb    Subtask: 007E1630
Stream 0.0.0.0..23           0.0.0.0..0          Listen 00000015
Name: TCPIPb    Subtask: 007E1AC8
Stream 0.0.0.0..6623          0.0.0.0..0          Listen 00000016
Name: TCPIPb    Subtask: 007E33F8
Stream 127.0.0.1..1025        127.0.0.1..1026      Estabsh 00000013
Stream 0.0.0.0..1025          0.0.0.0..0          Listen 0000000C
Name: TCPIPb    Subtask: 007E3BF8
Dgram 0.0.0.0..1252          *.*          UDP    000001FF
Name: TCPIPb    Subtask: 007EC1B0
Stream 127.0.0.1..1026        127.0.0.1..1025      Estabsh 00000012
Name: WEBSRV    Subtask: 007EC9B0
Stream 0.0.0.0..80           0.0.0.0..0          Listen 00000020

```

Figure 197. Report from netstat -p OS/390 UNIX command

- 1 This is the firewall server CFGSRV server listening on port 1014.
- 2 This is the firewall server ISAKMPD server waiting for UPD packets in all active interfaces on port 500.
- 3 This is the firewall server SYSLOGD server waiting for UDP packets in port 514.

Please see *OS/390 Firewall Technologies Guide and Reference*, SC24-5835 for more information about the commands and firewall configuration.

11.2.4.8 Installing firewall GUI configuration client

Now, we will install the GUI in a Windows 95 and Windows NT system. The GUI code is located in the /usr/lpp/fw/bin/fwtech.zip file. We have to move this code to the workstation using FTP or any other file transfer program. We did this using the FTP server in OS/390.

The workstation prerequisites to install the firewall GUI code are:

- Windows NT 4.0 or Windows 95

- A browser with Java and frames support
- A ZIP tool such as WinZip32 that handles long file names

Follow the steps below to install the GUI:

- Download the code /usr/lpp/fw/fwtech.zip to your workstation. Do not forget to transfer the code in binary format.
- Unzip the code and run the SETUP.EXE program.
- Follow the instructions given to install the code.

11.2.4.9 Using the configuration client

Start the GUI from the Windows start menu. You will see the following screen:

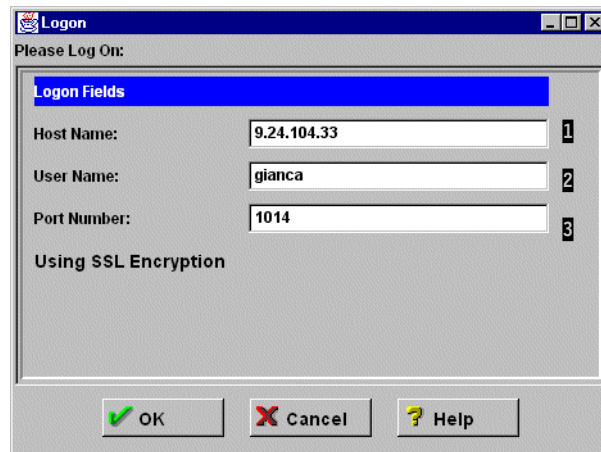


Figure 198. Firewall configuration client menu

- 1 This is the host IP address where the firewall is running.
- 2 The administrator user name you defined previously.
- 3 The port number you configured in the `FWDAEMON` command (-p parameter).

Note: Do not forget that this user must be permitted to the ICA.CFGSRV profile.

Click **OK** to continue. You will receive a password prompt:

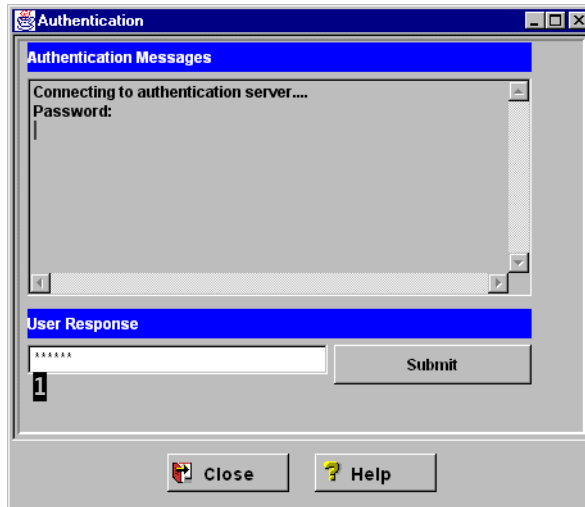


Figure 199. Firewall GUI password prompt

1 This is the RACF password for the user ID.

Click **Submit** to continue. Now you will see the firewall configuration client main screen:

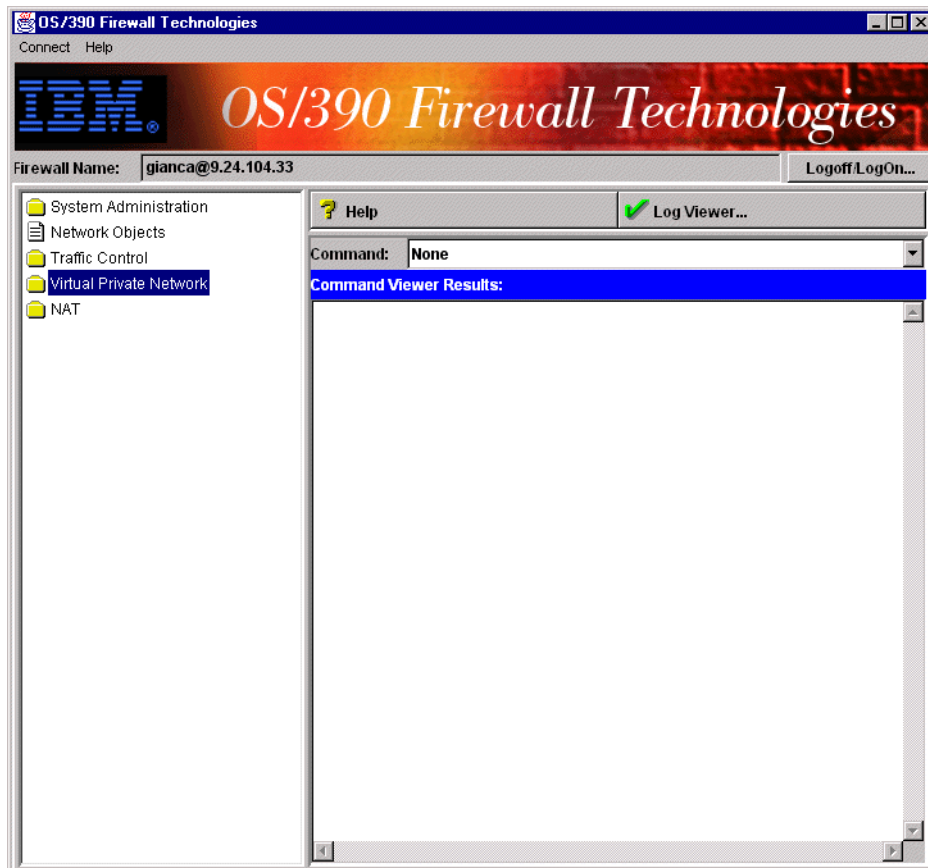


Figure 200. Firewall configuration client main screen

For more information about how to use the firewall configuration client see *OS/390 Firewall Technologies Guide and Reference, SC24-5835*.

11.3 Dynamic tunnel scenario

Before we start the Dynamic VPN configuration we have to exchange all IKE parameters with our tunnel partners. In this case we used three partners: one AS/400, one AIX system, and one Windows NT system running an IKE client.

The AS/400 and the Windows NT systems are located in the same subnetwork of OS/390. The AIX system is located in another subnetwork. The configuration client is located in another network. These three examples will show that the VPN Dynamic tunnels can be used in any type of network. It really does not matter if the endpoints of a VPN are in the same or different network. The VPN has to match your security issues. There are many cases when you would need a VPN inside your intranet. Look at Figure 201 to see our network scenario:

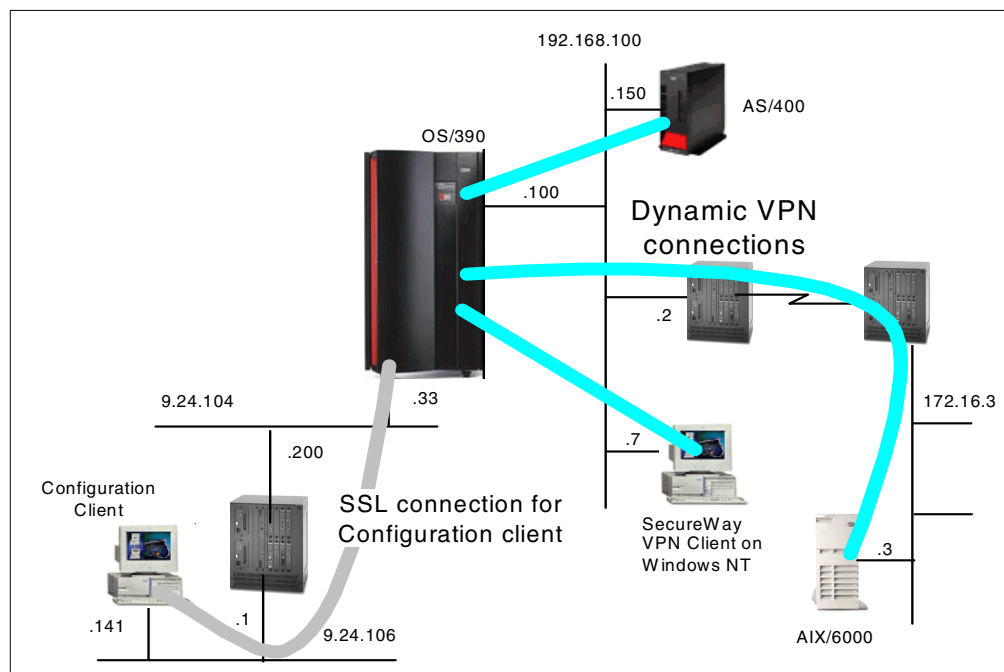


Figure 201. Network scenario of Dynamic VPN implementation

Look at the routing table in the TCPIP stack:

```
GIANCA @ RA03:/u/gianca>netstat -p tcpipb -r
MVS TCP/IP onetstat CS V2R8          TCPIP Name: TCPIPb          14:27:37
Destination      Gateway          Flags  Refcnt  Interface
-----
Defaultnet       192.168.100.2   G      000000  TR1B
9.24.104.0        0.0.0.0         U      000000  TR2B
9.24.106.0        9.24.104.200   UG     000001  TR2B
9.179.98.0        9.24.104.200   UG     000000  TR2B
172.16.233.3     0.0.0.0         UH     000000  EZASAMEMVS
172.16.233.28    0.0.0.0         UH     000000  EZAXCF28
172.16.233.39    0.0.0.0         UH     000000  EZAXCF39
192.168.10.0     9.24.104.5     UG     000000  TR2B
192.168.100.2    0.0.0.0         UH     000000  TR1B
192.168.100.150  0.0.0.0         UH     000001  TR1B
```

Figure 202. IKE function scenario - TCPIPb routing table

Now take a look at the sockets connection. Note that the IKE server is listening over all interfaces:

```
D TCPIP,TCPIPb,N,CON
EZZ2500I NETSTAT CS V2R8 TCPIPb 235
USER ID  CONN      LOCAL SOCKET      FOREIGN SOCKET      STATE
ICAPCFGS 000000F8 0.0.0.0..1014    0.0.0.0..0         LISTEN
INETD1   00000020 0.0.0.0..109     0.0.0.0..0         LISTEN
INETD1   0000001E 0.0.0.0..2023    0.0.0.0..0         LISTEN
INETD1   0000001F 0.0.0.0..110     0.0.0.0..0         LISTEN
TCPIPb   00000015 0.0.0.0..7723    0.0.0.0..0         LISTEN
TCPIPb   00000016 0.0.0.0..8823    0.0.0.0..0         LISTEN
TCPIPb   00000011 127.0.0.1..1026  127.0.0.1..1025    ESTABL
TCPIPb   00000014 0.0.0.0..6623    0.0.0.0..0         LISTEN
TCPIPb   00000012 127.0.0.1..1025  127.0.0.1..1026    ESTABL
TCPIPb   00000017 0.0.0.0..9923    0.0.0.0..0         LISTEN
TCPIPb   0000000C 0.0.0.0..1025    0.0.0.0..0         LISTEN
WEBSRVB  000000AF 0.0.0.0..80      0.0.0.0..0         LISTEN
ICAPIKED 000029C7 192.168.100.100..500  *.*                UDP
ICAPIKED 000029C6 9.24.104.33..500    *.*                UDP
ICAPIKED 000029C8 172.16.233.4..500  *.*                UDP
ICAPSLOG 000029C3 0.0.0.0..514      *.*                UDP
TCPIPb   00000100 0.0.0.0..1183    *.*                UDP
16 OF 16 RECORDS DISPLAYED
```

Figure 203. Report from NETSTAT CON command

We created a planning worksheet to be used to exchange the information. Look at the tables below:

Table 47. VPN planning worksheet - S/390 and AS/400

| VPN parameter | Value |
|---|-----------------|
| Key Policy, Proposal, Transform: | |
| Initiator Negotiation | Main |
| Responder Negotiation | Main |
| Authentication Method | Pre-Shared Keys |
| Hash Algorithm | MD5 |
| Encryption Algorithm | DES_CBC_8 |

| VPN parameter | Value |
|---|-----------------|
| Diffie-Hellman Group | Group 1 |
| Maximum Key Lifetime | 1440 |
| Maximum Size Limit | 1000 |
| Key Lifetime Range | 60-1440 |
| Size Limit Range | 1-1000 |
| Data Policy, Proposal, AH and ESP Transform: | |
| Perfect Forward Secrecy (PFS) | Group 1 |
| 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 |
| ESP Maximum Size Limit | 50000 |
| ESP Data Lifetime Range | 60-480 |
| ESP Size Limit Range | 1-50000 |
| 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 |
| Certificate Authority: | |
| Raccdert Label | Not applicable |
| Key Ring: | |
| User ID | Not applicable |
| Key Ring Name | Not applicable |
| Dynamic Connection: | |
| Source | 192.168.100.100 |

| VPN parameter | Value |
|---------------------------|-----------------|
| 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 |

Table 48. VPN planning worksheet - S/390 and RS/6000

| VPN parameter | Value |
|---|-----------------|
| Key Policy, Proposal, Transform: | |
| Initiator Negotiation | Main |
| Responder Negotiation | Main |
| Authentication Method | Pre-Shared Keys |
| Hash Algorithm | MD5 |
| Encryption Algorithm | DES_CBC_8 |
| Diffie-Hellman Group | Group 1 |
| Maximum Key Lifetime | 1440 |
| Maximum Size Limit | 0 |
| Key Lifetime Range | 60-1440 |
| Size Limit Range | 0-0 |
| Data Policy, Proposal, AH and ESP Transform: | |
| Perfect Forward Secrecy (PFS) | None |
| 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 |

| VPN parameter | Value |
|------------------------------------|------------------|
| ESP Authentication Algorithm | HMAC_MD5 |
| ESP Encryption Algorithm | DES_CBC_8 |
| ESP Maximum Data Lifetime | 60 |
| ESP Maximum Size Limit | 0 |
| ESP Data Lifetime Range | 60-480 |
| ESP Size Limit Range | 0-0 |
| Dynamic Tunnel Policy: | |
| Initiation | Either |
| Connection Lifetime | 0 |
| Authentication Information: | |
| Remote Key Server | 172.16.3.3 |
| Authentication Method | Pre-Shared Keys |
| Shared Key | 3132333435363738 |
| Certificate Authority: | |
| Racdcert Label | Not applicable |
| Key Ring: | |
| User ID | Not applicable |
| Key Ring Name | Not applicable |
| Dynamic Connection: | |
| Source | 192.168.100.100 |
| Destination | 172.16.3.3 |
| Source Port | 0 |
| Destination Port | 0 |
| Automatic Activation | No |
| Protocol | All |
| Remote Key Server | 172.16.3.3 |
| 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 | 172.16.3.3 |

Table 49. VPN planning worksheet - S/390 and Windows NT (SecureWay VPN client)

| VPN parameter | Value |
|---|-----------------|
| Key Policy, Proposal, Transform: | |
| Initiator Negotiation | Main |
| Responder Negotiation | Main |
| Authentication Method | Pre-Shared Keys |
| Hash Algorithm | MD5 |
| Encryption Algorithm | DES_CBC_8 |
| Diffie-Hellman Group | Group 1 |
| Maximum Key Lifetime | 1440 |
| Maximum Size Limit | 0 |
| Key Lifetime Range | 1-1440 |
| Size Limit Range | 0-0 |
| Data Policy, Proposal, AH and ESP Transform: | |
| Perfect Forward Secrecy (PFS) | None |
| 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 | 480 |
| ESP Maximum Size Limit | 0 |
| ESP Data Lifetime Range | 1-480 |
| ESP Size Limit Range | 0-0 |
| Dynamic Tunnel Policy: | |
| Initiation | Either |
| Connection Lifetime | 0 |
| Authentication Information: | |
| Remote Key Server | 192.168.100.7 |
| Authentication Method | Pre-Shared Keys |

| VPN parameter | Value |
|-------------------------------|------------------|
| Shared Key | 3132333435363738 |
| Certificate Authority: | |
| Raddcert Label | Not applicable |
| Key Ring: | |
| User ID | Not applicable |
| Key Ring Name | Not applicable |
| Dynamic Connection: | |
| Source | 192.168.100.100 |
| Destination | 192.168.100.7 |
| Source Port | 0 |
| Destination Port | 0 |
| Automatic Activation | No |
| Protocol | All |
| Remote Key Server | 192.168.100.7 |
| 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 | 192.168.100.7 |

Specify the information as part of the planning for your dynamic VPN tunnels. Create a worksheet for each TCP/IP stack planned to be configured with a dynamic tunnel.

Following we have an example of a cross-reference table utilized to match the parameters between the OS/390 and AS/400 systems:

Table 50. S/390 and AS/400 system VPN 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) Responder Negotiation = Main |
| Responder Negotiation = Main Mode only | (3) Authentication Method = Pre-Shared Keys |
| Key Protection Transforms | (5) Hash Algorithm = MD5 |
| Authentication Method = Pre-shared key | (6) Encryption Algorithm = DES_CBC_8 |
| Pre-shared key value = abcd | (7) Diffie-Hellman Group = Group 1 |
| Hash Algorithm = MD5 | (8) Maximum Key Lifetime = 1440 |
| Encryption Algorithm = DES-CBC | (9) Maximum Size Limit = 1000 |
| Diffie-Hellman Group = Default 768-bit MODP | Key Lifetime Range = 60-1440 |
| Key Management | Size Limit Range = 1-1000 |
| Maximum key lifetime (minutes) = 1440 | (13) Data Policy, Proposal, ESP Transform |
| Maximum size limit (kilobytes) = 1000 | (10) (11) PFS (Perfect Forward Secrecy) = Group 1 |
| Data Policy | (12) ESP Encapsulation Mode = Transport |
| Name = HtoH4AtoMFBS | (14) ESP Authentication Algorithm = HMAC_MD5 |
| Use Diffie-Hellman Perfect Forward Secrecy = Yes | (15) ESP Encryption Algorithm = DES_CBC_8 |
| Diffie-Hellman Group = Default 768-bit MODP | (16) ESP Maximum Data Lifetime = 60 |
| Data Protection Proposals | (17) ESP Maximum Size Limit = 50000 |
| Encapsulation mode = Transport | ESP Data Lifetime Range = 60-480 |
| Protocol = ESP | ESP Size Limit Range = 1-50000 |
| Algorithms | Dynamic Tunnel Policy |
| Authentication Algorithm = | (22) Initiation = Either |
| HMAC-MD5 | (23) Connection Lifetime = 0 |
| Encryption Algorithm = DES-CBC | Local Key Server |
| Key Expiration | Key Server Identity |
| Expire after (minutes) = 60 | (18) Authentication Identifier Type = IPv4 |
| Expire at size limit (kilobytes) = 50000 | (19) Authentication Identifier = 192.168.100.100 |
| Key Connection Group | Key Server Location |
| Name = HtoH4AtoMF | (19) IP address = 192.168.100.100 |
| Remote Key Server | Remote Key Server |
| Identifier Type = Version 4 IP address | Key Server Identity |
| IP address = 192.168.100.100 | (20) Authentication Identifier Type = IPv4 |
| Local Key Server | (21) Authentication Identifier = 192.168.100.150 |
| Identifier Type = Version 4 IP address | Key Server Location |
| IP address = 192.168.100.150 | (21) IP address = 192.168.100.150 |
| Key Policy = HtoH4AtoMFBS | Authentication Information |
| Dynamic Key Group | (3) Authentication Method = Pre-Shared Keys |
| Name = HtoH4AtoMF | (4) Shared Key = 61626364 |
| System Role = Both systems are hosts | Dynamic Connection |
| Initiation = Either systems can initiate the connection | (25) Source = 192.168.100.100 |
| Policy | (24) Destination = 192.168.100.150 |
| Data Management Security Policy = HtoH4AtoMFBS | (28) Source port = 0 |
| Connection Lifetime = Never expires | (27) Destination port = 0 |
| Local addresses = Filter rule | Automatic activation = No |
| Local ports = Filter rule | Protocol = All |
| Remote addresses = Filter rule | (26) Remote Key Server = 192.168.100.150 |
| Remote ports = Filter rule | (21) |
| Protocol = Filter rule | |
| Dynamic Key Connection | |
| Name = HtoH4AtoMFL1 | |
| Key Connection Group = HtoH4AtoMF | |
| Start when TCP/IP is started? = No | |
| IP Filters | |
| Name = HtoH4ASoMF3ip | |
| IPSEC rule | |
| Source address name = 192.168.100.150 | (24) |
| Destination address name = 192.168.100.100 | (25) |
| Connection name = HtoH4AtoMF | |
| Services | |
| Protocol = * | (26) |
| Source port = * | (27) |
| Destination port = * | (28) |

These tables are very useful because the Dynamic VPN definitions have many parameters. Using these tables can save a lot of time defining the VPN connection.

To create a Dynamic VPN connection we have to create all the objects listed in the figure below:

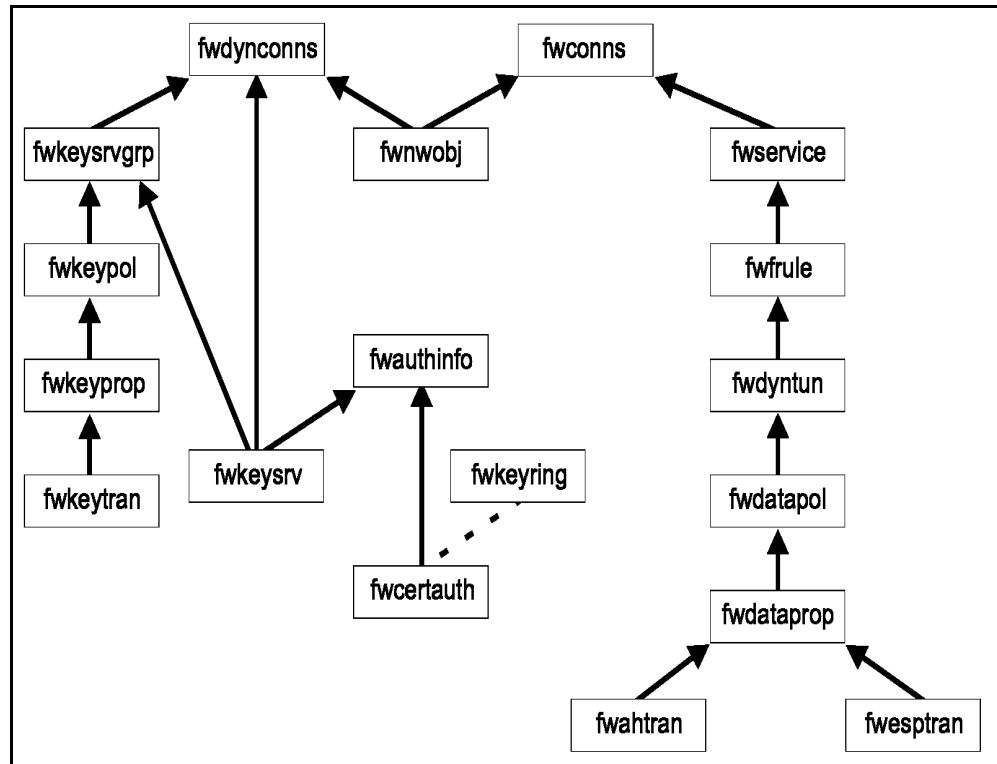


Figure 204. Firewall IKE objects relationship

- fwesptran: ESP transform object
- fwahtran: AH transform object
- fwdataprop: Data Proposal object
- fwdatapol: Data Policy object
- fwdyntun: Dynamic Tunnel Policy object
- fwfrule: Filter Rule object
- fwservice: Service object
- fwconns: Connection object
- fwnwobj: Network object
- fwdynconns: VPN Dynamic Connection object
- fwkeysvrgrp: Key Server Group object
- fwkeypol: Key Policy object
- fwkeyprop: Key Proposal object
- fwkeytran: Key Transform object
- fwkeysvr: Key Server object

- fwauthinfo: Authentication Information object
- fwcertauth: Certificate Authority object
- fwkeyring: Key Ring object

Figure 204 on page 279 shows the relationship between objects when you are defining a dynamic tunnel. Note that, in a particular configuration, not all objects have to be configured. For detailed information on these objects, consult *OS/390 Firewall Technologies Guide and Reference*, SC24-5835.

11.3.1 Creating a dynamic VPN connection using the GUI panels

Now we will use Table 47 on page 272 to create all VPN definitions that are necessary for these specific connections: OS/390 and OS/400.



Figure 205. Firewall configuration client main screen - dynamic VPN definition

Log on to the configuration client. At the main screen double-click **Traffic Control**, then expand the **Connection Templates** tree. Double-click **Virtual Private Networks**, then expand the **Dynamic** tree, expand the **VPN Key Servers** tree, expand the **Authentication** and **VPN Connection Templates** trees. Now

expand the **Data Management** and **Key Management** trees. You will see the screen above.

11.3.1.1 Key Management definition

We will start defining the Key Management object. We have to create a Key Transform object, and then associate it to a Key Proposal. Next we have to define a Key Policy using the Key Proposal. Follow the steps below:

The screenshot shows a dialog box titled "[9.24.104.33] Add Key Transform". It is divided into several sections:

- Identification:** Key Transform Name: R2612 AS/400 Key Transform; Description: R2612 AS/400 Key Transform
- Key Transform Composition:** Protocol: IKE; Authentication Method: Pre-shared Keys; Hash Algorithm: MD5; Encryption Algorithm: DES_CBC_8; Diffie-Hellman Group: Group 1
- Initiator Session Expiration:** Maximum Key Lifetime: 1440; Maximum Size Limit: 1000
- Responder Session Expiration:** Key Lifetime Range: 60 - 1440; Size Limit Range: 1 - 1000

Buttons at the bottom: OK, Cancel, Help.

Figure 206. Adding Key Transform on OS/390

At the main screen double-click **Key Transform** and at the next screen double-click **NEW** to add a Key Transform. You will see the screen above. Please fill in the fields as shown using Table 47 on page 272 and click **OK**. Now click **Close** and return to the main screen.

Key Transform

The Key Transform object defines the protection mechanisms used to secure subsequent exchanges between key servers. Key transforms specify how to use the Internet Key Exchange (IKE) protocol and include an authentication method and algorithm, a Diffie-Hellman group, and an encryption algorithm.

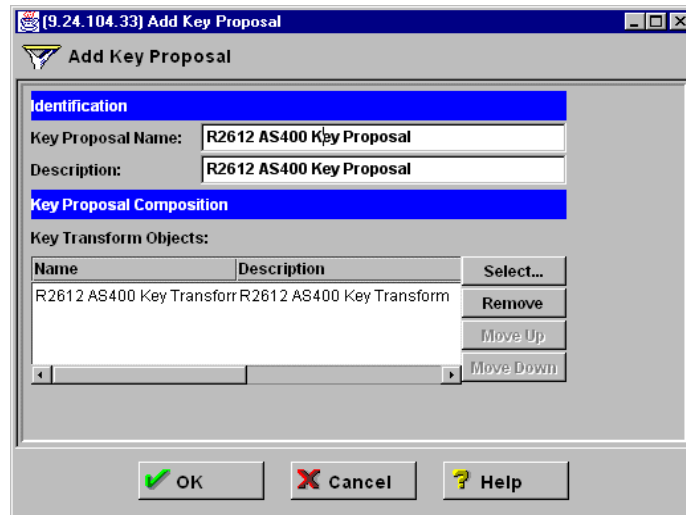


Figure 207. Adding Key Proposal on OS/390

At the main screen double-click **Key Proposal**, then double-click **NEW** to add a Key Proposal. You will see the screen above. Click **Select ...** and choose the Key Transform created in Figure 206 on page 281. Please fill in the fields as shown above and click **OK**. Now click **Close** and return to the main screen.

Key Proposal

The Key Proposal object contains an ordered list of key transforms that will be proposed during key management negotiation. This ordering is important when acting as an initiator of a dynamic connection. In this case, the key transforms are sent to the remote key server in the initiator's order of preference as defined in the key proposal definition. When acting as responder, the initiator's ordering takes precedence.

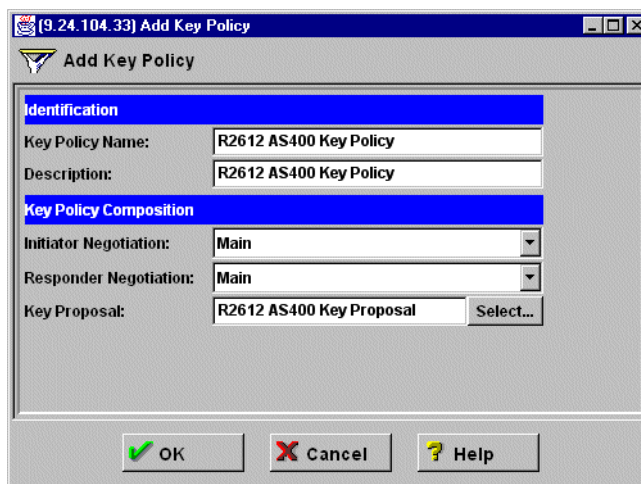


Figure 208. Adding Key Policy on OS/390

Now, at the main screen, double-click **Key Policy**, then double-click **NEW** to add a Key Policy. You will see the screen above. Please fill in the fields as shown in Table 47 on page 272. Click **Select ...** and choose the Key Proposal defined in

Figure 207 on page 282. Then click **OK**. At the next screen click **Close** and return to the main screen.

Key Policy

The Key Policy object contains the information required when initiating or responding to a key management security negotiation. The Key Policy defines this system's initiator and responder negotiation modes and the key proposal.

11.3.1.2 Data Management definition

Now we will define the Data Management objects. We have to define an AH and ESP Transform object, associate them to a Data Proposal object and then create a Data Policy using the Data Proposal object. Follow the steps below:

The screenshot shows a dialog box titled "[9.24.104.33] Add ESP Transform". It has a title bar with standard window controls. The main area is divided into several sections with blue headers: "Identification", "ESP Transform Composition", "Initiator Session Expiration", and "Responder Session Expiration". Each section contains input fields and dropdown menus. At the bottom, there are three buttons: "OK" with a green checkmark, "Cancel" with a red X, and "Help" with a question mark.

Figure 209. Adding ESP Transform on OS/390

At the main screen, double-click **ESP Transform**, then double-click **NEW** to add an ESP Transform. You will see the screen above. Please fill in the fields as shown in Table 47 on page 272. Then click **OK**. At the next screen click **Close** and return to the main screen.

ESP Transform

The ESP Transform object defines protection mechanisms used to secure exchanges between the data endpoints through encryption and optionally with authentication.

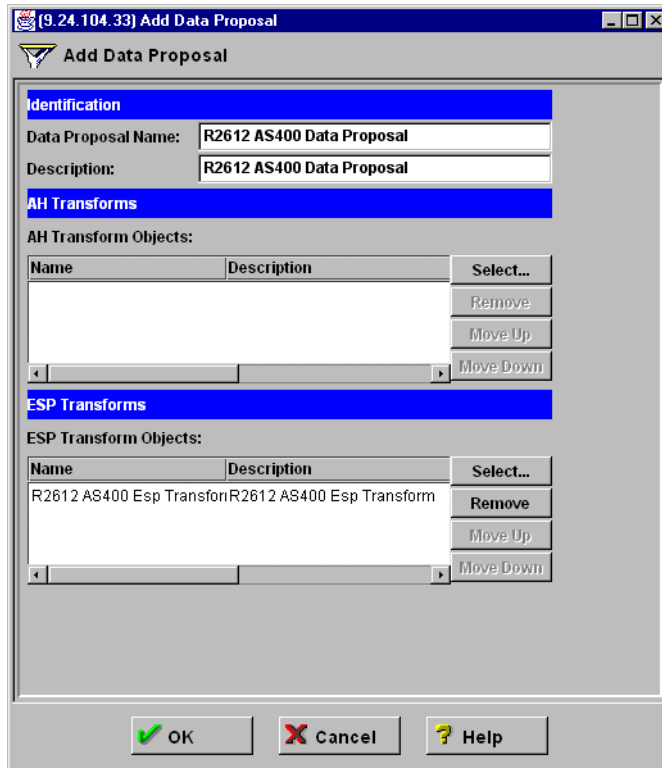


Figure 210. Adding Data Proposal on OS/390

At the main screen, double-click **Data Proposal**, then double-click **NEW** to add a Data Proposal. You will see the screen above. Please fill in the fields as shown. In this particular case we are not using AH Transform objects. In the ESP Transforms section click **Select ...** and choose the ESP Transform created in Figure 209 on page 283. Then click **OK**. At the next screen click **Close** and return to the main screen.

Data Proposal

The Data Proposal contains ordered lists of AH and ESP transforms used when negotiating a security association for data transmission. This ordering is important when acting as an initiator of a dynamic connection. In this case the ESP and AH transforms are sent to the remote key server in the initiator's order of preference as defined in the data proposal definition. When acting as responder, the initiator's ordering takes precedence.

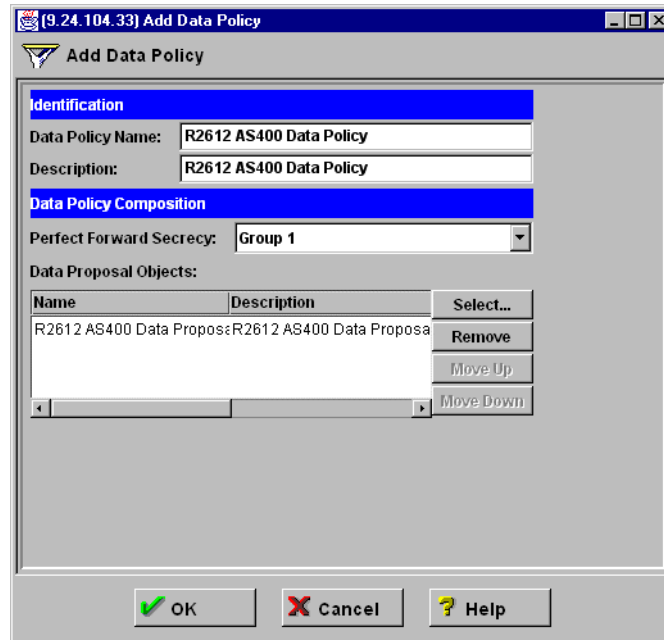


Figure 211. Adding Data Policy on OS/390

At the main screen, double-click **Data Policy**, then double-click **NEW** to add a Data Policy. You will see the screen above. Please fill in the fields as shown using Table 47 on page 272. Click **Select ...** and choose the Data Proposal created in Figure 210 on page 284. Then click **OK**. At the next screen click **Close** and return to the main screen.

Data Policy

The Data Policy object defines information required when negotiating keys for data exchanges. This information includes the perfect forward secrecy selection and list of data proposals. The ordering is important when acting as an initiator of a dynamic connection. In this case, the policies are sent to the remote key server in the initiator's order of preference as defined in the data policy definition. When acting as responder, the initiator's ordering takes precedence.

11.3.1.3 Dynamic Tunnel Policy definition

The Dynamic Tunnel Policy object will be associated with an anchor filter Rule object. To define the Dynamic Tunnel Policy object complete the following steps:

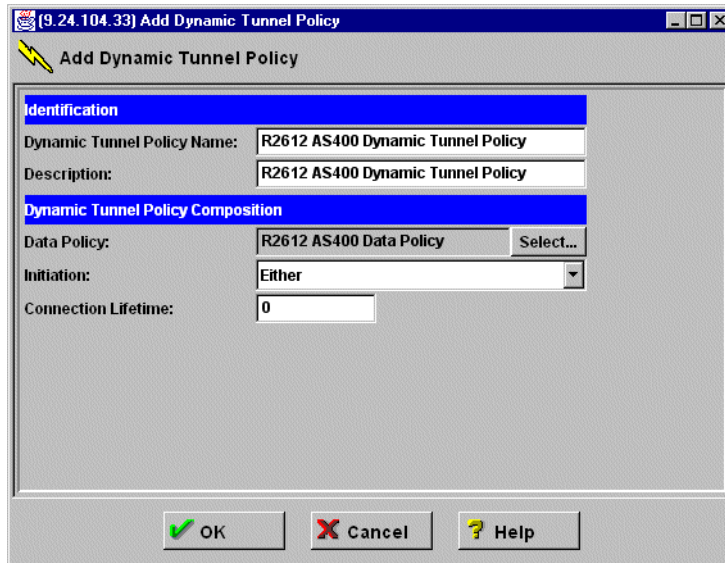


Figure 212. Adding Dynamic Tunnel Policy on OS/390

At the main screen, double-click **Dynamic Tunnel Policy**, then double-click **NEW** to add a Dynamic Tunnel Policy. You will see the screen above. Please fill in the fields as shown in Table 47 on page 272. Click **Select ...** and choose the Data Policy created in Figure 211 on page 285. Then click **OK**. At the next screen click **Close** and return to the main screen.

Dynamic Tunnel Policy

The Dynamic Tunnel Policy object defines generic information relative to a set of tunnels. This information includes the Data Policy object, Initiation role, and Connection Lifetime to use. Dynamic Tunnel Policy objects will be specified in filter Rule objects.

11.3.1.4 Key Server definitions

Now we will define the Key Server objects. We have to define two Key Server objects: the Local Key Server (OS/390) and the Remote Key Server (AS/400). Then, we have to define a Key Server Group using the Key Server definitions. Complete the following steps:

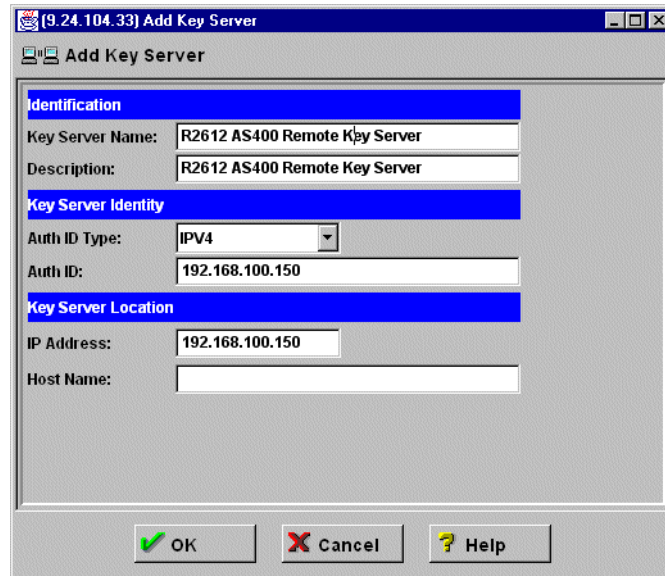


Figure 213. Adding Remote Key Server on OS/390

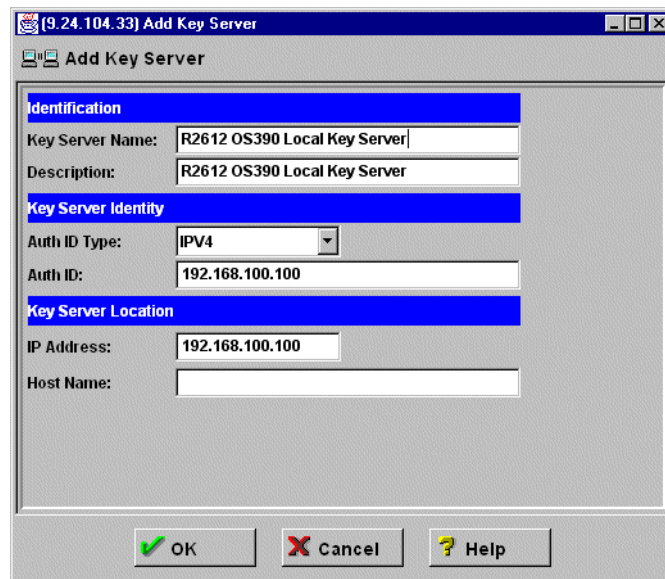


Figure 214. Adding Local Key Server on OS/390

At the main screen, double-click **Key Server**, then double-click **NEW** to add a Key Server. You will see the screen in Figure 213. Please fill in the fields as shown in Table 47 on page 272 for the Remote Key Server definition, then click **OK**. Again, double-click **NEW** to add a Key Server. You will see the screen in Figure 214. Please fill in the fields as shown in Table 47 on page 272 for the Local Key Server definition. Then click **OK**. At the next screen click **Close** and return to the main screen.

Key Server

The Key Server object defines information about key servers. Key servers negotiate security associations using the Internet Security Association Key Management Protocol (ISAKMP). A Key Server object defines an authentication identity by which a key server is known. A key server may have multiple identities.

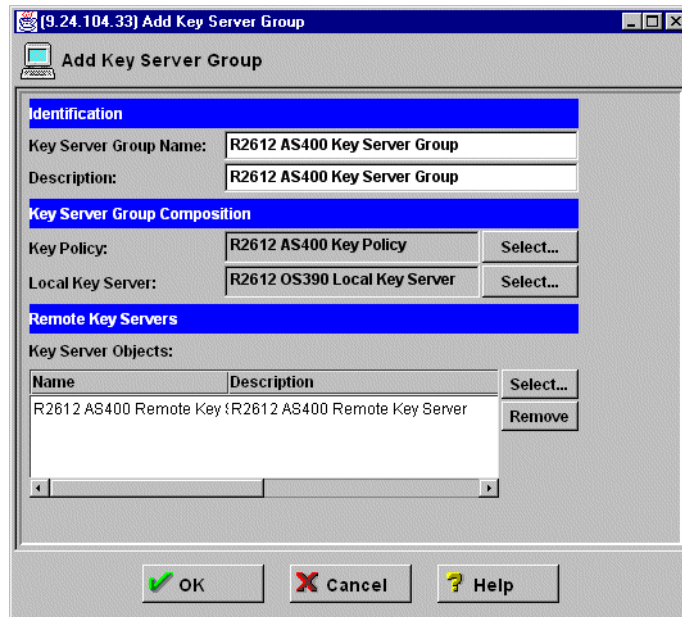


Figure 215. Adding Key Server Group on OS/390

At the main screen, double-click **Key Server Group**, then double-click **NEW** to add a Key Server Group. You will see the screen above. Click **Select ...** beside Key Policy and choose the Key Policy created in Figure 208 on page 282. Click **Select ...** beside Local Key Server and choose the Local Key Server created in Figure 214 on page 287. Click **Select ...** under Remote Key Servers and choose the Remote Key Server created in Figure 213 on page 287. Then click **OK**. At the next screen click **Close** and return to the main screen.

Key Server Group

The Key Server Group object defines information about key server groups. A key server group is an association of a local key server with a list of remote key servers. This establishes which combinations of local and remote key servers can negotiate key management security associations and the key policy that will be used during these negotiations. Key server groups are ordered among themselves. Searches will find the first instance of the key server found in all key server group objects. Therefore, the key server groups must be ordered. Key server group objects will be specified in dynamic VPN connection objects.

11.3.1.5 Authentication Information definition

Here we will define the Authentication Information definition object. The Remote Key Server will be authenticated by following these steps:

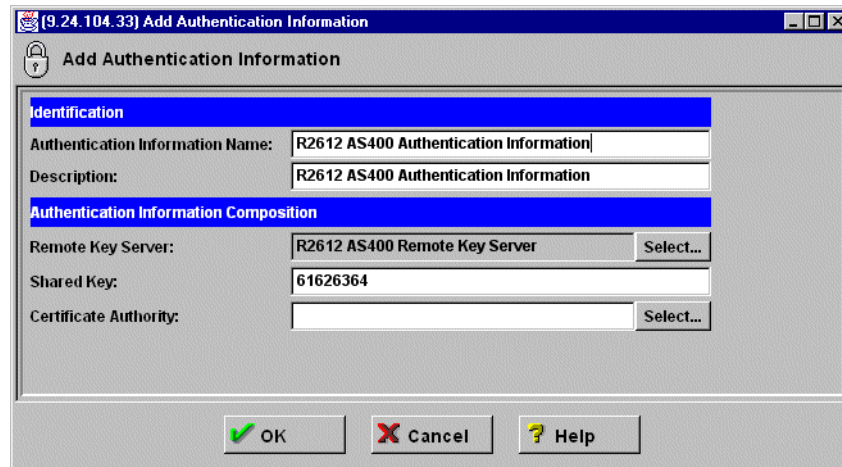


Figure 216. Adding Authentication Information on OS/390

At the main screen, double-click **Authentication Information**, then double-click **NEW** to add Authentication Information. You will see the screen above. Please fill in the fields as shown in Table 47 on page 272. Click **Select ...** and choose the Remote Key Server created in Figure 213 on page 287. Then click **OK**. At the next screen click **Close** and return to the main screen.

Note: The shared key must be entered as an even number of hex digits up to a length of 900 digits. The key 61626364 defined above is abcd in ASCII format.

Authentication Information

The Authentication Information object defines information required to authenticate the identity of the communicating peer. This information includes the remote key server object and the pre-shared key and/or certificate authority to use with it. Authentication information will be used when a dynamic connection is activated. The shared-key will always be typed in binary format (hexadecimal characters). The characters 61626364 in ASCII mean abcd.

11.3.1.6 Dynamic VPN Connection definition

Now we will define the Dynamic VPN Connection definition. We will associate the Network objects from both endpoints of the tunnel to the Remote Key Server and Key Server Group. Please complete the following steps:

We have to create two Network objects identifying the AS/400 and OS/390 systems:

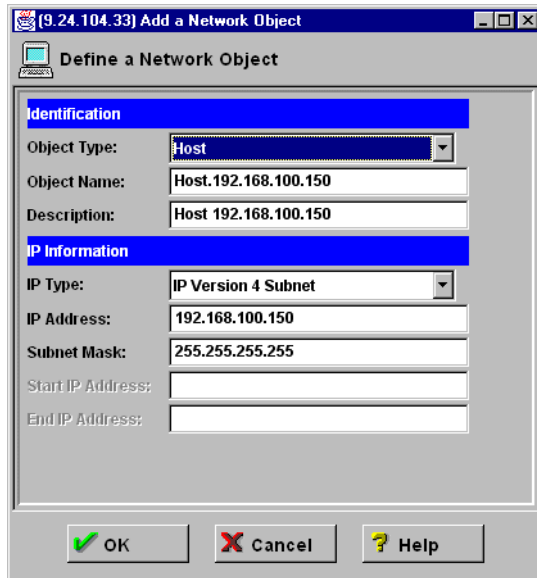


Figure 217. Adding Network object for AS/400

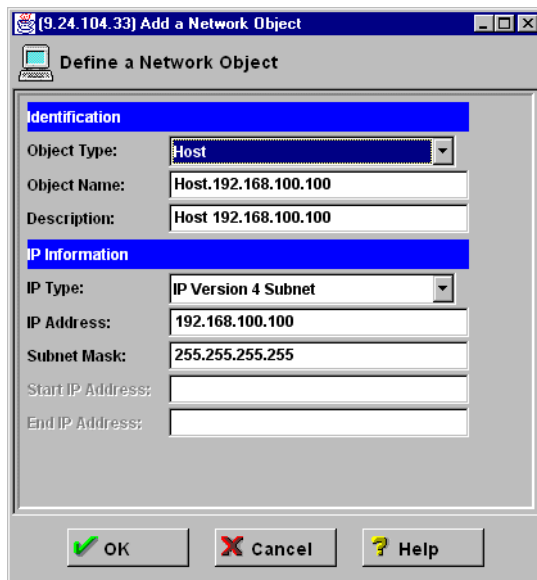


Figure 218. Adding Network object for OS/390

At the main screen, double-click **Network Objects**, then double-click **NEW** to add a Network object. You will see the screen in Figure 217. Please fill in the fields as shown. Then click **OK**, then double-click **NEW** to add a Network object. You will see the screen in Figure 218. Please fill in the fields as shown. Click **OK**. At the next screen click **Close** and return to the main screen.

Network Object

The Network Objects function allows you to maintain information about network addressable components on your network. This function acts as a central repository for use by other functions in the OS/390 system. Primarily, Network objects are used to designate source and destination addresses when you create your connections.

Now we will define the connection:

| Identification | |
|------------------------------|---|
| Dynamic VPN Connection Name: | R2612 AS400 Dynamic VPN Connection |
| Description: | R2612 AS400 Dynamic VPN Connection |
| Source: | Host.192.168.100.100 Select... |
| Destination: | Host.192.168.100.150 Select... |

| Dynamic VPN Connection Composition | |
|------------------------------------|--|
| Source Port: | 0 |
| Destination Port: | 0 |
| Automatic Activation: | No |
| Protocol: | all |
| Remote Key Server: | R2612 AS400 Remote Key Server Select... |
| Key Server Group: | R2612 AS400 Key Server Group Select... |

Figure 219. Adding Dynamic VPN connection on OS/390

At the main screen, double-click **VPN Connection Setup**, then double-click **NEW** to add a Dynamic VPN Connection. You will see the screen above. Please fill in the fields as shown in Table 47 on page 272. Click **Select ...** beside Source and choose the OS/390 Network object created in Figure 218 on page 290. Click **Select ...** beside Destination and choose the AS/400 Network object created in Figure 217 on page 290. Click **Select ...** beside Remote Key Server and choose the Remote Key Server created in Figure 213 on page 287. Click **Select ...** beside Key Server Group and choose the Key Server Group created in Figure 215 on page 288. Then click **OK**. At the next screen click **Close** and return to the main screen.

Dynamic VPN Connection

The Dynamic VPN Connection object defines information that is used to activate a specific connection between data endpoints. This information includes the source and destination objects, source and destination ports, and protocol supported for this connection along with the remote key server and key server group objects and an indicator of whether to auto-activate the connection.

11.3.1.7 Creating the anchor filter rules, services, and connections

Now we have to create the anchor filter rule and the service definition associated to it to create the dynamic filter rules. Additionally, a connection definition that allows the tunnel endpoints to use AH and ESP protocol is required. Follow the instructions below:

In this anchor filter rule we will allow all types of traffic to flow in the tunnel. We will also associate this anchor filter rule to a Dynamic Tunnel Policy.

The screenshot shows a window titled "(9.24.104.33) Add IP Rule" with a subtitle "Add a Rule Template.". The window is divided into several sections with blue headers:

- Identification:** Rule Name: R2612 AS400 Anchor Rule; Description: R2612 AS400 Anchor Rule; Action: Anchor; Protocol: all.
- Source Port / ICMP Type:** Operation: Any; Port #/Type: 0.
- Destination Port / ICMP Code:** Operation: Any; Port #/Code: 0.
- Interfaces Settings:** Interface: Both.
- Direction/Control:** Routing: both (selected), local, route; Direction: both (selected), inbound, outbound; Log Control: no (selected), yes, permit, deny.
- Tunnel Information:** Manual VPN Tunnel ID: (empty); Dynamic Tunnel Policy Name: R2612 AS400 Dynamic Tunnel Policy (selected).

At the bottom of the window are three buttons: OK (with a green checkmark), Cancel (with a red X), and Help (with a question mark).

Figure 220. Creating anchor filter rule on OS/390

At the main screen, double-click **Connection Templates** and **Rules**, then double-click **NEW** to add a new Rule. You will see the screen above. Please fill in the fields as shown. Click **Select ...** beside Dynamic Tunnel Policy Name and choose the Dynamic Tunnel Policy created in Figure 212 on page 286. Then click **OK**. At the next screen click **Close** and return to the main screen.

Anchor filter rule

Rules on the OS/390 system are used to screen traffic passing through the system. Rules can be set up to either allow or disallow traffic on the basis of certain criteria. When a dynamic VPN connection is activated, the anchor filter rule is used to determine the placement of the dynamically generated filter rules among the static permit and deny rules.

We have to create a Services object to establish the anchor filter rule between the connection endpoints. Complete these steps:

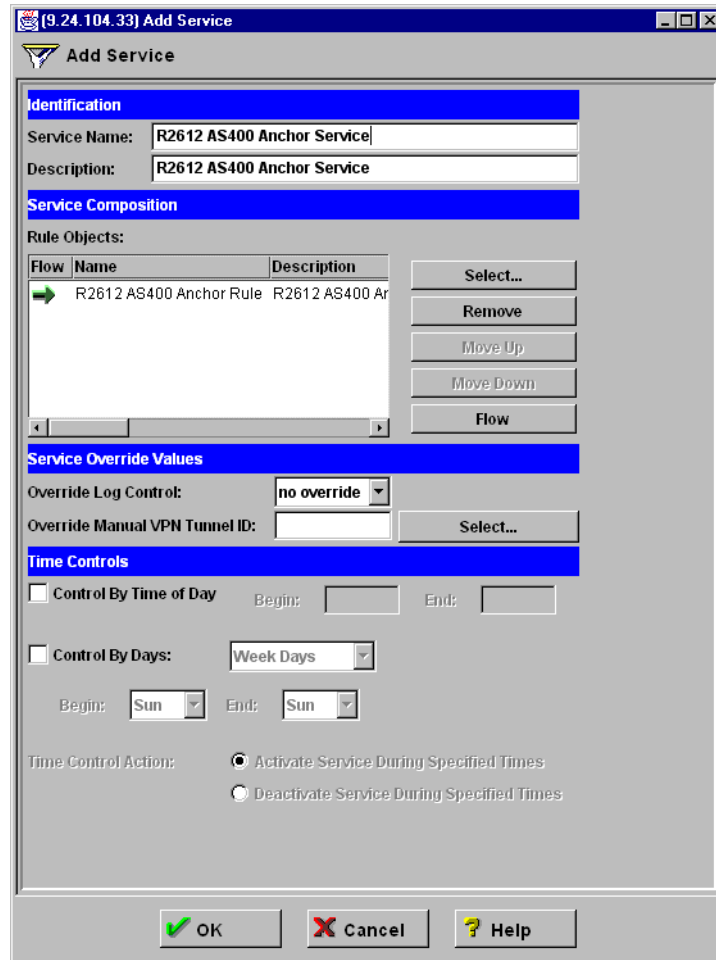


Figure 221. Adding Anchor Service on OS/390

At the main screen, double-click **Services**, then double-click **NEW** to add a new Service. You will see the screen above. Please fill in the fields as shown. Click **Select ...** under Rule Objects and choose the anchor filter rule created in Figure 220 on page 292. Then click **OK**.

Services

Services is a collection of rules or a set of instructions to permit or deny a particular type of traffic through the OS/390 system, for example, a Telnet session. Services figures prominently when defining connections, specifying the type of traffic that can or cannot take place between Network objects.

Now we will create the two connections to associate the services between the tunnel endpoints. Then we will activate the connection to create the filter rules. Follow these instructions:

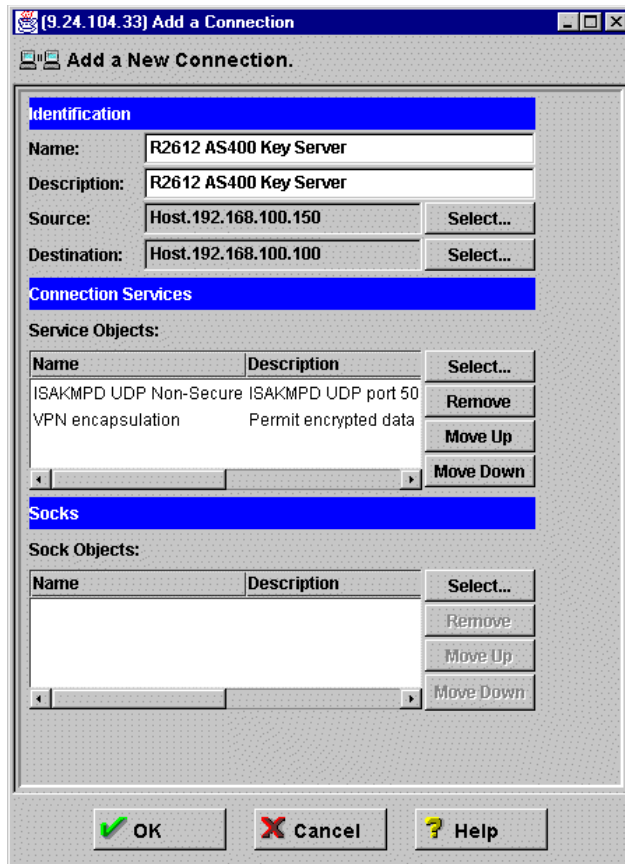


Figure 222. Adding Key Server Connection on OS/390

At the main screen, double-click **Connection Setup**, then double-click **NEW** to add a new Connection. You will see the screen above. Please fill in the fields as shown. Click **Select ...** beside Source and choose the Network object created in Figure 217 on page 290. Click **Select ...** beside Destination and choose the Network object created in Figure 218 on page 290. Then click **OK**.

The objects selected as the service object are predefined Service objects. These attributes are shown in Figure 223 and Figure 224 on page 295.

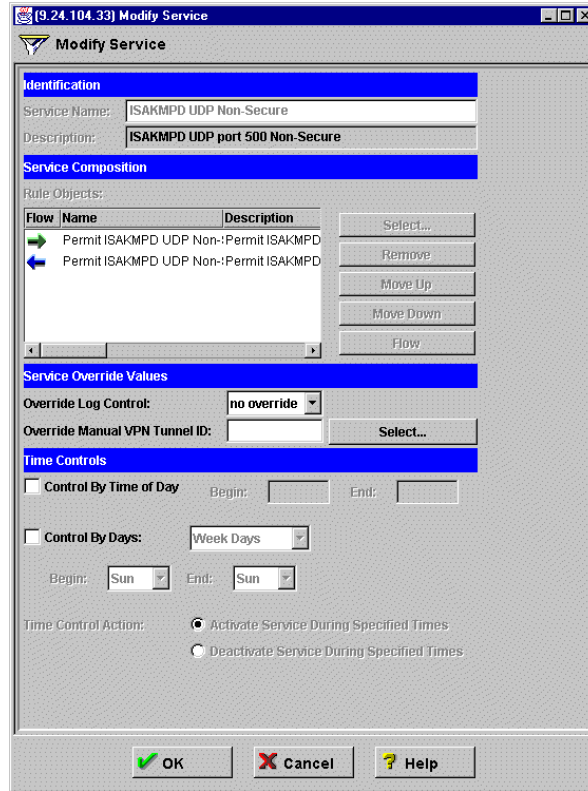


Figure 223. ISAKMPD UDP Non-Secure Service object

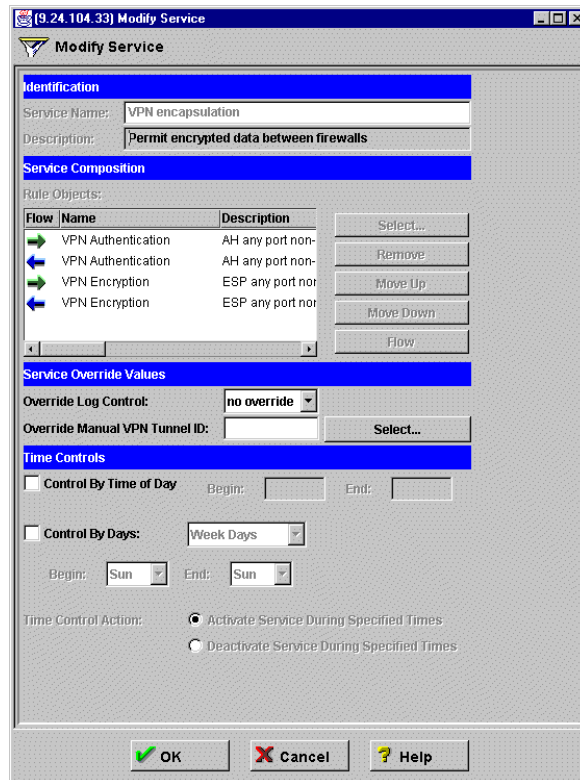


Figure 224. VPN encapsulation Service object

Then define the connection that sets up the anchor filter rules for connection endpoints.

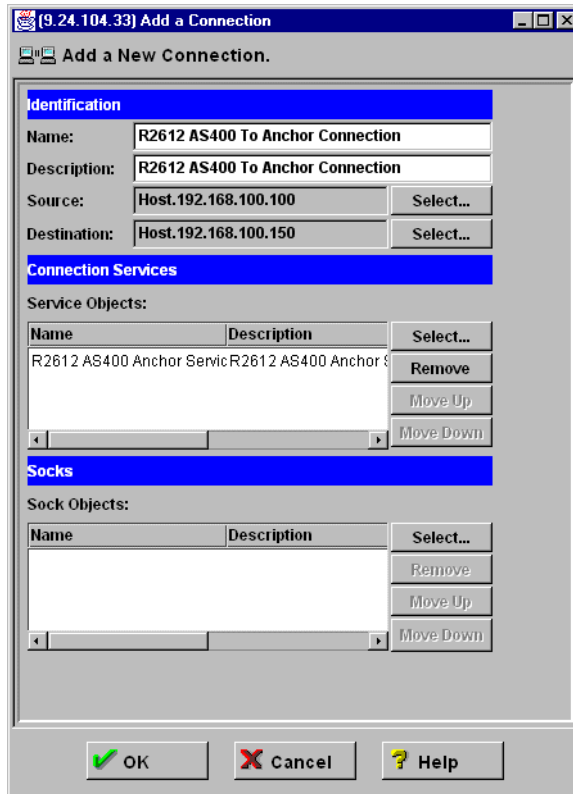


Figure 225. Adding Anchor Connection on OS/390

Double-click **NEW** to add a new Connection. You will see the screen above. Please fill in the fields as shown. Click **Select ...** beside Source and choose the Network object created in Figure 218 on page 290. Click **Select ...** beside Destination and choose the Network object created in Figure 217 on page 290. Then click **OK**.

Since an anchor filter rule generates both an inbound and outbound rule, you do not need have two connections that are defined for each direction.

Connections

The Connection function allows you to control the type of network traffic that can take place between two network entities that are connected through the OS/390 system. They permit or deny specified types of communications between two named endpoints or any type of Network object or group. After you have defined your Network objects and services, you create connections. In building connections, you will select one Network object to be the source and another Network object to be the destination for the traffic flow through the OS/390 system.

Note: The connection must be ordered in the following sequence: Key Server Connection and Anchor Connection. Check this in the Connections List screen

and reorder the connection if necessary. Access Help from the Connection Setup for more information.

11.3.1.8 Activating the filter rules and the dynamic VPN connection

Now we will activate the filter rules and the dynamic VPN connection. Please follow these instructions:

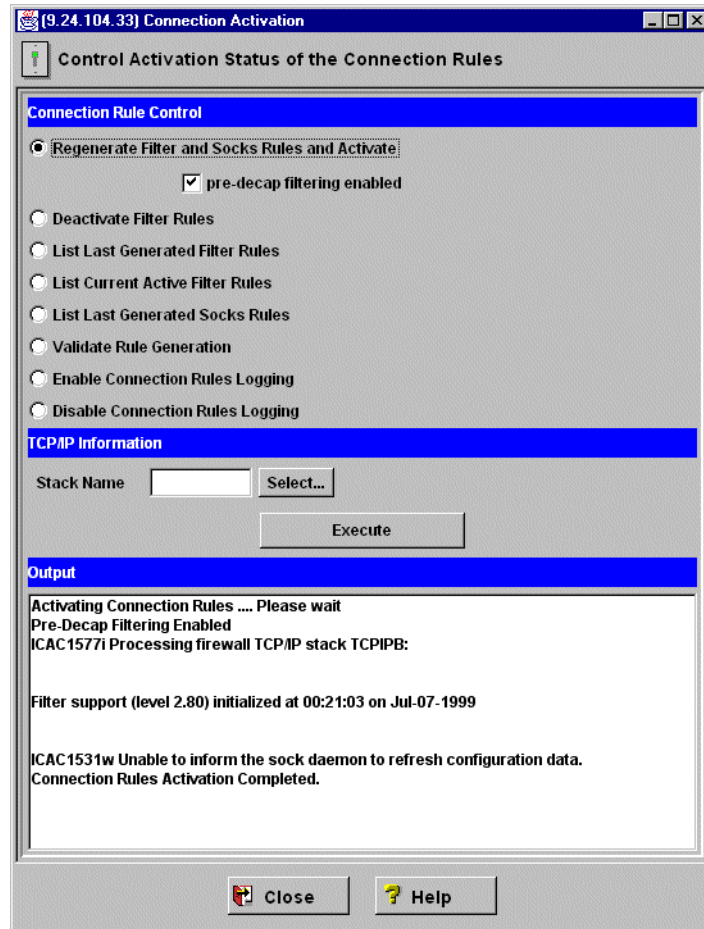


Figure 226. Connection Activation

At the main screen, double-click **Connection Activation**, then mark the boxes shown in the screen above and click **Execute**. Check the messages in the output area for errors. Then click **Close**.

Connection Activation

Use this function to generate the rules based upon the configurations defined in the connection setup panel and all of its subsidiary configurations (for example, services, rule templates, and SOCKS templates). Rules can also be generated depending upon settings in the security policy panel. These rules become the active set through which the OS/390 system can evaluate network datagrams. If there is a set of connection rules already active, this procedure updates the active rules with the contents of the newly generated set. Feedback about a successful activation or any errors will be displayed in the output section. **Note:** Checking the pre-decap filtering enabled check box results in AH and ESP packets being filtered before they are decapsulated. If there are concerns about AH and ESP packets in your network, then you may want to have the AH and ESP packets filtered before they are decapsulated.

Now we will activate the dynamic VPN connection:

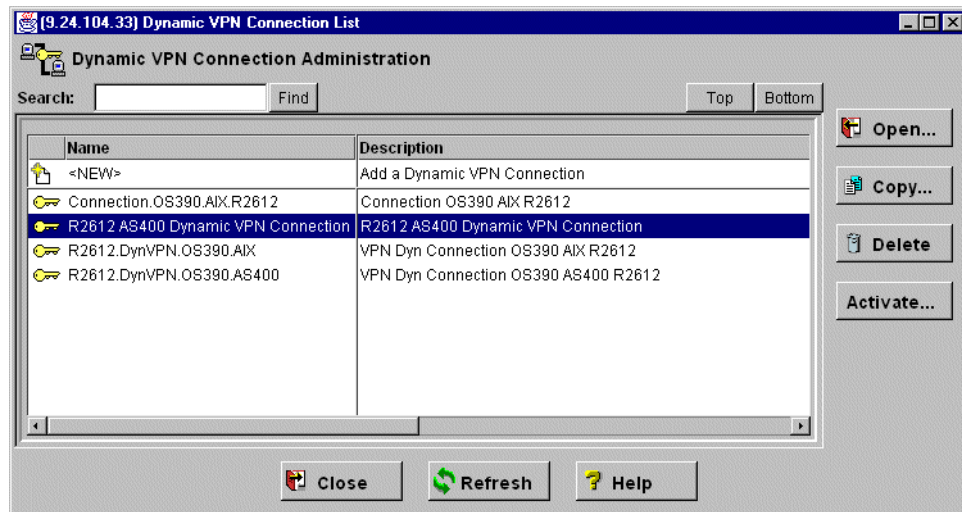


Figure 227. Dynamic VPN Connection activation

At the main screen, double-click **VPN Connection Setup**, then choose the Dynamic VPN Connection created in Figure 219 on page 291 and click **Activate...** You will receive the following message:

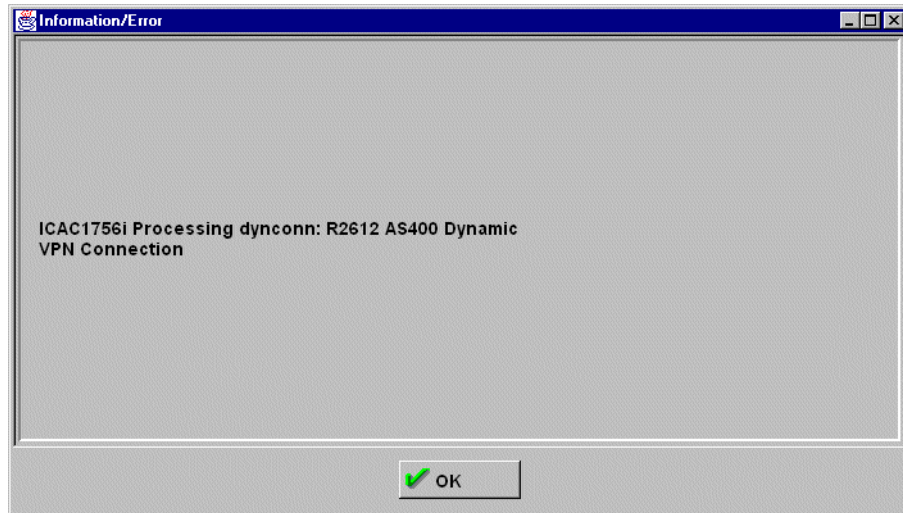


Figure 228. Dynamic Connection activation message

This message only tells you that the activation of the dynamic VPN connections is in progress. You have to check the VPN Connection Activation screen to see if the tunnel was activated. Follow these steps:

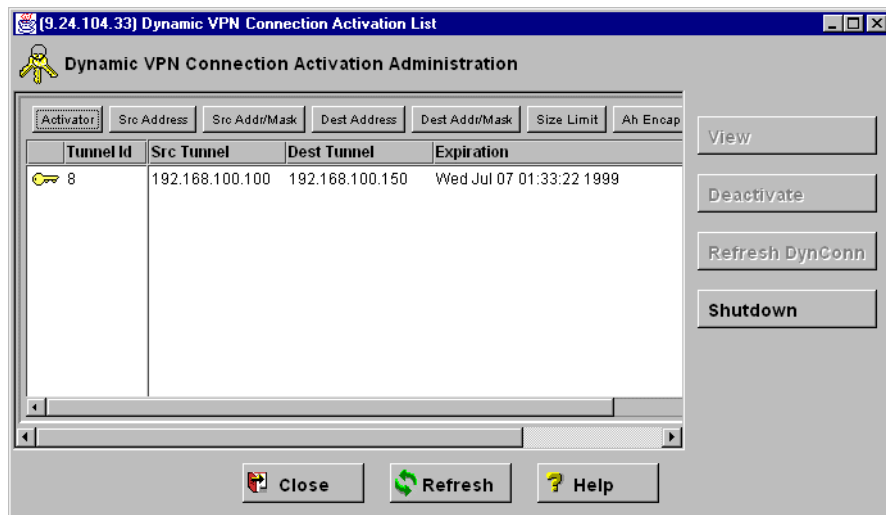


Figure 229. Dynamic Connection Activation List

To check all the parameters in the tunnel, you can double-click the tunnel, or select the tunnel and click **View**. You will receive the following screen showing all the definitions:

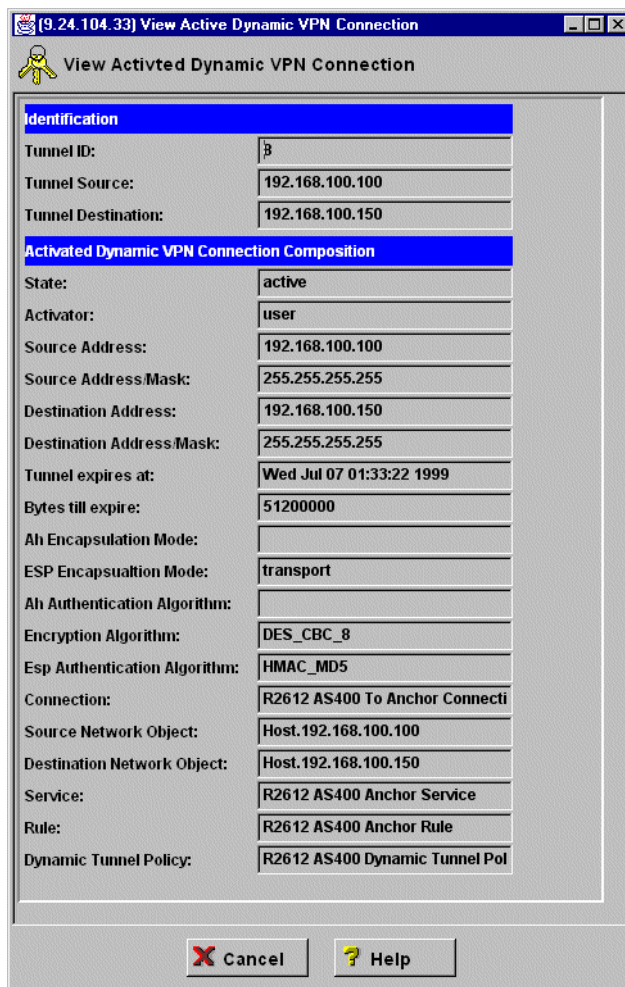


Figure 230. View Activated Dynamic VPN Connection

Now you can start the traffic between the two hosts. All types of traffic will be permitted.

11.3.1.9 Using the firewall log to check the tunnel status

There are some messages in the firewall log that can help you check the activation of the tunnel, to check if the traffic is flowing through the tunnel and so on. You can browse the log file using the `OBROWSE` command in a TSO session or using the Log Viewer in the configuration client. These messages are in the file `/tmp/firewall.all.log` as shown in Figure 185 on page 259.

```
ICA8233i;507;510; 1
ICA8227i;000000008;192.168.100.100;255.255.255.255;ALL;ALL;192.168.100.150; 2
ICA1073i;TCPIPB;R:p; o; ;192.168.100.100;s;192.168.100.100;d;192.168.100.150; 3
p;icmp;t;8;c;0;r;l;a;n;f;y;T;0000000512:0000000507:0000000510:0000000510:
00000510:0000000510:0000000530:0000000501:000000008"†"*;AH;0;ESP;0;l;284;
ICA1073i;TCPIPB;R:p; i; ;192.168.100.100;s;192.168.100.150;d;192.168.100.100; 4
p;icmp;t;0;c;0;r;l;a;n;f;y;T;0000000512:0000000507:0000000510:0000000510:
00000510:0000000510:0000000530:0000000501:000000008"†"*;AH;0;ESP;0;l;284;
```

Figure 231. Checking firewall log messages

1 This message indicates that an attempt to create a dynamic connection between the two Network objects is in progress. Checking these two Network objects in the UNIX System Services shell you will see:

```
GIANCA @ RA03:/u/gianca>fwnwobj cmd=list id=507 format=long
  id = 507
  type = Host
  name = Host.192.168.100.100
  desc = Host 192.168.100.100
  addr = 192.168.100.100
  mask = 255.255.255.255
  startaddr =
  endaddr =

GIANCA @ RA03:/u/gianca>fwnwobj cmd=list id=510 format=long
  id = 510
  type = Host
  name = Host.192.168.100.150
  desc = Host 192.168.100.150
  addr = 192.168.100.150
  mask = 255.255.255.255
  startaddr =
  endaddr =
```

Figure 232. Displaying tunnel endpoints Network objects

The two Network objects are the tunnel endpoints.

2 This message indicates that tunnel ID 8 was created.

3, 4 These messages show a PING (ICMP protocol) between the tunnel endpoints. Notice that the first ICMP message is from the OS/390 host and the second ICMP message is from the AS/400 host. These messages also indicate that the traffic is flowing through tunnel ID 8.

Please see *OS/390 Firewall Technologies Guide and Reference*, SC24-5835 for a more detailed explanation.

11.3.2 Creating a dynamic VPN using the shell commands

Now we will use the shell commands to define the tunnel based on Table 48 on page 274, between OS/390 and AIX/6000. You can either create a script and execute the script file or execute the commands from an OVMS shell prompt.

First we will define the Key Management objects: Key Transform, Key Proposal, and a Key Policy. A Key Policy contains a Key Proposal that contains one or more Key Transform objects.

```

fwkeytran cmd=add      name="R2612 AIX Key Transform" \
                      desc="R2612 AIX Key Transform" \
                      prot=IKE authmeth=SHAREDKEY \
                      hashalg=MD5 encralg=DES_CBC_8 dhgrp=GROUP1 \
                      itime=1440 isize=0 rtime=60-1440 rsize=0-0
fwkeyprop cmd=create  name="R2612 AIX Key Proposal" \
                      desc="R2612 AIX Key Proposal" \
                      keytranlist="R2612 AIX Key Transform"
fwkeypol  cmd=add     name="R2612 AIX Key Policy" \
                      desc="R2612 AIX Key Policy" \
                      imode=MAIN rmode=MAIN \
                      keyprop="R2612 AIX Key Proposal"

```

Figure 233. Key Management definition

Now we will define the Data Management objects: ESP Transform, Data Proposal, and Data Policy. A data policy contains one or more Data Proposal objects, each of which contains one or more ESP and AH Transform objects.

```

fwesptran cmd=add     name="R2612 AIX Esp Transform" \
                      desc="R2612 AIX Esp Transform" \
                      mode=TRANSPORT \
                      authalg=HMAC_MD5 encralg=DES_CBC_8 \
                      itime=60 isize=0 rtime=60-480 rsize=0-0
fwdataprop cmd=create name="R2612 AIX Data Proposal" \
                      desc="R2612 AIX Data Proposal" \
                      esptranlist="R2612 AIX Esp Transform"
fwdatapol cmd=create  name="R2612 AIX Data Policy" \
                      desc="R2612 AIX Data Policy" \
                      pfs=NONE \
                      dataproplist="R2612 AIX Data Proposal"

```

Figure 234. Data Management definition

Now we will define the Dynamic Tunnel Policy. The Dynamic Tunnel Policy will be associated to an anchor filter rule and will be used to set attributes for a dynamic tunnel.

```

fwdyntun  cmd=add     name="R2612 AIX Dynamic Tunnel Policy" \
                      desc="R2612 AIX Dynamic Tunnel Policy" \
                      datapol="R2612 AIX Data Policy" \
                      init=EITHER connlifetime=0

```

Figure 235. Dynamic Tunnel Policy definition

Now we will define the Key Server objects and the Key Server Group object. The Key Server objects define the endpoints of a VPN connection. The Local Key Server for this connection will be the same as defined in Figure 214 on page 287.

```

fwkeysrv cmd=add      name="R2612 AIX Remote Key Server" \
                    desc="R2612 AIX Remote Key Server" \
                    idtype=IPV4 \
                    authid=172.16.3.3 ipaddr=172.16.3.3
keysrvgrp cmd=create name="R2612 AIX Key Server Group" \
            desc="R2612 AIX Key Server Group" \
            keypol="R2612 AIX Key Policy" \
            lockysrv="R2612 OS390 Local Key Server" \
            remkeysrvlist="R2612 AIX Remote Key Server"

```

Figure 236. Key Server and Key Server Group definition

Now we will define the Authentication Information. This object is used to authenticate the key servers when you start a dynamic connection. You can use either Pre-Shared Keys authentication or RSA Signature (certificate based). The Shared-Key is always defined using a binary format. The characters 3132333435363738 in ASCII mean 12345678.

```

fwauthinfo cmd=add   name="R2612 AIX Authentication Information" \
                    desc="R2612 AIX Authentication Information" \
                    remkeysrv="R2612 AIX Remote Key Server" \
                    shkey=3132333435363738

```

Figure 237. Authentication Information definition

Now we will define an anchor filter Rule object and two Service objects. The anchor filter rule needs to be associated to a Dynamic Tunnel Policy object that allows dynamic connections to be created.

```

$ fwdyntun cmd=LIST dyntun="R2612 AIX Dynamic Tunnel Policy"
  id = 504 1
  name = R2612 AIX Dynamic Tunnel Policy
  desc = R2612 AIX Dynamic Tunnel Policy
  datapol = 504
  init = either
  connlifetime = 0

$ fwfrule cmd=ADD \
  name="R2612 AIX Anchor Rule" \
  desc="R2612 AIX Anchor Rule" \
  type=ANCHOR protocol=ALL \
  srcopcode=ANY srcport=0 \
  destopcode=ANY destport=0 \
  interface=BOTH routing=BOTH log=YES \
  tunnel=504 1

```

Figure 238. Anchor filter rule definition

1 You have to list the Dynamic Tunnel Policy to get the ID. This parameter will be used in the `fwfrule` command in the `tunnel` parameter.

Then create two Service objects: one service establishes the anchor filter rule between the connection endpoints and the other establishes the permit filter rules for the Key Server traffic.

```

$ fwfrule cmd=LIST name="R2612 AIX Anchor Rule"
    id = 531 1
    type = anchor
    name = R2612 AIX Anchor Rule
    desc = R2612 AIX Anchor Rule
    protocol = all
    srcopcode = any
    srcport = 0
    destopcode = any
    destport = 0
    interface = both
    routing = both
    log = yes
    tunnel = 504

$ fwservice cmd=CREATE \
    name="R2612 AIX Anchor Service" \
    desc="R2612 AIX Anchor Service" \
    rulelist=531/f 1

$ fwservice cmd=CREATE \
    name="R2612 AIX Key Server Service" \
    desc="R2612 AIX Key Server Service" \
    rulelist=136/b,136/f,5/f,11/f 2

$ fwservice cmd=LIST name="R2612 AIX Anchor Service" 3
    id = 512 3
    name = R2612 AIX Anchor Service
    desc = R2612 AIX Anchor Service
    rulelist = 531/f
    log = yes
    fragment =
    tunnel =
    time =
    month =
    day =
    weekday =
    timefilter =

$ fwservice cmd=LIST name="R2612 AIX Key Server Service" 3
    id = 513 3
    name = R2612 AIX Key Server Service
    desc = R2612 AIX Key Server Service
    rulelist = 136/f,136/b,5/f,11/f
    log = yes
    fragment =
    tunnel =
    time =
    month =
    day =
    weekday =
    timefilter =

```

Figure 239. Services definition

1 List the anchor filter rule to get its ID. It will be used to create the Anchor Service.

2 These rules are predefined. Rule 136 allows ISAKMPD traffic (UPD 500) in a nonsecure interface; rule 5 allows VPN Authentication, and rule 11 allows VPN Encryption.

3 List both services you have created and get their IDs. They will be used in the Connection definition.

```
$ fwnwobj cmd=ADD name=Host.172.16.3.3 desc="Host 172.16.3.3" \  
  type=HOST addr=172.16.3.3 mask=255.255.255.255  
  
$ fwnwobj cmd=list name=Host.172.16.3.3 1  
512 Host Host.172.16.3.3 Host 172.16.3.3  
  
$ fwnwobj cmd=list name=Host.192.168.100.100 1  
507 Host Host.192.168.100.100 Host 192.168.100.100  
  
$ fwconns cmd=CREATE name="R2612 AIX Key Server" \  
  desc="R2612 AIX Key Server" \  
  source=Host.172.16.3.3 \  
  destination=Host.192.168.100.100 \  
  servicelist=513  
  
$ fwconns cmd=CREATE  
  name="R2612 AIX Anchor Connection" \  
  desc="R2612 AIX Anchor Connection" \  
  source=Host.192.168.100.100 \  
  destination=Host.172.16.3.3 \  
  servicelist=507  
  
$ fwconns cmd=MOVE \  
  connection="R2612 AIX Anchor Connection" \  
  after="R2612 AIX Key Server" 2
```

Figure 240. Network objects and Connection definition

1 List the two Network objects to get their IDs. They will be used to define the connections.

2 The Key Server Connection must be in front of the Anchor Connection. To be sure move the two Anchor Connections after the Key Server Connection.

Now we will create the Dynamic VPN connection. The Dynamic VPN connection object defines information that is used to activate a specific connection between data endpoints.

```
$ fwdynconns cmd=ADD \  
  name="R2612 AIX Dynamic VPN Connection" \  
  desc="R2612 AIX Dynamic VPN Connection" \  
  src=Host.192.168.100.100 \  
  dest=Host.172.16.3.3 \  
  srcport=0 destport=0 prot=ALL \  
  remkeysrv="R2612 AIX Remote Key Server" \  
  keysrvgrp="R2612 AIX Key Server Group"
```

Figure 241. Dynamic VPN connection definition

Now you can activate and check if the Dynamic VPN connection is active.

```

GIANCA @ RA03:/u/gianca/firewall>fwdynconns cmd=activate dynconnlist="R2612 AIX
Dynamic VPN Connection"
ICAC1756i Processing dynconn: R2612 AIX Dynamic VPN Connection
GIANCA @ RA03:/u/gianca/firewall>fwdynconns cmd=listactive
11      192.168.100.100 192.168.100.7   active user
12      192.168.100.100 172.16.3.3   active user
GIANCA @ RA03:/u/gianca/firewall>fwdynconns cmd=listactive tunlist=12 format=lon
g
      TunnelID = 12
      TunSrc = 192.168.100.100
      TunDest = 172.16.3.3
      State = active
      Activator = user
      SrcAddr1 = 192.168.100.100
      SrcAddr2 = 255.255.255.255
      DestAddr1 = 172.16.3.3
      DestAddr2 = 255.255.255.255
Tunnel expires at = Wed Jul 07 18:57:41 1999 EDT
Bytes till expire = 0
      AH Encap Mode =
      ESP Encap Mode = transport
      AH Auth Alg =
      Encrypt Alg = DES_CBC_8
      ESP Auth Alg = HMAC_MD5
      ConnID = 509
      SrcObjID = 507
      DestObjID = 512
      SvcID = 512
      FruleID = 531
      DynTunID = 504

```

Figure 242. Activating and checking the connection status

Chapter 12. Nways routers using MRS/AIS/MAS V3.3

In this chapter we explain how to configure IPsec tunnels using Nways Multiprotocol Routing Services (MRS), Access Integrated Services (AIS) and Nways Multiprotocol Access Services (MAS) V3.3. We will show the relationship between policy and the IPsec feature and explain how policies are used by IPsec to direct traffic to and from IPsec tunnels. In earlier releases, we only had IPsec using manually configured tunnels and keys. You had to define the IPsec tunnel with all the relevant keying information and then define IP Packet filters: one to pass the traffic to IPsec to allow the secured packets in and out of the router, and one to confirm that the correct tunnel was used. For more information about IPsec configuration with prior releases, refer to 12.2, "Configuring IPsec on an Nways router" on page 309. With the introduction of the policy database, you no longer have to create two of the packet filters. As you define the policy, you define the "packet filter", now referred to as a rule, to pass the traffic to IPsec. The database also generates the rule to check that the traffic used the correct tunnel. You can define the manual tunnel either from the IPsec feature or from the policy feature. We will configure all three approaches for configuring the IPsec tunnel including the manual tunnel as below:

1. Manual tunnel with policy in CC5 (IP packet filters are used in CC4 instead of policy): manual key generation
2. IKE with pre-shared key, which is a new feature in CC5 for key management: automatic key generation
3. IKE with PKI, which is a new feature in CC5 for key management: automatic key generation with digital certification from CA

Next we will describe several useful commands to monitor IKE in order to give a basic understanding of the commands that are available, what they can show and how you can determine if IKE Phase 1 and 2 negotiations were successful.

Finally we briefly discuss adding routing protocols (default gateways, static routes and dynamic routes) to an IPsec configuration.

12.1 Policy engine

The policy engine was introduced in MAS/MRS/AIS 3.3. This policy engine is extensively described in Chapter 19 "Using the Policy Feature" of *Nways Access Integration Services V3.3 Using and Configuring Features*, SC30-3989.

The policy engine is a component that determines whether a packet should be secured by IPsec. RSVP and differentiated services are also used by the policy engine. The most important aspect of the policy engine is that it is engaged on the outbound port after the access control lists (ACLs). A packet enters the router and passes the port's input ACL, goes to the routing engine and passes the global ACL, gets forwarded by the routing engine to an outbound port where it passes the port's output ACL, and then the packet is interrogated by the policy engine. The packet must pass all ACLs; otherwise, the router would have discarded the packet before it reached the policy engine.

The other important point is that a packet must be forwarded before in order for it to be processed by the policy engine. To do this there must be a routing table entry for the packet. The examples in this chapter use static routes to ensure that

the router will forward the packet. If you do not wish to use static routes, perhaps due to the administrative overhead, you must enable a routing protocol.

The policy engine cannot support multicast packets. This is not normally a problem because IPsec currently only defines unicast packets. The reason for this is that the multicast packets are processed in a different part of the router from where unicast packets are processed. This part bypasses the policy engine altogether. This is why OSPF cannot be used as the routing protocol that traverses the IPsec tunnel, unless it is encapsulated in another protocol like a layer-2 tunneling protocol.

The following diagram describes the steps a packet goes through and how it interacts with the policy engine.

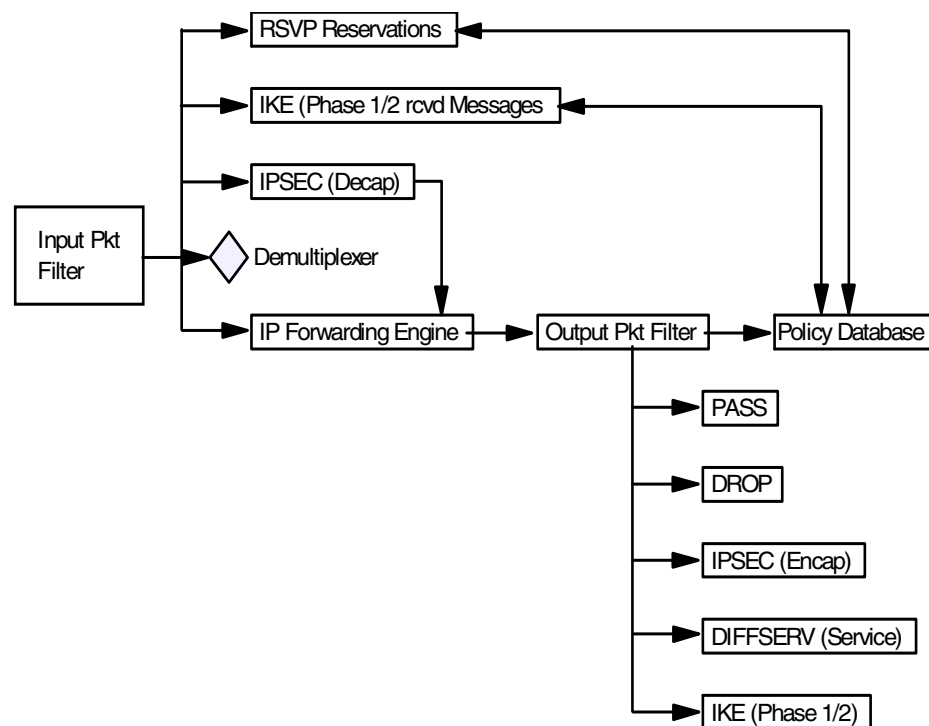


Figure 243. IP packet flow and the policy database

IP packets first must pass the input packet filter before any other actions can be taken. If the input packet filter has rules present then the packet may have some action taken on it. If there is a filter match that excludes the packet or there is no match found in the input packet filter then the packet is dropped.

If the packet passes the input packet filter it then goes to a demultiplexing filter, which checks to see whether the packet is locally destined. If it is, then depending on the type of packet, it is passed to other modules. These modules may be IPsec, IKE, RSVP, or others. If the packet is locally destined for IPsec, IKE, or RSVP then those modules may query the policy database to determine which action to take.

If the packet is not locally destined then it is given to the forwarding engine and a routing decision is made. If the routing decision does not drop the packet (policy-based routing may decide to drop the packet), then the packet goes to the

output packet filter. If filter rules are present in the output packet then the packet may have network address translation (NAT) performed, may be passed or may be dropped. If no filter rules are present then the packet is passed. If filter rules are present and no match is found then the packet is dropped. If the packet passes the Output Packet filter then the IP Engine queries the policy database to determine whether any other actions should be performed on this packet.

12.2 Configuring IPSec on an Nways router

The following steps in Figure 244 are recommended when configuring IPSec tunnels. However, depending on your current router configuration, some of these steps may be omitted.

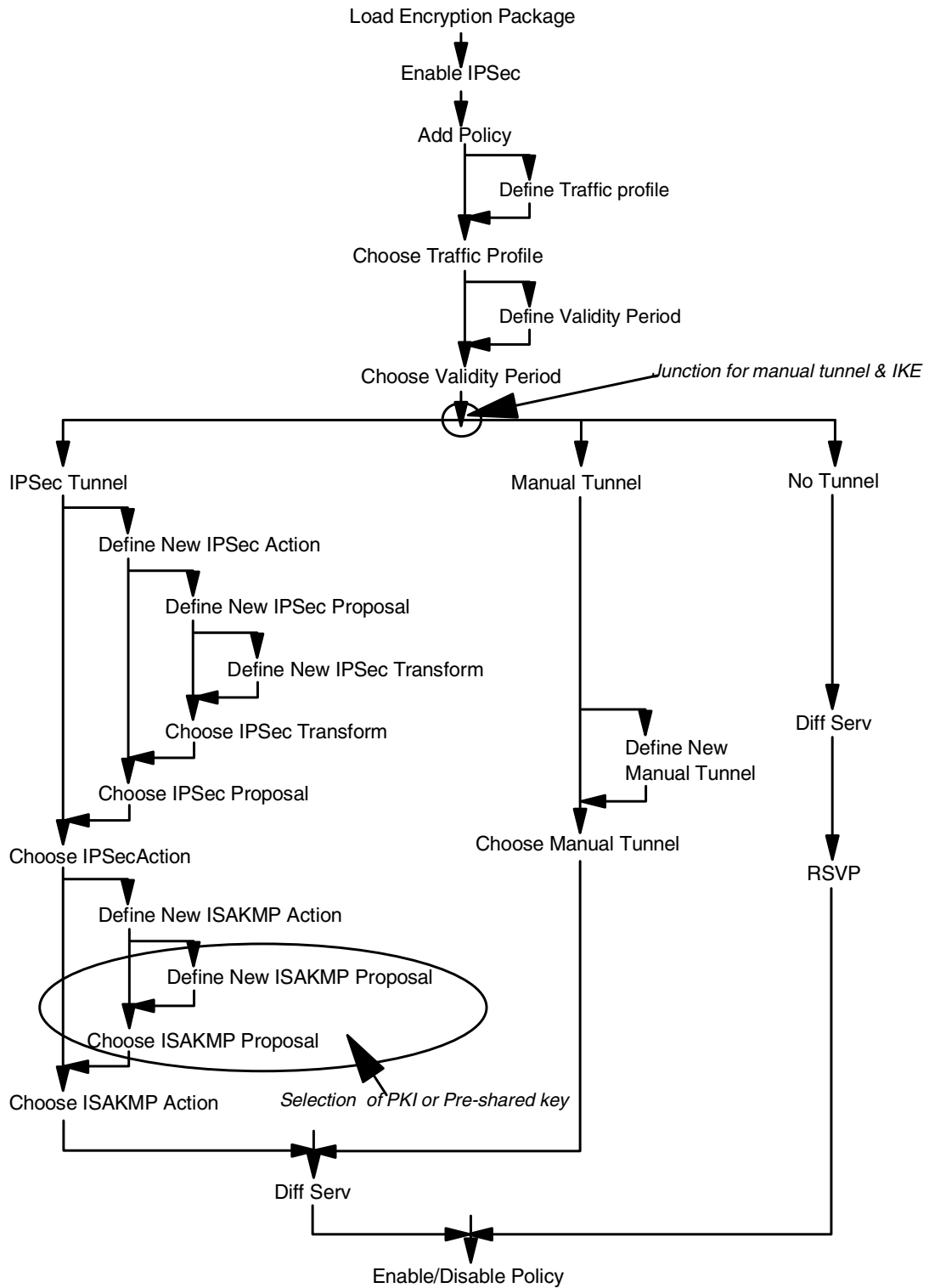


Figure 244. General steps for IPsec configuration

After choosing validity period, you are asked whether to use manual tunnel or IKE at the first circled junction in Figure 244 using the following questions:

Should this policy enforce an IPSEC action? [No]:

Do you wish to Map a Manual IPsec to this Policy? [No] :

And you select the authentication method (PKI or pre-shared key) at the second circled point. According to your selection, you configure different steps. For pre-shared key only one more step is required to *add remote end user*.

For PKI, the following additional steps in Figure 245 should be performed:

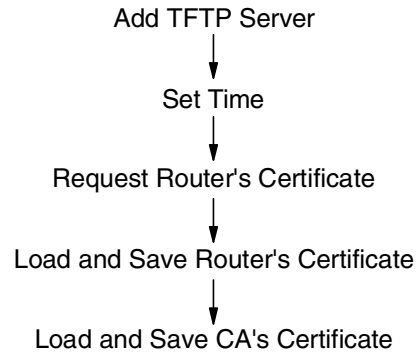


Figure 245. Steps for PKI configuration

Each of these steps is explained in the following sections. As an aid in understanding the different parameters used, we reference the sample network in Figure 246. In this configuration we want to authenticate all the traffic going between the 192.168.101.0 and 192.168.102.0 and the endpoints of the tunnel are 192.168.211.1 and 192.168.211.2.

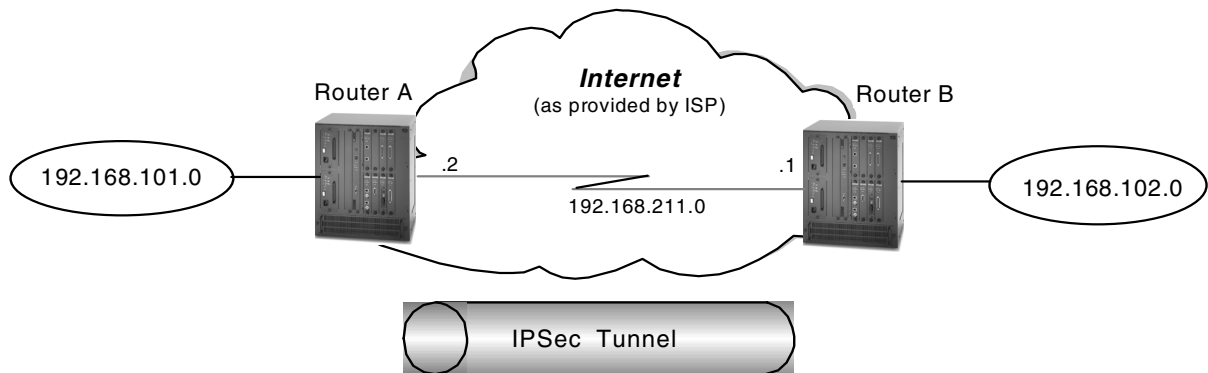


Figure 246. Sample network used in IPsec tunnel definition

To configure IPsec with MRS/AIS/MAS, an encryption package is required. For 2210, the encryption package is part of the running image. But IBM 2212 and 2216 routers need to load the encryption package. Reload (not restart) the router to effectively load the encryption package.

```
Config (only)>LOAD ADD PACKAGE encryption  
encryption package configured successfully  
This change requires a reload.  
Config (only)>RELOAD y
```

Figure 247. Loading encryption package

Another prerequisite for defining an IPsec tunnel is to configure your hardware interfaces, IP addresses and masks on each router interface that will serve as an IPsec tunnel endpoint. There are multiple ways to accomplish this using both the Config tool and the command line interface from the router console. These methods are not discussed in this redbook; however, Chapter 31, "Basic router AIS/MAS V3.3" in *A Comprehensive Guide to Virtual Private Networks, Volume II: BM Nways Router Solutions*, SG24-5234 shows one way to do it using the quick config command dialog from the router console.

Enabling IPsec is the final common step for three different IPsec tunnels. See Figure 248 to enable IPsec:

```
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>  
Branch *RESTART
```

Figure 248. Enabling IPsec

Now the IPsec architecture defines a policy database that is used to determine which packets should be processed by IPsec. Steps for defining the policy are composed of several various substeps according to the type of IPsec tunnel. Sections 12.2.1, "Configuring manual IPsec tunnels" on page 312, 12.2.2, "Configuring IKE with pre-shared keys" on page 322, and 12.2.3, "IKE with PKI configuration" on page 337 show how to configure each type of tunnel.

12.2.1 Configuring manual IPsec tunnels

Let us start with the manual tunnel that uses a manual key for an IPsec tunnel. The examples are based on configuring router A; router B is configured the same way. We chose to define the policy starting at the top of the tree and allowing the router to guide us through the creation of all the branches and leaves. Figure 249 shows what the contents of the policy tree are while configuring the manual tunnel in our sample network.

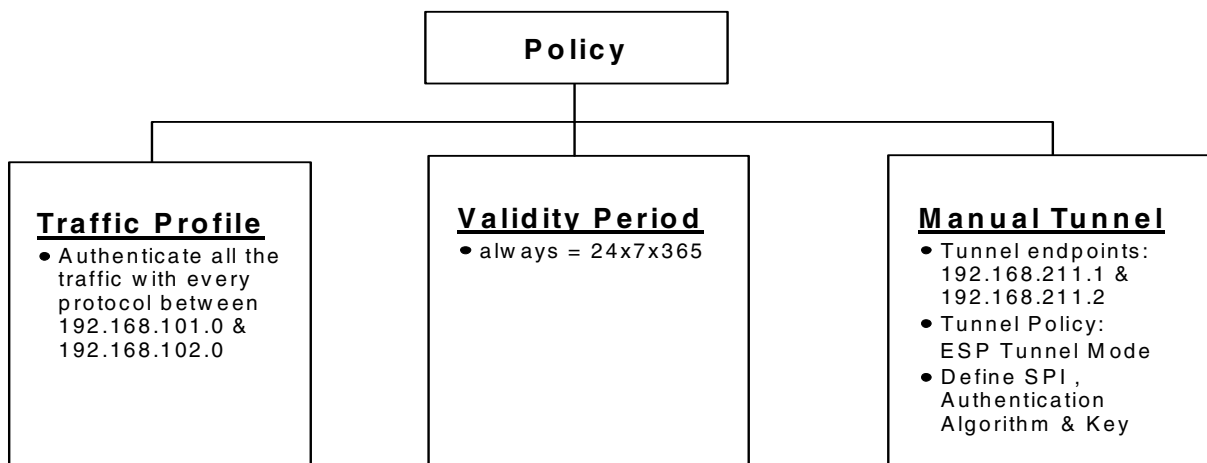


Figure 249. Policy tree for manual tunnel

12.2.1.1 Adding policy

The policy is configured from the policy feature through the `add policy` command. You are prompted for a name for the policy, which can be any name of your choice. The next question is the priority of this policy. The larger the numerical value of the number, the higher the priority. This is taken into consideration if a traffic flow matches more than two policies. Figure 250 shows this command:

```

Branch Config>FEATURE Policy
IP Network Policy configuration
Branch Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ipsec_man_101_102
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
  
```

Figure 250. Adding policies

12.2.1.2 Defining profiles in manual tunnel

Traffic profile details are defined in a left leaf of the policy tree as shown in Figure 249. Figure 251 on page 315 gives router commands for this configuration. As a profile does not exist, the only profile offered is option 0:new profile. If you had defined any profiles using the `add profile` command they would be listed here. The profile defines to what traffic this policy will be applied. The router can look at the source and destination IP addresses, protocol number, source and destination port, and TOS byte. As we selected option 0 we will be guided through creating a profile. You are asked for the name of the profile, so try to make the name as meaningful as possible, especially if you are going to use this profile in other policies. You are then prompted for the IP addresses. For both the source and destination you are asked if the address is netmask, range or single address. Netmask allows you to define a profile for a subnet, range defines a specific range of IP addresses. The subsequent questions for netmask are shown in Figure 251. For range you are asked for the starting IP address and ending IP address. In this scenario, we want the traffic profile to be going from the 192.168.101.0 network to the 192.168.102.0 network.

Note

If you say that the source and destination addresses are 0.0.0.0 with a mask of 0.0.0.0, that is all IP addresses.

After you are asked for details on the destination address format, you are asked about the IP protocol. You can say TCP only, UDP only, all protocols, or a specific range. If you take option 4 you will be asked for the starting protocol number and the ending protocol number. We want all the protocols to be secured. You are then asked which port numbers for both source and destination. If you want all port numbers, take 0 for the start and 65,535 for the end. You can only define one range per policy. In this example we want all ports. The next field of interest in the IP header is the DS byte. This used to be the TOS byte and has been renamed with the introduction of Differentiated Services. You are asked for the mask to be applied to the byte - this asks at which of the bits you wish to look. So 0 means that I do not care about the setting of this byte; FF means I care about the setting of all of these bits; E0 means I only care about the setting of the first three bits, etc. You are then asked for the value to match against after the mask has been applied. Let us look at a few examples:

- Mask of FF, value 00 = this policy will only apply to packets with zero in the DS byte.
- Mask of FF, value E0 = this policy will only apply to packets with a DS-byte of 1110000.
- Mask of E0, value E0 = this policy will only apply to packets with the first three bits set, that is, we do not care what the remaining 5 bits are.
- Mask of E0, value A0 = this policy will only apply to packets with the first three bits being 101 and we do not care about the remaining 5 bits.

This has completed which parts of the packets the router should look at and what values we wish to match against to apply this policy. You are then asked if you wish to configure local and remote IDs for ISAKMP - this tells the router how to identify an IKE peer. As we are using manually keyed tunnels, we cannot use IKE and therefore, we do not need to configure the ISAKMP details. As there are not interface pair groups defined there are none listed.

```

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 []? 101.0-to-102.0
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 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]? 1
Enter IPV4 Destination Address [0.0.0.0]? 192.168.102.0
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]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:

```

Figure 251. Defining traffic profiles

Now the router lists the profile you have created. You enter `yes` to confirm the profile or if you find anything to modify, enter `no`.

```

Here is the Profile you specified...

Profile Name      = 101.0-to-102.0
sAddr:Mask=     192.168.101.0 : 255.255.255.0   sPort=      0 : 65535
dAddr:Mask=     192.168.102.0 : 255.255.255.0   dPort=      0 : 65535
proto           =                0 : 255
TOS             =                x00 : x00
Remote Grp=All Users
Is this correct? [Yes]: Yes

```

Figure 252. Verifying traffic profiles

After verification, as a profile now exists, we are asked which profile do we wish to use with this policy, the one we have just created or do we wish to create another one. We will choose the one we have just created, `101.0-to-102.0`, which is option 1.

```
List of Profiles:
0: New Profile
1: 101.0-to-102.0

Enter number of the profile for this policy [1]?
```

Figure 253. Choosing traffic profiles for policy

12.2.1.3 Defining validity periods

The next leaf of Figure 249 is the validity period. Configuring the validity period is shown in Figure 254. As one does not exist, we are asked to create one. You are prompted for a name. The next piece is the lifetime of the policy - how long with this policy be valid. You can configure a start and end date which is in the numerical format of year, month, day, hour, minute and second. We want the policy to be valid forever so we have entered *. You are then asked for which months the policy is valid within that validity period. We want it to be valid for all months so we have selected the default of all. You can define that a policy should only be valid for certain days of the week - we have chosen every day. You can define time slots within a day - we have chosen * for all day. If you enter a start time you will be prompted for the finishing time. Note that this is in 24-hour clock format. If you are going to use a policy that specifies times and dates always ensure that your clock is correct within your router. You can inspect the time by using the time list command:

```
Config>time list

07:52:55 Monday July 19, 1999

Set by: internal clock

Time Host: 0.0.0.0 Sync Interval: 0 seconds

GMT Offset: 0 minutes

Config>
```

You can change the time using the `time set` command. There are also other options, such as synchronizing clocks between routers - see *MAS V3.2 Software User's Guide*, SC30-3886 for more details.

```
List of Validity Periods:
    0: New Validity Period

Enter number of the profile 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] :
```

Figure 254. Configuring validity periods

The validity period is listed in Figure 255. As a validity period now exists we are asked if we want to take the period we have just defined called “always” or create a new period. We will take the one we have just added.

```
List of Validity Periods:
0: New Validity Period
1: always

Enter number of the validity period for this policy [1]?
```

Figure 255. Defining policies - validity periods

Note

There are five predefined menus for the validity period in 2216:

0: New Validity Period

1: allTheTime : 24hoursx365days

2: allTheTimeMonThruFri : 24hours at Monday through Friday

3: 9to5MonThruFri : 9:00 a.m. to 5:00 p.m. at Monday through Friday

4: 5to9MonThruFri : 5:00 p.m. to 9:00 a.m. at Monday through Friday

12.2.1.4 Defining manual tunnel details

We are now asked to what sort of actions this policy should apply as shown in Figure 256 on page 321. We want a manual tunnel so we say no for an IPsec action and yes to manual. As no manual tunnels exist we are prompted to create one. The questions asked are exactly the same as the ones that were asked in early releases when you used the `add tunnel` command from the IPsec feature. In fact you can still add the tunnels from there, if you wish, but the policy can only be defined from the policy feature.

When the manual tunnel has been defined you are asked for which IPsec tunnel you wish to use - option 1 for one that we have just created, option 0 to create another tunnel. We have chosen option 1. The first part of the dialog defines the tunnel name, ID, tunnel lifetime, encapsulation mode, and tunnel policy. The tunnel lifetime defaults to 46080 minutes, which converts to 32 days. The maximum is 525600 minutes, which is one year. The tunnel encapsulation mode can be set to either tunnel mode or transport mode per the IPsec architecture. Tunnel mode is the normal case between routers that are using the public network to create a VPN. Transport mode is used to create a tunnel between two end stations.

The difference between the two modes is that with tunnel mode, the entire original IP packet is encapsulated within a new IP packet. This new packet has IP source and destination addresses of the tunnel endpoints. With transport mode, the original IP header is used with the original source and destination IP addresses. From Figure 256 on page 321, you can see that there are four choices for the tunnel policy:

- AH** This is the choice if you want to perform only authentication (the IPsec AH protocol) on packets going over this tunnel.
- ESP** This is the choice if you want to perform encryption (the IPsec ESP protocol) on packets going over this tunnel. Note that if you make this selection, you can also do authentication on the packets since the ESP protocol has an optional authentication feature.
- AH_ESP** This is the choice if you want to perform encryption and authorization using both the IPsec ESP and AH protocols. This selection indicates that for packets in the outbound direction, the packets will be encrypted first using the ESP protocol, then the AH algorithms will be run on the encrypted payload.

ESP_AH This choice also allows you to do both encryption and authorization using both the IPSec ESP and AH protocols. However, the order is reversed. With this selection, packets in the outbound direction will go through the AH algorithms first, then they will be encrypted using the ESP protocol.

At this point, the basic tunnel has been defined. Since we specified that this tunnel will use AH, the dialog now prompts us for the parameters that the AH algorithms will use. Figure 256 on page 321 shows an example of these prompts.

This first series of prompts are for the AH parameters at the local end of the tunnel (the router you are configuring is router A in Figure 246 in this example). We input Router A WAN interface IP address 192.168.211.2 as a local tunnel endpoint while we define a tunnel between 192.168.211.1 and 192.168.211.2. The parameters in local authentication must be the same as the parameters in remote authentication of the router at the other side of the tunnel. For example, if you choose the HMAC-MD5 algorithm for the local authentication algorithm, then you must configure HMAC-MD5 as the other router's *remote* AH algorithm. In effect, you are defining parameters for two unidirectional security associations (SAs) and each tunnel endpoint must agree on the parameters used for each SA. (Remember that two SAs exist for each IPSec tunnel: one in each direction.)

You can use different parameters for the SAs in each direction. However, the parameters specified for each SA have to match at each end of the IPSec tunnel. For example:

- The local key entered in router A must match the remote key entered in router B.
- The remote key entered in router A must match the local key entered in router B.

The same principle holds true for the SPI and the AH algorithm specified.

With this said, however, we recommend that you use the same parameters for both SAs unless you have a good reason to do otherwise.

SPI is the security parameter index. You can think of this as an index into the database where the parameters for this tunnel will be stored.

Since we configured the manual tunnel, this means that we manually enter the keys that will be used for the AH and ESP algorithms. We use simple keys in this example. We will configure the IBM Nways router to use ISAKMP/Oakley. In 12.2.2, "Configuring IKE with pre-shared keys" on page 322, the automated key management protocols will set the keys and refresh them periodically. The IPSec architecture specifies ISAKMP/Oakley as the protocols to use for its Integrated Key Exchange (IKE) framework.

In total, you have to enter four keys when configuring AH:

- Local key in router A
- Remote key in router A
- Local key in router B
- Remote key in router B

Also remember that each of the above keys must be typed twice to prevent mistakes. At the time of this writing, any typing mistakes will terminate the `add tunnel` command and you must start over.

After these parameters have been entered, the prompts switch to questions about the AH parameters for the remote end of the tunnel. As you might expect, the parameters entered for remote authentication must match parameters entered for local authentication of the router at the other side of the tunnel. For example, if you specify at the far end that outgoing packets should use the HMAC-MD5 algorithm to generate the Integrity Check Value (ICV), then you need to specify that incoming packets here at this end of the tunnel will be authenticated using the same HMAC-MD5 algorithm (and the same key). This is the idea behind configuring the parameters used at the remote end here at the local end of the tunnel. Figure 256 shows an example of these prompts.

The IPSec architecture defines a technique for ensuring that a hacker cannot intercept a datagram and play it back at some later time without being detected. This is called anti-replay or replay prevention support. Per the architecture, MRS/AIS/MAS implements this support using a sequence number that is included in the AH header of every packet. If enabled, the receiving side of the SA checks all sequence numbers on incoming packets to make sure that they fall within a window and have not been received previously. The sequence number is a 32-bit field in the header and is initialized to zero at the inception of the SA.

For manual IPSec implementations, it is not recommended to enable anti-replay support. This is because the architecture stipulates that the sequence number cannot wrap when it reaches the highest number in the range ($2^{32}=4.29$ billion packets). This means that if you enable anti-replay support, you have to ensure that the SA is re-established every 4.29 billion packets. When MRS/AIS/MAS implements ISAKMP/Oakley, there will be automated ways to refresh the SAs and hence this will not be a restriction.

You are then asked if the manual tunnel flows into another tunnel - this relates to the tunnel-in-tunnel feature that was first shipped in V3.2 of the code. We do not wish to use DiffServ or RSVP so our policy is completed.


```

Should this policy enforce an IPSEC action? [No]:
Do you wish to Map a Manual IPsec to this Policy? [No]: yes
Manual IPsec tunnels:
0: New IPSEC Manual Tunnel

Enter Tunnel ID of the Manual Tunnel Record [0]?
Adding tunnel 1.
Tunnel Name (optional) []? tun-101.0-102.0
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ah
Local IP Address [192.168.101.1]? 192.168.211.2
Local Authentication SPI (>= 256) [256]?
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex
(0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 192.168.211.1
Remote Authentication SPI (>= 256) [256]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex
(0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
A new tunnel is added. The policy must be configured
and reset.
Manual IPsec tunnels:
0: New IPSEC Manual Tunnel
Tunnel ID: 1Tunnel Start 192.168.211.2Tunnel End 192.168.211.1

Enter Tunnel ID of the Manual Tunnel Record [0]? 1
Does this manual tunnel flow into another Secure Tunnel? [No]:
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

```

Figure 256. Configuring manual tunnel detail

After the tunnel definition is completed, you can list the definition back out to check for errors such as incorrectly typed IP addresses. Figure 257 shows an example of this command:

```

Here is the Policy you specified...

Policy Name      = ipsec_man_101_102
State:Priority   =Enabled      : 5
Profile         =101.0-to-102.0
Valid Period    =always
Manual Tunnel   =1
TunnelInTunnel =No
Is this correct? [Yes]:
Branch Policy config>

```

Figure 257. Verifying manual tunnel detail

Note

This policy could have also been generated from the leaves with the following individual commands:

1. Create a profile `101.0-to-102.0` using the `add profile` command.
2. Create a validity period `always` using the `add validity-period` command.
3. Create a manual tunnel `tun-101.0-102.0` using the `add tunnel`.
4. Finally pull all the items together using the `add policy` command.

12.2.1.5 Activating policies defined

We could use either way to make the configuration changes active. Use the `reset database` command in talk 5 policy feature as shown in Figure 258:

```
Center *TALK 5
Center +FEATURE Policy
IP Network Policy console
Center Policy console>RESET DATABASE
Policy Database reset successful
```

Figure 258. Resetting database

Or use `restart` command as shown in Figure 259:

```
Branch *restart
```

Figure 259. Restarting router

12.2.2 Configuring IKE with pre-shared keys

Now we will create a secure IPSec tunnel between router A and router B that will use automatic key generation with pre-shared keys. The examples are based on configuring router B; router A is configured the same way.

Since the previous encryption package has been loaded, router interfaces with IP address are defined and IPSec is enabled, we start with defining a policy for IKE with a pre-shared key. We also will define the policy starting at the top of the tree and allowing the router to guide us through the creation of all the branches and leaves. Figure 260 defines the contents of the policy tree while configuring the IPSec tunnel using IKE with a pre-shared key in our sample network.

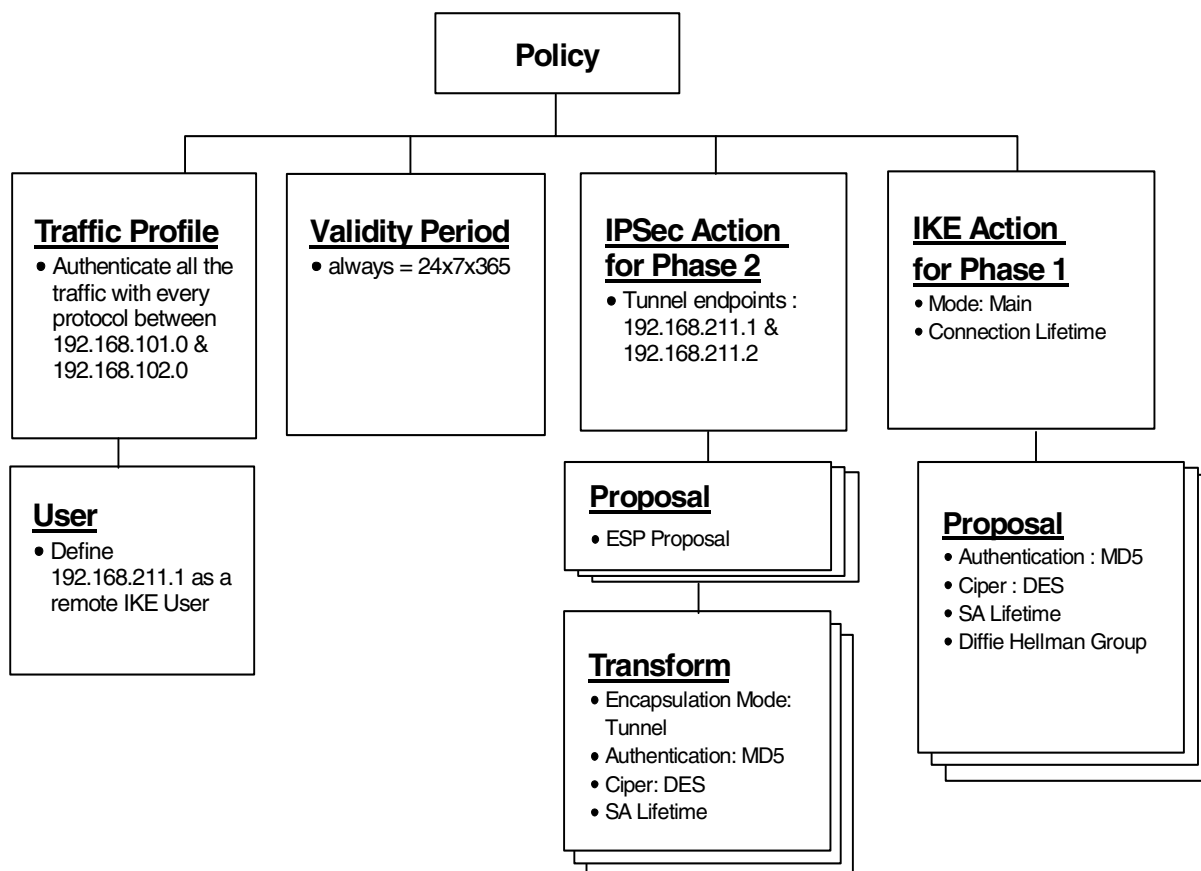


Figure 260. Policy tree for pre-shared key

12.2.2.1 Adding IKE peer user

The first step for configuring the policy for IKE pre-shared key is to define the remote IKE peer with pre-shared keys. The pre-shared keys of every remote peer need to be configured. This highlights why the use of pre-shared keys is not very scalable. Remember though that it is more secure than the manual tunnel approach (as shipped since V3.1 of the router code) because the derived keys are refreshed. The keys are defined in the policy feature.

The `talk 6 add user` command in the policy feature is used to configure the remote IKE peer and the keys shown in Figure 261 on page 324. The identifier chosen was the IP address. This must be the IP address of the tunnel endpoint - in this scenario, the IP address on the WAN interface. When you are defining the profile in the remote peer, ensure that "Enter local identification to send to remote" matches what was configured as the way to identify the user in the local router. Select the identifier of the remote end with care if you are performing Phase 1 negotiations in main mode. Recall that in main mode the identity of the peer is not exchanged until messages 5 and 6, but before reaching these messages the IKE peer must know the pre-shared key when it generates the keys. So at the time of performing the key generations, the only method of identifying the remote device is by its IP address. If the remote device's IP address is dynamically assigned, you must perform Phase 1 negotiations in aggressive mode as the identities are exchanged prior to the key generation.

Users can be grouped together, but it is most likely that the grouping will be used when the authentication is through digital signatures. Groups should be considered in situations in which the policy is wild-carded out for the destination addresses and you wish to specify a list of peers that are to be allowed access. These peers will still be authenticated by their key, but the policy database will perform an additional authentication step by ensuring that the local ID sent by the remote peer matches one of the IDs specified in the group of the policy's profile. Later we will see when a group of users can be associated with a particular policy. Add a user (for the remote IKE peer) and the pre-shared key. The IP address must be the same as the tunnel endpoint. The pre-shared secret does not show as you type it in. The talk 6 `add user` command in the policy feature is used to configure the keys shown in Figure 261:

```
Center Config>FEATURE Policy
IP Network Policy configuration
Center 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]? 192.168.211.2
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):
Enter the Pre-Shared Key again (8 characters) in ascii:
```

Figure 261. Adding user as a pre-shared key of remote end

Verify the user you defined as shown in Figure 262:

```
Here is the User Information you specified...

Name      = 192.168.211.2
Type      = IPV4 Addr
Group     =
Auth Mode =Pre-Shared Key
Is this correct? [Yes]:
```

Figure 262. Verifying user created

12.2.2.2 Adding policy

The pre-shared key has been configured; the next step is to add the policy. Now configure the policy of IPSec tunnel with the IKE pre-shared key `ike-pre-101-102` through the `add policy` command in Figure 263:

```
Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ike-pre-101-102
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
```

Figure 263. Adding policy

12.2.2.3 Defining profiles

After configuring a policy name, the next step is to define the profile as shown in Figure 264. The profile defines to what traffic flow this policy applies. The router can check the source and destination IP addresses, protocol number, source and destination port number, DS (TOS) byte in the IP header to determine if a traffic flow matches the policy. The router will list all the available profiles. As we defined manual tunnel in 12.2.1, “Configuring manual IPSec tunnels” on page 312, the router offers you two choices, 0 for a new profile and 1 for *101.0-to-102.0* defined for the manual tunnel. Since we created a new profile for IKE tunnel with a pre-shared key, choose 0. The profile could have been defined using the `add profile` command. In this scenario, we want the traffic profile to go from the 192.168.101.0 network to the 192.168.102.0 network with all protocols.

```
List of Profiles:
  0: New Profile
  1: 101.0-to-102.0

Enter number of the profile for this policy [1]? 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 [101.0-to-102.0]?
101.0-to-102.0-pre
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.0
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]? 192.168.101.0
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 264. Defining traffic profiles

You are then prompted to configure IDs for ISAKMP as shown in Figure 265. You must do this or the other peer will not be able to identify you. The method chosen here must match what you configure in the remote peer when defining the shared key - that is, to ensure your methods of identification are consistent. You are asked if this profile should be used by any users. Normally you will not need to restrict a profile to specific users since all ISAKMP Phase 1 negotiations are authenticated with either public certificates or pre-shared keys. However, in some remote access situations in which the policy is wild-carded out for the destination addresses, it may be wise to specify a list of users that are allowed access. These users will be authenticated through the normal ISAKMP authentication methods, but the policy database will perform an additional authentication step by

ensuring that the local ID sent by the remote peer matches one of the IDs specified in the group of the policy's profile. In this example we are not restricting the profile to a specific set of users. Figure 265 shows how to configure an ID for ISAKMP:

```
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 265. Configuring ID for ISAKMP

Confirm the traffic profile you create. Option 2 selects *101.0-to-102.0-pre* that has just been created.

```
Here is the Profile you specified...

Profile Name      = 101.0-to-102.0-pre
sAddr:Mask=      192.168.102.0 : 255.255.255.0   sPort=    0 : 65535
dAddr:Mask=      192.168.101.0 : 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: 101.0-to-102.0
  2: 101.0-to-102.0-pre

Enter number of the profile for this policy [1]? 2
```

Figure 266. Verifying traffic profile

12.2.2.4 Defining validity periods

The next step is to define the validity period as you can see in the policy tree in Figure 260 on page 323. Because we defined validity period "always" in 12.2.1, "Configuring manual IPSec tunnels" on page 312, the router prompts two choices, 0 for new and 1 for "always". The validity period could have been defined using the add validity period. Refer to 12.2.1, "Configuring manual IPSec tunnels" on page 312 for a predefined validity period menu of 2216 and how to define a new validity period.

```
List of Validity Periods:
0: New Validity Period
1: always

Enter number of the validity period for this policy [1]?
```

Figure 267. Configuring validity period

12.2.2.5 Defining IPsec action for IKE Phase 2

The next step is to create an IPsec action as shown in Figure 260 on page 323. In Figure 265 on page 326 as you create an IPsec action you will be prompted for details about the tunnel endpoints, and then be asked for the IKE Phase 2 proposals and transforms. As no IPsec actions exist you are prompted to create one, which we will call "tun-101-102". You would be prompted through the same questions if you used the `add ipsec-action` command.

The router will prompt whether this action is to block or permit. If you say block, the traffic will not be secured or forwarded. If you say permit, the traffic will be forwarded and the next question asks whether it should be in the clear or secured. If the answer is in the clear, the traffic will not be handled by IP Security. Clearly we need option 2, and now the router will prompt you through the details of the IPsec SAs. Our tunnel endpoint is our WAN interface of both routers, 192.168.211.1 and 192.168.211.2. Remember that we chose that our peers would be identified by the tunnel endpoint address so take care to ensure that this value matches the identifier that will be configured in the remote peer. Conversely ensure that the value you enter for the remote tunnel endpoint matches that configured for the identifier of the remote system. Note that if you are doing IPsec in a remote access scenario, you may not know the IP address in advance. In this case you would use a different identifier for the user (such as a fully qualified domain name) and specify the remote tunnel endpoint address as 0.0.0.0. The remote device must initiate the IKE negotiations and you must perform Phase 1 negotiations in aggressive mode as you need to know the identity of the remote end to locate the correct pre-shared keys so the master key can be generated.

You are then asked if this traffic will flow into another IPsec tunnel. This relates to the tunnel-in-tunnel function shipped in V3.2 of the router code. A sample diagram of this function is shown in Figure 268. Either tunnel can have any IPsec characteristics:

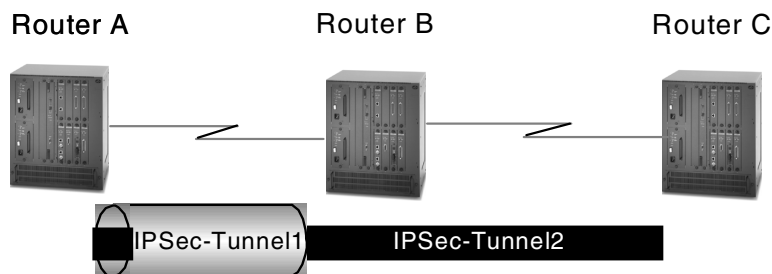


Figure 268. Tunnel-in-tunnel function

The router then prompts you through the SA characteristics for this tunnel. You are asked about percentages of the lifetime/time that are acceptable. This is used if the peer offers a different value of lifetime - if the SA lifetime/time received is less than 75% it will not be acceptable. When the IPsec header is created, many of the fields of the IP header are copied from the header of the packet being secured. You can control how the do not fragment field is set. You can either copy from the original packet, set the DF bit or if it is turned on in the original packet, turn it off.

“Enable replay prevention” defines whether the sequence numbers should be checked on received packets. The next question is whether this SA should be created as a system startup. Specifying no indicates that this SA should only be negotiated when packets are received that match this policy. We have now defined the contents of the IPsec header. We know we need to define what type of SA will be negotiated. That is what we need to define an IKE Phase 2 proposal and transform. As no proposals exist, we are prompted to create one. You would be prompted through the same questions if you used the `add ipsec-proposal` command.

```
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-101-102
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
[9.24.104.203]? 192.168.211.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
[0.0.0.0]? 192.168.211.2
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/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 269. Configuring IPsec action for IKE Phase 2

12.2.2.6 Defining IPsec proposal for IKE Phase 2

We are going to create a proposal called "esp-prop1" which states that we want to do ESP, but we do not require PFS. Each proposal requires a transform; the router prompts us to create one by choosing option 0.


```

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
    1: strongP2EspProp
    2: strongP2EspAhProp
    3: veryStrongP2EspProp
    4: veryStrongP2EspAhProp

Enter the Number of the IPSEC Proposal [1]? 0
Enter a Name (1-29 characters) for this IPsec Proposal []? esp-prop1
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 270. Configuring IPsec proposal

There are four predefined menus for the ESP proposal in 2216. Table 51 shows the predefined ESP proposals:

Table 51. Predefined ESP proposal

| ESP proposal | DH Grp | Encap | Transform name | Auth | Ciper |
|-----------------------|--------|--------|---------------------|----------|-------|
| StrongP2ESPProp | Grp1 | Tunnel | ESPTunnelMD5andDES | HMAC-MD5 | DES |
| | | | ESPTunnelSHAandDES | HMAC-SHA | DES |
| StrongP2ESPAhProp | Grp1 | Tunnel | ESPTunnelDES | None | DES |
| | | | ESPTunnel3DES | None | 3DES |
| VeryStrongP2ESPProp | Grp1 | Tunnel | ESPTunnelMD5and3DES | HMAC-MD5 | 3DES |
| | | | ESPTunnelSHAand3DES | HMAC-SHA | 3DES |
| VeryStrongP2ESPAhProp | Grp1 | Tunnel | ESPTunnel3DES | None | 3DES |

12.2.2.7 Defining IPsec transform for IKE Phase 2

We will make a transform called "esp-tun1" which is an ESP SA in tunnel mode. Figure 271 shows how to create an IPsec transform. You would be prompted through the same questions if you used the `add ipsec-transform` command.

There are six predefined menus for ESP transform in 2216. Now we create a new one by choosing option 0. We will do authentication using HMAC_MD5 and encryption using DES. You are prompted for the SA lifetime/lifesize of the Phase 2 tunnel. When the SA lifetime expires, IKE will perform another Phase 2 calculation to refresh the keys.

```

List of ESP Transforms:
  0: New Transform
  1: espTunnelMD5andDES
  2: espTunnelSHAandDES
  3: espTunnelMD5and3DES
  4: espTunnelSHAand3DES
  5: espTunnelDES
  6: espTunnel3DES
Enter the Number of the ESP transform [1]? 0
Enter a Name (1-29 characters) for this IPsec Transform [ ]? esp-tun1
List of Protocol IDs:
  1) IPSEC AH
  2) IPSEC ESP

Select the Protocol ID (1-2) [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) [2]?
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]?

```

Figure 271. Configuring IPsec transform

The router will list the transform you have defined. If it is correct, enter *yes*. The router prompts you for which transform the IKE proposal "esp-prop1" should use. Selecting option 7 takes the transform just created "esp-tun1", or you could choose to add additional transforms at this time. If you take the transform, you will then be asked if this proposal has more than one transform. In this example, we will only offer one transform. You could offer another ESP transform with different algorithms for authentication or encryption algorithms.

```

Here is the IPSec transform you specified...

Transform Name = esp-tun1
  Type =ESP   Mode =Tunnel   LifeSize= 50000 LifeTime= 3600
  Auth =SHA   Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
  0: New Transform
  1: espTunnelMD5andDES
  2: espTunnelSHAandDES
  3: espTunnelMD5and3DES
  4: espTunnelSHAand3DES
  5: espTunnelDES
  6: espTunnel3DES
  7: esp-tun1

Enter the Number of the ESP transform [1]? 7
Do you wish to add another ESP transform to this proposal? [No]:

```

Figure 272. Verifying IPSec transform

12.2.2.8 Choosing proposal and transform for IKE Phase 2

In Figure 273 you are prompted for which proposal this IPSec action should use. Option 5 selects the proposal that has just been created, or choose option 0 to create another one. If you wanted to have multiple proposals for this action you would answer yes to question **1** and you would be prompted to create more proposals (and transforms). Remember that a proposal is a set of transforms from which the IKE peer can choose. A proposal can have either or both of the IPSec protocols offered.

```

Here is the IPSec proposal you specified...

Name = esp-prop1
  Pfs = N
  ESP Transforms:
    esp-tun1
Is this correct? [Yes]:
List of IPSEC Proposals:
  0: New Proposal
  1: strongP2EspProp
  2: strongP2EspAhProp
  3: veryStrongP2EspProp
  4: veryStrongP2EspAhProp
  5: esp-prop1

Enter the Number of the IPSEC Proposal [1]? 5
Are there any more Proposal definitions for this IPSEC Action? [No]: 1

```

Figure 273. Verifying IPSec proposal

Now the router shows the IPSec action you defined in Figure 274. By choosing option 1 we select *tun-101-102* as our IPSec action.

```

Here is the IPSec Action you specified...

IPSECAction Name = tun-101-102
  Tunnel Start:End      = 192.168.211.1 : 192.168.211.2
  Tunnel In Tunnel     = No
  Min Percent of SA Life = 75
  Refresh Threshold    = 85 %
  Autostart            = No
  DF Bit               = COPY
  Replay Prevention    = Disabled
  IPSEC Proposals:
    esp-prop1
Is this correct? [Yes]:
IPSEC Actions:
  0: New IPSEC Action
  1: tun-101-102

Enter the Number of the IPSEC Action [1]?

```

Figure 274. Verifying IPSec action

12.2.2.9 Defining ISAKMP action for IKE Phase 1

The only missing information from our policy tree is what we wish to offer for IKE Phase 1. As no ISAKMP action exists, we are prompted to create one. You would be prompted through the same questions if you used the `add isakmp-action` command.

We are creating an ISAKMP action called "ike-1" which occurs in main mode in Figure 275. The `lifesize` and `lifetime` parameters define how long an IKE Phase 1 tunnel can exist even through refreshes. Once this parameter has been reached, the tunnel must be started from the beginning, rather than just generating refreshed keys. Note that in this release, the router actually rebuilds the tunnel when the SA `lifesize`/time is reached. You can also control if the SA is negotiated at system initialization or only when traffic is received that matches the policy (answer = no). The router needs to know what IKE Phase 1 proposals offer and as none exist, the router prompts the creation of one in Figure 275. You would be prompted through the same questions if you used the `add isakmp-proposal` command.

```

ISAKMP Actions:
  0: New ISAKMP Action
  1: generalPhase1Action

Enter the Number of the ISAKMP Action [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Action []? ike-1
List of ISAKMP Exchange Modes:
  1) Main
  2) Aggressive

Enter Exchange Mode (1-2) [1]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, 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]:

```

Figure 275. Configuring ISAKMP action

12.2.2.10 Defining ISAKMP proposal for IKE Phase 1

We will create an IKE Phase 1 proposal, called "ike-prop1" that offers pre-shared keys, with authentication using MD5, encryption by DES, an SA lifetime as shown in Figure 276 on page 334. The lifetime/lifesize is defined as the amount of time/size that the Phase 1 SA can exist before the keys are refreshed. Actually, in this release, this parameter defines when the Phase 1 SA tunnel will be torn down and negotiated from the beginning.

So what is the difference between connection lifetime and SA lifetime?

Assume that the connection lifetime is 15 hours and the SA lifetime is set to 1 hour. The Phase 1 tunnel can be refreshed every hour up to a maximum of 15 hours where the connection lifetime is hit and no refreshes are allowed without rebuilding from the ground up. In this release, the connection lifetime/size is the same as the SA lifetime/size. This means that the Phase 1 tunnel is torn down each time the SA lifetime/size is hit and not really refreshed. It will be rebuilt, however, when the Phase 2 tunnel needs to be refreshed. The parameter is still there because it is needed if the policy has been retrieved from LDAP.

Note

A pre-defined menu for IPsec action in 2216 is `generalPhase1Action`. IPsec action by `generalPhase1Action` is as follows:

- Exchange Mode: Main
- Lifetime in seconds: 30000
- Lifesize in KB: 5000
- ESP proposals
 - StrongP1PropSharedKey
 - StrongP1PropRSACert
 - VeryStrongP1PropSharedKey
 - VeryStrongP1PropRSACert

Refer to Table 52 on page 334 for details of each proposal.

```

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
  1: strongP1PropSharedKey
  2: strongP1PropRSACert
  3: veryStrongP1PropSharedKey
  4: veryStrongP1PropRSACert

Enter the Number of the ISAKMP Proposal [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Proposal []? ike-prop1

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]?
Security Association Lifetime, in seconds (120-2147483647) [15000]?

List of Diffie Hellman Groups:
  1) Diffie Hellman Group 1
  2) Diffie Hellman Group 2

```

Figure 276. Configuring ISAKMP Proposal

There are four predefined menus for the ISAKMP proposal in 2216. Table 52 shows the pre-defined ISAKMP proposals.

Table 52. Predefined ESP proposal

| ESP proposal | Auth | Hash | Ciper | DH Grp | Lifetime (sec) | Lifetime (KB) |
|---------------------------|---------------|------|-------|--------|----------------|---------------|
| StrongP1PropSharedKey | Pre-Shared | MD5 | DES | Grp1 | 15,000 | 1,000 |
| StrongP1PropRSACert | RSA Signature | MD5 | DES | Grp1 | 15,000 | 1,000 |
| VeryStrongP1PropSharedKey | Pre-Shared | SHA | 3DES | Grp1 | 15,000 | 1,000 |
| VeryStrongP1PropRSACert | RSA Signature | SHA | 3DES | Grp1 | 15,000 | 1,000 |

12.2.2.11 Choosing ISAKMP action and policy

Now confirm your ISAKMP proposal and if it is correct, choose option 5 created now. Next verify the ISAKMP action you specified and if it is correct then select option 2. This is shown in Figure 277.

```

Here is the ISAKMP Proposal you specified...

Name = ike-propl
  AuthMethod = Pre-Shared Key
  LifeSize   = 1000
  LifeTime   = 15000
  DHGroupID  = 1
  Hash Algo  = MD5
  Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
  0: New Proposal
  1: strongPlPropSharedKey
  2: strongPlPropRSACert
  3: veryStrongPlPropSharedKey
  4: veryStrongPlPropRSACert
  5: ike-propl

Enter the Number of the ISAKMP Proposal [1]? 5
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

ISAKMP Name      = ike-1
  Mode            =                Main
  Min Percent of SA Life =        75
  Conn LifeSize:LifeTime =      5000 : 30000
  Autostart       =                Yes
  ISAKMP Proposals:
    ike-propl
Is this correct? [Yes]:
ISAKMP Actions:
  0: New ISAKMP Action
  1: generalPhase1Action
  2: ike-1

Enter the Number of the ISAKMP Action [1]? 2
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

```

Figure 277. Verifying ISAKMP Proposal and ISAKMP Action

12.2.2.12 Verifying defined policy

We have defined every leaf for the policy ike-pre-101-102 now. Finally the router is prompted for confirming the policy as shown in Figure 278:

```

Here is the Policy you specified...

Policy Name      = ike-pre-101-102
  State:Priority  =Enabled      : 5
  Profile        =101.0-to-102.0-pre
  Valid Period   =allTheTime
  IPSEC Action   =tun-101-102
  ISAKMP Action  =ike-1
Is this correct? [Yes]:

```

Figure 278. Verifying policy

Note

The same configuration could have been created by using the following commands from the bottom of the policy tree:

- add `profile` to create the profile "101.0-to-102.0-pre"
- add `validity` to create the validity period "always"
- add `ipsec-transform` to create the IKE Phase 2 transform, "esp-tun1"
- add `ipsec-proposal` to create the IKE Phase 2 proposal "esp-prop1" which uses transform "esp-tun1"
- add `ipsec-action` to define the Phase 2 tunnel, "tun-101-102" using proposal "esp-prop1" and transform "esp-tun1"
- add `iskamp-proposal` to define the IKE Phase 1 proposal "ike-prop1"
- add `isakmp-action` to define the IKE Phase 1 tunnel "ike-1" which uses proposal "ike-prop1"
- add `policy` which uses profile "ike-pre-101-102", validity period "always", IPsec action "tun-101-102" and ISAKMP action "ike-1"

12.2.2.13 Viewing defined policy and disabling unused policy

After finishing defining policies we could list all the policies created and disable the policies we do not use. Since we have finished defining the required policy we list all the policies created and we disable the policy for the manual tunnel as shown in Figure 279:

```
Center Policy config>LIST POLICY ALL

Policy Name      = ipsec_man_101_102
  State:Priority =Enabled   : 5
  Profile        =101.0-to-102.0
  Valid Period   =allTheTime
  Manual Tunnel  =1
  TunnelInTunnel =No

Policy Name      = ike-pre-101-102
  State:Priority =Enabled   : 5
  Profile        =101.0-to-102.0-pre
  Valid Period   =allTheTime
  IPSEC Action   =tun-101-102
  ISAKMP Action  =ike-1

Center Policy config>DISABLE POLICY
Enter the Name of the Policy to disable (? for a List)
[?]?

      1: ipsec_man_101_102
      2: ike-pre-101-102

Number of policy [1]? 1
```

Figure 279. Listing and disabling policy

12.2.2.14 Activating policies defined

We could use either way to make the configuration changes active. Use `reset database` command in the talk 5 policy feature as shown in Figure 280.


```
Center *TALK 5
Center +FEATURE Policy
IP Network Policy console
Center Policy console>RESET DATABASE
Policy Database reset successful
```

Figure 280. Resetting database

Or use the `write` and `reload` or `restart` commands as shown in Figure 281:

```
Center Config>WRITE
Config Save: Using bank A and config number 3
ranch Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 281. Reloading router

12.2.3 IKE with PKI configuration

We will now implement a configuration that uses PKI (or certificates) for authentication. In this example define a PKI authenticated tunnel between Router A and Router B and enforce a policy where traffic originating from Router A destined to Router B (and vice versa) will be made to flow over the tunnel. This example could easily be extended to force other traffic flows over the tunnel, for example, traffic between subnets 198.168.100.0 and 198.168.101.0.

The first step is to disable all existing policies to avoid confusion and to assist in problem determination by isolating the scope of any problems that may be encountered. This is achieved by the `TALK 6`, `FEATURE POLICY`, `DISABLE POLICY` commands.

12.2.3.1 Define a policy

Once all the existing policies have been disabled the next step is to define a new traffic policy. This is done in the same way as described in previous examples in this chapter except the policy using PKI as its authentication method. The traffic profile that we will define in this example will send traffic to and from Router A and Router B over the PKI authenticated tunnel.

The traffic policy will be called `ike-ds-211-211`. The following screen shows what the definition looks like in Router A:

```
Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ike-ds-211-211
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
```

Figure 282. Definition of a new policy for PKI authentication

The router then prompts us for a traffic profile. We will define a new profile for this policy. Once the new profile has been defined the router prompts us again for the traffic profile. This time we select the profile that has just been defined.

```

List of Profiles:
  0: New Profile
  1: 101.0-to-102.0
  2: 101.0-to-102.0-pre
  3: 3.0-to-100.0.pre
  4: 211.0-to-211.0-pre

Enter number of the profile for this policy [1]? 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 []? 211.0-to-211.0-ds
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]? 192.168.211.1
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Destination Address [0.0.0.0]? 192.168.211.2

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]?
Configure local and remote ID's for ISAKMP? [No]: y
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]? 1
Any user within profile definition allowed access? [Yes]:
Limit this profile to specific interface(s)? [No]:

Here is the Profile you specified...

Profile Name      = 211.0-to-211.0-ds
  sAddr          = 192.168.211.1 : sPort=    0 : 65535
  dAddr          = 192.168.211.2 : dPort=    0 : 65535
  proto          =                0 : 255
  TOS            =                x00 : x00
  Remote Grp=All Users
Is this correct? [Yes]: y

```

Figure 283. Definition of a new profile for PKI authentication

```

List of Validity Periods:
  0: New Validity Period
  1: allTheTime
  2: allTheTimeMonThruFri
  3: 9to5MonThruFri
  4: 5to9MonThruFri

Enter number of the validity period for this policy [1]?

```

Figure 284. Setting the validity period of the profile

The next step is to enter the profile's validity period.

The router then asks us for an IPsec action. We will define a new IPsec action.

```

Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
  0: New IPSEC Action
  1: tun-101-102

Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? tun-101-102-ds
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
[192.168.211.1]?
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
[0.0.0.0]? 192.168.211.2
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA liveness/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]: y

```

Figure 285. Defining a new IPsec action for PKI authentication

As part of the definition of the IPsec action, the router prompts us for an IPsec proposal.

```

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
  1: strongP2EspProp
  2: strongP2EspAhProp
  3: veryStrongP2EspProp
  4: veryStrongP2EspAhProp

Enter the Number of the IPSEC Proposal [1]? 1
Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPsec Action you specified...

IPSECAction Name = tun-101-102-ds
  Tunnel Start:End      = 192.168.211.1 : 192.168.211.2
  Tunnel In Tunnel      = No
  Min Percent of SA Life = 75
  Refresh Threshold     = 85 %
  Autostart             = Yes
  DF Bit                = COPY
  Replay Prevention     = Disabled
  IPSEC Proposals:
    strongP2EspProp
Is this correct? [Yes]: y

```

Figure 286. Defining a new IPsec proposal for PKI authentication

Now that the IPsec action has been fully defined, the router then prompts us again for the IPsec action that we wish to use. We will respond with the one that was just defined.

The router then prompts us to define for an ISAKMP action. In this example we will define a new action. It is here where we actually define the fact that we want to use certificate-based authentication under the ISAKMP proposal strongP1PropRSACert.

```

ISAKMP Actions:
    0: New ISAKMP Action
    1: generalPhase1Action
    2: ike-1

Enter the Number of the ISAKMP Action [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Action []? ds-act1

List of ISAKMP Exchange Modes:
    1) Main
    2) Aggressive

Enter Exchange Mode (1-2) [1]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, 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]:
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
    1: strongP1PropSharedKey
    2: strongP1PropRSACert
    3: veryStrongP1PropSharedKey
    4: veryStrongP1PropRSACert

Enter the Number of the ISAKMP Proposal [1]? 2
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

ISAKMP Name      = ds-act1
    Mode          =          Main
    Min Percent of SA Life =          75
    Conn LifeSize:LifeTime =          5000 : 30000
    Autostart     =          Yes
    ISAKMP Proposals:
        strongP1PropRSACert
Is this correct? [Yes]:
ISAKMP Actions:
    0: New ISAKMP Action
    1: generalPhase1Action
    2: ike-1
    3: ds-act1

Enter the Number of the ISAKMP Action [1]? 3

```

Figure 287. Defining a new ISAKMP action and proposal for PKI authentication

The last set of parameters enable the policy and confirm the definitions of the policy.

```
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-ds-211-211  
State:Priority   =Enabled      : 5  
Profile          =211.0-to-211.0-ds  
Valid Period    =allTheTime  
IPSEC Action    =tun-101-102-ds  
ISAKMP Action   =ds-act1  
Is this correct? [Yes]: y
```

Figure 288. Enabling and confirming the new policy for PKI authentication

A similar process must be performed on Router B except the IP addresses are swapped around.

12.2.3.2 Configure the certificates

Now that the policy has been defined all that is required is to load the certificates into the router. The current level of the router software supports a PKI where there is only one CA. This means that the router can only authenticate other devices whose certificates were issued by the same CA.

Certificates and certificate requests are transferred to and from the router using TFTP. Therefore, a TFTP server must be initially configured to support this. Additionally, it is important that the router's clock is correctly set to UMT, since certificates and certificate requests have a time stamp which can cause problems if not set correctly. Once these two operations have been done the router must be restarted/reloaded.

```

Center Config>FEATURE IPsec
IP Security feature user configuration
Center IPsec config>PKI
Center PKI config>ADD SERVER
Name ? (max 65 chars) []? tftp server
Enter server IP Address []? 9.24.106.104
Transport type (Choices: TFTP/LDAP) [TFTP]?
Center PKI config>EXIT
Center IPsec config>EXIT
Center Config>
Center *TALK 6

Center Config>TIME SET
year (YYYY) [1999]?
month (MM) [7]?
date (DD) [8]?
hour (hh) [24 hour format] [16]? 20
minute (mm) [55]?
second (ss) [54]?
Date and time updated successfully
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
The configuration has been changed, save it? (Yes or [No] or Abort): y
Config Save: Using bank B and config number 4
The configuration has been saved.

```

Figure 289. Setting the TFTP server to transfer certificates and the router's clock to UMT

Once the router has been restarted/reloaded the next step is to get the router to generate a public and private key pair and to generate a certificate request with its identity and the public key. All management and configuration of certificates are done through `TALK 5 > IPSEC > PKI`.

```

Center *TALK 5

CGW Operator Console

Center +FEATURE IPSec
Center IPSP>PKI
Center PKI Console>CERT-REQ
Enter the following part for the subject name 1
  Country Name(Max 16 characters) []? us
  Organization Name(Max 32 characters) []? ibm
  Organization Unit Name(Max 32 characters) []? itso
  Common Name(Max 32 characters) []? center
Key modulus size (512|768|1024) 2
[512]?
Certificate subject-alt-name type: 3
  1--IPv4 Address
  2--User FQDN
  3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 192.168.211.1
Generating a key pair. This may take some time. Please wait ...
Cert Request format: 1--DER;2--PEM 4
[1]? 2
PKCS10 message successfully generated
Enter tftp server IP Address []? 9.24.106.104
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]? /temp/center_pkcs10
Memory transfer starting.
.Memory transfer completed - succesfully.
Certificate request TFTP to remote host successfully.
Generated private key stored into cache
Please download router certificate and save
both router certificate and its private key ASAP.

```

Figure 290. Generating a certificate request

- 1 Subject name is the X.500 name in the certificate.
- 2 Key modulus size is the modulus key size that will be used in generating the public and private key pairs.
- 3 Subject-Alt-Name is the name used in the certificate to identify the party.
- 4 Certificate request format is either in Distinguished Encoding Rules (DER) or Privacy Enhanced Mail (PEM). DER is a binary format while PEM is a text-based format. You must choose the format that your CA uses.

What you have just done is made the router generate a public and private key pair and formed a certificate request with that public key in the file which was uploaded to the TFTP server. The private key never leaves the router. If the router is restarted before the certificate has been downloaded to the router and saved a new certificate request must be performed.

Once you have the certificate request you then must ask the CA for a certificate. This is dependent on how your CA has implemented the issuing of certificates. In this example we will use the Entrust Web site (<http://www.entrust.com>) which issues temporary demonstration certificates at no cost. The Web site simply asks you to copy and paste the certificate request after which it generates a certificate that you can copy and paste. This is why PEM was used in this example so that it could be manipulated with a text editor.

The first step is to copy the certificate request onto the clipboard. You could use Notepad or Wordpad to do this, but these editors seem to have trouble with the CR/LF characters at the end of each line in the certificate request. The best way is to simply perform a DOS `TYPE` command to display the certificate request and then to mark and copy straight out of the DOS window.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB0zCCATwCAQAwSzELMAkGA1UEBhMCVVMxDTALBgNVBAgTBE4uQy4xDDAKBgNV
BAoTA01CTTENMAsgA1UECXMESVRITzEQMA4GA1UEAxMHcGM3NTAtcjCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwYkCgYEAj5jIPsbpJ1Cn2Ux19si60CFQqpUYGKIEBZg/
HROqhEwOi/51jYV0SLiXD86WY1iQx6rVtLBYLhwZU1bThjJcYnyZ6sMMndX3OigB
hKogJkGQF+7v6OxmxCXYR4ng+Pod04m1K0siGgX7s8AYsC9qR2sjGAz1vjXkD0qa
/VwqLskCAwEAAABIMEYGCsGSIb3DQEJJDjE5MDcwNQYDVR0RBC4wLiCErBADB4ES
cGM3NTAtckB1cy5pYm0uY29tghBpdHNvLnJhbC5pYm0uY29tMA0GCSqGSIb3DQEB
BAUAA4GBADDk31RQma1sIJmdi63bhtZ57W1eaXCF4/d5YuyZzp5gjsWTozP0zohy
F+ZVCnamLwLE7Iv0+3eL/iPpVUJb8ysGAM89AZUqhwR58ITb1SetFeT41W1jNcU
p1UhD7M9peEw9mWZPaqWDE9NCPcoAZn4G1NSK6gUgiuEv+5ACUk6
-----END NEW CERTIFICATE REQUEST-----
```

Figure 291. Using the DOS `TYPE` command to display the certificate request

Make sure when you mark the window you include the header and footer which mark the start and end of the certificate.

Once the certificate request has been copied onto the clipboard, go to the Entrust Web site at <http://www.entrust.com> to request a free demonstration certificate. The free certificates are accessible from the downloads section where you will be able to request a VPN certificate. Some personal details must be entered before you can request the certificate.

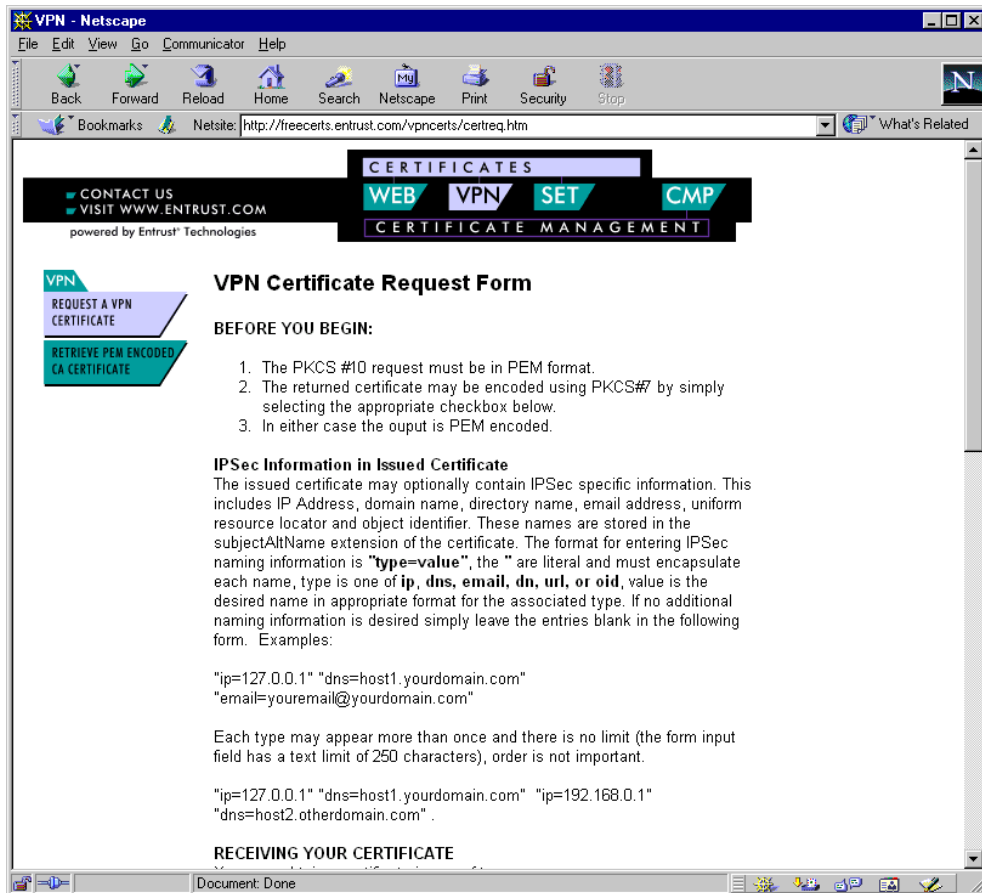


Figure 292. Entrust certificate request Web page - top half

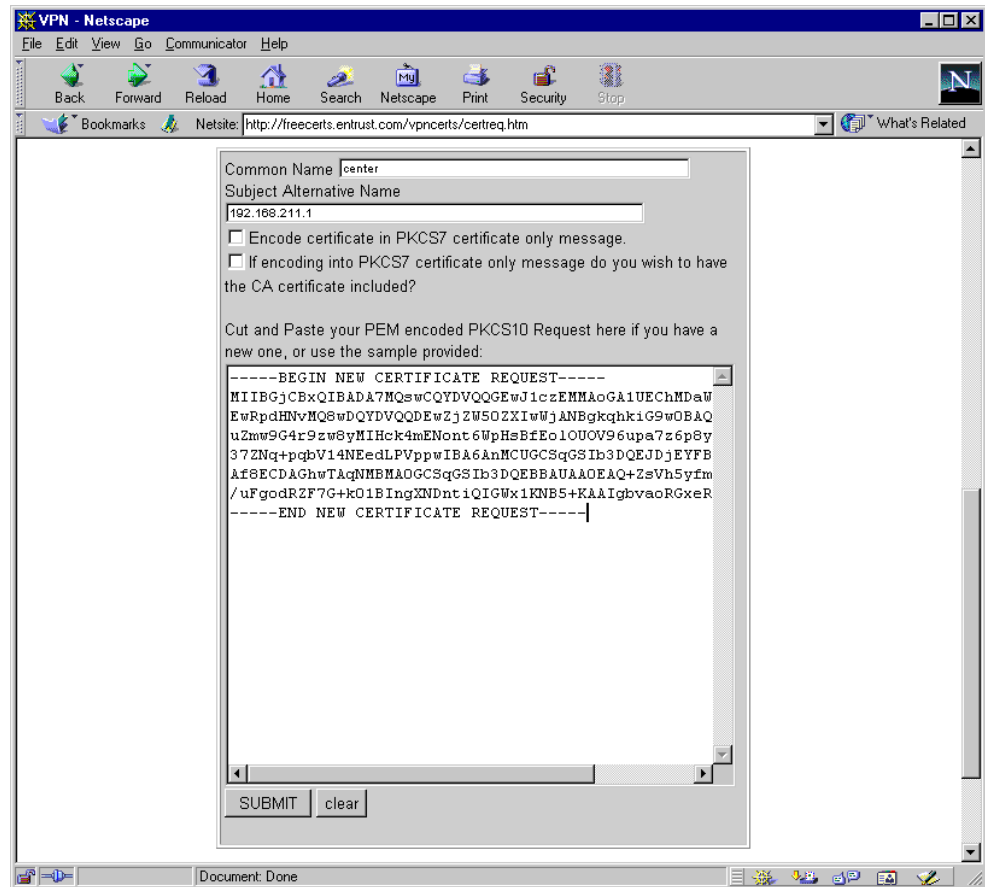


Figure 293. Entrust certificate request Web page - bottom half

Once you have reached the page to request a certificate, simply paste the certificate request into the appropriate area, fill in the fields for Common Name and Subject Alternative Name, uncheck the option, Encode certificate in PKCS7 certificate only message, and then click **SUBMIT**. Then after a period of time a certificate will be generated.

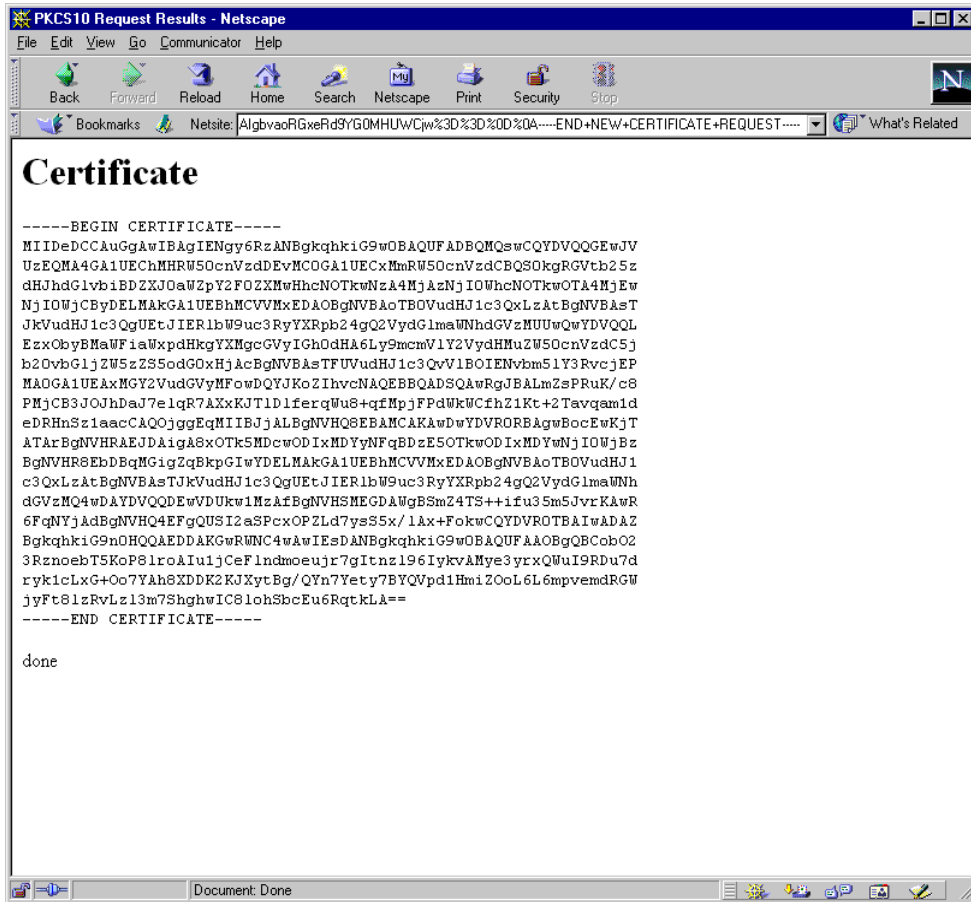
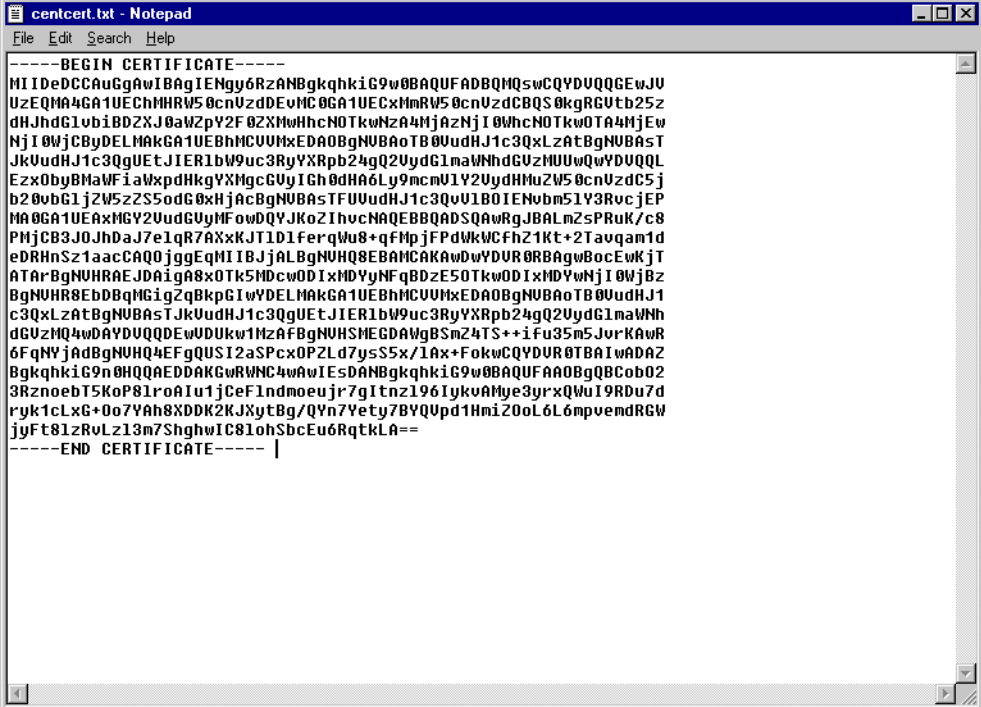


Figure 294. Router's certificate generated by the Entrust Web page

Once the certificate has been generated simply mark and copy the certificate including the header and footer which mark the beginning and end of the certificate. Using Notepad, paste it into an empty document and save the file to an area accessible by the TFTP server.



centcert.txt - Notepad

```
-----BEGIN CERTIFICATE-----
MIIDeCCAUgGAWIBAgIENgy6RzANBgkqhkiG9w0BAQUFAADBQMQuwCQYDVQQGEwJU
UzEQHh44GA1UEChMHRW50cnVzdDEvMC8GA1UEC3MHRW50cnVzdDBQSQ0kgRGTb25z
dHJhdG1ubjBDZXJ0aWZpY2F0ZXNwHhcNMDk0MzA4MjAzNjI0WzcvMC8GA1UEAzoT
NjI0WjCBYDELMAkGA1UEBhMCVVhEADA0BgNUBA0TB0UudHJ1c3QxLzAtBgNUBA0T
JkUudHJ1c3QgUETJIER1bW9uc3RyYXRpb24gQ2UydG1maW5hdGUzMUUwQWYDUQL
Ezx0byBHaWFiZW90dHkgYXN0YyIGh0dHA6Ly9mcnU1Y2UyYyYyYyYyYyYyYyYyYyYy
b20vbG1jZW5zZW50dG8xHjAcBgNVBA0TFUudHJ1c3QxLzAtBgNUBA0Tb25zZDQw
MA0GA1UEAxMGMGYyUudGUyMFowDQYJKoZIhvcNAQEBBQADSwAwRgJBALm2sPRuK/c8
PMjCB3JOJhdAJ7e1qR7AXxKJT1D1FerqWu8+qFmpjFPdWkWCfhZ1Kt+2Tavqam1d
eDRHnSz1aacCAQ0jggEqMIIBJjALBgNVHQ8EBAMCAKAwDwYDVR0RBBAgWocEwKjT
AATarBgNVHRAEJDaiGA8xOTk5MDcwODIxMDYyNFqBdzE50TkWODIxMDYyNjI0WjBz
BgNVHR8EBDBqMG1gZkBkP6IwYDELMAkGA1UEBhMCVVhEADA0BgNUBA0TB0UudHJ1
c3QxLzAtBgNUBA0TJkUudHJ1c3QgUETJIER1bW9uc3RyYXRpb24gQ2UydG1maW5h
dGUzMUUwQWYDUQL4wDAYDUQDEwUDUKw1HzAFBgNVHSMGDAWgBsmZ4TS++iFu35m5
JurKAAR6FqNYjadBgNVHQ4EFgQUSI2aSPcx0PZLd7ysS5x/1Ax+FokwCQYDUR0TB
AIwADAZBgkqhkiG9w0HQQAEDDAKgwRwNc4wAwIESDANBgkqhkiG9w0BAQUFAA0B
GQCOB023RZnoebI5KoP81roAIu1jCeF1ndmoeujr7gltnz196IykvAMye3yrxQWu
I9RDu7d ryk1cLxG+0o7VAh8XDDK2KjXytBg/QVn7Yety7BYQUpd1HmiZ0oL6L6mp
vemdRGWjyFt8LzRvLz13m7ShghwIC81ohSbcEu6RqtKLA==
-----END CERTIFICATE-----
```

Figure 295. Router's certificate copied into Notepad

You should now have a certificate for the router stored as a text file on the TFTP server. The next step is to load the certificate onto the router.

```
Center PKI Console>LOAD CERTIFICATE
Enter the type of the certificate:
Choices: 1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]? 2
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]? 2
Server info name []? tftp server
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /tmp/centce
rt.txt

Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - succesfully.
Router Certificate loaded into run-time cache
```

Figure 296. Loading the certificate onto the router

A problem that may occur at this time is that the certificate fails to load.

```
Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - succesfully.
Error occurred in storing certificate in cache!
```

Figure 297. Failing to load the router's certificate

The corresponding messages in the event log are:

```

00:06:29 DOLOG: DEBUG: BSAFE req allocated

00:06:29 DOLOG: DEBUG: came out of wait with opc = 0

00:06:29 DOLOG: CERT: get_DN_DER()  e~•@: , ,ÿlè~Àè°ñ

00:07:32 DOLOG: der =286 pem =382

```

Figure 298. Event log when the router failed to load its certificate

If you encounter this problem then the most likely reason for the failure is the clock in the router. It is imperative that the clock is set correctly before the certificate request is generated.

Once the router has successfully loaded its certificate you must then save the certificate to ensure the certificate and its corresponding private key are stored in nonvolatile memory.

```

Center PKI Console>CERT-SAVE
Enter type of certificate to be stored into SRAM:
  1)Root certificate;
  2)Box certificate with private key;
Select the certificate type (1-2) [2]? 2
SRAM Name for certificate and private key []? entrust-center-19990708
Load as default router certificate at initialization? [No]: y
Both Router Certificate and private key saved into SRAM successfully

```

Figure 299. Saving the router's certificate and private key into nonvolatile memory

The router can now be restarted without losing its private key and corresponding certificate.

The next step is to load the certificate of the CA. This is done in exactly the same way as loading the router's certificate. The certificate of the CA can be found at the CA, and is basically a self-signed certificate. At the Entrust Web site there is a link in the VPN Certificates page. Instead of pressing the button that requests a certificate, there is a link that allows you to retrieve a PEM-encoded CA certificate. Again you will be prompted to enter personal information before you get to the page with the actual certificate.



Figure 300. The CA's certificate from the Entrust Web page

We only need the information directly under CA Certificate, so simply mark and copy that area onto the clipboard. Using the Notepad paste the contents of the clipboard into an empty document. Then add the header and footer to indicate the beginning and end of the certificate. These are exactly the same as those found in the Router certificate.

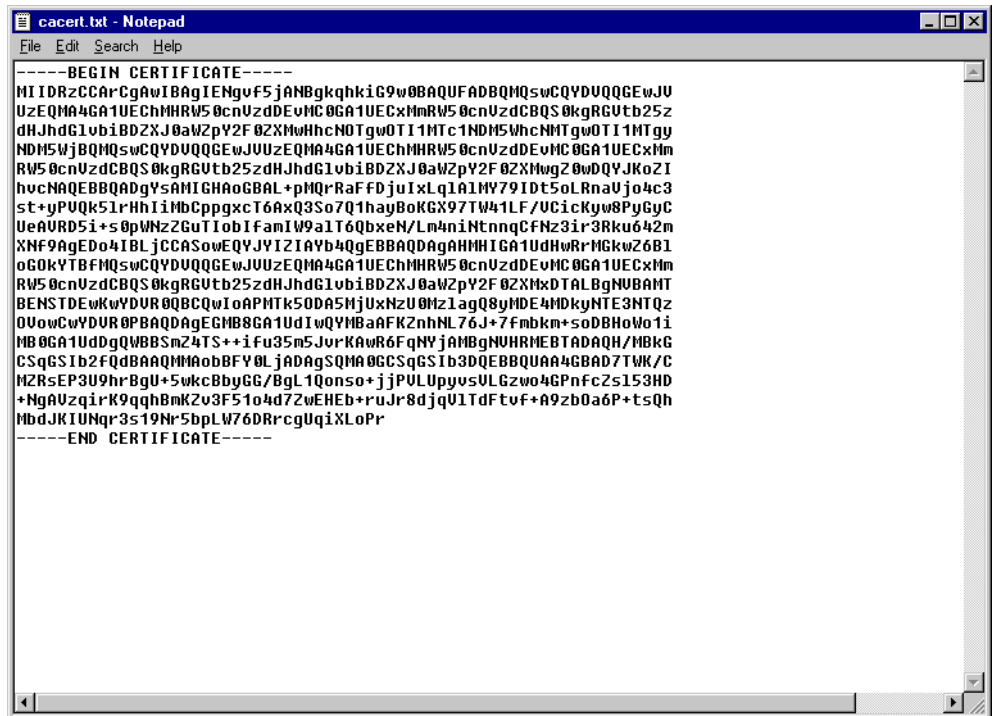


Figure 301. CA's certificate copied into Notepad with a header and footer

Once the header and footer are in place save the file to an area accessible by the TFTP server.

The next step is to load the CA certificate onto the router and save it into nonvolatile memory. The process is almost exactly the same as described for the router's certificate.

```
Center PKI Console>LOAD CERTIFICATE
Enter the type of the certificate:
Choices: 1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]? 1
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]? 2
Server info name []? tftp server
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /temp/cacert
.txt

Attempting to load certificate file. Please wait ...
Memory transfer starting.
Memory transfer completed - successfully.
Root CA Certificate loaded into run-time cache
Center PKI Console>CERT-SAVE
Enter type of certificate to be stored into SRAM:
  1)Root certificate;
  2)Box certificate with private key;
Select the certificate type (1-2) [2]? 1
SRAM Name to store Root Certificate? []? entrust-ca-19990708
Load as default root certificate at initialization? [No]: y
Root Certificate saved into SRAM successfully.
```

Figure 302. Loading and saving the CA's certificate

You can view the certificates that have been loaded onto the router.

```
Center PKI Console>LIST CERTIFICATE
Router certificate
  Serial Number: 906803783
  Subject Name: /c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
/ou=No Li/c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
  Issuer Name: /c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
  Subject alt Name: 192.168.211.1
  Key Usage: Sign & Encipherment
  Validity: 1999/7/8 20:36:24 -- 1999/9/8 21:06:24

Root CA certificate
  Serial Number: 906747878
  Subject Name: /c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
  Issuer Name: /c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
  Validity: 1998/9/25 17:54:39 -- 2018/9/25 18:24:39
```

Figure 303. Viewing certificates that have been loaded onto the router

12.2.3.3 Event log

By displaying all IKE and PKI subsystem messages you are able to see the process that the router goes through to set up a tunnel using certificate-based authentication.

```
00:00:00 GW.002: Portable CGW Center Rel 2216-MAS Feature 2895 V3.3 Mod 0 PTF
0 RPQ 0 MAS.FF6 cc50_9d
strtd
00:00:00 GW.005: Bffrs: 400 avail 400 idle fair 51 low 80
00:00:00 PKI.041: X500DN initialized. Total X500 Attribute name 11

00:00:00 PKI.070: Store my private key into cache success. key buffer length=34
4
00:00:00 PKI.065: PKI Cert key usage (Signature) check success
00:00:00 PKI.009: Validity check: success. Current date: 1999/7/9, Time: 1:23:1
1. Cert valid date: 1999/7/8 20:6:24 -- 1999/9/8 20:6:24.

00:00:00 PKI.066: Store local cert life from router start 5341393

00:00:00 PKI.056: PKI cert validity check status successful

00:00:00 PKI.053: PKI alt-name IPv4 Addr Value 192.168.211.1

00:00:00 PKI.061: PKI cert alt-name processing status: successful

00:00:00 PKI.059: PKI store Router cert ID status successful

00:00:00 PKI.060: PKI processing Router cert successful

00:00:00 PKI.069: Store my cert into cache success. cert length=892
00:00:00 PKI.034: Load Router Cert Success. cert ID=ENTRUST-CENTER-19990708

00:00:00 PKI.071: Store root cert into cache success. cert length=843
00:00:00 PKI.034: Load Root CA Cert Success. cert ID=ENTRUST-CA-19990708

00:00:00 PKI.048: PKI initialized.
```

Figure 304. PKI initialization in the event log

You can see what the router tries to do immediately after bootup. Initially it loads its private key into cache and checks the validity of its own certificate. If everything is OK it then loads its certificate into cache. The last step in the PKI initialization is to load the CA's certificate. This is shown in Figure 304 on page 353.

After the PKI initialization the router then tries to set up the tunnel. The router tries to initiate the tunnel by starting an IKE Phase 1 main mode negotiation. (See Figure 305 on page 355.)

The router receives a Phase 1 main mode initiator message from the other router so it quickly terminates the Phase 1 negotiations it started and starts the Phase 1 negotiation as the responder. The first two messages of Phase 1 negotiate the ISAKMP SA policies. This router examines the proposals that the other router sent and chooses one. In our configuration there was only one proposal. This router finds the proposal acceptable and responds to the other router by sending a message with that proposal.

The next two messages exchange information to determine the shared secret keys that will be used in subsequent messages. Here you see the router receive the components to be able to perform a Diffie-Hellman operation to generate the keys. This router also responds to the other router in the same way. Notice that each party requested the certificate of the other party. This request will be satisfied in the next two message flows.

Now all subsequent messages will be encrypted with the keys that were just generated. The next two messages authenticate the routers. Each router will send a signed message containing its ID and certificate. Each router will then perform the following checks on the messages they have just received:

- Certificate can be used for signing
- Validity date of the certificate is still current
- Certificate was issued by the correct CA
- Validates the identity in the certificate with the identity in the message
- Checks the signature

Phase 1 negotiations have now been completed.

```

00:00:00 IKE.018: IKE Public Key module init success. Exit point: Normal 0
00:00:00 IKE.009: Begin Main mode - Initiator
00:00:00 IKE.013: To Peer: 192.168.211.2 MM HDR SA
00:00:00 IKE.001: Trace IKE packet to 192.168.211.2
00:00:00 DOLOG: .....Remote Logging Facility is now available.....

00:00:05 IKE.011: No response from Ike peer: Retransmit packet
00:00:05 IKE.001: Trace IKE packet to 192.168.211.2
00:00:10 IKE.011: No response from Ike peer: Retransmit packet
00:00:10 IKE.001: Trace IKE packet to 192.168.211.2
00:00:12 IKE.001: Trace IKE packet from 192.168.211.2
00:00:12 IKE.013: From Peer: 192.168.211.2 MM HDR SA
00:00:12 IKE.014: Phase 1 SA DELETED for Peer: 192.168.211.2
00:00:12 IKE.014: Phase 2 SA DELETED for Peer: 192.168.211.2
00:00:12 IKE.009: Begin Main mode - Responder
00:00:13 IKE.014: Oakley proposal is acceptable. Peer: 192.168.211.2
00:00:13 IKE.013: To Peer: 192.168.211.2 MM HDR SA
00:00:13 IKE.001: Trace IKE packet to 192.168.211.2
00:00:13 IKE.001: Trace IKE packet from 192.168.211.2
00:00:13 IKE.013: From Peer: 192.168.211.2 MM HDR KE NONCE CERT_REQ
00:00:13 IKE.003: Processing ISA_KE
00:00:14 IKE.003: Processing NONCE
00:00:14 IKE.013: To Peer: 192.168.211.2 MM HDR KE NONCE CERT_REQ
00:00:14 IKE.001: Trace IKE packet to 192.168.211.2
00:00:14 IKE.001: Trace IKE packet from 192.168.211.2
00:00:14 IKE.002: Trace IKE payload after decryption from Peer: 192.168.211.2
00:00:14 IKE.013: From Peer: 192.168.211.2 MM HDR* ID CERT SIG
00:00:14 PKI.065: PKI Cert key usage (Signature) check success
00:00:14 PKI.009: Validity check: success. Current date: 1999/7/9, Time: 1:23:2
5. Cert valid date: 1999/7/8 20:59:3 -- 1999/9/8 20:59:3.

00:00:14 PKI.066: Store local cert life from router start 5340952
00:00:14 PKI.056: PKI cert validity check status successful
00:00:14 PKI.010: Root CA in cache? Yes length=843.
00:00:14 PKI.057: PKI cert root CA check status successful
00:00:14 PKI.058: PKI store peer public key status success
00:00:14 PKI.058: PKI store peer public key status successful

00:00:14 PKI.053: PKI alt-name IPv4 Addr Value 192.168.211.2

00:00:14 PKI.061: PKI cert alt-name processing status: successful

00:00:14 PKI.059: PKI store Peer cert ID status successful

00:00:14 PKI.060: PKI processing Peer cert successful

00:00:14 IKE.016: process_cert: ID match: cert ID: 192.168.211.2
00:00:14 IKE.016: ID payload ID: 192.168.211.2
00:00:14 IKE.003: Processing RSA signature
00:00:14 PKI.068: Retrieve peer cert public key successful
00:00:14 IKE.020: IKE signature public key verification success
00:00:14 IKE.021: IKE signature matched
00:00:14 IKE.014: ValidatePhase1ID: cpeP1Handles match. Peer: 192.168.211.2
00:00:14 PKI.072: Get my cert from cache success. cert length=32026724
00:00:14 IKE.019: IKE signature private key signing success
00:00:14 IKE.010: Finished Main mode -responder
00:00:14 IKE.013: To Peer: 192.168.211.2 MM HDR* ID CERT SIG
00:00:14 IKE.002: Trace IKE payload before encryption to Peer: 192.168.211.2
00:00:14 IKE.001: Trace IKE packet to 192.168.211.2

```

Figure 305. Phase 1 negotiation in the event log

Notice that a challenge to encrypt a random message does not need to occur. This is because the signature process effectively does the same thing, encrypting a hash of the message. The original message itself contains information from messages 1 through 4 and the generated master key, which effectively makes the message random.

The Phase 2 negotiations must now occur. (See Figure 306 on page 356.) This router tries to initiate the Phase 2 negotiation but soon realizes that the other router has already started and therefore terminates the one it started and begins acting as responder for Phase 2.

There are only three messages in a Phase 2 negotiation. The first message was received by this router indicating that the remote router wishes to initiate a Phase 2 negotiation. This router examines the request and checks all the relevant fields. It then sends a similar message back to the other router. Notice that there is no key exchange attribute in these first two messages. This is because PFS was not requested, because the key exchange is only needed to perform a new Diffie-Hellman operation for PFS.

The third message from the other router is to ensure the liveness of the operation.

The router then loads two SAs, one for each direction of traffic.

```
00:00:14 IKE.009: Begin Quick mode - Initiator
00:00:14 IKE.013: To Peer: 192.168.211.2 QM HDR* HASH SA NONCE ID ID
00:00:14 IKE.002: Trace IKE payload before encryption to Peer: 192.168.211.2
00:00:14 IKE.001: Trace IKE packet to 192.168.211.2
00:00:14 IKE.001: Trace IKE packet from 192.168.211.2
00:00:14 IKE.009: Begin Quick mode - Responder
00:00:14 IKE.002: Trace IKE payload after decryption from Peer: 192.168.211.2
00:00:14 IKE.013: From Peer: 192.168.211.2 QM HDR* HASH SA NONCE ID ID
00:00:14 IKE.003: Processing Quick Mode ID
00:00:14 IKE.003: Processing Quick Mode ID
00:00:14 IKE.015: Acceptable phase 2 proposal # 1
00:00:14 IKE.003: Processing NONCE
00:00:14 IKE.013: To Peer: 192.168.211.2 QM HDR* HASH SA NONCE ID ID
00:00:14 IKE.002: Trace IKE payload before encryption to Peer: 192.168.211.2
00:00:14 IKE.001: Trace IKE packet to 192.168.211.2
00:00:14 IKE.001: Trace IKE packet from 192.168.211.2
00:00:14 IKE.011: isakmp_input: drop incoming retransmitted message
00:00:14 IKE.001: Trace IKE packet from 192.168.211.2
00:00:14 IKE.002: Trace IKE payload after decryption from Peer: 192.168.211.2
00:00:14 IKE.013: From Peer: 192.168.211.2 QM HDR* HASH
00:00:14 IKE.008: Load Out SA: Alg=18 Prot=3 Sec=3600 KB=50000 SPI=705313650
00:00:14 IKE.008: Load In SA: Alg=18 Prot=3 Sec=3600 KB=50000 SPI=470776623
```

Figure 306. Phase 2 negotiation in the event log

12.2.3.4 Controlling user access

With certificate-based authentication you have the ability to easily scale up your VPN network. All that is required is to deploy your own CA which controls what certificates are issued and therefore, access to the network. There are cases where you will want to deny access even if the device was issued with a valid certificate.

1. The current level of software does not check for CRL. This means that if you wish to revoke access to a device or user the fact that the router does not check the CRL means that access will still be permitted. The router simply checks that they have a valid certificate, that is, signed and issued by the authorized CA and has not expired.
2. Some organizations may not want to deploy their own PKI, and instead will outsource the issuing of certificates to another organization. In situations like these you only want to give access to those users and devices within your organization, rather than anybody who has had a certificate issued by the same CA.

What is required is the ability to deny access to users. Even if they passed the certificate authentication it is like saying that you definitely knew the identity of the other person but you still do not want to give access. The example above allows access to all users who were authenticated because we took the default answer of yes when we were asked the question, Any user within profile definition allowed access?, when defining the traffic profile (see Figure 283 on page 338).

If you wish to restrict access to a particular set of users you must first define users into a user group:

```
Center 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]? 192.168.211.2
Group to include this user in []? branch office
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]? 2

Here is the User Information you specified...

Name      = 192.168.211.2
Type      = IPV4 Addr
Group     =branch office
Auth Mode =Certificate
Is this correct? [Yes]: y
```

Figure 307. Add a user into a user group

Once you have defined all your users into the user group you then simply change the traffic profile to restrict access. Keep all the existing values the same until you get to the question, "Any user within profile definition allowed access?"

Note

To answer the "Any user within profile definition allowed access?" question, you must say yes to the "Configure local and remote IDs for ISAKMP?" question.

```

Configure local and remote ID's for ISAKMP? [No]: y
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]: n
Select the user group to allow access:

Group Name:
User List:
  grp1.company.com
  9.24.106.96
  192.168.88.5
  172.16.3.7
  192.168.212.2

Group Name: branch office
User List:
  192.168.211.2

Enter the name of the user group []? branch office
Limit this profile to specific interface(s)? [No]:

Here is the Profile you specified...

Profile Name = 211.0-to-211.0-ds
sAddr:Mask= 192.168.211.1 : 255.255.255.255 sPort= 0 : 65535
dAddr:Mask= 192.168.211.2 : 255.255.255.255 dPort= 0 : 65535
proto      = 0 : 255
TOS        = x00 : x00
Remote Grp=branch office
Is this correct? [Yes]: y

```

Figure 308. Allowing access to a particular user group only

Part 3. VPN scenarios using IBM VPN platforms

Chapter 13. Building branch office VPNs

This chapter describes how IBM VPN solutions can be used to implement virtual private networks based on the branch office interconnection scenario. Essentially, this means extending the corporate intranet to remote sites across a public network.

This scenario can be also deployed in one intranet. It may be reasonable to connect in this way, for example, two highly secure development laboratory networks over the existing corporate network infrastructure.

Consider a company that was running its own private network, using its own routers, bridges, and private lines. If the company had campuses at geographically dispersed sites, it may prove more economical to break the corporate network into pieces (the intranets), add a firewall to control traffic flow across the intranet/Internet boundary, and then procure service from one or more ISPs to interconnect the intranets over the Internet backbone.

13.1 Design considerations

Let us consider how company A could construct a virtual private network for interconnecting its intranets securely. In the discussion we do not take into account the basic Internet access issues, since these can be well separated and are outside the scope of this redbook.

13.1.1 Authenticating backbone traffic

The Internet will be carrying traffic not just from company A's VPN, but also from other VPNs. Company A's firewalls must admit only traffic from company A's VPNs and must reject all other incoming traffic. They might admit non-VPN incoming traffic destined to them in case they provide general Internet connectivity, for example, if they operate proxies or SOCKS servers. However, in the case of a large company with many VPNs it is worth considering the separation of functions, that is, dedicated security gateways for VPNs and others for general Internet access. It is more expensive but dedicated VPN gateways are much harder to bring down by denial of service attacks, because they accept only authenticated traffic. Companies in most cases are much more sensible to the loss of branch connectivity than to the loss of Web access.

Deploying IPSec's authentication protocols in company A's firewalls (or IPSec-enabled routers) at the intranet boundary will accomplish these goals. IPSec's authentication techniques are cryptographically strong, so they provide significantly better protection against address spoofing and denial of service attacks than would rely on conventional, noncryptographic filtering techniques. In this scenario, cryptographic authentication using HMAC will be the first line of defense. Having established that the traffic has come from somewhere within company A's network, noncryptographic filtering can then be used as the second line of defense to provide more granular access control, if desired.

13.1.2 Data confidentiality

It should be obvious that company A will want to keep its data confidential (that is, encrypted) while it is in transit across the public Internet. But it is not always clear

if the data should also be protected when it flows within its own intranets. If the company had not previously encrypted its internal traffic when it used a monolithic private network, it may not see value in encrypting it when it flows within its intranets.

If a company does not believe that it is subject to internally mounted attacks, the simplest solution is to encrypt and authenticate traffic flowing between firewalls, and make no security-related changes to the end systems themselves. This has the advantage of much fewer security associations to manage: two per firewall for bidirectional data flow, compared to two per host for host-to-host encryption. But it has the disadvantage that traffic is exposed to relatively simple attacks while it flows in the intranet. Since authentication is also needed between firewalls, the simplest branch office VPN will use ESP in tunnel mode with authentication between the two firewalls. Another solution is the combination of AH and ESP in tunnel mode, which has the advantage of authentication of the outer IP header as well, thus avoiding the denial of service attacks.

For considerations on how to configure a VPN solution between branch offices that can protect you against threats both in the Internet and in your company's intranet, please refer to Chapter 14, "Building business partner/supplier VPNs" on page 403, where we discuss this topic in a slightly different context of two different companies. However, the solution is the same.

13.1.3 Addressing issues

We assumed that company A previously had a traditional network in place, where its various intranets were interconnected over private facilities, such as leased lines or frame relay. We also assumed that company A has already developed an address plan for its network. Since the network was self-contained and the backbone used only private facilities, company A could have used either globally ambiguous (private) IP addresses (that is, of the form 10.x.y.z) or globally unique (public) addresses obtained from the Network Information Center (NIC).

Because assignment of public IP addresses is coordinated through a global authority, they are unambiguous. Public addresses are routable everywhere. However, because private address assignments are facilitated locally without coordination by a global authority, they are ambiguous when used in the public Internet; they are routable only within a company's own private network.

In summary:

1. If company A uses public addresses in its network, the addresses can continue to be used without change in the VPN environment. If it is desired to hide them while the datagram is in transit over the Internet, an ESP tunnel can be used between firewalls.
2. If company A uses private IP addresses in its network, the addresses can also continue to be used on all subnets that have no physical connection to the public Internet. But for those subnets that do connect to the public Internet, typically the exit links at the boundary of the intranet, a public IP address must be used.

ESP tunnel mode or AH and ESP in tunnel mode between firewalls handles both situations. The tunnel's new IP header will use the global addresses of the two firewalls, allowing datagrams to be routed over the Internet between the two firewalls (or routers). The header of the original (inner) IP datagram will use the IP

addresses assigned for use in the intranet; since these addresses will be hidden from view by ESP's encryption protocol, they can be either publicly or privately assigned.

13.1.4 Routing issues

Because a VPN in fact resembles a set of IP networks, all but the smallest VPNs will typically need to deploy an IP routing protocol between the gateway machines (firewalls or routers) at the boundaries of the company's intranets. Routing protocols typically exchange information that will describe the topology of the VPN. That is, the topology updates will describe the IP addresses that are reachable within each intranet that participates in the VPN. IPSec can be used to both encrypt and authenticate the routing information, thus hiding topological details of the intranet as they are exchanged across the public network.

The company's network administrator(s) can incorporate conventional IP routing protocols into the VPN gateways, and then use IPSec protocols to encrypt and authenticate the exchange of routing information among the firewalls. Figure 309 illustrates this concept schematically for a sample configuration that consists of three branch offices of a given company that need to communicate among themselves via the public Internet.

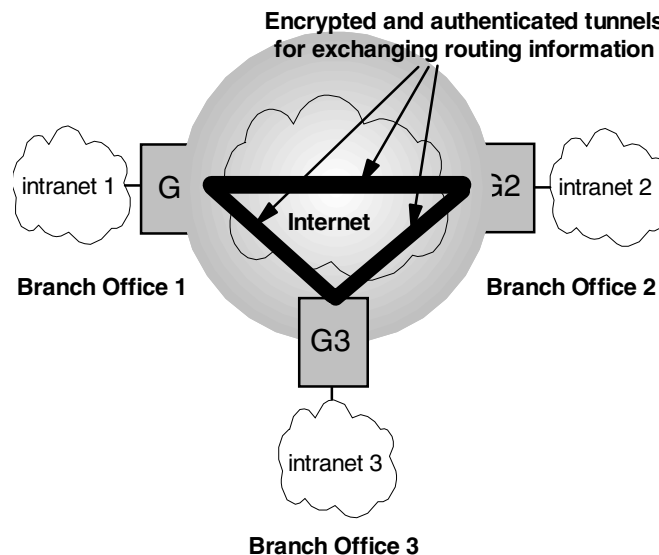


Figure 309. Exchanging routing information securely

When an IPSec tunnel is established between a pair of firewalls, they appear to be logically adjacent to one another, even though there may be several routers along the actual physical path. Each pair of virtually adjacent security gateways will set up a security association between themselves, using ESP in tunnel mode with authentication or AH and ESP in tunnel mode to provide both encryption and authentication. The routing information that is exchanged will then be hidden from view because it will have been encrypted.

Because the set of firewalls participate in a common routing protocol, they will know the correct firewall for reaching any given destination host within the intranets. Hence, traffic arriving at an exit firewall can be sent via an ESP tunnel, using its authentication option or a combined AH-ESP tunnel, and can then be

authenticated by the entry firewall that protects the remote branch office's intranet.

Thus, IPSec makes it possible to exchange routing information and user data between branch offices over the Internet while preserving the confidentiality of both user data and intranet topology information. Because routing information (for example, IP addresses) is visible only to other members of the corporate network, this scheme can be used regardless of whether addresses used in the interior of an intranet are globally unique or privately assigned.

To be more specific, since the intranet addresses are carried within encrypted routing update messages, they are neither visible to, nor used by, any of the routers in the Internet. Therefore, if company A's intranets use a self-consistent addressing scheme, either public or private, network address translation is not needed for intranet addresses. Encapsulating encryption already hides the interior addresses, and all backbone routing is based only on the public IP addresses of the boundary gateways. Finally, depending on the sophistication of the routing algorithms, it may also be possible to support redundant entry/exit points into a corporate network.

Important!

Some routing protocols use multicast or broadcast addresses, for example, OSPF and RIP. IPSec currently only defines the use of unicast addresses, which means these routing protocols can only be supported using a layer-2 tunnel which can then be secured using an IPSec tunnel. This does, however, add unnecessary overhead to support the layer-2 tunnel even though the only traffic that would be flowing would be layer-3 IP traffic.

BGP is a routing protocol that uses unicast addresses. Many organizations use this protocol to interconnect branch offices because of the small amount of bandwidth it takes, and its strong ability to control and filter the routing tables that are propagated and advertised in the network.

13.1.5 Summary: branch office connection

This application replaces existing private lines or leased lines in a corporate network, and uses the public Internet as the backbone for interconnecting a company's branch offices. (This solution is not limited only to branch offices, but can also be applied between any collection of a company's geographically dispersed sites, such as labs, manufacturing plants, warehouses, etc.) This solution does not mandate any changes in the clients (PCs or servers) unless it is desired to protect against internal attacks as well as external ones.

The design features are:

- Client machines (hosts and servers) need not support IPSec if the intranets are considered to be trusted and secure. This minimizes the migration issues of moving to a VPN approach and maintains the pre-existing host-to-host security policies and procedures of the original network. IPSec support will be required only at the intranet boundaries, that is, in the VPN gateway boxes. Also, there will be no security-related protocols required in any of the routers, bridges, or switches that are located either in the interior of the intranets or in the public backbone Internet.

- VPN gateways situated at the perimeter of each branch office intranet implement the basic firewall functions (for example, packet filtering) and also support IPSec protocols to build secure and authenticated tunnels between all VPN gateways of the branch office networks that comprise the VPN.

User data traffic will be both authenticated and encrypted. Any inbound traffic that cannot be authenticated by the VPN gateway will not be delivered into the intranet. Authentication will be cryptographically based, using AH or the authentication option for IPSec's ESP protocol.

- Routing control messages will be exchanged among the set of VPN gateways, and these messages will also be encrypted and authenticated using IPSec procedures, as long as a routing protocol is chosen that does not require IP multicasting.
- If the number of VPN gateways in the initial VPN deployment is small, key distribution and security association definition can be handled by manual methods. But as the VPN's size grows to encompass more and more intranets, the automated IKE procedures will rapidly become a necessity.
- Security associations will be set up among the set of VPN gateways. Because the source and destination hosts (that is, clients and servers) are not required to support IPSec, no security associations need to be set up between hosts, and no keys need to be assigned to them. In the future, if even stronger security is desired for host-to-host communications, then clients and servers will need to support the IPSec protocols.
- The IP addresses assigned for use in the intranets can be used as is, regardless of whether they were assigned from a public or a private address space. Only the interfaces of the VPN gateways that attach to the Internet backbone are required to use globally unique IP addresses.
- Packet filtering rules, if any, that were used in the pre-VPN network should be installed on the VPN gateway to control traffic that enters the branch office intranet. They can be used as a second line of defense, after the packets have been authenticated by IPSec's AH protocol.
- If end-to-end IPSec functions are deployed between hosts, then new packet filtering rules will be needed in the firewalls to recognize the IPSec AH and ESP headers.

13.2 Central site - small enterprise

In this section we will introduce possible IBM VPN solutions for a small enterprise and discuss some considerations related to small enterprise branch office VPN connections.

13.2.1 Considerations

The following considerations pertain to this VPN scenario.

13.2.1.1 Cost-effective solutions

It is now much cheaper for small companies to connect their branch offices to central site than it used to be. Lots of small enterprises can now afford VPN solutions. Generally, they need cost-effective solutions that do not require changes on current network configuration.

13.2.1.2 Low complexity

A VPN solution can be implemented without complex designing. This will reduce the implementation and management effort dramatically compared to big and complex networks. They generally have few branches that have leased-line connections to the central site.

13.2.1.3 Security requirements

Generally, small enterprises do not need rather complex security solutions as they are less vulnerable to attacks from the outside. The optimal security solution can be implemented by determining company security policy.

13.2.2 Gateway-to-gateway tunnel with IPSec between IBM routers

In this scenario, we are presenting one branch office that needs to access the central site network over the Internet. The branch office will access all resources in the central site and will be treated as a part of the network.

Even though the IBM 2216 is not a low-cost router, we are using it in this scenario because our test network was set up that way. The same configuration can also be created using IBM 2210 and IBM 2212 routers in any pair or mixed combination. Using IBM 2212 routers is not only cost-effective but also offers high performance for VPNs.

13.2.3 Scenario characteristics

- A branch office will have access to all resources on the central site. Therefore, a gateway-to-gateway VPN tunnel solution is appropriate. With this solution, any host on the central site will be able to access the branch office and any host on the branch office will be able to access the central site using a VPN tunnel secured by the IPSec protocol.
- Both networks are connected to the Internet through routers. A gateway-to-gateway VPN tunnel will be implemented between the central site router and branch office router.

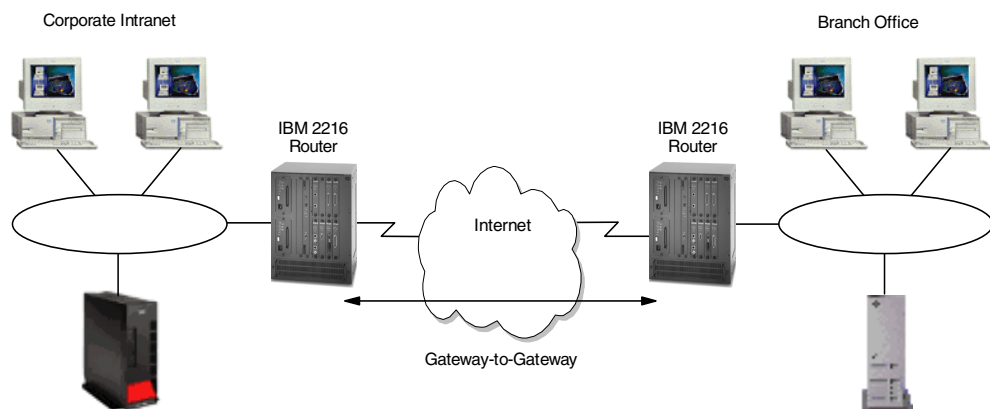


Figure 310. Branch office VPN solutions - small enterprise gateway-to-gateway solution

13.2.3.1 Scenario objectives

The objectives of this scenario are:

- All traffic between the branch office and the central site must be protected by IPSec.

- All the users in the branch office can access all resources in the central site's network and vice versa.
- The data traffic can flow in the clear in both internal networks behind the VPN gateways. The central site and the branch office belong to the same company.

13.2.3.2 Scenario network configuration

Figure 311 shows our simple network configuration for the gateway-to-gateway VPN tunnel between two IBM 2216 routers:

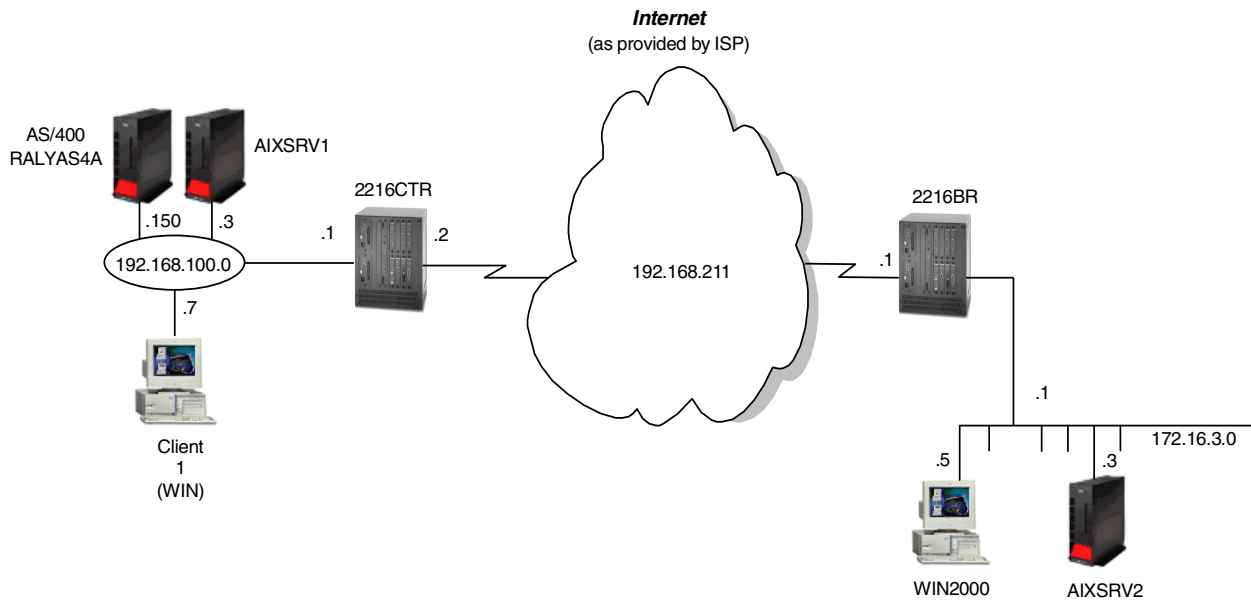


Figure 311. Branch office VPN solutions - small enterprise gateway-to-gateway scenario

13.2.4 Implementation tasks - summary

The following is a summary of 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 the planning worksheets for the two routers.
3. Configure VPN tunnels in the routers.
4. Start the VPN connection.
5. Perform verification tests.

13.2.4.1 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the data center and the branch office network are correct.

1. From PC1 in the data center network, PING PC2 at the branch office. Enter the following PING command:

```
PING 172.16.3.7
```

2. Repeat the PING command in the reverse direction from PC2 at the branch office to PC1 at the data center:

PING 192.168.100.7

Both tests must succeed before you can continue. In a real Internet environment, there might be routers on the way disallowing the PING command.

13.2.5 Completing the IBM 2216 router planning worksheet

Complete the IBM 2216 router planning worksheets as shown in Table 53 through Table 61. The planning worksheets allow you to gather all the configuration data before the actual implementation. In this scenario, we completed the planning worksheets from the perspective of a central site router.

Table 53. IBM 2216 router configuration - remote user definitions

| Information you need to create your VPN | Branch Router | Center Router |
|--|-------------------------|-------------------------|
| How to identify the remote IKE peer (user): 1: IP address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID | Option 1: IP-address | Option 1: IP-address |
| IP address that distinguishes this user? | 192.168.211.1 | 192.168.211.2 |
| Authenticate user with 1: Pre-shared key? 2: Public certificate? | pre-shared key | pre-shared key |
| Mode in which you will enter the pre-shared key: 1: ASCII 2: HEX | Option 1: ASCII | Option 1: ASCII |
| Pre-shared key (even number of characters): | 87654321 | 87654321 |

Table 54. Policy definitions

| Information you need to create your VPN | Branch Router | Center Router |
|---|----------------------|----------------------|
| Policy name: | ike-pre-3-100 | ike-pre-3-100 |
| Priority of this policy in case of multiple policies: | 5 | 5 |

Table 55. IBM 2216 router configuration - definition of the policy profile

| Information you need to create your VPN | Branch Router | Center Router |
|---|-------------------------|-------------------------|
| Profile name: | 3.0-to-100.0-pre | 3.0-to-100.0-pre |
| Source address format 1: NetMask 2: Range 3: Single address | NetMask | NetMask |
| IPv4 Source Address | 172.16.3.0 | 192.168.100.0 |
| IPv4 Source Mask (255.255.255.0) | 255.255.255.0 | 255.255.255.0 |
| Destination address format 1: NetMask 2: Range 3: Single address | NetMask | NetMask |

| Information you need to create your VPN | Branch Router | Center Router |
|--|---|---|
| Destination address | 192.168.100.0 | 172.16.3.0 |
| IPv4 Destination Mask (255.255.255.0) | 255.255.255.0 | 255.255.255.0 |
| Select the protocol to filter on 1: TCP 2: UDP 3: All protocols 4: Specify range | Option 3: All protocols | Option 3: All protocols |
| Starting value for the source port: 0 for all protocols | 0 | 0 |
| Ending value for the source port: 65535 for all protocols | 65535 | 65535 |
| Starting value for the destination port: 0 for all protocols | 0 | 0 |
| Ending value for the destination port: 65535 for all protocols | 65535 | 65535 |
| Enter the mask to be applied to the Received-DS-byte | 0 | 0 |
| Enter the value to match against after the mask has been applied to the Receive-DS-byte | 0 | 0 |
| Do you want to configure local and remote IDs for ISAKMP? | Yes | Yes |
| Select the identification type of the local ID to be sent to the remote IKE peer 1: Local tunnel endpoint address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID (any string) | Option 1: local tunnel endpoint address | Option 1: local tunnel endpoint address |
| Any user within profile allowed access | Yes | Yes |
| Do you want to limit this profile to specific interface(s)? | No | No |

Table 56. IBM 2216 router configuration - definition of policy validity profile

| Information you need to create your VPN | Branch Router | Center Router |
|--|---------------------|---------------------|
| Validity profile name: | Option 1: always | Option 1: always |
| Enter the lifetime of this policy yyymmddhhmmss:yyymmddhhmmss or * denotes forever | * | * |
| During which months should this profile be valid? ALL to signify all year round | all | all |
| During which days should this profile be valid? ALL to signify all week | all | all |

| Information you need to create your VPN | Branch Router | Center Router |
|---|---------------|---------------|
| During which hours should this profile be valid? * denotes all day | * | * |

Table 57. IBM 2216 router configuration - definition of IPSec action profile Phase 2

| Information you need to create your VPN | Branch Router | Center Router |
|---|----------------------|----------------------|
| IPSec action profile name: | tun-3-100 | tun-3-100 |
| Select the IPSec security action type: 1: Block 2: Permit | permit | permit |
| Should the traffic flow into a secure tunnel or in the clear? 1: Clear 2: Secure tunnel | Secure tunnel | Secure tunnel |
| What is the tunnel start point IP address? | 192.168.211.2 | 192.168.211.1 |
| What is the tunnel endpoint IP address? | 192.168.211.1 | 192.168.211.2 |
| Does this IPSec tunnel flow within another IPSec tunnel? | No | No |
| Percentage of SA lifesize/lifetime to use as the acceptable minimum? Default is 75 % | 75 | 75 |
| Security association refresh threshold in percent Default is 85 % | 85 | 85 |
| Select the option for the DF bit in the outer header 1: Copy 2: Set 3: Clear | Copy | Copy |
| Do you want to enable replay prevention? | Disable | Disable |
| Do you want to negotiate the security association at system initialization (autostart)? | No | No |

Table 58. IBM 2216 router configuration - IPSec proposal

| Information you need to create your VPN | Branch Router | Center Router |
|--|------------------|------------------|
| What name do you want to give this IPSec proposal? | esp-prop1 | esp-prop1 |
| Does this proposal require Diffie-Hellman Perfect Forward Secrecy? | No | No |
| Do you wish to enter any AH transforms for this proposal? | No | No |
| Do you wish to enter any ESP transforms for this proposal? | Yes | Yes |

Table 59. IBM 2216 router configuration - IPSec transform for IKE Phase 2

| Information you need to create your VPN | Branch Router | Center Router |
|---|------------------------|------------------------|
| IPSec ESP transform name: | esp-tun1 | esp-tun1 |
| Select the protocol ID: 1: IPSec AH 2: IPSec ESP | Option 2: IPSec ESP | Option 2: IPSec ESP |
| Select the encapsulation mode: 1: Tunnel 2: Transport | Option 1: Tunnel | Option 1: Tunnel |
| Select the ESP authentication algorithm: 1: HMAC_MD5 2: HMAC_SHA | Option 2: HMAC_SHA | Option 2: HMAC_SHA |
| Select the ESP cipher algorithm: 1: ESP DES 2: ESP 3DEC 3: ESP CDMF 4: ESP NULL | Option 1: ESP DES | Option 1: ESP DES |
| What is the SA lifiesize, in KB? Default is 50000 KB | 50000 | 50000 |
| What is the SA lifetime? Default is 3600 sec | 3600 | 3600 |

Table 60. IBM 2216 router configuration - Definitions for ISAKMP action for IKE Phase 1

| Information you need to create your VPN | Branch Router | Center Router |
|--|-------------------|-------------------|
| ISAKMP action name: | ike-1 | ike-1 |
| Select the ISAKMP exchange mode: 1: Main 2: Aggressive | Option 1: Main | Option 1: Main |
| Percentage of SA lifiesize/lifetime to use as the acceptable minimum: Default is 75 % | 75 | 75 |
| What is the ISAKMP connection lifiesize, in KB? Default is 5000 KB | 5000 | 5000 |
| What is the ISAKMP connection lifetime in seconds? Default is 30000 sec | 30000 | 30000 |
| Do you want to negotiate the SA at system initialization (autostart)? | Yes | Yes |

Table 61. IBM 2216 router configuration - definitions for ISAKMP proposal for IKE Phase 2

| Information you need to create your VPN | Branch Router | Center Router |
|--|--|--|
| ISAKMP proposal name: | ike-prop1 | ike-prop1 |
| Select the authentication method 1: Pre-shared key 2: Digital certificate | Option 1: Pre-shared key | Option 1: Pre-shared key |
| Select the hashing algorithm 1: MD5 2: SHA | Option 1: MD5 | Option 1: MD5 |
| Select the cipher algorithm 1: DES 2: 3DES | Option 1: DES | Option 1: DES |
| What is the SA lifesize, in KB? Default is 1000 KB | 1000 | 1000 |
| What is the SA lifetime? Default is 15000 sec | 15000 | 15000 |
| Select the Diffie-Hellman Group ID 1: Diffie-Hellman Group 1 2: Diffie-Hellman Group 2 | Option 1: Diffie-Hellman Group 1 | Option 1: Diffie-Hellman Group 1 |
| Do you wish to map a DiffServ Action to this policy? | No | No |
| What will the status of the policy be? 1: Enabled 2: Disabled | Option 1: Enabled | Option 1: Enabled |

13.2.6 Configuring the VPN in the IBM 2216 routers

We will only give necessary configuration information for this particular scenario, in this section. Please refer to 12.2, “Configuring IPsec on an Nways router” on page 309 for more details on IPsec VPN tunnel configuration on IBM routers.

Perform the following steps to configure a gateway-to-gateway VPN on a central site router. Unless otherwise specified use the default values.

1. Use the `add user` command in the policy feature to add a user and use the following values:
 - User identification type: **IP Address**
 - IP address of the user: **192.168.211.2**
 - Pre-shared key: **87654321**
2. If you have not defined a validity period, you can do that using the `add validity-period` command. In all our scenarios, we have defined a period that enables the policy for all times:
 - Validity-period name: **always**
 - Duration: **Forever**
 - Months: **All**
 - Days: **All**

- Hours: **All Day**
3. Use the `add isakmp-proposal` command in policy feature to add a ISAKMP proposal for the ISAKMP action and use the following values:
 - ISAKMP proposal name: **ike-prop1**
 - Authentication Method: **Pre-shared Key**
 - Hashing Algorithm: **MD5**
 - Cipher Algorithm: **DES**
 4. Use `add isakmp-action` command in the policy feature to add an isakmp-action and use the following values:
 - ISAKMP action name: **ike-1**
 - ISAKMP action mode: **Main**
 - ISAKMP proposal to be used: **ike-prop1**
 5. Use the `add ipsec-transform` command in the policy feature to add an ipsec-transform to be used for the IPsec proposal and use the following values:
 - IPsec transform name: **esp-tun1**
 - Protocol ID: **IPSEC ESP**
 - Encapsulation Mode: **Tunnel**
 - IPsec Authentication Algorithm: **HMAC-SHA**
 - ESP Cipher Algorithm: **ESP DES**
 - SA Lifesize, in Kilobytes: **1000**
 - SA Lifetime: **3600**
 6. Use the `add ipsec-proposal` command in the policy feature to add an ipsec-proposal to be used for the IPsec action and use the following values:
 - IPsec proposal name: **esp-prop1**
 - Use PFS: **No**
 - Use AH: **No**
 - Use ESP: **Yes**
 - Name of the IPsec transform to be used: **esp-tun1**
 7. Use the `add ipsec-action` command in the policy feature to add an ipsec-action to be used for tunnel profile and use the following values:
 - IPsec action name: **tun-3-100**
 - IPsec security action type: **permit**
 - Traffic flow into a secure tunnel or clear: **Secure Tunnel**
 - Tunnel start point IPv4 address: **192.168.211.1**
 - Tunnel endpoint IPv4 address: **192.168.211.2**
 - Options for DF bit in outer header: **Copy**
 - Enable replay prevention: **No**
 - Name of the IPsec proposal to be used: **esp-prop1**

8. Use the `add profile` command in the policy feature to add a profile to be used for the policy pertaining to the tunnel and use the following values:
 - Profile name: **3.0-to-100.0-pre**
 - Source Address Format: **Netmask**
 - IPv4 Source Address: **192.168.100.0**
 - IPv4 Source Mask: **255.255.255.0**
 - Destination Address Format: **Netmask**
 - IPv4 Destination Address: **172.16.3.0**
 - IPv4 Destination Mask: **255.255.255.0**
 - Protocol IDs: **All Protocols**
 - Configure local and remote IDs for ISAKMP: **Yes**
 - Identification to send to remote: **Local Tunnel Endpoint Address**
 - IPsec action to be used for this profile: **tun-3-100**
9. Use the `add policy` command to define a policy and use the following values:
 - Policy name: **ike-pre-3-100**
 - Profile name to be used for this policy: **3.0-to-100.0-pre**
 - Validity-period name to be used for this policy: **always**
10. Reload the router for the changes to take effect.

You should configure the branch office router with the same parameters above except for the tunnel endpoint definitions. Follow the above steps and use the following parameters for the steps specified below:

1. Adding user:
 - IP Address of the user: **192.168.211.1**
6. Adding IPsec action:
 - Tunnel start point IPv4 address: **192.168.211.2**
 - Tunnel endpoint IPv4 address: **192.168.211.1**
7. Adding Profile:
 - Source Address Format: **Netmask**
 - IPv4 Source Address: **172.16.3.0**
 - IPv4 Source Mask: **255.255.255.0**
 - Destination Address Format: **Netmask**
 - IPv4 Destination Address: **192.168.100.0**
 - IPv4 Destination Mask: **255.255.255.0**

13.2.7 Connection verification and testing

IKE policies are activated as soon as the configuration is reloaded. To verify that IKE negotiations have been successful, enter the following command in the talk 5 mode:

```
feature ipsec->ipv4->list tunnel active
```

To verify that IPSec traffic is being processed as defined, enter the following command:

```
feature policy->list stats
```

To take down an IPSec tunnel, use the tunnel ID that you got from the list tunnel active command and issue:

```
disable tunnel [ID]
```

Table 62 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 13.2.3.1, “Scenario objectives” on page 366.

Table 62. Verification test - OS/400 to 2210 router gateway to gateway scenario

| Direction | TELNET | FTP | TFTP | PING |
|---|--------|-----|------|------|
| From Center subnet to Branch subnet hosts | YES | YES | YES | YES |
| From Branch subnet hosts to Center | YES | YES | YES | YES |

13.3 Central site - medium enterprise

In this section we will introduce possible IBM VPN solutions for a medium enterprise and discuss some considerations related to medium enterprise branch office VPN connections.

13.3.1 Considerations

The following considerations pertain to this VPN scenario.

13.3.1.1 Use of proven technology

Enterprises of medium and larger sizes are likely to have firewall systems in place, at least on the main sites. This often also implies a DMZ installation, and in many cases a good firewall is built on a UNIX system, such as AIX. Time and effort have been put into these firewall solutions and enough expertise and confidence is available to trust these systems with the additional task of branch office VPNs.

13.3.1.2 Network management

UNIX systems are usually well integrated in network management processes. Even though VPN-specific management features are now only rudimentarily available, a UNIX system as a VPN gateway is a good candidate from a systems management standpoint.

Another important factor to consider here is ease of use because you would not want your network administrator to manually define, activate, and deactivate tunnels whenever traffic needs to flow between branch offices. Therefore, a VPN gateway that supports IKE and on-demand tunnels will reduce management efforts significantly.

13.3.1.3 Availability

If properly designed, firewalls tend to be fairly stable and the same holds true for UNIX systems. To a company of medium and larger size the availability of corporate security gateways is essential. The gateway is usually the only

connection to the outside. If it is down, loss of business can be substantial. The gateway also performs security features that must be in place for the corporate security policy to be effective. If the gateway was down or attacked and temporarily replaced by a lesser system, damage done by malicious outsiders could be severe.

13.3.1.4 Scalability

Medium size companies may have reached a point where future growth is a major worry for I/S managers because the grown infrastructure will not meet it without redesign. It is essential that important systems such as security and VPN gateways be designed in a way that support future growth without compromising the mission of such systems.

13.3.2 Gateway-to-gateway tunnel with IPSec between IBM AIX systems

In this scenario, we are presenting one branch office that needs to access the central site network over the Internet. The branch office will access all the resources in the central site and will be treated as a part of the network.

Even though AIX is designed to be a server rather than a firewall, we are using AIX 4.3.3 for this scenario to substitute a firewall in place of an IBM firewall product that supports IKE. We are doing this for several reasons, which may or may not apply to a given customer situation, but we would like to point out that a scenario like this is not entirely academic.

- AIX 4.3.3 offers improved IP filtering and VPN capabilities and also performance enhancements.
- AIX 4.3.2 and 4.3.3 fully support VPN gateway capabilities for IPSec.
- The same scenario can be established using IBM eNetwork Firewall V3.3 for AIX and Windows NT, with the exception that IKE is not available on those platforms. Therefore, manual IPSec tunneling must be used, which bears management and scalability problems for medium to larger networks.
- The same scenario can be established using IBM routers as described in 13.2.2, "Gateway-to-gateway tunnel with IPSec between IBM routers" on page 366.
- We wanted to illustrate an AIX-to-AIX gateway-to-gateway scenario.

From a design standpoint, we admit that a firewall would be the VPN gateway of choice for this scenario.

13.3.3 Scenario characteristics

- The branch office will have access to all the resources on the central site. Therefore, a gateway-to-gateway VPN tunnel solution is appropriate. With this solution, any host on the central site will be able to access the branch office, and any host on the branch office will be able to access the central site using a VPN tunnel secured by the IPSec protocol.
- Both networks are connected to the Internet through routers. A gateway-to-gateway VPN tunnel will be implemented between the central site router and branch office router.

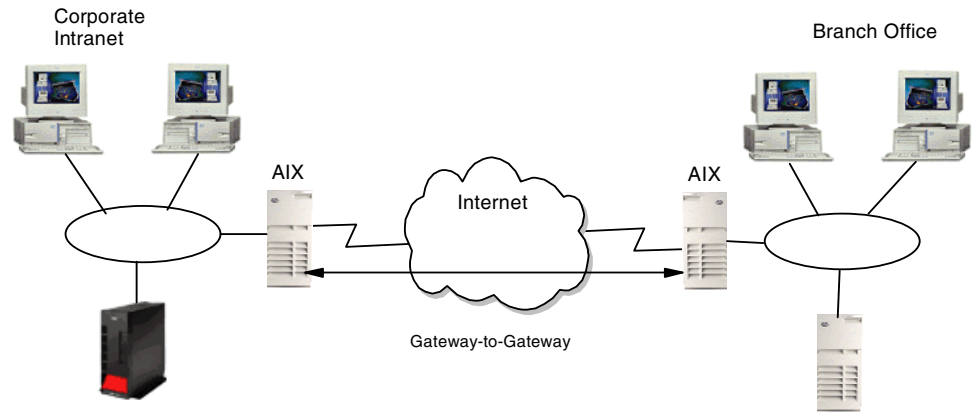


Figure 312. Branch office VPN solutions - small enterprise gateway-to-gateway solution

13.3.3.1 Scenario objectives

The objectives of this scenario are:

- All traffic between the branch office and the central site must be protected by IPSec.
- All the users in the branch office can access all resources in the central site's network and vice versa.
- The data traffic can flow in the clear in both internal networks behind the VPN gateways. The central site and the branch office belong to the same company.

13.3.3.2 Scenario network configuration

Figure 313 shows our simple network configuration for the gateway-to-gateway VPN tunnel between two AIX systems:

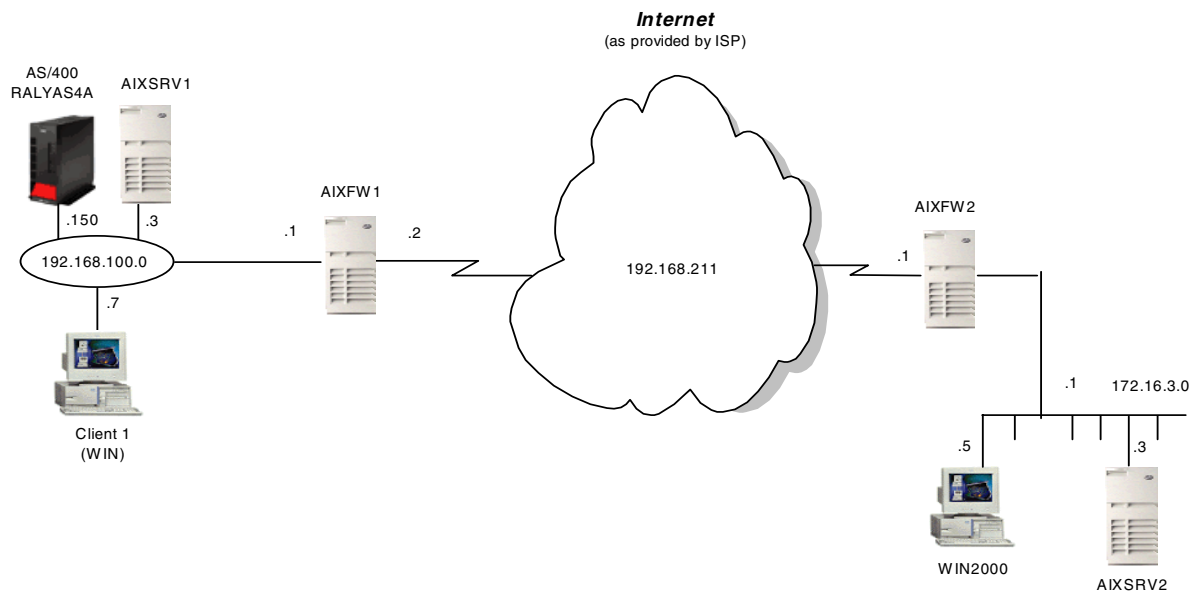


Figure 313. Branch office VPN solutions - small enterprise gateway-to-gateway scenario

13.3.4 Implementation tasks - summary

The following is a summary of 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 the planning worksheets for the two AIX gateways.
3. Configure VPN tunnels in the AIX gateways.
4. Start the VPN connection.
5. Perform verification tests.

13.3.4.1 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the data center and the branch office network are correct.

1. From PC1 in the data center network, PING PC2 at the branch office, and enter the following PING command:

```
PING 172.16.3.7
```

2. Repeat the PING command in the reverse direction from PC2 at the branch office to PC1 at the data center:

```
PING 192.168.100.7
```

Both tests must succeed before you can continue. In a real Internet environment, there might be routers on the way disallowing the PING command.

13.3.5 Completing the AIX planning worksheet

The parameters used in this scenario are shown in Table 63 on page 378. We have used the IBM_low_prekey IKE policy and the IBM_low_ESP_tunnel IPsec policy, which are supplied by default with the pre-version of AIX 4.3.3 we were using. If this policy does not meet your security requirements, you can define a different policy using the AIX IKE configuration GUI. This process is described in detail in 9.1.4, "AIX V4.3.2 IP Security IKE advanced setup" on page 141, and in 9.2.4, "IP Security IKE tunnel advanced setup" on page 160.

In particular, we discourage you from using IKE aggressive mode with pre-shared keys in this scenario because this exposes the identities of the gateways during the Phase 1 exchange. We also recommend that you not use too low SA lifetimes between gateways because of the rekeying overhead. However, the lifetimes should be adequate to the level of encryption you are using so that security is not compromised. For DES, a lifetime of several hours is usually okay.

Table 63. AIX - gateway-to-gateway VPN connection IPsec parameters

| IPsec parameters and pertinent information on both parties | |
|--|---------------|
| Local | |
| Key Server Hostname | AIXFW1 |
| Key Server IP Address | 192.168.102.2 |
| Role | Initiator |
| Tunnel Endpoint (IP Subnet) | 192.168.100.0 |

| IPSec parameters and pertinent information on both parties | | |
|---|----------------------|-----|
| Tunnel Endpoint Mask | 255.255.255.0 | |
| Protocols | 0 (all) | |
| Remote | | |
| Key Server Hostname | AIXFW2 | |
| Key Server IP Address | 192.168.101.2 | |
| Role | Responder | |
| Tunnel Endpoint (IP Subnet) | 172.16.3.0 | |
| Tunnel Endpoint Mask | 255.255.255.0 | |
| Protocols | 0 (all) | |
| Key Management Tunnel (Phase 1) | | |
| Mode | Aggressive | |
| Encryption | DES | |
| Authentication Algorithm | MD5 | |
| Key Exchange Group | 1 | |
| Key Lifetime | 480 min (default) | |
| Negotiation ID | IP Address | |
| Pre-Shared Key (ASCII) | abcdef0987654321 | |
| 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 | Tunnel | |
| Perfect Forward Secrecy (PFS) | No | |
| Tunnel Lifetime | 30 days | |
| SA Lifetime | 10 min (default) | |
| Start Tunnel On-Demand | Yes | |

13.3.6 Configuring the central site gateway

Perform the following steps to configure a host-to-host VPN on AIXSRV1. We start from the Internet Key Management (IKE) Tunnel configuration panel.

1. Select **Tunnel -> New Tunnel -> New Key Management Tunnel** to open the Key Management (Phase 1) Tunnel Properties window.

2. On the Identification panel, enter the key management tunnel name. In this case, AIXFW1_AIXFW2.
3. Select **IP address** as the Host Identity type for the local and remote endpoint for the tunnel and enter the IP addresses of the local (192.16.102.2) and remote (192.168.101.2) hosts.
4. Click the **Key (Phase 1) Policy** tab.
5. Select the **IBM_low_prekey** policy from the defined key management (phase 1) policies and click **Associate**.
6. Click the **Key** tab.
7. Enter the pre-shared key. Use the ASCII or hexadecimal notation. In the case of two AIX systems this does not matter, but in heterogeneous scenarios you may be better off using ASCII.
8. Click **OK**.

The key management tunnel has been configured. Next you configure the data management tunnel associated to the key management tunnel.

9. Select **Tunnel -> New Tunnel -> New Data Management Tunnel** on the Internet Key Exchange (IKE) Tunnels configuration panel to open the Data Management (Phase 2) Tunnel Properties window.
10. On the Identification panel, enter the data management tunnel name. In this case, AIXFW_AIXFW2.
11. Choose the key management tunnel name you want to be associated, in this case, AIXFW1_AIXFW2, and click the **Associate** button.
12. Click the **Endpoints** tab.
13. Select **Subnet** as the endpoint type for the local and remote data endpoints.
14. Enter the local (192.168.100.0) and remote (172.16.3.0) IP address in the Subnet ID field.
15. Enter the local (255.255.255.0) and remote (255.255.255.0) subnet mask in the Subnet Mask field.
16. Leave local and remote ports and protocols as is (0 and all) to allow all traffic between the central and branch office to be protected by this tunnel.
17. Click the **Data (Phase 2) Policy** tab.
18. Select the **IBM-low_ESP_tunnel** policy from the defined data management (phase 2) policies and click the **Associate** button.
19. Click the **Options** tab.
20. Uncheck the **Automatically start data management tunnel** box if your side will be the responder or you do not want to establish the data management tunnel at system restart.
21. Check the **Activate tunnel on demand** box.
22. Click **OK**. Now the data management tunnel is configured successfully.
23. Highlight the new data management (phase 2) tunnel and click the green button to activate the on-demand tunnel.

The IKE tunnels on AIXFW1 are now ready to be activated as soon as the first packet arrives that is destined to the network behind the partner gateway.

13.3.7 Configuring the branch office gateway

The steps to configure the AIX gateway in the branch office, AIXFW2, are essentially the same as for the central site gateway, AIXFW1. Use the configuration worksheet from Table 63 on page 378 to determine the appropriate configuration values and settings for this gateway.

If AIXFW2 was merely acting as a responder, you would not have to activate the tunnels at this point. However, in a branch office scenario traffic is likely to originate from either side and if the on-demand tunnel was not activated, no IKE negotiations would be initiated and no traffic could flow back to the central site without manual intervention by an administrator.

13.3.8 Connection verification and testing

Use the IKE Tunnel Monitor on both gateways to check the status of the VPN connection. After the on-demand tunnels have been activated, they should show a status of Dormant. This means that the necessary filter rules are in place to identify any traffic that matches the profile for this tunnel. As soon as the first matching packet arrives, IKE negotiations will be started and the tunnels activated. Applications may expect a slight delay during negotiations and a slightly decreased response time once the IPsec tunnel is active. Otherwise, this process is designed to be nondisruptive.

Once traffic has initiated the tunnels to be activated, the IKE Tunnel Monitor lists the status for the key management (phase 1) and data management (phase 2) as Active.

Table 64 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 13.3.3.1, "Scenario objectives" on page 377.

Table 64. Verification test - OS/400 to 2210 router gateway-to-gateway scenario

| Direction | TELNET | FTP | TFTP | PING |
|---|--------|-----|------|------|
| From AIXFW1 subnet to AIXFW2 subnet hosts | YES | YES | YES | YES |
| From AIXFW2 subnet hosts to AIXFW1 | YES | YES | YES | YES |

13.4 Central and regional sites - large enterprise

In this section we will introduce possible IBM VPN solutions for a large enterprise and discuss some considerations related to large enterprise branch office VPN connections.

13.4.1 Considerations

The following considerations pertain to this VPN scenario.

13.4.1.1 Policy deployment and management

For a large scale enterprise that has central and regional sites and many security gateways, servers, and clients, policy deployment and management is a great concern. The enterprise should enforce a security policy to all segments of its network. If the enterprise does not use a good policy management method, for example, to change the corporate security policy for encryption from DES to

3DES, would require a change in the configuration of each device on the extended network.

One of the possible alternatives is the Lightweight Directory Access Protocol (LDAP), which was developed to provide standards for accessing the data in network directories. As the use of LDAP grew and its benefits became apparent, the stand-alone LDAP server could build directories that could be accessed by the LDAP client. A common directory infrastructure encourages new uses. The Directory Enabled Networks (DEN) specification allows information about network configuration, protocol information, router characteristics, and so on to be stored in an LDAP directory. Refer to Chapter 6, "Directory-assisted policy management" on page 97 for more details on directory-assisted policy management.

13.4.1.2 PKI requirement

Even if you maintain a policy using LDAP, therefore, the pre-shared key, there are still a number of advantages of PKI over pre-shared key:

- More secure
- Highly scalable
- Does not require CA to be online to authenticate
- Authentication mechanism of PKI is strong
- You can use dispersed authorities

Refer to Chapter 4, "Certificates and Public Key Infrastructures (PKIs)" on page 73 for more details on certificates and PKI.

13.4.1.3 Network management

The general design consideration for Internet VPN is limiting the automatic network discovery function, therefore, an NMS must use a seed file for network discovery. For a normal IP network, NMS can discover as many network nodes as its network has. But in case of Internet VPN, specific IP addresses for each node must be defined before discovery. Sometimes, intermediate routers cannot provide IP address and interface information at the NMS's request.

13.4.1.4 Backup

Service availability is a key factor for large enterprises. A good VPN design should therefore provide for backup solutions in case a VPN gateway goes down. This can be achieved in a couple of ways:

- By having a standby device configured and ready to take over for the failing device.
- By having multiple VPN gateways at the central site across which VPN connections to the branch offices are distributed. In case one gateway fails, connections can be rerouted to another gateway. This also provides some degree of load-splitting between the gateways.

With today's technology, the takeover of a VPN gateway is usually disruptive but the down time is only as long as IKE needs for renegotiations - usually under one minute.

13.4.1.5 Performance

Large companies are likely to continuously transfer high volumes of traffic between central and branch offices. Therefore, performance and throughput of network gateways is key in large networks. This holds true whether a VPN is in place or not, hence a VPN gateway not only has to keep up with the traffic but it must also be capable of adding authentication and encryption to that traffic without much delay. VPN gateways with hardware encryption support are preferred devices in this environment. The IBM 2212, for instance, provides VPN performance up to multiple T1 speeds.

13.4.1.6 Extending network to global size

In large companies, providing for future growth is an ongoing effort for I/S managers to ensure that the present infrastructure will meet it without redesign. It is essential that important systems such as security and VPN gateways be designed in a way that supports future growth without compromising the mission of such systems. A high degree of scalability, flexibility, and automation is therefore desired and a VPN gateway that supports IKE, on-demand tunnels, PKI and policy retrieval via LDAP fulfills these requirements.

13.4.2 IBM AS/400 to IBM 2210 gateway-to-gateway tunnel with IPSec

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 at both networks are allowed to access all systems and applications on the remote network. Figure 314 on page 384 represents this scenario. Although this scenario does not meet all the criteria described above, it illustrates the multitude of possible VPN gateway solutions that can be found in today's large corporate networks.

13.4.3 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 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 nonsecure interface.
 - TOKENRING1 connects the gateway to the internal data center network and represents the secure interface. See Figure 315 on page 384.

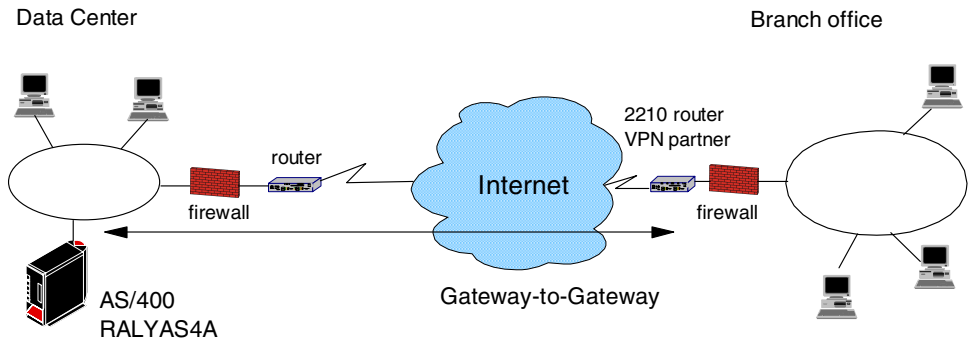


Figure 314. Branch office VPN - gateway-to-gateway AS/400 system to 2210 router

Note

For a higher level of security, the 2210 VPN partner should be placed in the secure side of the firewall at the branch office.

13.4.3.1 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.

13.4.3.2 Scenario network configuration

Figure 315 shows our simple network configuration for the gateway-to-gateway AS/400 system to 2210 router:

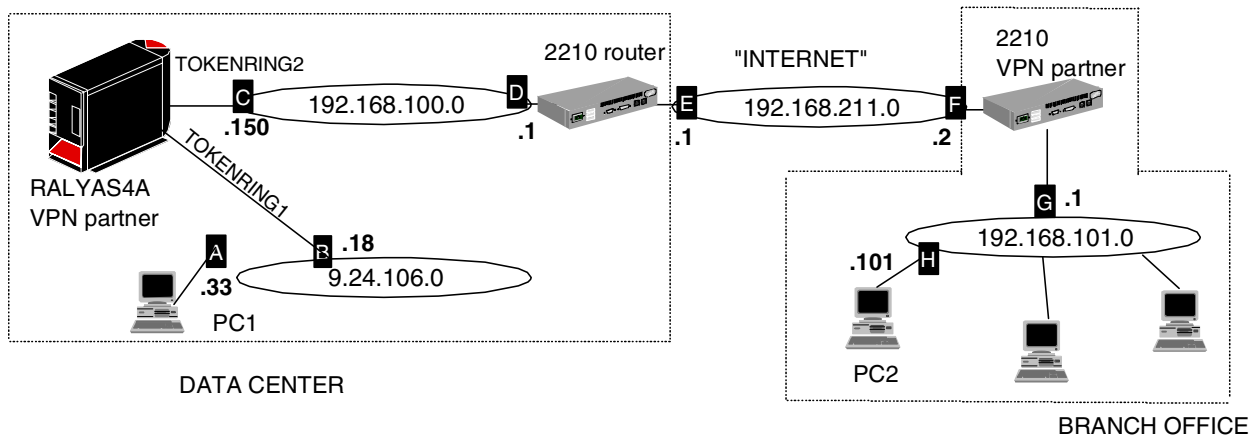


Figure 315. Gateway-to-gateway - OS/400 to 2210 router

13.4.4 Implementation tasks - summary

The following is a summary of 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 the planning worksheets for the 2210 router.
3. Complete the planning worksheets for the AS/400 system.
4. Configure a VPN in the 2210 router.
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.

13.4.4.1 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the data center and the branch office network are correct.

1. From PC1 in the data center network to 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 can continue. In a real Internet environment, there might be routers along the way disallowing the PING command.

13.4.5 Completing the 2210 router planning worksheet

Complete the 2210 router planning worksheets as shown in Table 65 through Table 73. The planning worksheets allow you to gather all the configuration data before the actual implementation. We completed the planning worksheets from the perspective of the 2210 router in this scenario.

Table 65. IBM 2210 router configuration - remote user definitions

| Information you need to create your VPN | Scenario answers |
|--|-----------------------------------|
| How to identify the remote IKE peer (user): 1: IP address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID | Select IP address with AS/400 |
| IP address that distinguishes this user? | 192.168.100.150 |
| Authenticate user with: 1: Pre-shared key? 2: Public certificate? | Select pre-shared key with AS/400 |
| Mode in which you will enter the pre-shared key: 1: ASCII 2: HEX | Select ASCII with AS/400 |
| Pre-shared key (even number of characters): | 87654321 |

Table 66. 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 67. IBM 2210 router configuration - policy profile

| Information you need to create your VPN | Scenario answers |
|--|---|
| Profile name | 101-to-106 |
| Source address format 1: NetMask 2: Range 3: Single address | NetMask |
| Source address | 192.168.101.0 |
| Destination address format 1: NetMask 2: Range 3: Single address | NetMask |
| Destination address | 9.24.106.0 |
| Select the protocol to filter on 1: TCP 2: UDP 3: All protocols 4: 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 Received-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 1: Local tunnel endpoint address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID (any string) | Select local tunnel endpoint address with AS/400 |

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Do you want to limit this profile to specific remote users? | Yes |
| Do you want to limit this profile to specific interface(s)? | No |

Table 68. 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:yyymmddhhmmss or * 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 69. 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: 1: Block 2: Permit | permit |
| Should the traffic flow into a secure tunnel or in the clear? 1: Clear 2: Secure tunnel | Secure tunnel |
| What is the tunnel start point 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 lifeseize/lifetime to use as the acceptable minimum? Default is 75 % | 75 % |
| Security association refresh threshold in percent Default is 85 % | 85 % |
| Select the option for the DF bit in the outer header 1: Copy 2: Set 3: Clear | Copy |

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Do you want to enable replay prevention? | Disable |
| Do you want to negotiate the security association at system initialization (autostart)? | No |

Table 70. 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 71. 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: 1: IPSec AH 2: IPSec ESP | IPSec ESP |
| Select the encapsulation mode: 1: Tunnel 2: Transport | Tunnel |
| Select the ESP authentication algorithm: 1: HMAC_MD5 2: HMAC_SHA | HMAC_MD5 |
| Select the ESP cipher algorithm: 1: ESP DES 2: ESP 3DEC 3: ESP CDMF 4: ESP NULL | ESP DES |
| What is the SA lifesize, in KB Default is 50000 KB | 50000 |
| What is the SA lifetime? Default is 3600 sec | 86400 |

Table 72. IBM 2210 router configuration - ISAKMP action

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| ISAKMP action name: | ike-6 |

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Select the ISAKMP exchange mode: 1: Main 2: Aggressive | Aggressive |
| Percentage of SA lifesize/lifetime to use as the acceptable minimum: Default is 75 % | 75 % |
| What is the ISAKMP connection lifesize, in KB? Default is 5000 KB | 5000 |
| What is the ISAKMP connection lifetime in seconds? Default is 30000 sec | 30000 |
| Do you want to negotiate the SA at system initialization (autostart)? | No |

Table 73. IBM 2210 router configuration - ISAKMP proposal

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| ISAKMP proposal name: | ike-prop6 |
| Select the authentication method 1: Pre-shared key 2: Digital certificate | Pre-shared key |
| Select the hashing algorithm 1: MD5 2: SHA | MD5 |
| Select the cipher algorithm 1: DES 2: 3DES | DES |
| What is the SA lifesize, in KB? Default is 1000 KB | 1000 |
| What is the SA lifetime? Default is 15000 sec | 15000 |
| Select the Diffie-Hellman Group ID 1: Diffie-Hellman Group 1 2: Diffie-Hellman Group 2 | 1 |
| Do you wish to map a DiffServ Action to this policy? | No |
| What will the status of the policy be? 1: Enabled 2: Disabled | Enabled |

13.4.6 Completing the AS/400 system planning worksheet

Complete the AS/400 system planning worksheets as shown in Table 74 and Table 75. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 74. Planning worksheet - New Connection Wizard - RALYAS4A

| This information is 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 | 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 74) 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*, and the pre-shared key is a random string of characters, *87654321*.

Table 75. 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 remote 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 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 address(es)? Use this name as the <i>source address</i> on the IPSEC filter | 9.24.106.0 |
| | 255.255.255.0 |
| | AS4Asubnets |
| If the remote 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 address(es)? 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 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 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 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> . | |

We also completed the IP filter rules planning worksheet (Table 75) 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 secure tunnel traffic is allowed to flow in the TOKENRING2 interface. When the filter rules were activated, they allowed only 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 from and to the internal network since no filter rules are activated on TOKENRING1.

13.4.7 VPN configuration cross-reference table - OS/400 to 2210 router

Table 76 summarizes the AS/400 system and 2210 router configuration and provides a cross-reference list.

Table 76. AS/400 and 2210 router VPN configuration cross-reference table

| <u>AS/400</u> | <u>ROUTER</u> |
|--|--|
| Key Policy | ISAKMP-Action |
| Name = GtoGRto4ABS | (1),(2) Mode = Aggressive |
| Initiator Negotiation = Aggressive Mode (1) | (31) Autostart=N |
| Responder Negotiation = Aggressive Mode only (2) | |
| Key Protection Transforms | ISAKMP-Proposal |
| Authentication Method = Pre-shared key (3) | (3) AuthMethod = Pre-shared key |
| Pre-shared key value = 87654321 (4) | (9) LifeSize = 1000 |
| Hash Algorithm = MD5 (5) | (8) LifeTime = 3600 |
| Encryption Algorithm = DES-CBC (6) | (7) DHGroupID = 1 |
| Diffie-Hellman Group = Default 768-bit MODP (7) | (5) Hash Algorithm = MD5 |
| Key Management | (6) Encryption Algorithm = DES |
| Maximum key lifetime (minutes) = 60 (8) | |
| Maximum size limit (kilobytes) = 1000 (9) | IPSEC Action |
| | (18) Tunnel Start = 192.168.211.2 |
| Data Policy | (20) Tunnel End = 192.168.100.150 |
| Name = GtoGRto4ABS | Tunnel-in-Tunnel = N |
| Use Diffie-Hellman Perfect Forward Secrecy = No (10) | (31) Autostart = N |
| Diffie-Hellman Group = Not Applicable | Replay Prevention = N |
| Data Protection Proposals | IPSEC Proposal |
| Encapsulation mode = Tunnel (11) | Diffie-Hellman Perfect Forward Secrecy = N |
| Protocol = ESP (12) | |
| Algorithms | IPSEC Transform |
| Authentication Algorithm = HMAC-MD5 (13) | (12) Type = IPsec ESP |
| Encryption Algorithm = DES-CBC (14) | (11) Mode = Tunnel |
| Key Expiration | (16) LifeSize = 50000 |
| Expire after (minutes) = 1440 (15) | (15) LifeTime = 86400 |
| Expire at size limit (kilobytes) = 50000 (16) | (13) Authentication Algorithm = HMAC-MD5 |
| | (14) Cipher Algorithm = ESPDES |
| Key Connection Group | Validity Period |
| Name = GtoGRto4A | (21) Life Time = Always |
| Remote Key Server | User |
| Identifier Type = Version 4 IP address (17) | Name = 192.168.100.150 |
| IP address = 192.168.211.2 (18) | (19) Type = IPV4 address |
| Local Key Server | (3) Authentication Mode = Pre-shared key |
| Identifier Type = Version 4 IP address (19) | Key Mode = ASCII |
| IP address = 192.168.100.150 (20) | (4) Pre-shared key = 87654321 |
| Key Policy = GtoGRto4ABS | |
| Dynamic Key Group | Policy Profile |
| Name = GtoGRto4A | Source Address Format = NetMask |
| System Role = Both systems are gateways (23)(27) | Source Address = 192.168.101.0 |
| Initiation = Either systems can initiate the connection (22)(27) | Source Mask = 255.255.255.0 |
| Policy | Destination Address Format = NetMask |
| Data Management Security Policy = GtoGRto4ABS (25)(26) | Destination Address = 9.24.106.0 |
| Connection Lifetime = Never Expires (21) | (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 = GtoGRto4AL1 | |
| Key Connection Group = GtoGRto4ABS | |
| Start when TCP/IP is started? = No | |
| IP Filters | |
| Name = GtoG_RTRtoAS13P | |
| Defined Addresses = RTRsubnets | |
| Subnet mask = 255.255.255.0 (22) | |
| IP addresses = 192.168.101.0 (23) | |
| Defined Addresses = AS4Asubnets | |
| Subnet mask = 255.255.255.0 (24) | |
| IP addresses = 9.24.106.0 (25) | |
| IPSEC rule | |
| Source address name = AS4Asubnets (26) | |
| Destination address name = RTRsubnets (27) | |
| Connection Name = GtoGRto4A | |
| Services | |
| Protocol = * (28) | |
| Source port = * (29) | |
| Destination port = * (30) | |

13.4.8 Configuring the VPN in the 2210 router

An IBM 2210 router was used as the branch office VPN partner in our example scenario. We will give only necessary configuration information for this particular scenario in this section. Please refer to 12.2, “Configuring IPsec on an Nways router” on page 309 for more details on IPsec VPN tunnel configuration on IBM routers.

Perform the following steps to configure a gateway-to-gateway VPN on a central site router. Unless otherwise specified use the default values.

1. Use the `add user` command in the policy feature to add a user and use the following values:
 - User identification type: **IP Address**
 - IP address of the user: **192.168.100.150**
 - Pre-shared key: **87654321**
2. If you have not defined a validity period, you can do that using the `add validity-period` command. In all our scenarios, we have defined a period that enables the policy for all times:
 - Validity-period name: **always**
 - Duration: **Forever**
 - Months: **All**
 - Days: **All**
 - Hours: **All Day**
3. Use the `add isakmp-proposal` command in the policy feature to add an isakmp-proposal for the ISAKMP action and use the following values:
 - ISAKMP proposal name: **ike-prop6**
 - Authentication Method: **Pre-shared Key**
 - Hashing Algorithm: **MD5**
 - Cipher Algorithm: **DES**
4. Use the `add isakmp-action` command in the policy feature to add an isakmp-action and use the following values:
 - ISAKMP action name: **ike-6**
 - ISAKMP action mode: **Aggressive**
 - ISAKMP proposal to be used: **ike-prop6**
5. Use the `add ipsec-transform` command in the policy feature to add an ipsec-transform to be used for IPsec proposal and use the following values:
 - IPsec transform name: **esp-trans6**
 - Protocol ID: **IPSEC ESP**
 - Encapsulation Mode: **Tunnel**
 - IPsec Authentication Algorithm: **HMAC-MD5**
 - ESP Cipher Algorithm: **ESP DES**
 - SA Lifesize, in Kilobytes: **50000**
 - SA Lifetime: **86400**

6. Use the `add ipsec-proposal` command in the policy feature to add an ipsec-proposal to be used for the IPsec action and use the following values:
 - IPsec proposal name: **esp-prop6**
 - Use PFS: **No**
 - Use AH: **No**
 - Use ESP: **Yes**
 - Name of the IPsec transform to be used: **esp-trans6**
7. Use the `add ipsec-action` command in the policy feature to add an ipsec-action to be used for the tunnel profile and use the following values:
 - IPsec action name: **tun-16**
 - IPsec security action type: **permit**
 - Traffic flow into a secure tunnel or clear: **Secure Tunnel**
 - Tunnel start point IPv4 address: **192.168.211.2**
 - Tunnel endpoint IPv4 address: **192.168.100.150**
 - Options for DF bit in outer header: **Copy**
 - Enable replay prevention: **No**
 - Name of the IPsec proposal to be used: **esp-prop6**
8. Use the `add profile` command in the policy feature to add a profile to be used for the policy pertaining to the tunnel and use the following values:
 - Profile name: **101-to-106**
 - Source Address Format: **Netmask**
 - IPv4 Source Address: **192.168.101.0**
 - IPv4 Source Mask: **255.255.255.0**
 - Destination Address Format: **Netmask**
 - IPv4 Destination Address: **9.24.106.0**
 - IPv4 Destination Mask: **255.255.255.0**
 - Protocol IDs: **All Protocols**
 - Configure local and remote IDs for ISAKMP: **Yes**
 - Identification to send to remote: **Local Tunnel Endpoint Address**
 - IPsec action to be used for this profile: **tun-16**
9. Use the `add policy` command to define a policy and use the following values:
 - Policy name: **ike-pre-101-106**
 - Profile name to be used for this policy: **101-to-106**
 - Validity-period name to be used for this policy: **always**
10. Reload the router for changes to take effect.

13.4.9 Configuring the VPN on the AS/400 system (RALYAS4A)

We will only give necessary configuration information for this particular scenario in this section. Please refer to 10.5, “VPN configuration” on page 199 for more details on IPSec VPN tunnel configuration on the AS/400 system.

Perform the following steps to configure a gateway-to-gateway VPN on a central site router. Unless otherwise specified use the default values.

1. Start AS/400 Operations Navigator from the desktop.
2. Expand the AS/400 system, in this case, **RALYAS4A**. 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. Both functions must be configured, 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 either be Started or Stopped during the following steps.

5. Double-click **Virtual Private Networking** to start the Virtual Private Networking graphical user interface (GUI).
6. Select **File** from the main menu, and then select **New Connection**.
7. Select **Gateway To Gateway** from the drop-down menu. This starts the New Connection Wizard for a gateway-to-gateway connection.
8. Click **Next** after reading the Welcome window.
9. Enter the Name, GtoGRto4A, for the connection group. Recall that GtoGRto4A is the name from the worksheet in Table 74 on page 390. The name specified here is the name for all objects the wizard creates for this particular connection. It is case-sensitive. Also enter a description of the configuration.
10. Click **Next**.
11. In the Key Policy window, 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 worksheet. The wizard chooses the appropriate encryption and authentication algorithms based on the selection made here.
12. Click **Next**.
13. In 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 the 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 2210 router. Refer to the planning worksheet (Table 74 on page 390) and to the network configuration in Figure 315 on page 384; for RALYAS4A, this is **192.168.100.150** (interface C).

14. Click **Next**.
15. Use the Remote Network window to enter details about the remote key server, as well as the pre-shared key. The remote key server is the 2210 router with IP Address 192.168.211.2. This is interface F in Figure 315 on page 384. Refer also to the planning worksheet in Table 74 on page 390. Specify 87654321 in the pre-shared key parameter. Remember, exactly the same pre-shared key must be entered when configuring VPN on the remote 2210 router.
16. Use the Data Policy window to specify what 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.
17. Click **Next**.
18. Click **Next**.
19. The final window 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**.

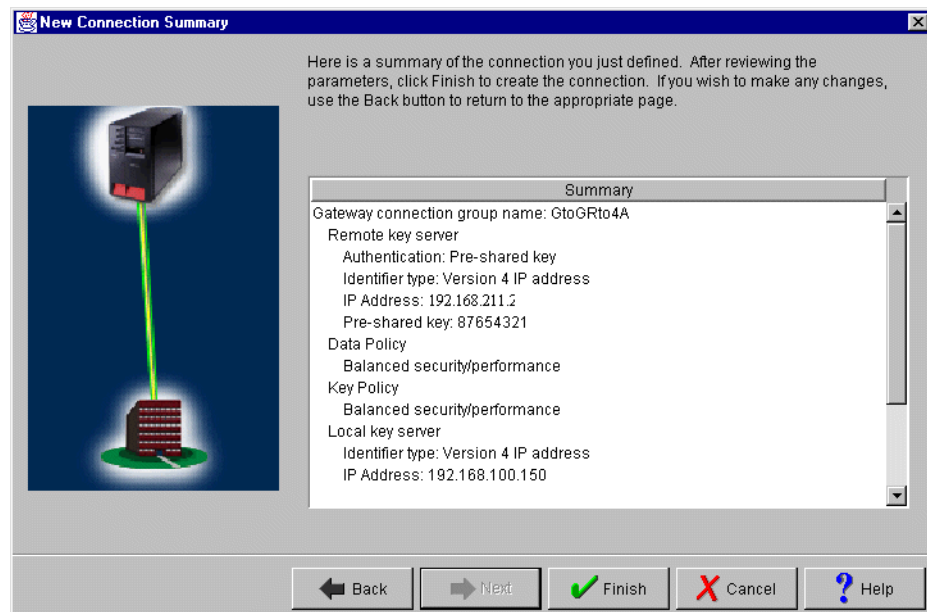


Figure 316. New Connection Summary window RALYAS4A

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.

13.4.10 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 to the connection group created by the wizard. Use IP Packet Security in AS/400 Operations Navigator to configure filters.

1. 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, subnet mask 255.255.255.0. Refer to the planning worksheet for RALYAS4A in Table 75 on page 391 and to Figure 315 on page 384.
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, subnet mask 255.255.255.0. Refer to the planning worksheet for RALYAS4A in Table 75 on page 391 and to Figure 315 on page 384.
3. Create two filters rules to allow Internet Key Exchange (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.

1. 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 2210 router address, `192.168.211.2`, 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.

2. 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, and the local AS/400 system address, `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.

4. Create a filter rule with action IPSEC to define the data endpoints that use the secure tunnel.

Use the same filter set name, `VPNIFC`. The action is IPsec, and the 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 menu to see all the data connections configured in your system and select one of them. In this scenario, select **GtoG4AtoR**.

5. Click the **Service** tab to specify the protocols and ports allowed in the tunnel. In this scenario, we selected the wildcard (*) in the Protocol, Source port, and Destination port fields. This allows any protocol using any port through the secure tunnel.

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.
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.

13.4.11 Starting IP filters

Activate the filter rules. At the IP Packet Security window click **File -> Activate**. The syntax is verified and, if correct, the filters are activated.

After activating the filter rules and before starting the VPN connection, verify the IP connectivity again:

1. From PC1 in the data center network (Figure 315 on page 384) PING PC2 in the remote subnet. Enter the following PING command:

```
PING RMTSYS ('192.168.101.101')
```

The ping request fails.

2. Repeat the test from PC2 in the branch office subnet to PC1 in the data center network:

```
PING 9.24.106.33
```

The ping request fails.

13.4.12 Starting the VPN connection

This section explains how to start the VPN connection. Before starting the connection, verify that the IP filters and the VPN servers are started. Refer to 10.7.3, "Starting the VPN connection" on page 230 for more information.

To start the GtoGRto4A connection, perform the following steps:

1. Right-click the **GtoGRto4A:L1** connection in the right panel and select **Start** to initiate a VPN connection to the 2210 router.
2. Display the connection to verify it is active. At the Virtual Private Networking window, select **View -> Active Connections**.
3. Use the 2210 router console to verify that the VPN connection is successfully established. Figure 317 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 317. Verifying the VPN connection status on the 2210 router

- Use the 2210 router console command `STATS` to display the VPN tunnel traffic statistics (see Figure 318).

```

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 318. Displaying the VPN tunnel traffic statistics on the 2210 router

- Switch to the IKE section of the IBM 2210 console (see Figure 319). Verify the security association established through IKE. The information provided includes 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 319. Checking the IKE status on the 2210 router

6. 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 320. Checking the IKE statistics on the 2210 router

7. Use the `LIST STATS` command shown in Figure 321 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 321. Checking the policy statistics on the 2210 router

13.4.13 Verification tests

Table 77 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 13.4.3.1, “Scenario objectives” on page 384.

Table 77. Verification test - OS/400 to 2210 router gateway-to-gateway scenario

| Description | TELNET | FTP | PING |
|-------------------------------------|--------|-----|------|
| From AS4Asubnets to RTRsubnet hosts | YES | YES | YES |
| From RTRsubnet hosts to RALYAS4A | YES | YES | YES |

Chapter 14. Building business partner/supplier VPNs

This chapter describes how IBM VPN solutions can be used to implement virtual private networks based on the business partner/supplier scenario. Essentially, this means building an extranet between different companies.

Consider a situation where a manufacturing company needs to communicate regularly with its suppliers, for example, to facilitate just-in-time delivery of parts, to settle invoices among themselves, or for any number of other reasons. There are two issues to consider:

- **Access control:** While it may be a business necessity for supplier A to have access to some of company X's internal resources (such as databases), there will also be valid business reasons to prevent the supplier from having access to all of company X's databases.
- **Data confidentiality:** Clearly the data should be hidden from general view while it is in transit over the public Internet. But there may be even more stringent requirements. Company X may consider its own intranet to be trusted, but its suppliers may not. For example, a supplier may want to ensure that its sensitive data, while traveling through company X's intranet, is hidden until it reaches its final destination. For example, the supplier may be worried that an unscrupulous eavesdropper inside company X may try to intercept the data and sell it to a competitor. And company X may have the same concerns about its data as it travels through the supplier's intranet. Thus, it will not be unusual for each party to treat the other's intranet as untrusted.

14.1 Design considerations

This scenario is an extension of the multiple branch office scenario. Here we have multiple supplier intranets that need to access a common corporate network over the Internet. Each supplier is allowed access to only a limited set of destinations within the corporate network. Even though traffic from the different suppliers flows over common data links in both the public Internet and in the destination intranet, the VPN must be constructed to guarantee that no traffic from a given supplier will be visible to any other supplier or to any system other than its intended destination.

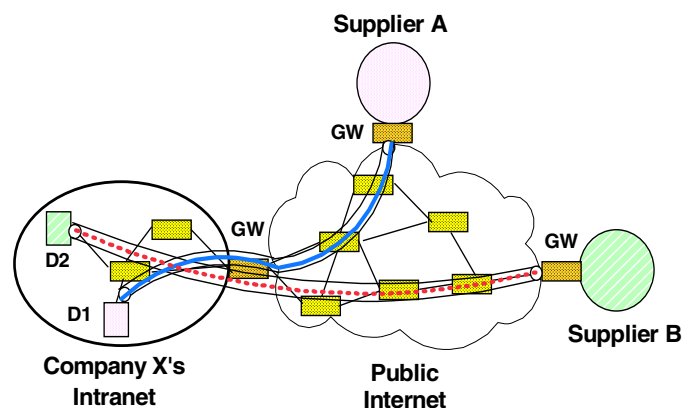


Figure 322. A typical supplier configuration

Figure 322 illustrates how the two data paths, represented by the dashed and solid lines inside the VPN tunnels, can flow through several common boxes. In this example, supplier A can talk only to destination D1 and supplier B can talk only to destination D2. Traffic from suppliers A and B can be intermixed both within the Internet and within company X's intranet.

IPSec provides a secure solution in this environment, but it will be more complex than for the branch office scenario outlined in Chapter 13, "Building branch office VPNs" on page 361. The extra complexity arises from the following factors:

- There can be multiple suppliers who need to communicate with the manufacturer. Hence, it may be necessary to ensure that supplier A can never see any other supplier's data in cleartext form, either on the Internet or in the manufacturer's intranet.
- If the manufacturer and the suppliers, or some subset of them, use private addressing in their respective intranets, then it is possible that *routing collisions* can occur if the same private address has been assigned to multiple hosts. To avoid this possibility, the members of the VPN must either use public IP addresses in their intranets, coordinate the assignment of private IP addresses among the systems participating in the VPN, or adopt some sort of network address translation strategy.
- Because security coverage extends from host-to-host (client-to-server) rather than just from gateway-to-gateway, there will be many more security associations to be negotiated, and many more keys to be securely distributed and refreshed, as compared to the branch office scenario. Hence, the automated secure functions of IKE become even more important.
- Because security coverage extends from host-to-host, IPSec functions will need to be supported in clients, servers, and firewalls.

14.1.1 Authenticating and encrypting supplier traffic

As shown in Figure 322 on page 403, the VPN gateway that guards the entry to company X's intranet must accept traffic from both supplier A and supplier B. This can be accomplished by using IPSec's AH protocol. There will be one tunnel between the firewall of company X and supplier A and another between the firewall or router of company X and supplier B. The AH protocol will be used in tunnel mode, providing cryptographically strong access control. Therefore, systems in supplier A's intranet can communicate with destination D1, and systems in supplier B's intranet can communicate with destination D2.

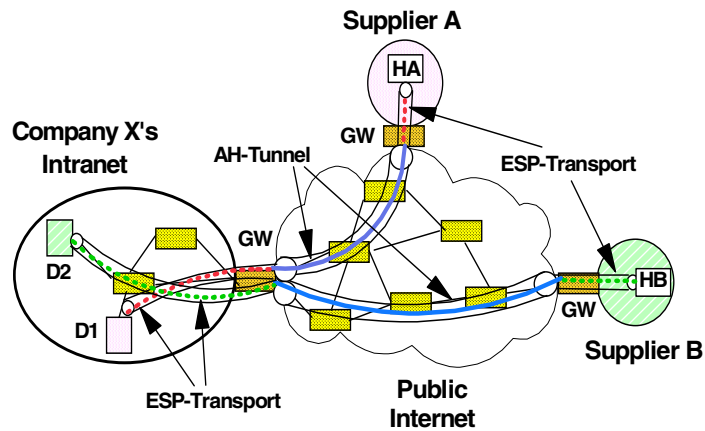


Figure 323. A typical supplier configuration

But as we have noted, there is a need for even finer-grained authentication, namely, each source to its intended destination. For example, in Figure 322, we need to ensure that destination D1 will accept traffic only from host HA and not from host HB. To achieve data confidentiality, we will use end-to-end encryption between each host and its intended destination server (for example, from host HA to destination D1). IPsec protocols provide the means to accomplish this by using *bundled security associations* (SA bundles), which make use of both tunnel and transport modes of operation simultaneously.

To handle the host-to-host authentication and encryption requirements, we will establish a security association (SA) between each client machine and its server. The protocol will be ESP with authentication, and the type of SA will be transport mode, since this is an end-to-end security association.

Next, we establish a different security association between the gateways that protect company X's intranet and the supplier's intranet. This SA applies over only part of the complete path, so it will use the AH protocol in tunnel mode. Because of tunnel mode, the packet will have the gateway's IP addresses in the "outer" IP header. Therefore, private addresses could also be used on the intranets. (See 14.1.2, "Addressing issues" on page 406.) Between firewalls or routers, an ESP security association will be nested inside the AH security association. Figure 324 illustrates the structure of the datagram that flows between firewalls or routers. An inner datagram is nested inside an outer datagram to support two distinct bundled security associations: client-to-server and gateway-to-gateway.

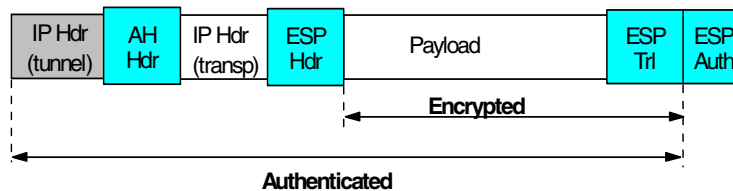


Figure 324. A typical supplier scenario datagram

Note that IPSec protocols enforce two levels of authentication: firewall-to-firewall and client-to-server. The firewall-to-firewall authentication prevents denial-of-service attacks by making sure that only traffic from legitimate suppliers can enter company X's intranet; the host-to-host authentication ensures that the destination will accept traffic only from its intended partner machines.

This considerably exacerbates scaling issues. Unlike the branch office case where security associations were established only between VPN firewalls or routers, it is now necessary to establish two additional security associations per client. Each security association will require its own set of cryptographic keys. This scenario illustrates the need for automated IKE-based methods, both for negotiating multiple bundled security associations and for distributing the associated keys.

14.1.2 Addressing issues

In Figure 323 there are tunnels between supplier A and company X, and also between supplier B and company X, but there is no tunnel between supplier A and supplier B. For routing purposes, supplier A and company X will run a mutually acceptable routing protocol over their tunnel, and company X and supplier B will also independently run their own routing protocol. Because each tunnel has its own security association, routing data for supplier A can be kept secret from supplier B, and vice versa. As in the case of the branch office interconnection scenario, each security association will use IPSec's ESP protocol to both encrypt and authenticate the routing updates.

Unlike the branch office case, where we could assume that a consistent addressing plan had been applied across all the company's intranets, in this configuration it is very likely that company X and each of its suppliers have administered their own addressing plan independently of one another. For example, it would be possible that supplier A and supplier B both used private (globally ambiguous) IP addresses in their networks, and it would be possible for some or all of their addresses to overlap. In this case, conventional IP routing protocols will not be able to resolve these ambiguities. Hence, we will make the assumption that the IP addresses of all systems, both in the corporate intranet and in the suppliers' intranets, have been assigned so that they are nonoverlapping. That is, we will assume that when private IP addresses are used, there will be coordination between the communicating intranets.

Note

As mentioned in 5.2, "Network address translation (NAT)" on page 89, NAT will not help in this case because it will change IP address information which will cause IPSec authentication to fail. In fact, since we need to build end-to-end IPSec tunnels in this scenario, NAT will prohibit the proper setup of security associations altogether.

14.1.3 Packet filtering and proxies

In this configuration, we have seen that there is a requirement for end-to-end encryption. This can cause problems for conventional packet filtering techniques, since the TCP header is part of the encrypted payload field and is no longer visible to the VPN firewalls or routers. Another area that needs to be addressed is the nesting of IPSec protocols. This means that the VPN firewall or router must

be able to handle IP packets where the next protocol field might indicate AH or ESP. It may also mean that packet filters will need to operate on both "inner" and "outer" IP address information, in cases where tunnel mode is used.

This area needs more study. The effectiveness of packet filtering will be significantly reduced, since unencrypted upper layer data is no longer available for examination by the VPN firewall or router. As the cryptographic techniques become used more widely for end-to-end protection, more and more access control decisions in a firewall will be handled via the AH protocol, and conventional packet filtering will become less and less useful. However, for traditional non-VPN traffic such as everyday World Wide Web access or news, packet filtering will still play its usual role. At the final destination host, where cleartext data is once again available, packet filtering will also continue to play a useful role for providing finer-grained level of access control within the destination host itself.

14.1.4 Summary: intercompany interconnection

This application of IPSec uses the public Internet to connect a company and its suppliers. It requires upgrades to existing client and server machines, since they must now support the IPSec protocol suite. It requires enhancements to conventional packet filtering techniques, because some headers from upper layer protocols may no longer be able to be decrypted at the VPN firewall or router. And finally, it makes use of IPSec's nesting capabilities. The major elements of complexity, compared to the branch office case, are summarized below:

- Client machines (hosts and servers) must support IPSec's ESP protocol, both for encryption and authentication.
- The number of machines that need to participate in the IPSec protocols has increased significantly. Security associations will need to be set up both end-to-end and gateway-to-gateway.
- For very small configurations, manual key distribution and manual configuration of security associations may be possible, but for any medium to large-sized configuration, support for ISAKMP/Oakley in clients, servers, and VPN firewalls will rapidly become a necessity.
- New packet filtering rules will need to be developed to accommodate: a) encrypted upper layer payloads, and b) pairs of inner and outer cleartext headers that arise when IPSec protocols are nested within one another. It remains to be seen if firewall or router filtering rules in the presence of end-to-end encryption will continue to serve a useful purpose. In the long term, filtering's importance will probably diminish as cryptography-based access control techniques become more widely used.

14.2 Nested tunnel configurations with IKE

As discussed in the introduction to this chapter, the business partner/supplier VPN scenario essentially consists of end-to-end connections between one or more systems in an external network and one or more systems in the internal network. From a security perspective, these end-to-end connections may need to be encrypted to prevent unauthorized disclosure in both the external and internal networks. This can be provided by IPSec or SSL. The connections should also be authenticated to thwart spoofing and hijacking, which can be better achieved with IPSec than with SSL.

To avoid the problem of not being able to route private IP addresses, either NAT or SOCKS can be used with SSL, but those techniques do not work with end-to-end IPSec. Therefore, this scenario uses an IPSec tunnel between the VPN gateways - IBM 2216 routers - through which the end-to-end connections are flowing. This also provides better protection than would be possible with NAT or SOCKS.

To avoid the problem of overlapping IP addresses, there are several solutions:

- Either NAT or a proxy server must be used. From a security perspective, using a proxy server behind or at the VPN gateway in the internal network should be preferred because it provides application control.
- The clients in the external network must use addresses that do not overlap addresses in the internal network. They should therefore be on a separate, maybe even isolated, LAN segment or have multiple interfaces. The latter is discouraged for security reasons.

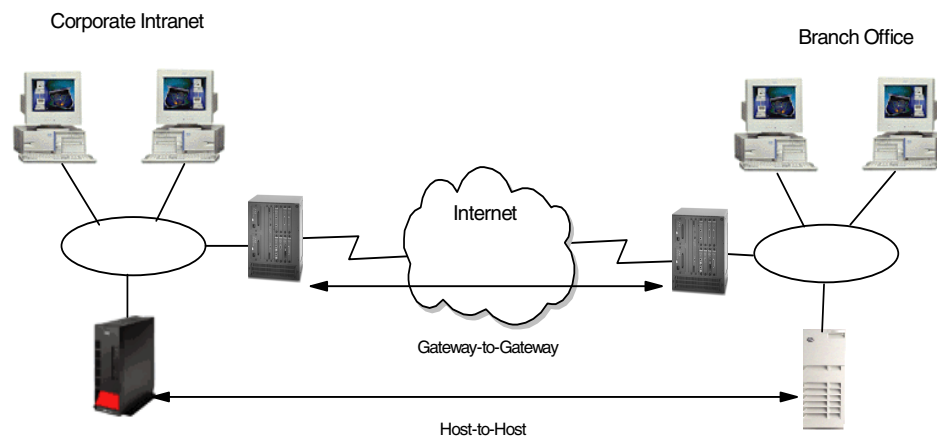


Figure 325. Nested tunnel scenario

14.2.1 IBM router configuration

To build this scenario we need to build two policies. The first policy will allow the ISAKMP messages to go through so that the hosts will be able to form an IPSec tunnel between them. The second policy will actually allow the ESP encapsulated IPSec packets through. Since the hosts will be encrypting their packets, the backbone tunnel only needs to be an AH tunnel, since double encryption will slow things down. However, it can add the benefit of hiding the internal addresses of the endstations.

14.2.1.1 Configure policy for IKE traffic

Let us first define the policy that will allow the ISAKMP messages through. The key aspect here is that we defined the profile to capture UDP port 500 messages to and from the host systems. We have also given the policy a different priority from that of the default to ensure it does not conflict with the IPSec AH policy that will be defined later on.


```

Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? nested_tunnel_ike
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]? 10
List of Profiles:
    0: New Profile
    1: routerware

Enter number of the profile for this policy [1]? 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 []? nested_tunnel_ike
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.2
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Destination Address [0.0.0.0]? 192.168.101.2

Protocol IDs:
    1) TCP
    2) UDP
    3) All Protocols
    4) Specify Range

Select the protocol to filter on (1-4) [3]? 2
Enter the Starting value for the Source Port [0]? 500
Enter the Ending value for the Source Port [65535]? 500
Enter the Starting value for the Destination Port [0]? 500
Enter the Ending value for the Destination Port [65535]? 500
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]?
Configure local and remote ID's for ISAKMP? [No]: y
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]:

Here is the Profile you specified...

Profile Name      = nested_tunnel_ike
sAddr             = 192.168.102.2 : sPort= 500 : 500
dAddr             = 192.168.101.2 : dPort= 500 : 500
proto             =                17 : 17
TOS               =                x00 : x00
Remote Grp=All Users
Is this correct? [Yes]:

```

Figure 326. Nested tunnels - IKE traffic policy - part 1

```

List of Profiles:
  0: New Profile
  1: routerware
  2: nested_tunnel_ike

Enter number of the profile for this policy [1]? 2
List of Validity Periods:
  0: New Validity Period
  1: always

Enter number of the validity period for this policy [1]? 1
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
  0: New IPSEC Action
  1: routerware

Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? nested_tunnel
List of IPsec Security Action types:
  1) Block (block connection)
  2) Permit

Select the Security Action type (1-2) [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
[192.168.102.1]? 9.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
[0.0.0.0]? 9.2.2.1
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/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 327. Nested tunnels - IKE traffic policy - part 2

After defining the validity period the IPsec action is defined. Here we simply define the tunnel endpoints and then we define the IPsec proposal for this IPsec action.

```

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
    1: routerware

Enter the Number of the IPSEC Proposal [1]? 0
Enter a Name (1-29 characters) for this IPsec Proposal []? nested_tunnel
Does this proposal require Perfect Forward Secrecy? (Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]: y
List of AH Transforms:
    0: New Transform

Enter the Number of the AH transform [0]? 0
Enter a Name (1-29 characters) for this IPsec Transform []? nested_tunnel
List of Protocol IDs:
    1) IPSEC AH
    2) IPSEC ESP

Select the Protocol ID (1-2) [1]?
List of Encapsulation Modes:
    1) Tunnel
    2) Transport

Select the Encapsulation Mode(1-2) [1]?
List of AH Authentication Algorithms:
    1) HMAC-MD5
    2) HMAC_SHA

Select the AH Authentication Algorithm (1-2) [1]? 2
Security Association Lifesize, in kilobytes (1024-2147483647) [50000]?
Security Association Lifetime, in seconds (120-2147483647) [3600]?

Here is the IPsec transform you specified...

Transform Name = nested_tunnel
    Type =AH    Mode =Tunnel    LifeSize= 50000 LifeTime= 3600
    Auth =SHA   Encr =None
Is this correct? [Yes]: y
List of AH Transforms:
    0: New Transform
    1: nested_tunnel

Enter the Number of the AH transform [1]?
Do you wish to add another AH transform to this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]:

```

Figure 328. Nested tunnels - IKE traffic policy - part 3

The IPsec proposal that is defined uses tunnel mode with AH. Next we simply confirm the IPsec proposal and action we just defined.

```

Here is the IPSec proposal you specified...

Name = nested_tunnel
Pfs = N
AH Transforms:
    nested_tunnel
Is this correct? [Yes]:
List of IPSEC Proposals:
    0: New Proposal
    1: routerware
    2: nested_tunnel

Enter the Number of the IPSEC Proposal [1]? 2
Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPSec Action you specified...

IPSECAction Name = nested_tunnel
Tunnel Start:End = 9.1.1.1 : 9.2.2.1
Tunnel In Tunnel = No
Min Percent of SA Life = 75
Refresh Threshold = 85 %
Autostart = No
DF Bit = COPY
Replay Prevention = Disabled
IPSEC Proposals:
    nested_tunnel
Is this correct? [Yes]:
IPSEC Actions:
    0: New IPSEC Action
    1: routerware
    2: nested_tunnel

Enter the Number of the IPSEC Action [1]? 2

```

Figure 329. Nested tunnels - IKE traffic policy - part 4

The next step is to define the ISAKMP action and proposal. In this scenario we will simply be using pre-shared key authentication.

```

ISAKMP Actions:
    0: New ISAKMP Action
    1: routerware

Enter the Number of the ISAKMP Action [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Action []? nested_tunnel

List of ISAKMP Exchange Modes:
    1) Main
    2) Aggressive

Enter Exchange Mode (1-2) [1]? 1
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, 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]:
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
    1: routerware

Enter the Number of the ISAKMP Proposal [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Proposal []? nested_tunnel

List of Authentication Methods:
    1) Pre-Shared Key
    2) Certificate (RSA SIG)

Select the authentication method (1-2) [1]? 1

List of Hashing Algorithms:
    1) MD5
    2) SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
    1) DES

Select the Cipher Algorithm (1-2) [1]?
Security Association Lifesize, in kilobytes (100-2147483647) [1000]?
Security Association Lifetime, in seconds (120-2147483647) [15000]?

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]?

Here is the ISAKMP Proposal you specified...

Name = nested_tunnel
AuthMethod = Pre-Shared Key
LifeSize   = 1000
LifeTime   = 15000
DHGroupID  = 1
Hash Algo  = SHA
Encr Algo  = DES CBC
Is this correct? [Yes]:

```

Figure 330. Nested tunnels - IKE traffic policy - part 5

```

List of ISAKMP Proposals:
  0: New Proposal
  1: routerware
  2: nested_tunnel

Enter the Number of the ISAKMP Proposal [1]? 2
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

ISAKMP Name      = nested_tunnel
  Mode           =                Main
  Min Percent of SA Life =        75
  Conn LifeSize:LifeTime =      5000 : 30000
  Autostart      =                Yes
  ISAKMP Proposals:
    nested_tunnel
Is this correct? [Yes]:
ISAKMP Actions:
  0: New ISAKMP Action
  1: routerware
  2: nested_tunnel

Enter the Number of the ISAKMP Action [1]? 2
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      = nested_tunnel_ike
  State:Priority =Enabled   : 10
  Profile        =nested_tunnel_ike
  Valid Period   =always
  IPSEC Action   =nested_tunnel
  ISAKMP Action  =nested_tunnel
Is this correct? [Yes]:

```

Figure 331. Nested tunnels - IKE traffic policy - part 6

Once the ISAKMP action is defined we simply confirm our definitions and the policy.

14.2.1.2 Configure IPsec traffic policy

Now we have to define a similar policy to let the IPsec AH traffic through. The important aspect in this definition is to build a profile that defines IP protocol number 50, the IPsec ESP protocol number.

```

Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? nested_tunnel_AH
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
    1: routerware
    2: nested_tunnel_ike

Enter number of the profile for this policy [1]? 0
Profile Configuration questions. Note for Security Policies, the Source
Address and Port Configuration Proxy 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 []? nested_tunnel_AH
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.2
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Destination Address [0.0.0.0]? 192.168.101.2

Protocol IDs:
    1) TCP
    2) UDP
    3) All Protocols
    4) Specify Range

Select the protocol to filter on (1-4) [3]? 4
Enter the Starting value for the IP Protocol ID [0]? 50
Enter the Ending value for the IP Protocol ID [255]? 50
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]?
Configure local and remote ID's for ISAKMP? [No]: y
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]? 1
Any user within profile definition allowed access? [Yes]:
Limit this profile to specific interface(s)? [No]:

Here is the Profile you specified...

Profile Name      = nested_tunnel_AH
  sAddr          = 192.168.102.2 :
  dAddr          = 192.168.101.2 :
  proto          =                50 : 50
  TOS            =                x00 : x00
  Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
    0: New Profile
    1: routerware
    2: nested_tunnel_ike
    3: nested_tunnel_AH

Enter number of the profile for this policy [1]? 3

```

Figure 332. Nested tunnels - IPSec AH traffic policy - part 1

```

List of Validity Periods:
  0: New Validity Period
  1: always

Enter number of the validity period for this policy [1]?
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
  0: New IPSEC Action
  1: routerware
  2: nested_tunnel

Enter the Number of the IPSEC Action [1]? 2
ISAKMP Actions:
  0: New ISAKMP Action
  1: routerware
  2: nested_tunnel

Enter the Number of the ISAKMP Action [1]? 2
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      = nested_tunnel_AH
State:Priority   =Enabled      : 5
Profile          =nested_tunnel_AH
Valid Period     =always
IPSEC Action     =nested_tunnel
ISAKMP Action    =nested_tunnel
Is this correct? [Yes]:

```

Figure 333. Nested tunnels - IPsec AH traffic policy - part 2

The validity period is then defined. We will reuse the IPsec and ISAKMP actions that were previously defined as they will be the same for this policy.

The last step is to define the user of the remote tunnel so that the correct pre-shared key is used.


```

Center 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]? 9.2.2.1
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):
Enter the Pre-Shared Key again (2 characters) in ascii:

Here is the User Information you specified...

Name      = 9.2.2.1
Type      = IPV4 Addr
Group     =
Auth Mode =Pre-Shared Key
Is this correct? [Yes]:

```

Figure 334. Nested tunnels - IPSec AH traffic policy - part 3

The definitions on the remote router are identical except for the IP addresses being reversed.

14.3 End-to-end tunnels with IPSec

In this scenario, we are presenting 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 and therefore, they want to ensure the connection is protected by IPSec protocols to the very hosts they want to connect.

14.3.1 Scenario characteristics

- Both networks, the distributor's and the manufacturer's, 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 hosts' VPN partners.

A sample configuration for this scenario is illustrated in Figure 325 on page 408.

14.3.1.1 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.

14.3.1.2 Scenario network configuration

Figure 335 shows our simple network configuration for the host-to-host AS/400 system to AIX server:

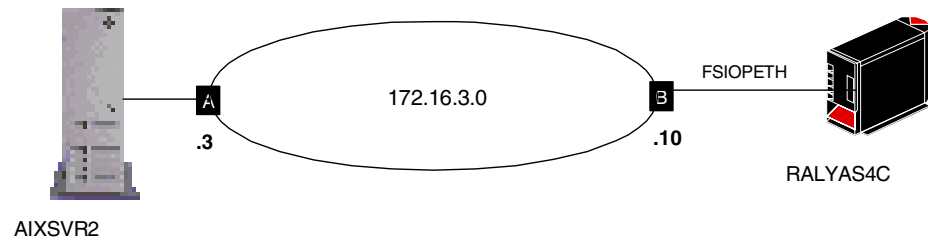


Figure 335. Host-to-host AS/400 - AIX - scenario network configuration

14.3.2 Implementation tasks - summary

The following is a summary of 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 worksheets for the AIX server.
3. Complete planning worksheets for the AS/400 system.
4. Configure a host-to-host VPN in the AIX server.
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.

14.3.2.1 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the two hosts is correct. A PING command accomplishes this task:

```
PING RMTSYS ('172.16.3.3') LCLINTNETA ('171.16.3.10')
```

14.3.3 Completing the AIX server planning worksheet

Complete the AIX planning worksheet as shown in Table 78. The planning worksheet allows you to gather all the configuration data before the actual implementation. We completed this planning worksheet from the perspective of AIXSVR2 in this scenario.

Table 78. 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 |

| Information you need to configure VPN in the AIX server | Scenario answers | |
|---|---------------------------------------|-----|
| 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 12345677) | |
| 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 | |

14.3.4 Completing the AS/400 system planning worksheet

Complete the AS/400 system planning worksheet as shown in Table 79. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 79. AS/400 planning worksheet - New Connection Wizard - RALYAS4C

| 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-host |
| 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 79) 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 expects it in hexadecimal format.

Table 80 shows the planning worksheet that we used to configure the AS/400 IP filters in this scenario.

Table 80. Planning worksheet - IP filter rules RALYAS4A

| This is the information you need to create your IP filters to support your VPN | Scenario answers |
|---|---------------------------|
| Is your VPN server acting as a host or gateway? Is the data endpoint the same as the authentication/encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway. | host |
| Is the remote 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? | AIXSet |
| If your 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 address(es)? Use this name as the <i>source address</i> on the IPSEC filter | n/a n/a n/a |
| 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 address(es)? Use this name as the <i>destination address</i> on the IPSEC filter | n/a n/a n/a |
| If you will limit services allowed through the VPN ... (use the information below in the IPSEC filter rule Services options) | |
| - What protocol will be allowed? | TCP |
| - What source port will be allowed? | Any (*) |
| - What destination port will be allowed? | 23 |
| 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 for the <i>source address</i> on the IPSEC filter if your server is acting as a host | 172.16.3.10 |
| 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 | 172.16.3.3 |

| This is the information you need to create your IP filters to support your VPN | Scenario answers |
|---|------------------|
| Is your VPN server acting as a host or gateway? Is the data endpoint the same as the authentication/encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway. | host |
| Is the remote 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? | AIXSet |
| If your 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 address(es)? Use this name as the <i>source address</i> on the IPSEC filter | n/a |
| | n/a |
| | n/a |
| 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 address(es)? Use this name as the <i>destination address</i> on the IPSEC filter | n/a |
| | n/a |
| | n/a |
| What is the name of the interface (for example, the token-ring or Ethernet line) to which these filters will be applied? | FSIOPETH |
| 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 denied. | 10.0.0.0 |

We also completed the IP filter rules planning worksheet (Table 80) 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. We defined a subnet 10.0.0.0 to permit traffic from and to the internal network. This general traffic is not shown in the example.

14.3.5 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 to open the Internet Key Management (IKE) Tunnel configuration panel. The Internet Key Exchange (IKE) Tunnels configuration panel is displayed.
5. Select **Tunnel -> New Key Management Tunnel** to open the Key Management (Phase 1) Tunnel Properties window.
6. On the Identification panel, enter the key management tunnel name. In this scenario RALYAS4C_AIXSRV2.
7. Select **IP address** as Host Identity type for local and remote endpoint for tunnel and 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 is displayed.
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 is displayed.
11. Enter the pre-shared key using 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 Management Tunnel** on the Internet Key Exchange (IKE) Tunnels configuration panel to open the Data Management (Phase 2) Tunnel Properties window.
14. On the Identification panel, enter the data management tunnel name; in this scenario, RALYAS4C_AIXSRV2.
15. Select the key management tunnel that should be associated with this data management tunnel; in this scenario, RALYAS4C_AIXSRV2, and click **Associate**.

Note

Do not check Automatic data management tunnel if your side is the responder or you do not want to establish the data management tunnel at system restart.

16. Click **Endpoints**. The Data Management (Phase 2) Tunnel Properties window is displayed.
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 is displayed.
 20. Select the **ESP_DES_MD5_TRANSPORT_NO_PFS** policy from Defined data management (phase 2) policies and 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 the Virtual Private Networks (IP Security) Network panel. When the tunnel has been activated, the status of the phase 1 and phase 2 tunnels is displayed as shown in Figure 336:

The screenshot shows a window titled ':IKE Tunnel Monitor : loopback'. It has a menu bar with 'Monitor', 'Selected', 'View', 'Options', and 'Help'. Below the menu bar is a toolbar with several icons. The main area contains a table with the following data:

| Tunnel | Phase | ID | Status | Local ID | Remote ID | |
|--------|-------|----|--------|----------|------------|-------------|
| | 2 | 1 | 2 | Active | 172.16.3.3 | 172.16.3.10 |
| | 1 | 2 | 1 | Active | 172.16.3.3 | 172.16.3.10 |

Figure 336. AIX 4.3.2 - IKE Tunnel Monitor

14.3.6 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 AS/400 Operations Navigator from your desktop.
2. Expand your AS/400, in this case, **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. This starts a new connection wizard for a host-to-hosts connection. The wizard welcome window is displayed.
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 79 on page 420. The name you specify here is the name for all objects the wizard creates for this particular connection. It is case-sensitive. Also enter a Description of the configuration you are creating.
9. Click **Next**.
10. On the Key Policy window, specify what 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 worksheet. The wizard chooses the appropriate encryption and authentication algorithms based on the selection you make here.
11. Click **Next** when complete.
12. On the Local Identifier window, 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 end point for the connection. 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 of the interface that is connecting to the remote VPN server. Refer to the planning worksheet in Table 79 on page 420; for RALYAS4C, this is 172.16.3.10 (interface B in Figure 335 on page 418).
13. Click **Next**.
14. Use the Remote Identifier window 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 335 on page 418). Specify *12345678* in the *Pre-shared key* field. Remember, the same pre-shared key must be entered exactly when configuring VPN on the remote AIX server, but when entering this value in the AIX configuration, it must be in hexadecimal format (*3132333435363738*).
15. Click **Next**.
16. Use the Data Policy window to specify what level of authentication or encryption 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 79 on page 420).
17. Click **Next**.
18. The final window summarizes the configuration values you entered.

If you scroll down, you can also see a list of the configuration objects that the wizard will create when you click **Finish** (Figure 337 on page 426). Check the configuration values against your worksheet. If changes need to be made, click **Back**.

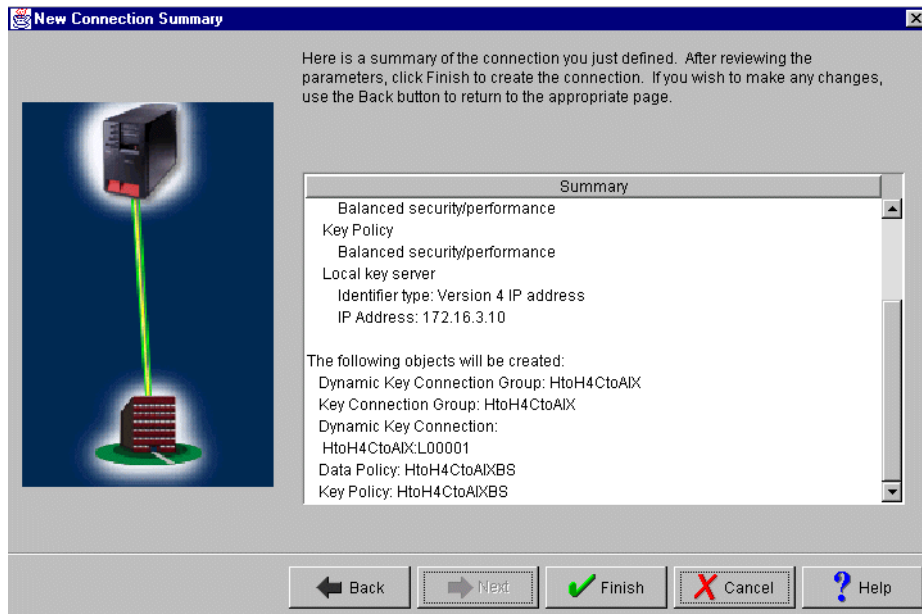


Figure 337. New Connection Summary window - host-to-host - AS/400 system to AIX server

19. If everything is OK, 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.

14.3.7 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 in 14.3.6. However, the wizard configures default values that you may need to change to match the VPN partner's configuration. Refer to 10.5.3, "Changing the New Connection Wizard default values" on page 204 for a discussion on how to change the default values configured by the wizard. In this scenario, we changed 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 the Initiator negotiation and **Require identity protection** for the Responder negotiation.
4. To change Phase 1 key lifetime, from the Key Policies - Properties window, select the **Transforms** tab.
5. Select the transform you want to change.

6. Click **Edit**.
7. Change the Maximum key lifetime to **480** minutes.
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.
15. Click **OK**.

To enforce the requirement stated in 14.3.1.1, “Scenario objectives” on page 417 that only the distributor’s system, RALYAS4C, can initiate the connection, perform 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.
17. At the Properties window, select **Only the local system can initiate the connection**.

Table 81 summarizes the OS/400 and AIX VPN configuration and provides a cross-reference list.

Table 81. OS/400 - AIX cross-reference VPN configuration table

| | |
|---|--|
| <p><u>Key Policies</u></p> <p>Initiator Negotiation = Identity Protection (main mode) 1</p> <p>Responder Negotiation = Required 1</p> <p>Key Protection Transforms</p> <p>Authentication Method = Pre-shared key 2</p> <p>Pre-shared key value = 12345678</p> <p>Hash Algorithm = MD5 3</p> <p>Encryption Algorithm = DES-CBC 4</p> <p>Diffie-Hellman Group = Default 768-bit MODP 5</p> <p>Key Management 6</p> <p>Maximum key lifetime (minutes) = 480</p> <p>Maximum size limit (Kilobytes) = No size limit</p> | <p><u>Key management (phase 1) tunnel</u></p> <p>1 Policy role & Identity Protection = BOTH(I,R) & MAIN</p> <p>Transform Property</p> <p>2 Authentication Method = PSK</p> <p>Preshared key = 3132333435363738</p> <p>3 Hash algorithm = HMAC_MD5</p> <p>4 Encryption algorithm = DES</p> <p>5 Diffie-Hellman group = Group 1</p> <p>6 Key lifetime</p> <p>Time (minutes) = 480</p> <p>Size (Kilobytes) = 0</p> <p>14 Policy Role = Allow responder negotiations only</p> |
| <p><u>Data Policies</u></p> <p>Use Diffie-Hellman Perfect Forward Secrecy = No 7</p> <p>Data Protection Proposals</p> <p>Encapsulation mode = Transport 8</p> <p>Transforms</p> <p>Protocol = ESP 9</p> <p>Algorithms</p> <p>Authentication Algorithm = HMAC-MD5 9</p> <p>Encryption Algorithm = DES-CBC 10</p> <p>Key Expiration</p> <p>Expire after (minutes) = 30</p> <p>Expire at size limit (Kbytes) = No size limit</p> | <p><u>Data management (phase 2) tunnel</u></p> <p>7 Perfect Forward Secrecy (PFS) = No</p> <p>8 Encapsulation mode = Transport</p> <p>Protocol = ESP 9</p> <p>AH authentication algorithm =</p> <p>9 ESP authentication algorithm = MD5</p> <p>ESP encryption algorithm = DES</p> <p>Key lifetime 10</p> <p>Time (minutes) = 30</p> <p>Size (Kilobytes) = 0</p> <p>End Points -> End point type = Host</p> |
| <p><u>Key Connection Groups</u></p> <p>Remote key server</p> <p>Identifier type = IPV4 11</p> <p>IP address = 172.16.3.3</p> <p>Local key server</p> <p>Identifier type = IPV4 12</p> <p>IP address = 172.16.3.10</p> <p><u>Dynamic Key Group</u> 13</p> <p>System role = Both systems are hosts</p> <p>Initiation = only the local system can initiate the connection 14</p> | <p>13 <u>Key management (phase 1) tunnel</u></p> <p>Remote endpoint for tunnel</p> <p>12 Host identity tye = IP address</p> <p>Host identity = 172.16.3.10</p> <p>Local endpoint for tunnel</p> <p>Host identity tye = IP address 11</p> <p>Host identity = 172.16.3.3</p> |

You have now completed the VPN configuration for RALYAS4C. You will configure AS/400 IP filtering in the next task.

14.3.8 Configuring IP filters on the AS/400 system (RALYAS4C)

The wizard does *not* configure IP filtering. You must complete this task manually by using AS/400 Operations Navigator. If IP filtering is already configured and active, then any new filters must be integrated with those already in existence.

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 338 on page 428 and Figure 339 on page 428.

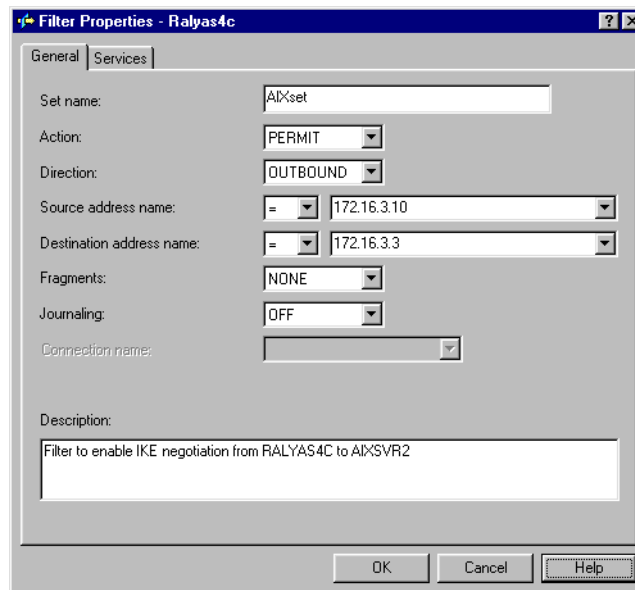


Figure 338. IP filter for outbound IKE messages - RALYAS4C to AIXSVR2

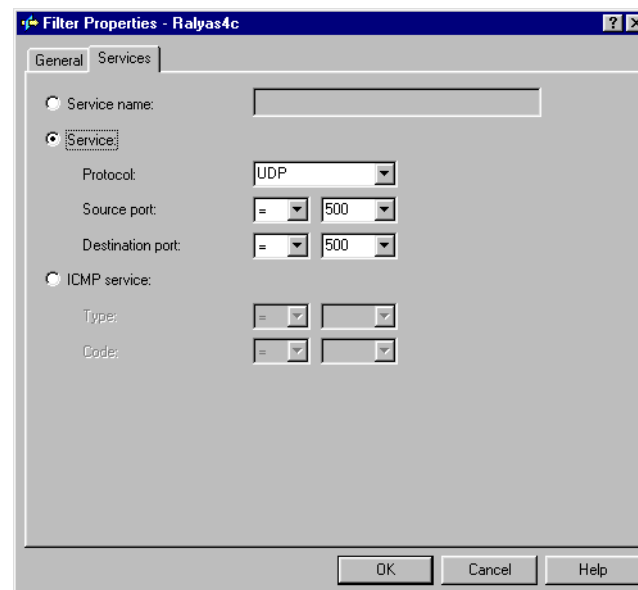


Figure 339. Services for IKE negotiation

2. Configure the inbound filter to allow IKE negotiation between the key servers as shown in Figure 340 on page 429 and Figure 341 on page 429.

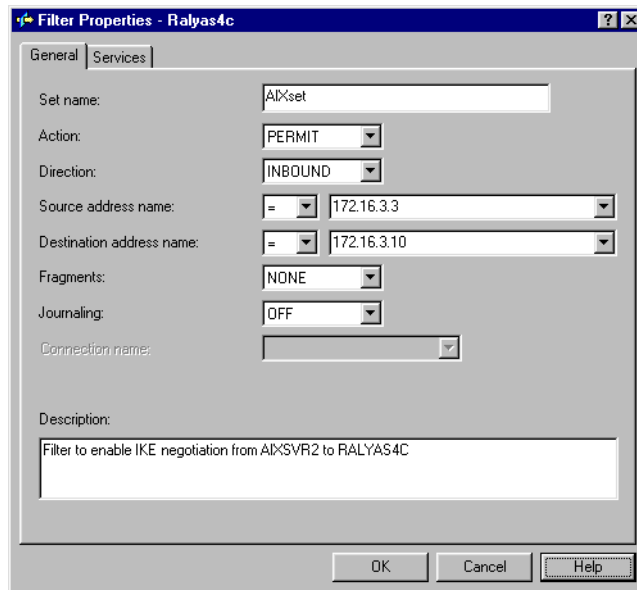


Figure 340. IP filter for inbound IKE messages - AIXSVR2 to RALYAS4C

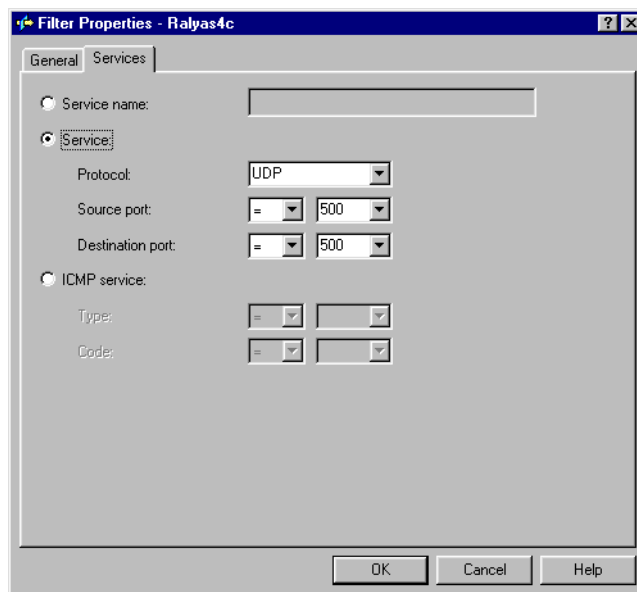


Figure 341. Services for IKE negotiation

3. 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 hosts' IP addresses for RALYAS4C and AIXSVR2.

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 have been configured on this system and select the

one required. In this example, you select **HtoH4CtoAIX**. See Figure 342 on page 430.

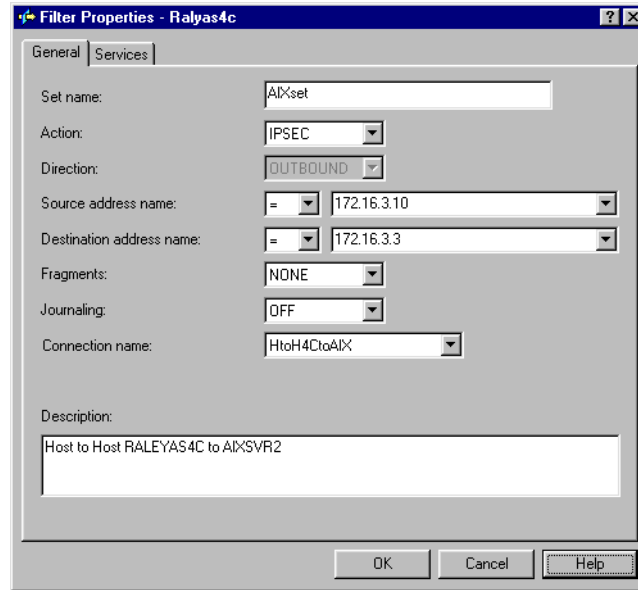


Figure 342. Host-to-host connection - IPSec filter rule

When you complete the required fields, click on the **Services** tab.

4. Enter **TCP** in the Protocol field; wildcard (*) in the Source port field, and **23** (Telnet) in the Destination port field. This allows only Telnet using port 23 to use this filter rule and hence, the VPN tunnel. See Figure 343:

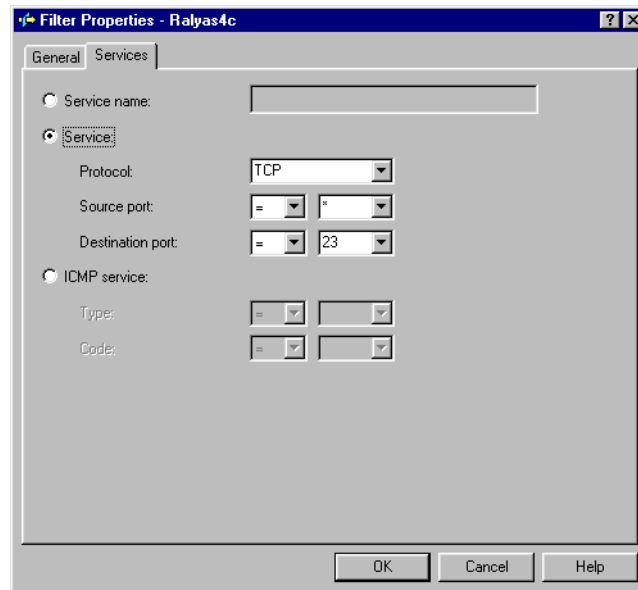


Figure 343. IPSec filter rule service - limiting the services to Telnet

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 343 on page 430. 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 344 on page 431).

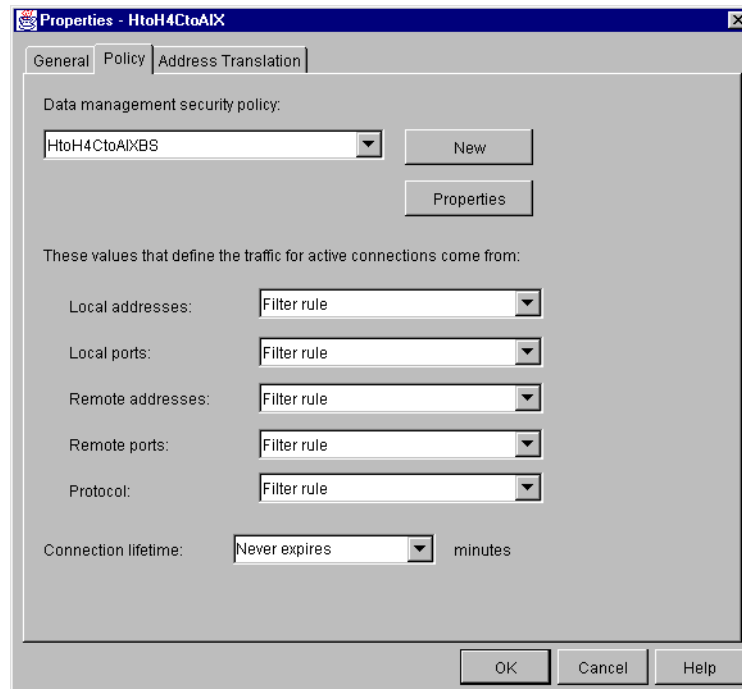


Figure 344. Dynamic key group - values that define traffic for active connections

14.3.9 Starting the VPN connection

This section explains how to start the VPN connection configured in the previous sections. Before starting the connection you must verify that the IP filters and the VPN servers are started.

To start the HtoH4CtoAIX connection perform the following steps:

1. Right-click the **HtoH4CtoAIX** connection and click **Start** from the pull-down menu (Figure 345 on page 432).

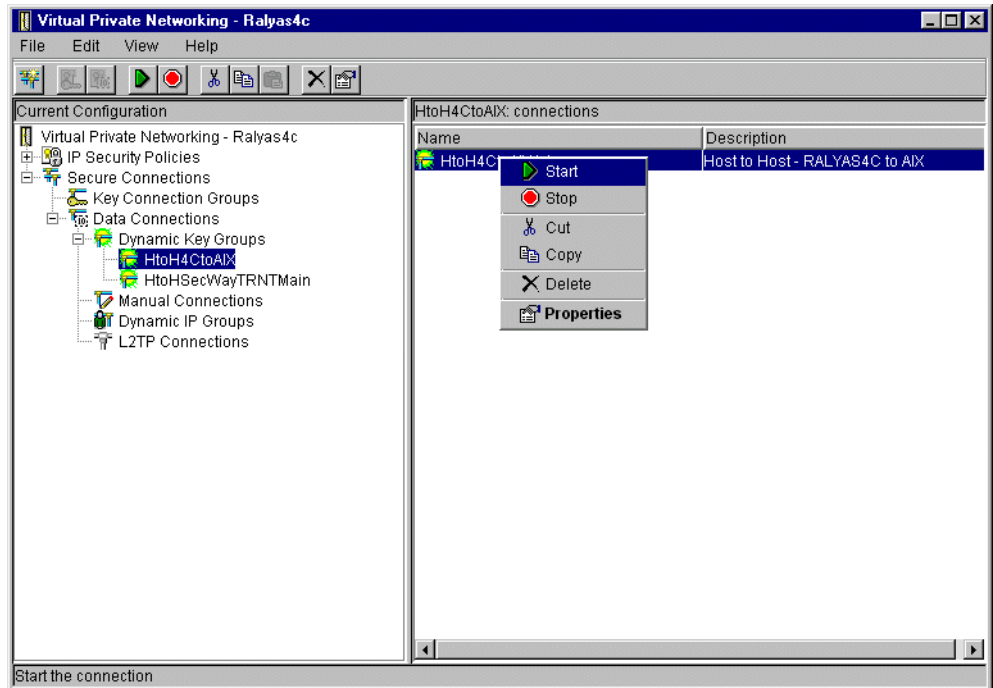


Figure 345. Starting the host-to-host connection - HtoH4CtoAIX

Note: Only RALYAS4C is allowed to initiate the connection as configured in 14.3.7, “Matching the AIX server VPN configuration” on page 426.

2. 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 346:

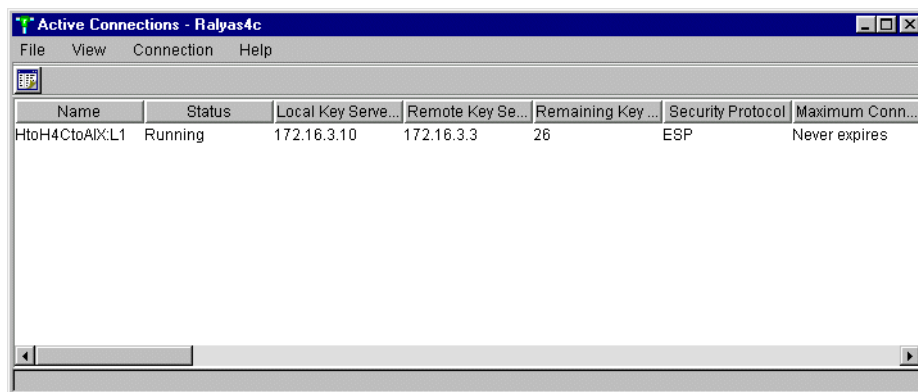


Figure 346. Active Connections window

14.3.10 Verification tests

Table 82 on page 433 presents a summary of the verification tests run after the host-to-host VPN was configured. The tests verify the scenario objectives stated in 14.3.1.1, “Scenario objectives” on page 417.

Table 82. Verification test - OS/400 to AIX server host-to-host scenario

| Direction | Start connection | TELNET | FTP | PING |
|--------------------------|-------------------------|---------------|------------|-------------|
| From RALYAS4C to AIXSVR2 | YES | YES | NO | NO |
| From AIXSVR2 to RALYAS4C | NO | NO | NO | NO |

Chapter 15. Building remote access VPNs

This chapter describes how IBM VPN solutions can be used to implement virtual private networks based on the remote access scenario. Essentially, this means extending a company's intranet to the locations of remote users who employ dial-in connectivity from Internet service providers.

With the advent of tele-working, remote access to corporate networks is increasingly important these days. The traditional way of deploying modem pools and remote access servers is expensive because of the dedicated equipment needed and especially because of the long-distance telephone costs involved. As the Internet has become virtually omnipresent, just a local phone call away, the remote access costs can be greatly reduced by using the Internet as the access infrastructure to the corporate network.

For this scenario, let us assume that company A has procured Internet access from an ISP and wants to enable its mobile work force to access the resources located in the corporate network over the Internet. For simplicity we do not consider other possible connections, such as Internet access or other VPN scenarios. These issues can be dealt with separately. The techniques described here can also be applied to secure traditional dial-in connections.

15.1 Design considerations

The major issue to be addressed is the inherently dynamic nature of this scenario. Typically, SAs cannot be preconfigured because the clients' addresses cannot be predicted. ISPs assign addresses dynamically. At some ISPs it is possible to request fixed addresses for dial-in connections, but only at an extra charge.

We need to be able to identify the remote client by its name rather than by its IP address. IKE has this ability. The filter rules associated with a dynamic tunnel are automatically effective at client connection time and cease operation when the client closes the tunnel. These dynamic filter rules are always checked *before* the static filter rules and cannot be modified. Advantages of this mode of operation are the ease of use and the guaranteed functionality. The security policy for the secure network, not the firewall, is what determines the access for the remote client once connected and authenticated.

If the clients' addresses are known (preassigned by the ISP), then we are not limited to dynamic tunnels and the clients mentioned. Basically, any kind of valid combination listed in 8.3, "IBM VPN platforms - interoperability matrix for IKE" on page 124 will work.

Another important design point is whether to extend IPSec tunnels to the hosts in the intranet or not. Most companies trust their intranets; for them there is no reason to do so. This approach has the advantage of a much smaller number of SAs to be managed. Also, the end systems do not need to be modified to support IPSec.

Sometimes very stringent security regulations are in place and the intranet is untrusted. In this case the IPSec tunnels should go directly to the destination host. IPSec should be deployed to those hosts and a large number of SAs should

be managed. These factors could have significant cost and system management implications.

Extending a tunnel from the client to the server also could make sense in another, very special situation: when the client is a *foreign* one, for example a traveling business partner's notebook that is allowed to connect to a corporate server. This setup resembles the business partner/supplier scenario, the difference being that all tunnels originate from the client itself.

15.1.1 Data Confidentiality and authentication

It is obvious that company A wants the dial-in traffic to be encrypted. Authentication is also needed because the corporate firewall must admit only traffic from the remote clients. Thus, either ESP tunnels with authentication option or combined AH-ESP tunnels should be used. The latter is the only possibility to provide both authentication and encryption with the current IBM firewall.

15.1.2 Addressing and routing issues

Unlike in the branch office connection or business partner/supplier scenarios, here we have one endpoint of the tunnels in the Internet. The clients will have automatically assigned public IP addresses by the ISP at connect time. These are routable everywhere. The router installed by the ISP at company A's site knows how to route to the Internet. Therefore, the only requirement for the internal routers is to have routes that direct Internet traffic to the corporate firewall, which in turn routes to the ISP's router. This should be the case anyway.

The IPSec code at the dial-in clients should be capable of differentiating between the corporate traffic that is to be tunneled and the ordinary Internet traffic that requires no special treatment. If they sent all traffic through the tunnel, then the remote user would lose the ability to access Internet resources while operating that tunnel, because the firewall normally would drop the packets retrieved from a tunnel that has nonsecure source and destination addresses.

The addressing scheme of the intranet needs no modification to support dial-in clients. If the intranet uses private addresses, it will still be reachable, because packets with private IP addresses are tunneled and the tunnel endpoints have public addresses. Only the subnets with direct connection to the Internet need to have public addresses. This is no new requirement.

15.1.3 Multiprotocol support

If protocols other than IP should be supported for the remote clients, then besides IPSec an appropriate tunneling protocol that will carry the non-IP payload must be supported by the firewall and by the ISP's point of presence. However, these protocols do not offer robust cryptographic features comparable to IPSec. Therefore, the solution is to use IPSec to protect the traffic that flows in the multiprotocol tunnel.

In this case a viable choice is L2TP, which is likely to be supported by more and more ISPs. Note that the non-IP protocol must not only be supported at the remote client and at the destination server, but also at the firewall. Otherwise the firewall would have no means to send the decapsulated non-IP payload to its ultimate destination.

With L2TP, the PPP connection that was in place between the remote client and the ISP is now extended to the corporate firewall. This results in the client and the firewall being on the same IP subnet and allows for the firewall to assign the client's address itself.

15.1.4 Summary: remote access

This application of VPN technology replaces existing direct dial-in lines to the corporate network and instead uses the Internet as the access infrastructure. Here are the major design considerations:

- The solution does not require changes at the servers in the corporate network unless the dial-in traffic is to be protected against attacks on the intranet as well. However, clients have to support the IPSec protocols.
- Because client addresses are typically dynamic, clients need to use an identifier other than an IP address to authenticate themselves to the VPN gateway. IKE has that capability.
- The dial-in traffic will be encrypted and authenticated. Any traffic that cannot be authenticated will be rejected by the VPN gateway.
- Existing packet filtering rules, if any, do not interfere with the dynamic filter rules. They can be used without modification.
- Explicit filter rules to protect the corporate intranet against non-VPN traffic are not required because the IPSec authentication will provide this protection.

15.2 Remote access with IPSec

In previous chapters we described how remote access VPNs can be established using various kinds of layer-2 tunneling protocols, some of which have been secured using IPSec. It is, of course, also possible to facilitate remote access VPNs based entirely on traditional PPP dial-up combined with IPSec tunnels and IKE authentication.

There are, however, significant differences between this scenario and using layer-2 tunneling:

1. IPSec dial-up does not support multiprotocol traffic.
2. The remote client has access to the Internet and the corporate network at the same time, which can pose a security exposure.
3. IPSec dial-up allows packets with external addresses on the corporate network. It depends on the placement of the VPN gateway relative to the corporate firewall as to how the security policy must be defined to allow this.
4. Because the remote client in this case is using an ISP-assigned IP address, return routes from the corporate network to the client may or may not be available depending on how many exit paths exist from the corporate network back to the Internet.

As an option to overcome issues 3 and 4 described above, a remote access client could employ a virtual IP address assigned from within the corporate network address range and emulate a branch office.

15.2.1 Description of the scenario

To implement remote access with IPSec, you need a client that supports PPP dial-up and IPSec as well as IKE. Because in most cases the client will get a different IP address from an ISP each time it connects, the IP address cannot be used as the IKE peer identity. Therefore, IKE must either be used in aggressive mode (if pre-shared key authentication has to be used) or with certificate-based authentication (then main mode or aggressive mode can be used). Our environment is based on an IRE SafeNet VPN client dialing in to an IBM 2212 router acting as the ISP and then establishing IKE negotiation and IPSec tunnels to an IBM 2216 router acting as the corporate VPN gateway.

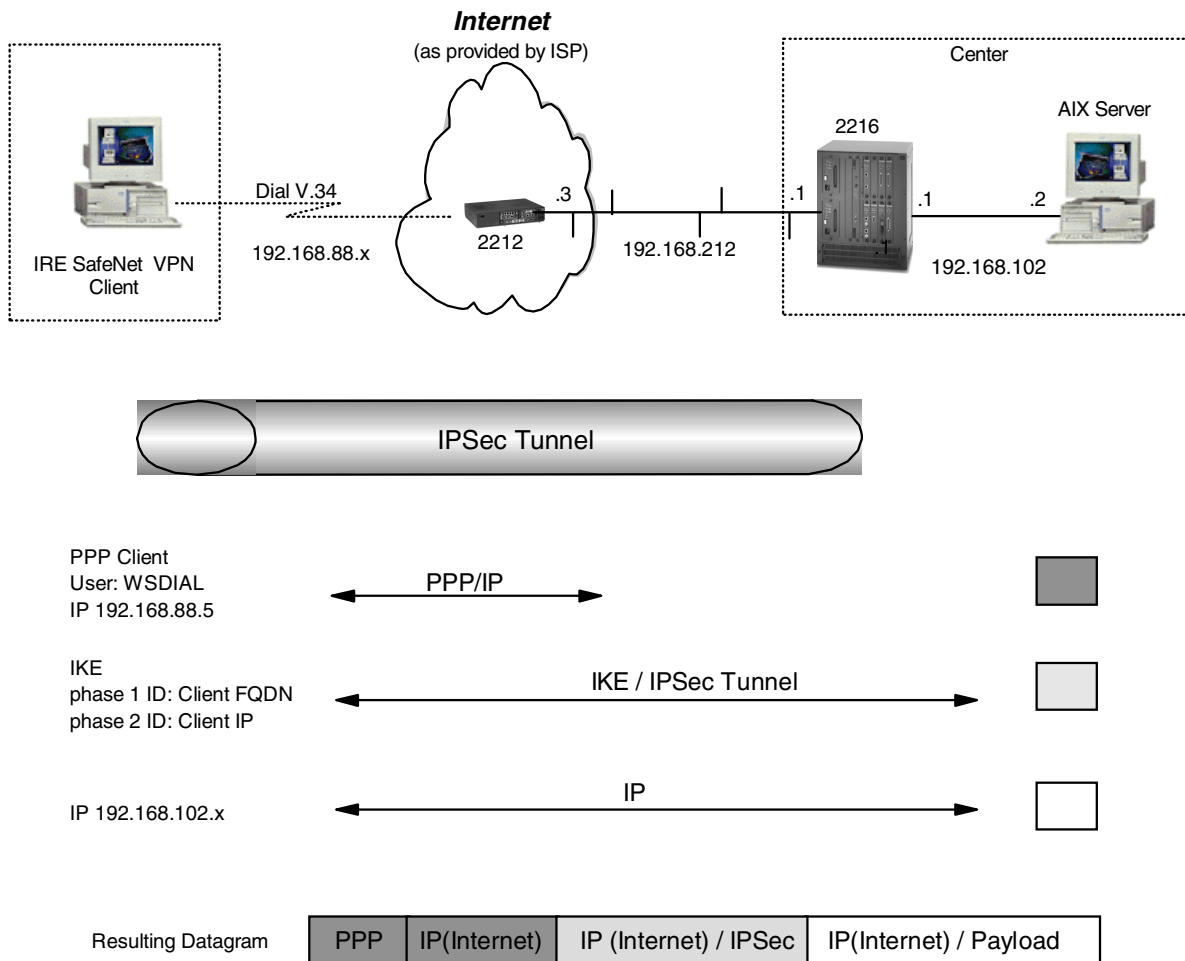


Figure 347. Remote access - IPSec dial-up scenario

In this scenario, the remote client is accessing the secure network with an external IP address. To limit this type of packet on the internal network, we are restricting the client in this scenario to access only one specific server or firewall. In general, access to the whole internal network can be given to a client in this case, but it depends on where the VPN gateway is placed relative to the corporate firewall in order to determine how the firewall is to handle this kind of traffic.

Because all client packets arrive via a secure tunnel there is no exposure associated with them other than the general tunnel fear that the client could have been attacked by a cracker and what arrives through the tunnel is malevolent traffic. This is no different from other remote access VPN scenarios.

15.2.2 Configuration of the ISP router

For this example we used a 2212 as the ISP router.

For the configuration of the 2212 we have to perform the following steps:

- Preparation.
- Add PPP user for the dial-in workstation.
- Add IP address and enable ARP subnetrouting.
- Activate the definition.

Note that in our case the ISP router does not establish the PPTP tunnel. Therefore, we do not need to add a tunnel definition. This differs from L2F and L2TP as PPTP does not do tunnel authentication.

15.2.2.1 Preparation

Perform the following steps so prepare the router for PPP dial-in.

Define and configure a V.34 interface for the user dial-in

Net 0 is used as the V.34 dial-in interface. Net 5 is assigned by the router as a virtual dial circuit interface. The virtual dial interface must be mapped to the physical V.34 interface (Figure 348):

Configure the V.35 WAN physical interface. The cable type and clocking may be different depending on your environment (`set hdlc cable v35 ...`, `set hdlc clocking...`, `set hdlc speed`). These commands are not shown here.

```
ISP Config>
ISP Config>set data-link v34
Interface Number [0]? 0
ISP Config>
ISP Config>add device dial-in
Enter the number of PPP Dial-in Circuit interfaces [1]?
Adding device as interface 5
Defaulting data-link protocol to PPP
Base net for this circuit [0]? 0
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.
Add more dial circuit interface(s)? (Yes or [No]):
Use "set data-link" command to change the data-link protocol
Use "net <intf #>" command to configure dial circuit parameters
ISP Config><
```

Figure 348. Configuring the dial-in interface

Set the modem initialization string

You can also set the modem initialization string and speed.

Note: We used a 3Com-US Robotics modem. Therefore, it was necessary to add `&B1` to the end of the default Modem initialization string. The resulting string is `AT&S1L1&D2&C1X3&B1` (Figure 349):

```

ISP Config>n 0
V.34 Data Link Configuration
ISP V.34 System Net Config 0>set modem-init
Modem initialization string [AT&S1L1&D2&C1X3]? AT&S1L1&D2&C1X3&B1
ISP V.34 System Net Config 0>

```

Figure 349. Set modem initialization string

15.2.2.2 List Configuration

You can check the parameters that you configured with the `list all` command (Figure 350).

```

ISP Config>n 0
V.34 Data Link Configuration
ISP V.34 System Net Config 0>
ISP V.34 System Net Config 0>li all
      V.34 System Net Configuration:
Local Network Address Name   = default_address
Local Network Address       = 9999999
Non-Responding addresses:
Retries                     = 1
Timeout                     = 0 seconds

Mode                         = Switched

Call timeouts:
Command Delay               = 0 ms
Connect                    = 60 seconds
Disconnect                  = 2 seconds

Modem strings:
Initialization string       = AT&S1L1&D2&C1X3&B1

Speed (bps)                 = 9600
ISP V.34 System Net Config 0>

```

Figure 350. Command list all on the V.34 interface

15.2.2.3 Add PPP user for the dial-in workstation

Add the PPP-user definition for the dial-in workstation. Assign it an IP address or create an IP-pool.

Note: The password does not show when typed but has been shown for illustration.


```

ISP Config>
ISP Config>add ppp-user
Enter name: []? wsdial
Password:wsdial
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route? (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]? 192.168.88.5
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]

      PPP user name: wsdial
      User IP address: 192.168.88.5
      Netroute Mask: 255.255.255.255
      Hostname: <undefined>
      Virtual Conn: disabled
      Time allotted: Box Default
      Callback type: disabled
      Dial-out: disabled
      Status: enabled
      Account Expiry: <unlimited>
      Password Expiry: <unlimited>

Is information correct? (Yes, No, Quit): [Yes] y

User 'wsdial' has been added
ISP Config>

```

Figure 351. Command `add ppp-user`

15.2.2.4 Add IP address

To route IP through the V.34 interface, an IP address must be assigned to the interface. The router adds a static route to the V.34 virtual interface when the Client dials in. You can assign a real IP address or use, as we have, IP unnumbered. For IP unnumbered the format of the address is 0.0.0.n where n is the interface number.

```

ISP Config>list device
Ifc 0      V.34 Base Net
Ifc 1      WAN PPP
Ifc 2      WAN PPP
Ifc 3      WAN PPP
Ifc 4      2-port IBM Token Ring          Slot: 1      Port: 1
Ifc 5      PPP Dial-in Circuit
ISP Config>protcool ip
Internet protocol user configuration
ISP IP config>add address 5 0.0.0.5 0.0.0.0
ISP IP config>

```

Figure 352. Adding an IP address to the dial-in interface

Note:

IP address is added in the format: add address x y.y.y.y z.z.z.z, where x is the interface number, y.y.y.y is the IP address of the interface and z.z.z.z is the subnet mask of the interface address

15.2.2.5 Activate the definitions on the ISP router

You activate the definitions on the ISP with the command `restart` (Figure 353 on page 442):

```
ISP Config>
ISP *restart
Are you sure you want to restart the gateway? (Yes or [No]): y
The configuration has been changed, save it? (Yes or [No] or Abort): y
Config Save: Using bank B and config number 2
```

Figure 353. Restarting the ISP router

15.2.3 Configuration of the VPN Gateway (Center 2216 Router)

For the configuration of the 2216 in the center we have to perform the following steps:

- Preparation
- Configure Policy and validity period for IPSec and IKE
- Configure IPSec action and proposal
- Configure ISAKMP action and proposal
- Activate the Definitions on the Center Router

15.2.3.1 Preparation

We assume that the permanent Ethernet connection to the ISP is already established. Therefore, we can concentrate on the dial-in features of this connection.

15.2.3.2 Configure policy profile for IPSec and IKE

The first step is to configure a policy that will encapsulate client traffic in an IPSec tunnel. When configuring the profile it is important that you select an address range rather than a netmask or single IP address. This is because if you use netmask the ID comparisons will fail because the netmask is of a subnet type while the ID type that will be received by the client is an IP address type. Of course you cannot use a single IP address because you do not know what IP address the client will get from the ISP.

```

Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ire
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

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 []? ire
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.2
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 2
Enter IPV4 Starting Destination Address [0.0.0.0]?
Enter IPV4 Ending Destination Address [0.0.0.0]? 255.255.255.255

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]?
Configure local and remote ID's for ISAKMP? [No]: y
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]? 1
Any user within profile definition allowed access? [Yes]:
The Source and/or Destination Address information you specified
includes all addresses. You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy. The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]:

```

Figure 354. Center router IKE policy configuration for IPSec dial-up

```

Here is the Profile you specified...

Profile Name      = ire
sAddr            = 192.168.102.2 : sPort=    0 : 65535
dAddr:End       =      0.0.0.0 : 255.255.255.255 dPort=    0 : 65535
proto           =                0 : 255
TOS             =                x00 : x00
Remote Grp=All Users

Is this correct? [Yes]:
List of Profiles:
    0: New Profile
    1: ire

Enter number of the profile for this policy [1]?

```

Figure 355. Center router profile configuration for IPSec dial-up

15.2.3.3 Configure validity period

The next step is to define a validity period.

```

List of Validity Periods:
    0: New Validity Period

Enter number of the validity period for this policy [0]? 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 356. Center router validity period configuration for IPSec dial-up

15.2.4 Configure IPsec action and proposal

The next step is to define the IPsec action and proposal. You should note that you do not know the tunnel endpoint, so 0.0.0.0 is entered as the destination tunnel endpoint.

```
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
    0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
Enter a Name (1-29 characters) for this IPsec Action []? ire
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
[192.168.102.1]? 192.168.212.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
[0.0.0.0]?
Percentage of SA lifesize/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]?
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 []? ire
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]: y
List of ESP Transforms:
    0: New Transform

Enter the Number of the ESP transform [0]? 0
Enter a Name (1-29 characters) for this IPsec Transform []? ire
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]? 2
```

Figure 357. Center router IPsec policy configuration for IPsec dial-up- part 1

```

List of IPsec Authentication Algorithms:
  0) None
  1) HMAC-MD5
  2) HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]?
List of ESP Cipher Algorithms:
  1) ESP DES
  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]?

Here is the IPsec transform you specified...

Transform Name = ire
      Type =ESP   Mode =Transport   LifeSize=   50000   LifeTime=   3600
      Auth =SHA   Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
  0: New Transform
  1: ire

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [No]:

Here is the IPsec proposal you specified...

Name = ire
      Pfs = N
      ESP Transforms:
          ire
Is this correct? [Yes]:
List of IPSEC Proposals:
  0: New Proposal
  1: ire

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPsec Action you specified...

IPSECAction Name = ire
      Tunnel Start:End      = 192.168.212.1 : 0.0.0.0
      Min Percent of SA Life = 75
      Refresh Threshold     = 85 %
      Autostart              = No
      DF Bit                 = COPY
      Replay Prevention      = Disabled
      IPSEC Proposals:
          ire
Is this correct? [Yes]:
IPSEC Actions:
  0: New IPSEC Action
  1: ire

Enter the Number of the IPSEC Action [1]?

```

Figure 358. Center router IPsec policy configuration for L2TP + IPsec - part 2

15.2.5 Configure ISAKMP action and proposal

Once the IPsec action and proposal has been fully defined the next step is to define the ISAKMP action and proposal. The main point in this step is that aggressive mode must be used because the IP address of the client will not be known. In main mode the IDs are exchanged in message 5 and 6. However, the keys must be known before then to encrypt message 5 and 6 themselves. In aggressive mode the IDs are exchanged at the beginning so the keys to be used can be determined at the beginning.

```
ISAKMP Actions:
  0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
Enter a Name (1-29 characters) for this ISAKMP Action []? ire

List of ISAKMP Exchange Modes:
  1) Main
  2) Aggressive

Enter Exchange Mode (1-2) [1]? 2
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, 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]:

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 []? ire

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]? 2

List of Cipher Algorithms:
  1) DES

Select the Cipher Algorithm (1-2) [1]?
Security Association Lifesize, in kilobytes (100-2147483647) [1000]?
Security Association Lifetime, in seconds (120-2147483647) [15000]?

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 359. Center router ISAKMP action configuration for IPsec dial-up - part 1

```

Here is the ISAKMP Proposal you specified...

Name = ire
  AuthMethod = Pre-Shared Key
  LifeSize   = 1000
  LifeTime   = 15000
  DHGroupID  = 1
  Hash Algo  = SHA
  Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
  0: New Proposal
  1: ire

Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

ISAKMP Name      = ire
  Mode            = Aggressive
  Min Percent of SA Life = 75
  Conn LifeSize:LifeTime = 5000 : 30000
  Autostart       = Yes
  ISAKMP Proposals:
    ire
Is this correct? [Yes]:
ISAKMP Actions:
  0: New ISAKMP Action
  1: ire

Enter the Number of the ISAKMP Action [1]?
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      = ire
  State:Priority =Enabled : 5
  Profile        =ire
  Valid Period   =always
  IPSEC Action   =ire
  ISAKMP Action  =ire
Is this correct? [Yes]:

```

Figure 360. Center router ISAKMP action configuration for IPSec dial-up - part 2

The last step of the policy definition is to enter the user as a fully qualified domain name (FQDN). This is the ID type that must be used because IP addresses are not known.


```

To authenticate the ISAKMP Peer with Pre-Shared Key a User
must be added. Add a USER now? [Yes]: y
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]? 2
Enter the FQDN to distinguish this user (No spaces allowed) []? wtr05999.itso.ral.ibm.com
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):
Enter the Pre-Shared Key again (8 characters) in ascii:

Here is the User Information you specified...

Name      = wtr05999.itso.ral.ibm.com
Type      = FQDN
Group     =
Auth Mode =Pre-Shared Key
Is this correct? [Yes]:

```

Figure 361. Center router ISAKMP ID configuration for IPSec dial-up

The FQDN configured in Figure 361 must match the FQDN that is specified at the client as described in 15.2.6.2, “Configure the SafeNet VPN Client” on page 450.

15.2.5.1 Add default route

These steps and the reasons for performing them are the same as described in 19.4.2.9, “Add default route and enable ARP subnet routing” on page 635 for the PPTP scenario.

15.2.6 Configuration of the IRE SafeNet VPN Client

Information Resource Engineering, Inc. (IRE) is a company that develops software for other vendors to include in their products. Cisco Systems, Inc., for example, has licensed SafeNet as its client solution for VPNs. IRE also distributes some of their products commercially. The generally available version of the IRE VPN client is called SafeNet. We used Version 2.0.7, build 18, of SafeNet for our interoperability scenarios. To find more information about SafeNet and how you can purchase it, please access the URL below:

<http://www.ire.com>

Details on how to install and configure the IRE client for a LAN VPN connection can be found in 19.1, “IRE SafeNet VPN client” on page 597.

For a dial-up connection, you have to perform the client configuration and also create a dial-up networking entry to connect to your ISP.

15.2.6.1 Configure a dial-up connection to the ISP

Before you can use the VPN client in this scenario, you have to create a dial-up networking configuration to access your ISP. The IPSec tunnel will be established over this connection so it needs to be defined first. Add a DUN client to the ISP by double-clicking **Make New Connection**. Specify user ID/password (wsdial/wsdial), keep the default device for your modem and click the **Next**

button. Enter the telephone number and click **Next**. The installation of the ISP connection is finished.

15.2.6.2 Configure the SafeNet VPN Client

Table 83 shows the parameters that will be configured on the Client. Unless otherwise stated, other values that are not covered in the table will remain as defaults:

Table 83. IRE SafeNet VPN client- host-to-gateway VPN connection IPsec parameters

| IPsec parameters and some pertinent information on the other party | | | | | | | | | | | | | |
|--|-------------------------|--------------------|--|--|--|---------------------|--|---|------------------|-----|---|----------------------|-----|
| Local | | | | | | | | | | | | | |
| IP Address | unknown (ISP-assigned) | | | | | | | | | | | | |
| Role | Initiator | | | | | | | | | | | | |
| Remote | | | | | | | | | | | | | |
| IP Address | 192.168.212.1 | | | | | | | | | | | | |
| Role | Responder | | | | | | | | | | | | |
| Key Management Tunnel (Phase 1) | | | | | | | | | | | | | |
| Mode | Aggressive | | | | | | | | | | | | |
| Encryption | DES | | | | | | | | | | | | |
| Authentication Algorithm | SHA | | | | | | | | | | | | |
| Key Exchange Group | 1 | | | | | | | | | | | | |
| Key Lifetime | 86400 sec (default) | | | | | | | | | | | | |
| Negotiation ID | Domain name | | | | | | | | | | | | |
| Pre-Shared Key | 1234567890 | | | | | | | | | | | | |
| Data Management Tunnel (Phase 2) | | | | | | | | | | | | | |
| Remote Host IP Address | 192.168.102.2 | | | | | | | | | | | | |
| Remote Host Subnet Mask | 255.255.255.255 | | | | | | | | | | | | |
| Port | * (all protocols/ports) | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th colspan="3">Security Protocols</th> </tr> </thead> <tbody> <tr> <td></td> <td>AH (Authentication)</td> <td></td> </tr> <tr> <td>✓</td> <td>ESP (Encryption)</td> <td>DES</td> </tr> <tr> <td>✓</td> <td>ESP (Authentication)</td> <td>SHA</td> </tr> </tbody> </table> | | Security Protocols | | | | AH (Authentication) | | ✓ | ESP (Encryption) | DES | ✓ | ESP (Authentication) | SHA |
| Security Protocols | | | | | | | | | | | | | |
| | AH (Authentication) | | | | | | | | | | | | |
| ✓ | ESP (Encryption) | DES | | | | | | | | | | | |
| ✓ | ESP (Authentication) | SHA | | | | | | | | | | | |
| Encapsulation Mode | Tunnel | | | | | | | | | | | | |
| Perfect Forward Secrecy (PFS) | No | | | | | | | | | | | | |
| SA Lifetime | 28800 sec (default) | | | | | | | | | | | | |

Follow the steps below to configure the IRE client for dial-up connections.

1. Create a new connection via **File -> New Connection**.
2. Check **Secure** to protect this connection with IPSec. Enter the remote parties IP address, which in our case is a single server behind the corporate VPN gateway. Check connect via security gateway and enter the appropriate IP address for that gateway. This means that the client is using IPSec tunnel mode to the VPN gateway and all traffic to the server in the corporate network flows through that tunnel across the Internet and in the clear inside the corporate network.
3. Expand all objects in the connection tree by clicking the (+) signs next to them, then click **Security Policy** and select **Aggressive Mode**. This triggers a wider choice of selections for the IKE Phase 1 identity.
4. Next, click **My Identity** and select **FQDN**. The client then pulls the configured host and domain name from the Windows Networking TCP/IP properties and inserts them into the configuration. You cannot change that field.

Reminder

IKE Phase 1 with pre-shared key authentication only allows an IP address as the peer ID. Since you are using pre-shared keys in this scenario but do not know your IP address in advance as it will be provided by the ISP, you must use aggressive mode and an ID different from the IP address. Because SafeNet can use certificates where the ID for Phase 1 will be whatever the certificate says, you first have to tell the client that you want to use aggressive mode or it will not let you choose anything other than IP address for My ID.

5. Select a dial-up interface or leave the selection as any. On Windows NT, you must have a dial-up connection established before it will appear in this list.
6. Enter the value for the pre-shared key.
7. Enter the transforms for the Phase 1 proposal. You can add multiple proposals if you wish.
8. Enter the transforms for the Phase 2 proposal. You can add multiple proposals if you wish.
9. Save the policy and then select **Reload Policy** from the task bar icon context menu.

15.2.7 Testing and verifying the connection

To establish an IPSec tunnel using the IRE SafeNet VPN client, you need to use one DUN session to connect to the Internet (in our case, to the ISP's router).

15.2.7.1 Dialing to ISP router

We launch the PPP dial-up connection, which establishes the Internet connection and log on with the user ID `wsdial`. Remember to stop the VPN client until the dial-up link is active.

The screen below shows the output from the `netstat -ra` command, which lists the IP routing table after dialing the ISP, and it also lists the active ports at the client showing UDP port 500 (sytek) active, which means IKE is ready.

```

=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 01 50 56 67 80 ..... Ashley Laurent Virtual Private Network
=====

Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.88.5    192.168.88.5    1
127.0.0.0                  255.0.0.0        127.0.0.1       127.0.0.1       1
192.168.88.0               255.255.255.0    192.168.88.5    192.168.88.5    1
192.168.88.5               255.255.255.255  127.0.0.1       127.0.0.1       1
192.168.88.255            255.255.255.255  192.168.88.5    192.168.88.5    1
224.0.0.0                  224.0.0.0        192.168.88.5    192.168.88.5    1
255.255.255.255           255.255.255.255  192.168.88.5    192.168.88.5    1
=====

Route Table

Active Connections

Proto Local Address          Foreign Address        State
TCP   vpnclient:135          0.0.0.0:0              LISTENING
TCP   vpnclient:135          0.0.0.0:0              LISTENING
TCP   vpnclient:500          0.0.0.0:0              LISTENING
TCP   vpnclient:1026         0.0.0.0:0              LISTENING
TCP   vpnclient:1025         0.0.0.0:0              LISTENING
TCP   vpnclient:1025         localhost:1026          ESTABLISHED
TCP   vpnclient:1026         localhost:1025          ESTABLISHED
UDP   vpnclient:135          *: *
UDP   vpnclient:sytek       *: *

```

Figure 362. IBM SecureWay VPN Client - list routes and active connections

15.2.7.2 Starting negotiation

Once the policy has been reloaded, the SafeNet VPN client is checking any outgoing packet to see if it matches a secure traffic profile. If it does, than IKE negotiations are started as defined in the security policy. If successful, matching traffic will be secured with IPSec as defined in the security policy.

Likewise, any incoming packet is checked to see if it matches a secure traffic profile. If it does, IPSec will be used as defined in the security policy, or, in case of IKE packets, appropriate IKE response messages will be sent to negotiate new SAs for that traffic. If successful, matching traffic will be secured with IPSec as defined in the security policy.

This is exactly the behavior described in 3.3.1, “Outbound IPSec processing for host systems” on page 69.

From the context menu, select **Log Viewer** to determine if everything goes as it should. To initiate IKE negotiations, simply access AIXSRV2 for which a security policy has been defined. Provided the partner is ready to respond, you see in the log that IKE main mode and quick mode are completed successfully and SAs are established to protect traffic with IPSec.

15.2.8 Using a private IP address with the IRE SafeNet VPN client

The SafeNet VPN client can optionally be configured to use a private IP address. This means that the client uses an IP address preassigned from a corporate

address pool. The ISP-assigned IP address will then only be used for the IPSec tunnel between the client and the corporate VPN gateway. The private IP address will be used for all data traffic between the client and the corporate network, which will be tunneled through the VPN connection.

The benefit of this feature is that a corporate firewall would no longer have to allow traffic from all IP addresses to pass but could restrict access to a subnet that is being used for remote clients. This feature also renders unnecessary service level agreements with ISPs assigning fixed IP addresses to corporate remote clients. However, no dynamic address assignment is provided by this feature as it would, for instance, with L2TP.

To enable this option, use the Security Policy Editor, click **Options -> Global Settings** and check **Allow to Specify Internal Network Address** (see Figure 363).

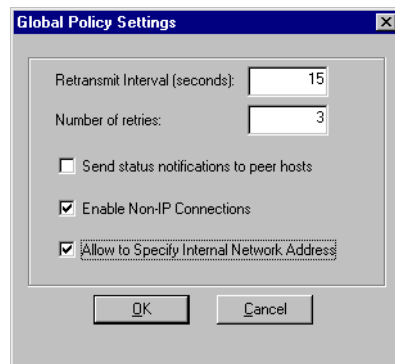


Figure 363. IRE SafeNet - enable private IP address

Once the private IP address option has been enabled, a field is added to the My Identity configuration window that allows you to enter that address, as shown in the example in Figure 364 on page 453.

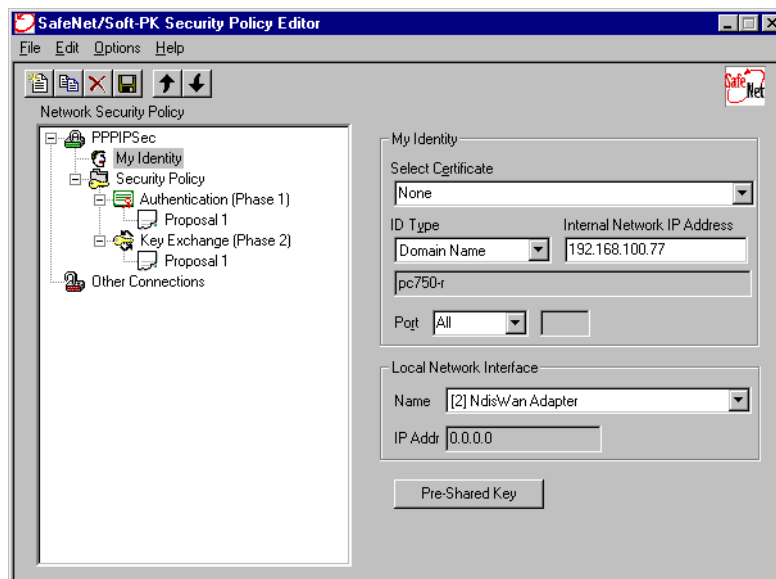


Figure 364. IRE SafeNet - use private IP address

Further configuration of the SafeNet VPN client and the VPN gateway is done in a way that resembles a branch office scenario, as shown in Figure 365.

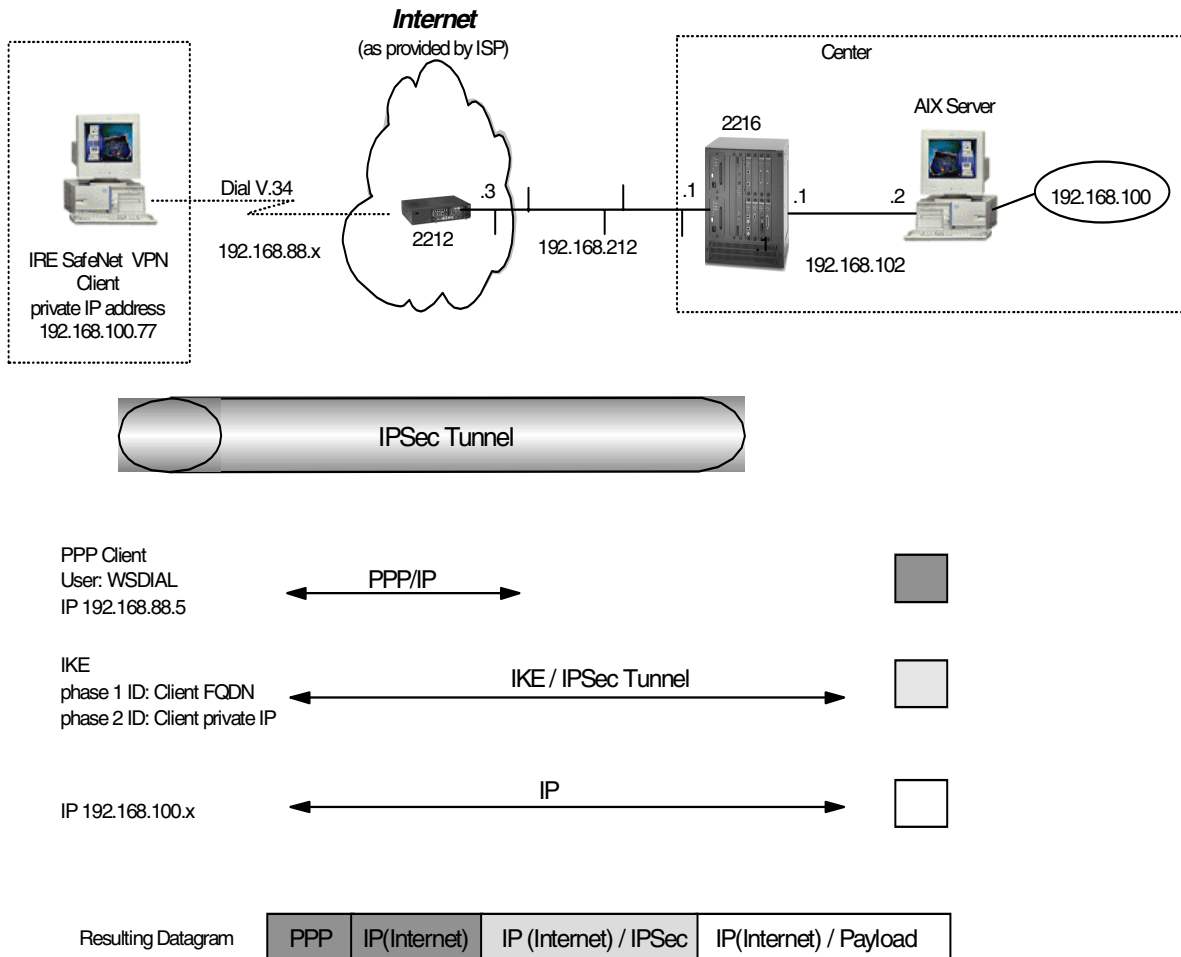


Figure 365. IRE SafeNet - private IP address scenario

15.3 End-to-end connections using L2TP and IPsec

Apart from using IKE and IPsec to establish a secure tunnel between a remote client and a corporate VPN gateway, you can use layer-2 tunneling protocols to extend PPP connections back to the corporate gateway and then protect this tunnel with IPsec.

We have included three such scenarios in this redbook, two for plain layer-2 tunneling (see 19.3, "Network TeleSystems TunnelBuilder" on page 618 and 18.4, "Windows 2000 remote access using L2TP" on page 583) and one for layer-2 tunneling with IPsec protection (see 19.2, "WinVPN client from Wind River Systems" on page 612).

15.4 Dial-on-Demand via ISP using L2TP

Apart from connecting remote users via dial-up connections across the Internet using either layer-2 tunneling techniques or IPsec or both combined, companies

may have a business requirement to connect branch offices via such a connection.

The business model for that scenario could be one where data transfer is only required at certain times of the day for synchronization, updates, maintenance, and similar purposes. For the remainder of the day, the branch office operates in offline mode. An example of this is a supermarket where cash registers are updated via a local server in the morning with the price and item lists for the day. The server receives that information during the night and feeds back all business transactions, accounting and store inventory data the following night.

Another business model is one where access to the central site is provided via a terminal gateway that initiates connections on-demand, and such requests are usually few during the day.

Having a permanent connection of any kind would be too costly in those environments, but occasional Internet access is affordable and a dial-up VPN connection is the solution to the problem.

Both models could also be extended to a hub-and-spoke network where intermittent dial-up connections between branch offices are provided via a central gateway, as illustrated in Figure 366.

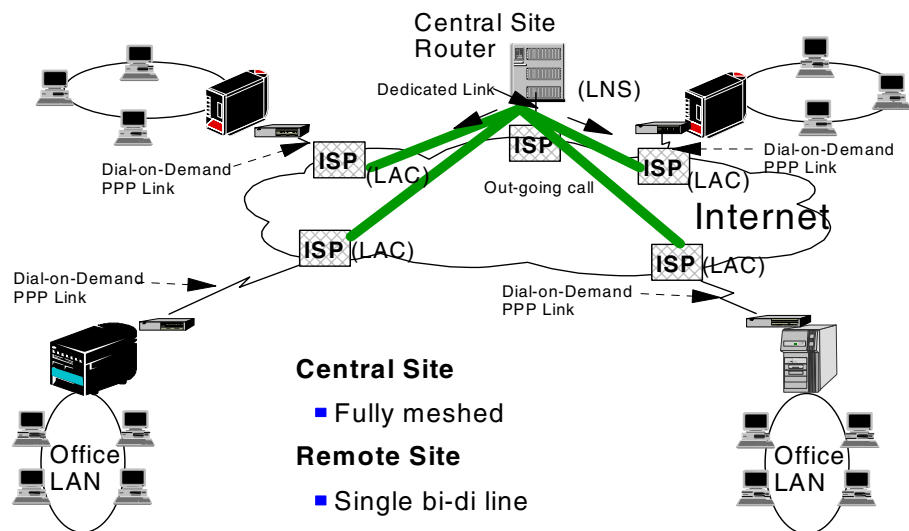


Figure 366. Dial-on-demand hub-and-spoke VPNs

Scenarios for both variants, the remote branch office access using voluntary layer-2 tunneling and the remote access using compulsory layer-2 tunneling which is required for hub-and-spoke connections, are illustrated in detail in *A Comprehensive Guide to Virtual Private Networks, Volume II*, SG24-5234-01.

Scenarios involving layer-2 tunneling VPNs with IBM AS/400 are described in the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

Chapter 16. VPN Troubleshooting

This chapter describes how to deal with problems in a VPN environment. Such problems can originate from configuration errors, network errors, program failures, or attacks. We first describe general troubleshooting facilities and concepts. Platform-specific troubleshooting examples are shown thereafter.

16.1 Log Files

The analysis of log files is the first step to identify problems and isolate possible cause. For VPNs, in general, two types of log files can be used:

1. IPsec daemon log file
2. Packet filter log file

The IP Security daemon consists of the IPsec daemon and the ISAKMP daemon. The IPsec daemon handles the IP Security protocol stack and the ISAKMP daemon handles IKE messages. But the name of the daemon and roles are different from platform to platform. The platform has a packet filtering capability and has a packet filter log file. The packet filter function is used in conjunction with the IP Security function and sometimes the packet filtering function may cause problem when the tunnel is established. So these daemon log files and packet filter log file must be investigated if there's trouble.

These log facilities provide log levels for focusing on the problem easily. Upon first investigation, the most robust log level (for example, debug) is preferred to get more detailed information. And you have to change the log level to a less detailed option and focus on the troublesome area if possible.

In normal conditions, it is desirable to set a minimum log level for periodic review to check the health of the daemon and attacks from outside.

16.2 Alerting and monitoring

Alerting is the auto-generated message when the error or warning condition occurs. This message will be forwarded to the system console or a responsible person. The alerting condition can be set and actions (for example, e-mail, console display) also can be set. Alerting is based on the monitoring of resources in network nodes.

16.3 Traces, dumps and traffic analysis

In this section we describe advanced methods of problem determination.

16.3.1 Traces and dumps

Tracing is a debug facility for tracing inside of code. The traces can be used to get more specific information about events or errors occurring in the communication stack or tunnel code. In general, the trace facility captures information on errors, filters, tunnels, capsulation/decapsulation, and crypto files. Comparing log files, the trace provides more detailed information for problem determination and may have an impact on system performance. The

tracing/dump information will also be required when speaking with an IBM technician.

16.3.2 Traffic analysis

To analyze the problem further or if the problem is not identified using logs, traffic analysis is needed. The network sniffing tools such as IBM DataGlance, Network Associates Sniffer, or Microsoft Network Monitor, are used to capture network traffic and analyze captured traffic. The commercial network sniffing tool can interpret traffic in network layers and fields in each layer. IKE is a newly adopted VPN standard and may not be interpreted in some sniffing tools.

In this section, we show practical sniffer traces between two hosts and explain successful IKE negotiations and some typical failed negotiation cases.

The IKE tunnel negotiation consists of two phases, key management tunnel (Phase 1) and data management tunnel (Phase 2).

In this explanation, Host-A (172.16.3.2) and Host-B (172.16.3.3) are used. Host-A activates a tunnel as an initiator and Host-B replies to this IKE negotiation. For this tunnel, the transport mode is used and main mode is used for Phase 1 negotiation and the preshared key is used for authentication. The configuration is shown in Figure 367.

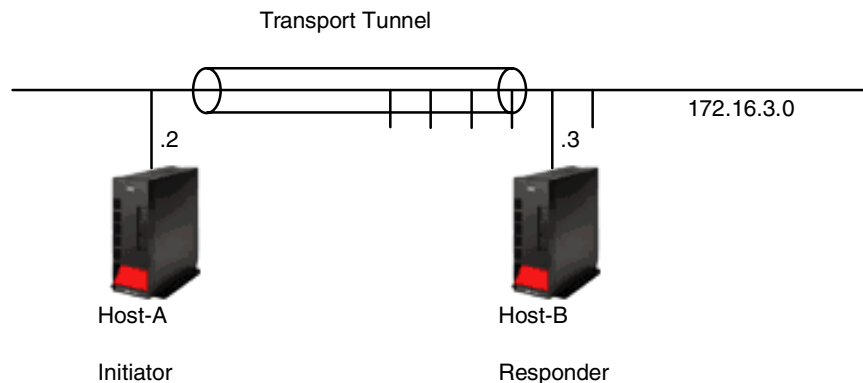


Figure 367. Tunnel Configuration

Table 84 shows the IKE parameters used in this trace.

Table 84. AIX - host-to-host VPN connection IPsec parameters

| IPSec parameters and some pertinent information on the other party | |
|--|------------|
| Local | |
| Hostname | Host-A |
| IP Address | 172.16.3.2 |
| Role | Initiator |
| Remote | |
| Hostname | Host-B |

| IPSec parameters and some pertinent information on the other party | | |
|--|----------------------|-----|
| 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 Life Time | 480 min (default) | |
| Negotiation ID | IP Address | |
| Preshared Key | 3132333435363738 | |
| Data Management Tunnel (Phase 2) | | |
| Security Protocols | | |
| | AH (Authentication) | |
| ✓ | ESP (Encryption) | DES |
| ✓ | ESP (Authentication) | MD5 |
| Encapsulation Mode | Transport | |
| Perfect Forward Secrecy (PFS) | No | |
| Tunnel Lifetime | 30 min | |
| SA Lifetime | 30 min (default) | |

Figure 368 shows Phase 1 negotiation traffic flow that uses main mode with the preshared key. Main mode consists of six messages for Phase 1. Figure 369 on page 460 shows Phase 2 quick mode negotiation traffic flow.

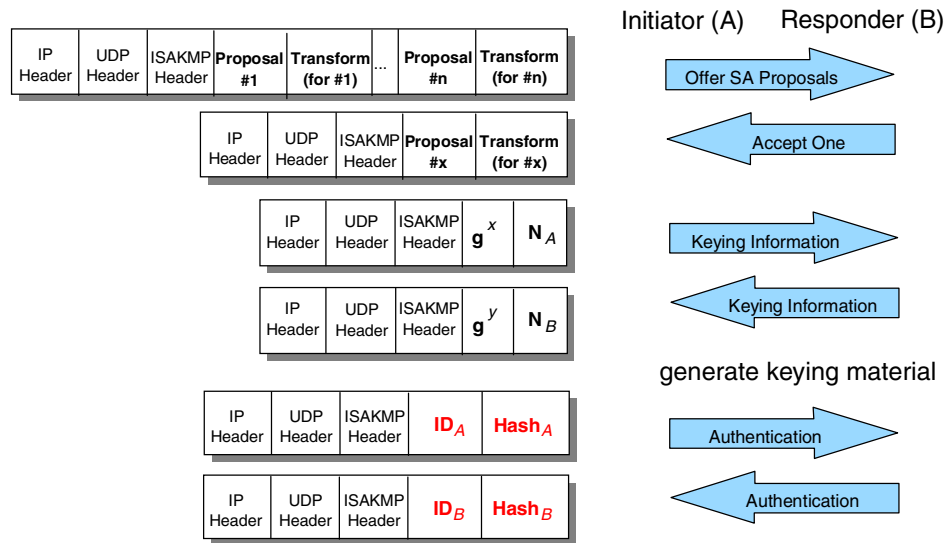


Figure 368. IKE Phase 1 message format - preshared key - main mode

The security associations that protect the ISAKMP messages themselves are set up during the Phase 1 exchanges. Since we are starting "cold" (no previous keys or SAs have been negotiated between Host-A and Host-B), the Phase 1 exchanges will use the ISAKMP Identity Protect exchange (also known as Oakley Main Mode). Six messages are needed to complete the exchange:

- Messages 1 and 2 negotiate the characteristics of the security associations. Messages 1 and 2 flow in the clear for the initial Phase 1 exchange, and they are unauthenticated.
- Messages 3 and 4 exchange nonces and also execute a Diffie-Hellman exchange to establish a master key (SKEYID). Messages 3 and 4 flow in the clear for the initial Phase 1 exchange, and they are unauthenticated.
- Messages 5 and 6 exchange digital signatures, and optionally the pertinent user-based certificates for the purpose of mutually authenticating the parties' identities. The payloads of messages 5 and 6 are protected by the encryption algorithm and keying material established with messages 1 through 4.

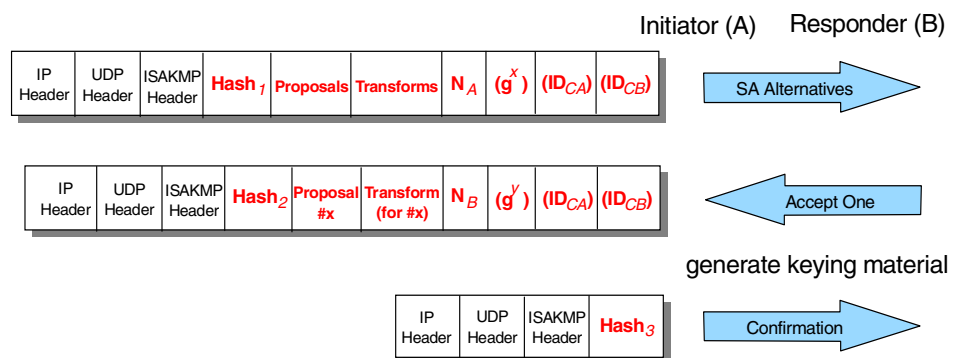


Figure 369. IKE Phase 2 quick mode message format

After having completed the Phase 1 negotiation process to set up the ISAKMP security associations, Host-A's next step is to initiate the ISAKMP/OAKLEY Phase 2 message exchanges (also known as Oakley Quick Mode) to define the security associations and keys that will be used to protect IP datagrams exchanged between the pair of users. Three messages are needed to complete the exchange:

- Message 1 of a quick mode exchange allows Host-A to authenticate itself, to select a nonce, to propose security association(s) to Host-B, to execute an exchange of public Diffie-Hellman values, and to indicate if it is acting on its own behalf or as a proxy negotiator for another entity.
- After Host-B receives message 1 from Host-A and successfully authenticates it using HASH_1, it constructs a reply, message 2, to be sent back to Host-A.
- At this point, Host-A and Host-B have exchanged all the information necessary for them to derive the necessary keying material. The third message in the quick mode exchange is used by Host-A to prove its liveness, which it does by producing a hash function that covers the message ID and both nonces that were exchanged in messages 1 and 2.

The summary traffic trace for IKE Phases 1 and 2 is shown below:

| Frame | Source Address | Dest. Address | Size | Summary |
|-------|----------------|---------------|------|--------------------------|
| 1 | [172.16.3.2] | [172.16.3.3] | 122 | UDP: D=500 S=500 LEN=88 |
| 2 | [172.16.3.3] | [172.16.3.2] | 122 | UDP: D=500 S=500 LEN=88 |
| 3 | [172.16.3.2] | [172.16.3.3] | 182 | UDP: D=500 S=500 LEN=148 |
| 4 | [172.16.3.3] | [172.16.3.2] | 182 | UDP: D=500 S=500 LEN=148 |
| 5 | [172.16.3.2] | [172.16.3.3] | 102 | UDP: D=500 S=500 LEN=68 |
| 6 | [172.16.3.3] | [172.16.3.2] | 102 | UDP: D=500 S=500 LEN=68 |
| 7 | [172.16.3.2] | [172.16.3.3] | 174 | UDP: D=500 S=500 LEN=140 |
| 8 | [172.16.3.3] | [172.16.3.2] | 174 | UDP: D=500 S=500 LEN=140 |
| 9 | [172.16.3.2] | [172.16.3.3] | 94 | UDP: D=500 S=500 LEN=60 |

Frames 1 to 6 show Phase 1 of the IKE main mode negotiation and frames 7 to 9 show Phase 2 of the IKE quick mode exchange.

The ISAKMP messages are sent using UDP. So there is no guaranteed delivery for them and there is a retransmission mechanism working when one party does not receive corresponding message from another party.

You can investigate a negotiation problem using a summary of IKE traffic. The typical symptom when the negotiation fails is that the length of each message is different. For example, if a preshared key does not match, messages 3 and 4 of Phase 1 have different lengths.

Next we will explain the ISAKMP header format used in the IKE tunnel negotiation before going through each IKE messages of Phases 1 and 2. The ISAKMP header format is shown in Figure 370.

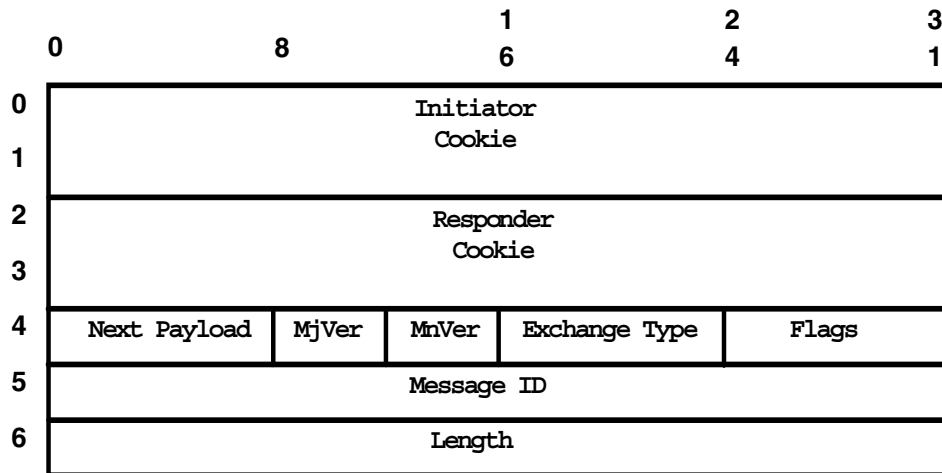


Figure 370. ISAKMP header format

An ISAKMP message has a fixed header format followed by a variable number of payloads.

- Initiator Cookie (8 octets) is the cookie of the entity that initiated an SA establishment, SA notification, or SA deletion.
- Responder Cookie (8 octets) is the cookie of the entity that is responding to an SA establishment request, SA notification, or SA deletion.
- Next Payload (1 octet) indicates the type of the first payload in the message.

| Next Payload Type | Value |
|---------------------------|-----------|
| NONE | 0 |
| Security Association (SA) | 1 |
| Proposal (P) | 2 |
| Transform (T) | 3 |
| Key Exchange (KE) | 4 |
| Identification (ID) | 5 |
| Certificate (CERT) | 6 |
| Certificate Request (CR) | 7 |
| Hash (HASH) | 8 |
| Signature (SIG) | 9 |
| Nonce (NONCE) | 10 |
| Notification (N) | 11 |
| Delete (D) | 12 |
| Vendor ID (VID) | 13 |
| RESERVED | 14 - 127 |
| Private USE | 128 - 255 |

- Major Version (4 bits) indicates the major version of the ISAKMP protocol in use. Implementations based on this version of the ISAKMP Internet-Draft *must* set the major version to 1.
- Minor Version (4 bits) indicates the minor version of the ISAKMP protocol in use. Implementations based on this version of the ISAKMP Internet-Draft *must* set the minor version to 0.
- Exchange Type (1 octet) indicates the type of exchange being used. This dictates the message and payload orderings in the ISAKMP exchanges:

| Exchange Type | Value |
|---------------------|-------|
| NONE | 0 |
| Base | 1 |
| Identity Protection | 2 |
| Authentication Only | 3 |
| Aggressive | 4 |
| Informational | 5 |

```

ISAKMP Future Use      6 - 31
DOI Specific Use       32 - 239
Private Use            240 - 255

```

- **Flags (1 octet)** indicates specific options that are set for the ISAKMP exchange. The flags listed below are specified in the ISAKMP DOI document.
 - **E(ncryption Bit) (1 bit)** - The bit position is bit 0 of the Flags field. If set (1), all payloads following the header are encrypted using the encryption algorithm identified in the ISAKMP SA.
 - **C(ommit Bit) (1 bit)** - The bit position is bit 1 of the Flags field. This bit is used to signal key exchange synchronization. It is used to ensure that encrypted material is not received prior to completion of the SA establishment.
 - **A(uthentication Only Bit) (1 bit)** - The bit position is bit 2 of the Flags field. This bit is intended for use with the Informational Exchange with a Notify payload and will allow the transmission of information with integrity checking, but no encryption (for example, "emergency mode").
- **Message ID (4 octets)** is the unique message identifier used to identify a protocol state during Phase 2 negotiations. During Phase 1 negotiations, the value *must* be set to 0.
- **Length (4 octets)** - Length of total message (header + payloads) in octets. Encryption can expand the size of an ISAKMP message.

For more information on ISAKMP header format, refer to RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP).

We will explain highlights in each frame.

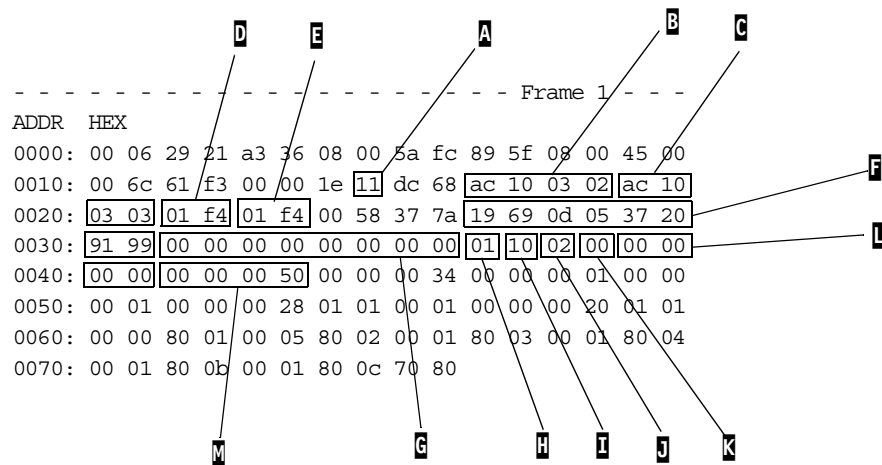


Figure 371. Message 1 of Phase 1

- A** - Upper layer protocol in IP header. Hex 11 (dec 17), UDP protocol, is used.
- B** - Source IP address. In this case, the IP address is 172.16.3.2
- C** - Destination IP address. In this case, the IP address is 172.16.3.3
- D** - Source port in UDP protocol. Hex 01 f4 (dec 500) is used for ISAKMP.
- E** - Destination port in UDP protocol. Hex 01 f4 (dec 500) is used for ISAKMP.

- F** - Initiator cookie.
- G** - Responder cookie. This field must be 0 in message 1 of Phase 1.
- H** - Next payload. This field must be 01, security association (SA), in message 1 and 2 of Phase 1.
- I** - Major version and minor version. The current implementation uses 10.
- J** - Exchange type. This field can be 02, identity protection, in messages 1 to 6 of Phase 1 when main mode is used.
- K** - Flag. This flag must be 00 in message 1 to 4 of Phase 1.
- L** - Message ID. This must be 0 in messages 1 to 6 of Phase 1. The only way to identify that an ISAKMP message is part of a Phase 1 flow rather than a Phase 2 flow is to check the Message ID field in the ISAKMP header. For Phase 1 flows, it must be 0, and for Phase 2 flows, it must be nonzero.
- M** - Length.

```

- - - - - Frame 2 - - -
ADDR  HEX
0000: 08 00 5a fc 89 5f 00 06 29 21 a3 36 08 00 45 00
0010: 00 6c d4 9e 00 00 1e 11 69 bd ac 10 03 03 ac 10
0020: 03 02 01 f4 01 f4 00 58 48 25 19 69 0d 05 37 20
0030: 91 99 9f 7d bc ce 48 fd 4a 0b 01 10 02 00 00 00
0040: 00 00 00 00 00 50 00 00 00 34 00 00 00 01 00 00
0050: 00 01 00 00 00 28 01 01 00 01 00 00 00 20 01 01
0060: 00 00 80 01 00 05 80 02 00 01 80 03 00 01 80 04
0070: 00 01 80 0b 00 01 80 0c 70 80

```

N

Figure 372. Message 2 of Phase 1

- N** - Responder cookie. This value is delivered from the responder.

```

- - - - - Frame 3 - - -
ADDR  HEX
0000: 00 06 29 21 a3 36 08 00 5a fc 89 5f 08 00 45 00
0010: 00 a8 61 f7 00 00 1e 11 dc 28 ac 10 03 02 ac 10
0020: 03 03 01 f4 01 f4 00 94 37 8c 19 69 0d 05 37 20
0030: 91 99 9f 7d bc ce 48 fd 4a 0b 04 10 02 00 00 00
0040: 00 00 00 00 00 8c 0a 00 00 64 4b f8 01 27 6c 30
0050: 1d 18 ff 5f 44 81 61 57 91 15 f2 b0 35 9e c5 2b
0060: 4c cd 45 55 9b fd 58 77 38 5b 5d 35 90 bb 73 0b
0070: 51 a7 c5 11 f5 33 b5 b6 22 b2 94 d2 0a 72 0d af
0080: ea c8 c4 fd f5 a8 4f 5c 2e 7d 1c ca 02 15 fa 31
0090: 66 24 51 d3 3d 04 41 dd 90 eb 5c 95 0c a4 34 b3
00a0: 4f a8 1a ea 92 9e 03 93 c0 86 00 00 00 0c d2 76
00b0: 92 86 e5 f4 1b f1

```

O

Figure 373. Message 3 of Phase 1

- O** - Next payload. This field must be 04, Key Exchange (KE), in messages 3 and 4 of Phase 1.


```

- - - - - Frame 4 - - -
ADDR  HEX
0000: 08 00 5a fc 89 5f 00 06 29 21 a3 36 08 00 45 00
0010: 00 a8 d4 9f 00 00 1e 11 69 80 ac 10 03 03 ac 10
0020: 03 02 01 f4 01 f4 00 94 24 cd 19 69 0d 05 37 20
0030: 91 99 9f 7d bc ce 48 fd 4a 0b 04 10 02 00 00 00
0040: 00 00 00 00 00 8c 0a 00 00 64 2f 4f de e5 80 d7
0050: 00 48 0d 4a 5f d5 ab 2f 6e f1 c2 24 67 e4 0c 97
0060: 1a 3a 92 15 15 e6 dd 85 7c 50 11 47 d1 43 87 50
0070: 76 f3 db 62 8e 26 73 38 63 0f f5 b5 f8 1f 3c 89
0080: 39 35 30 61 a0 c4 31 d0 ac bb 72 fe 19 93 43 d7
0090: 97 41 9f 3c d5 5e c7 a5 bf c2 91 94 cc 68 db be
00a0: 52 bb db 06 89 40 f9 57 f7 e4 00 00 00 0c 1f c7
00b0: 7f 9e 82 c6 83 64

```

Figure 374. Message 4 of Phase 1

```

- - - - - Frame 5 - - -
ADDR  HEX
0000: 00 06 29 21 a3 36 08 00 5a fc 89 5f 08 00 45 00
0010: 00 58 61 f8 00 00 1e 11 dc 77 ac 10 03 02 ac 10
0020: 03 03 01 f4 01 f4 00 44 f4 dd 19 69 0d 05 37 20
0030: 91 99 9f 7d bc ce 48 fd 4a 0b 05 10 02 01 00 00
0040: 00 00 00 00 00 3c 98 74 38 26 a2 40 fa 5d fd 2f
0050: e5 62 24 25 02 1c c0 aa 77 f4 a6 b9 4a 29 8b a6
0060: 5a aa 03 8b 39 45

```

P Q

Figure 375. Message 5 of Phase 1

- P** - Next payload. This field must be 05, Identification (ID), in messages 5 and 6 of Phase 1.
- Q** - Flag. This flag must be 01 in messages 5 and 6 of Phase 1 and messages 1 to 3 of Phase 2; 01 means the encryption bit is set to 1 and the message is encrypted.

```

- - - - - Frame 6 - - -
ADDR  HEX
0000: 08 00 5a fc 89 5f 00 06 29 21 a3 36 08 00 45 00
0010: 00 58 d4 a1 00 00 1e 11 69 ce ac 10 03 03 ac 10
0020: 03 02 01 f4 01 f4 00 44 a5 36 19 69 0d 05 37 20
0030: 91 99 9f 7d bc ce 48 fd 4a 0b 05 10 02 01 00 00
0040: 00 00 00 00 00 3c 42 f4 35 1a fe 12 84 1e a0 1d
0050: 86 9e dc 53 29 34 40 7e b5 76 57 72 52 80 c7 24
0060: c7 94 b3 49 09 e9

```

Figure 376. Message 6 of Phase 1

```

- - - - - Frame 7 - - -
ADDR  HEX
0000: 00 06 29 21 a3 36 08 00 5a fc 89 5f 08 00 45 00
0010: 00 a0 62 09 00 00 1e 11 dc 1e ac 10 03 02 ac 10
0020: 03 03 01 f4 01 f4 00 8c a8 5f 19 69 0d 05 37 20
0030: 91 99 9f 7d bc ce 48 fd 4a 0b 08 10 20 01 fb 4a
0040: 87 7f 00 00 00 84 75 61 21 e8 fd dc d8 ed bc 2f
0050: 9d bf be 18 fc 26 23 cc 86 14 95 99 f5 d6 b7 5c
0060: 44 c2 07 20 48 c3 25 65 04 9c a7 14 8a 1d 30 fb
0070: d5 8f 7f ce ca 79 b9 23 0a 01 9b 2d 79 fc 52 44
0080: 9d 53 98 b4 78 71 84 7e b5 0a 32 d2 31 f2 f4 f0
0090: 37 80 3d 03 d8 be 58 d5 20 22 39 17 87 53 f0 bf
00a0: 6f 12 8a 2d f2 23 81 fa 5d 03 70 40 9c 9c

```

Figure 377. Message 1 of Phase 2

- R** - Next payload. This field must be 08, Hash (HASH), in messages 1 to 3 of Phase 2.
- S** - Exchange type. This field can be Hex 20 (dec 32), DOI specific use, in messages 1 to 3 of Phase 2.
- I** - Message ID. This must be nonzero in messages 1 to 3 of Phase 2.

```

- - - - - Frame 8 - - -
ADDR  HEX
0000: 08 00 5a fc 89 5f 00 06 29 21 a3 36 08 00 45 00
0010: 00 a0 d4 b4 00 00 1e 11 69 73 ac 10 03 03 ac 10
0020: 03 02 01 f4 01 f4 00 8c a8 11 19 69 0d 05 37 20
0030: 91 99 9f 7d bc ce 48 fd 4a 0b 08 10 20 01 fb 4a
0040: 87 7f 00 00 00 84 07 b0 7e d0 10 e5 f6 04 e3 ab
0050: 46 e6 76 1e 2c e7 df 36 48 44 30 b4 0d 7d 00 8b
0060: 57 e3 79 b5 20 1e a2 b6 69 6f 78 95 ee 3f 4d 04
0070: 24 a3 a2 33 e0 1c fb 9d a9 fd 8b d3 ce 18 86 d2
0080: d5 e4 0a 57 fb 6f 1b 7e 1a 57 7c 00 25 d6 e9 97
0090: 80 00 0f 55 c7 9b 51 e9 ae 2a 22 aa ce 82 6d 3a
00a0: 6c 4d dc f3 b6 36 7b ed d4 0d f3 23 35 a8

```

Figure 378. Message 2 of Phase 2

```

- - - - - Frame 9 - - -
ADDR  HEX
0000: 00 06 29 21 a3 36 08 00 5a fc 89 5f 08 00 45 00
0010: 00 50 62 0c 00 00 1e 11 dc 6b ac 10 03 02 ac 10
0020: 03 03 01 f4 01 f4 00 3c c6 c7 19 69 0d 05 37 20
0030: 91 99 9f 7d bc ce 48 fd 4a 0b 08 10 20 01 fb 4a
0040: 87 7f 00 00 00 34 ab 84 62 cc ef 46 e9 03 7d cd
0050: 1f 5b d2 8b ed c7 a8 28 c5 3e 16 70 85 24

```

Figure 379. Message 3 of Phase 2

After successful tunnel creation, the data transferred between two hosts flows through the established tunnel and data is encrypted. The following is a summary of ping traffic in ESP mode:

| Frame | Source Address | Dest. Address | Size | Summary |
|-------|-----------------|-----------------|------|--------------------------|
| 1 | [172.16.3.7] | [192.168.100.7] | 110 | IPv4: ESP SPI=2538192414 |
| 2 | [192.168.100.7] | [172.16.3.7] | 110 | IPv4: ESP SPI=1590842174 |
| 3 | [172.16.3.7] | [192.168.100.7] | 110 | IPv4: ESP SPI=2538192414 |
| 4 | [192.168.100.7] | [172.16.3.7] | 110 | IPv4: ESP SPI=1590842174 |

The traffic is interpreted as ESP and SPIs are displayed. You can examine if the traffic is authenticated or encrypted using the sniffer trace file.

A negotiation failure case is shown below:

| Frame | Source Address | Dest. Address | Size | Summary |
|-------|----------------|---------------|------|--------------------------|
| 7 | [172.16.3.2] | [172.16.3.3] | 174 | UDP: D=500 S=500 LEN=140 |
| 8 | [172.16.3.3] | [172.16.3.2] | 110 | UDP: D=500 S=500 LEN=76 |

The Phase 1 negotiation is successful, but in Phase 2, message 1 is sent and message 2 is received with different lengths. The detailed messages are shown in Figure 380:

```

- - - - - Frame 8 - - -
ADDR  HEX
0000: 08 00 5a fc 89 5f 00 06 29 21 a3 36 08 00 45 00
0010: 00 60 ce a1 00 00 1e 11 6f c6 ac 10 03 03 ac 10
0020: 03 02 01 f4 01 f4 00 4c b5 d2 20 a6 dc ae 7a c0
0030: aa 35 6c 04 53 00 78 a4 22 34 08 10 05 01 13 fd
0040: db ac 00 00 00 44 e7 6a 38 40 20 de b1 6b 8c d2
0050: 55 5c 63 de 63 2e 13 1d 51 bb 21 68 d9 96 53 52
0060: a9 88 cb b6 4a f3 c9 17 2b f4 87 7a e3 3a

```

Figure 380. Message with informational exchange type

A: Exchange type. This field has 05, Informational, in message 2 of Phase 2. In this case, the responder sent an informational packet instead of a corresponding reply because the responder cannot decrypt the initiator’s message.

16.4 Interfaces to systems management tools

The SNMP is the simplest way to interface with a system management tool. Before investigating log files, traces, or dumps, the SNMP MIB values tell much to the troubleshooter, such as configuration or status. The SNMP traps can be used for troubleshooting in a timely manner. Some informative SNMP traps may be sent from a network device before a critical error occurs and the troubleshooter can use this information as a complement when he or she investigates the log file or trace. For more information on the SNMP trap or network management system (SNMP manager), see Chapter 7, “Network management for VPNs” on page 109.

16.5 Ethical Hacking

Ethical hacking occurs when a real hacker’s attacks are simulated in a controlled manner under an agreement with target organizations. This approach can help organizations recognize their potential security risk in their network and data and fix their problems before experiencing service disruption, loss of confidential information, or vandalism. In general, the ethical hacking services provide:

Network design review

The network design is reviewed from a security viewpoint and is verified if a network complies with the security policy.

Intrusion test

The intrusion test is performed on the network and data system from multiple locations outside and inside.

Reporting

Report includes test results, strengths and weaknesses, and recommendations.

From the Internet VPN viewpoint, IP Security consists of three protocols: AH, ESP, and IKE. IP Security provides the following security functions to protect data transmitted through Internet from others:

- Authentication
- Encryption
- Data integrity
- Replay protection

These security functions prevent some typical hacking threats listed below:

- IP spoofing attack
- Sniffing attack
- Resource-clogging attack
- Connection hijacking

IP Security still has potential risks and may be vulnerable to other types of hacking, for example, denial of services. The system security on the VPN host must be considered as part of network security.

In addition to IP network ethical hacking, some VPN unique threats must be considered in ethical hacking:

- Secure key distribution
- Strength of algorithm
- Validity of security policy

16.6 Troubleshooting for AIX 4.3.x

This section describes the troubleshooting method for VPN features in AIX 4.3.X.

16.6.1 IP Security log file

This section describes the configuration and format of the system log relating to IPSec IKE. As hosts communicate with each other to establish a tunnel, the system log daemon, syslogd, logs important messages about IPSec IKE. An administrator may choose to monitor this logging information for debugging assistance. The first step for setting up the logging facility is to modify the `/etc/syslog.conf` file and add the following entry:

```
local4.debug /var/adm/ipsec.log
```

Of course you can choose any other location on your disk. We recommend that you create a new file system (for instance, /var/log) and put the file there.

Note

The logging of filter events can create significant activity at the IPSec host and can consume large amounts of storage.

Use the local4 facility to record IPSec IKE events. Standard AIX priority levels apply. We recommend setting the priority level of debug until traffic through the IPSec tunnels and filters shows stability and proper movement.

Once you have added the entry, save /etc/syslog.conf, go to the directory you specified for the log file and create an empty file with the same name. In the case above, you would change to the /var/adm directory and issue the command:

```
touch ipsec.log
```

After these two steps have been completed, issue a refresh command to the syslogd subsystem:

```
refresh -s syslogd
```

Below is a sample log file containing IKE log entries:

1. Jun 21 21:30:30 AIXSRV1 : mkfilt: Filter rules updated at 21:30:30 on 06/21/99
2. Jun 21 21:30:30 AIXSRV1 : mkfilt: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 all any 0 any 0 both both l=n f=y t=0
3. Jun 21 21:30:30 AIXSRV1 : mkfilt: Filter rules updated at 21:30:30 on 06/21/99
4. Jun 21 21:30:30 AIXSRV1 : mkfilt: #:1 permit :: 0 :: 0 all any 0 any 0 both both l=n f=y t=0
5. Jun 21 21:12:24 AIXSRV1 Tunnel Manager: 0: TM is processing a List_tunnels_msg
6. Jun 21 21:13:39 AIXSRV1 Tunnel Manager: 0: TM is processing a Connection_request_msg
7. Jun 21 21:13:39 AIXSRV1 Tunnel Manager: 2: Creating new P1 tunnel object (tid)
8. Jun 21 21:13:39 AIXSRV1 Tunnel Manager: 2: TM is processing a P1_sa_created_msg (tid)
9. Jun 21 21:13:39 AIXSRV1 Tunnel Manager: 2: Received good P1 SA, updating P1 tunnel (tid)
10. Jun 21 21:13:39 AIXSRV1 Tunnel Manager: 0: Checking to see if any P2 tunnels need to start
11. Jun 21 21:14:03 AIXSRV1 Tunnel Manager: 0: TM is processing a Connection_request_msg
12. Jun 21 21:14:03 AIXSRV1 Tunnel Manager: 0: Received a connection object for an active P1 tunnel
13. Jun 21 21:14:03 AIXSRV1 Tunnel Manager: 3: Created blank P2 tunnel (tid)
14. Jun 21 21:14:03 AIXSRV1 Tunnel Manager: 0: Checking to see if any P2 tunnels need to start
15. Jun 21 21:14:03 AIXSRV1 Tunnel Manager: 3: Starting negotiations for P2 (P2 tid)
16. Jun 21 21:14:03 AIXSRV1 Tunnel Manager: 0: TM is processing a P2_sa_created_msg
17. Jun 21 21:14:03 AIXSRV1 Tunnel Manager: 3: received p2_sa_created for an existing tunnel as initiator (tid)

```

18.Jun 21 21:14:03 AIXSRV1 Tunnel Manager: 3: Filter::AddFilterRules: Created
   filter rules for tunnel
19.Jun 21 21:26:38 AIXSRV1 Tunnel Manager: 3: TM is processing a
   P2_remove_tunnel_msg (tid)
20.Jun 21 21:26:38 AIXSRV1 Tunnel Manager: 3: Removed P2 tunnel from collection
   (tid)
21.Jun 21 21:26:41 AIXSRV1 Tunnel Manager: 0: TM is processing a
   List_tunnels_msg
22.Jun 21 21:26:43 AIXSRV1 Tunnel Manager: 0: TM is processing a
   List_tunnels_msg
23.Jun 21 21:27:29 AIXSRV1 Tunnel Manager: 2: TM is processing a
   P1_remove_tunnel_msg (tid)
24.Jun 21 21:27:29 AIXSRV1 Tunnel Manager: 2: Removed P1 tunnel from collection
   (tid)
25.Jun 21 21:27:32 AIXSRV1 Tunnel Manager: 0: TM is processing a
   List_tunnels_msg
26.Jun 21 21:29:12 AIXSRV1 rmtun: Session key engine shut down
27.Jun 21 21:29:13 AIXSRV1 rmtun: Recv'd indication to remove all tunnels
28.Jun 21 21:29:13 AIXSRV1 : mkfilt: Filter rules updated at 21:29:13 on
   06/21/99
29.Jun 21 21:29:13 AIXSRV1 : mkfilt: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   all any 0 any 0 both both l=n f=y t=0
30.Jun 21 21:29:13 AIXSRV1 rmtun: Recv'd indication to remove all tunnels
31.Jun 21 21:29:13 AIXSRV1 : mkfilt: Filter rules updated at 21:29:13 on
   06/21/99
32.Jun 21 21:29:13 AIXSRV1 : mkfilt: #:1 permit :: 0 :: 0 all any 0 any 0 both
   both l=n f=y t=0
33.Jun 21 21:29:14 AIXSRV1 Tunnel Manager: 0: Error with socket connection
   MSG_PEEK
34.Jun 21 20:30:47 AIXSRV1 Tunnel Manager: 0: TM is processing a
   List_tunnels_msg

```

Followings are explanations to the points illustrated above:

- 1 - 4: The IP Security daemon is activated.
- 5 - 10: The key management tunnel is activated and is established successfully.
- 11 - 18: The data management tunnel is activated and is established successfully.
- 19 - 21: The data management tunnel is deactivated and is released successfully.
- 22 - 25: The key management tunnel is deactivated and is released successfully.
- 26 - 33: The IP Security daemon is deactivated.
- 34: The IKE tunnel monitor queries tunnel status.

The log entries explained above can be seen if the system acts as an IPSec IKE initiator. That means this system activates the key management tunnel and data management tunnel.

As a responder, the system waits for the creation and/or release tunnel request from the opposite system. In this case, the log entries are different from the initiator case.

Below is a sample log for IKE as the responder:

1. Jun 21 22:34:34 AIXSRV1 Tunnel Manager: 0: TM is processing a P1_sa_created_msg (tid)
2. Jun 21 22:34:34 AIXSRV1 Tunnel Manager: 0: Received P1 SA as a responder
3. Jun 21 22:34:34 AIXSRV1 Tunnel Manager: 0: Received P1 SA -- Creating new tunnel
4. Jun 21 22:36:16 AIXSRV1 Tunnel Manager: 0: TM is processing a P2_sa_created_msg
5. Jun 21 22:36:16 AIXSRV1 Tunnel Manager: 0: received p2_sa_created with us being a responder
6. Jun 21 22:36:16 AIXSRV1 Tunnel Manager: 0: Writing filter rules
7. Jun 21 22:36:16 AIXSRV1 Tunnel Manager: 1: Filter::AddFilterRules: Created filter rules for tunnel
8. Jun 21 22:38:03 AIXSRV1 Tunnel Manager: 0: TM is processing a P2_sa_removed_msg
9. Jun 21 22:39:39 AIXSRV1 Tunnel Manager: 0: TM is processing a P1_sa_removed_msg

Following are explanations to points illustrated above:

- 1 - 3: The system receives the key management tunnel creation request.
- 4 - 7: The system receives the data management tunnel creation request.
- 8: The system receives the data management tunnel release request.
- 9: The system receives the key management tunnel release request.

Note

IKE log entries as a responder provide very limited information, so using the IKE log file on the initiator side is better to debug a problem effectively. For further investigation, the network sniffing tool can be used together.

16.6.2 ISAKMPD log file

The IKE tunnels are set up by the communication of the `ike` command or VPN Web-based System Manager panels with two daemons: the tunnel manager daemon, `tmd` and the ISAKMP daemon `isakmpd`. For IKE tunnels to be set up, both of these daemons must be running. If IP Security is set up to start on reboot, these daemons will be started automatically. Otherwise, they can be started manually.

The tunnel manager gives requests to the `isakmpd` to start a tunnel. If the tunnel already exists or is not a valid tunnel (invalid remote address, for instance), it will report an error. If a negotiation is started, it may take some time (depending on network latency) for the negotiation to complete. The `ike` command can be used to list the state of the tunnel to determine if the negotiation was successful. The tunnel manager logs events to `syslogd` to debug, event and information levels that can be monitored to track the progress of the negotiation. The sequence will be:

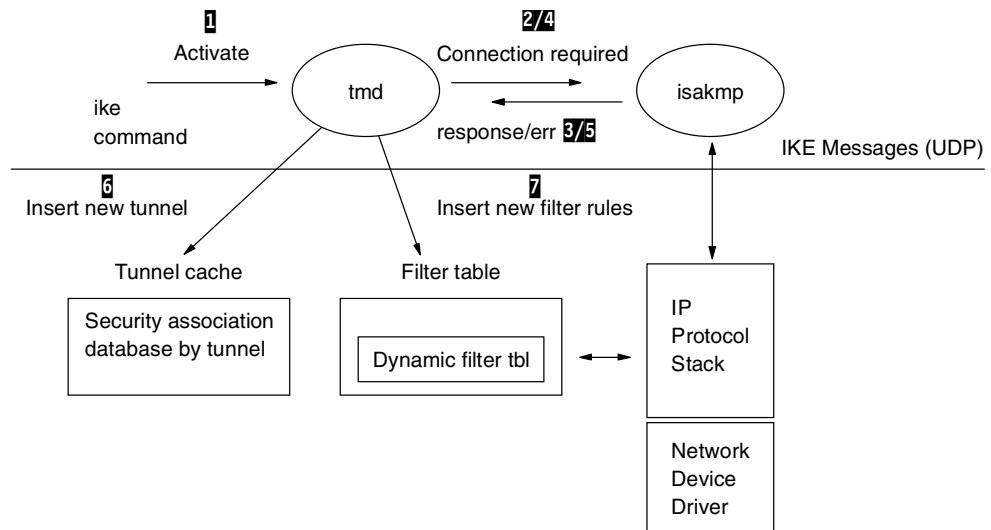


Figure 381. Process flow of initiating an IKE tunnel

1. Use the GUI or the `ike` command to initiate a tunnel.
2. The `tmd` daemon gives `isakmpd` a connection request for key management (Phase 1).
3. The `isakmpd` daemon responds with an SA created or an error.
4. The `tmd` daemon gives `isakmpd` a connection request for a data management tunnel (Phase 2).
5. The `isakmpd` daemon responds with an SA created or an error.
6. Tunnel parameters are inserted into the kernel tunnel cache.
7. Filter rules are added to the kernel dynamic filter table.

In the case where the machine is acting as a responder, the `isakmpd` daemon will notify the tunnel manager daemon `tmd` that a tunnel has been successfully negotiated and a new tunnel will be inserted into the kernel. Therefore, the process will start with step 3, and continue until step 7 without the `tmd` issuing connection requests.

The `isakmpd` logs to a separate log because of the number and size of logging messages. The logging can be enabled by the `ike` command by issuing:

```
ike cmd=log
```

The configuration file `/etc/isakmpd.conf` can be set up to specify the output files for each logging level. Levels may be set to none, errors, events, and information.

The `isakmpd` daemon code will either initiate or respond by sending or evaluating a proposal. If the proposal is accepted, a Security Association will be created and the tunnel will be set up. If the proposal is not accepted or the connection times out before the negotiation completes, the daemon will indicate an error. The entries in `syslog` from the `tmd` will indicate if the negotiation succeeded or not. To find out the exact cause of a failed negotiation, the `isakmpd` log needs to be checked.

16.7 Troubleshooting for OS/400

In this chapter we discuss the steps to efficiently diagnose problems that may occur during the initial configuration of dynamic tunnels. Also discussed is the steps required in Phase 1 and Phase 2 to initiate a virtual private network tunnel.

For more detail information, please refer to the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

16.7.1 Available methods for troubleshooting virtual private networks

When you create a virtual private networks (VPN) connection through the wizard, you configure a minimum number of parameters. This allows little space to make mistakes. However, you may need to change a parameter at a later time. For example, let's say that the remote connection or data endpoint is not an AS/400 system, or perhaps you need to change authentication algorithms. Before you change any configuration properties, you must be aware that there are many parameters that might cause problems if you configure them incorrectly.

In addition to the traditional methods of problem isolation, AS/400 offers a new approach by using AS/400 Operations Navigator. This task covers the most important sources for VPN troubleshooting information. These are:

- Job logs
- Journals
- The Active Connections window
- Communication trace
- Trace TCP Application

16.7.2 General guidelines for VPN troubleshooting

There are several ways to begin your problem analysis procedure. This list gives you some rules on how to start VPN troubleshooting:

- Obtain any error messages found in the Active Connections window or in the VPN server job logs for both the local and remote systems. Most of the time you will find a good explanation of why the connection failed.
- If the error messages you find do not provide enough information to solve the problem, check the IP filter and VPN journals.
- The communication trace on the AS/400 system offers you a third chance to find general information about whether the local system receives or sends connection requests.
- The Trace TCP Application (`TRCTCPAPP`) command provides yet another way to isolate problems.

If you set up a connection and you are not sure where in the network the error has occurred, reduce the complexity of your environment. For example, instead of investigating all parts of a VPN connection at the same time, just start with the IP connection itself. The following list gives you some basic guidelines on how to start VPN problem analysis, from the simplest IP connection to the more complex VPN connection:

1. Start with an IP configuration between the local and remote host. Does the connection work between those two systems?
 - Yes Go to step 2.
 - No Verify your IP configuration, interface status, and routing entries. Verify that IP filter rules have not been loaded. If the configuration is correct and filters have not been loaded, use a communication trace to check, for example, that a PING request leaves the system. If you send a PING request but you receive no response, the problem is within the network or remote system.

2. Set up the filter rules for VPN and activate the filters. Does filtering start successfully?
 - Yes Go to step 3.
 - No Check for error messages in the IP Packet Security window. Ensure that the filter rules do not specify native network address translation (NAT) for any VPN traffic.

3. Start your VPN connection. Does the connection start successfully?
 - Yes Go to step 4.
 - No Check the Active Connections window, QTOVMAN and QTOKVPNIKE jo logs as well as VPN journals for errors.

When using VPN, the Internet service provider (ISP) and every security gateway in your network must support the Authentication Header (AH) and Encapsulated Security Payload (ESP) protocols. Whether you enable AH or ESP depends on the proposals you define for your VPN connection.

Ensure you defined the proper filter rules for Internet Key Exchange (IKE) on port 500.

Check that the proper connection group is selected in the IPsec filter rule.

4. Are you able to activate a user session over the VPN connection?
 - Yes The VPN connections work as desired.
 - No Check the IP filter rules and the VPN connections groups for filter definitions that do not allow the desired user traffic. Also verify that the IPsec filter rule is loaded below the IP filter rules that allow IKE on port 500.

16.7.3 Using and customizing the Active Connections window

The Active Connections window should always be the entry point for VPN troubleshooting. It gives you various kinds of information according to the options set for active connections and connections in error. By default, the Active Connections window displays basic information that tells you what connection is running and which connection is in error. The Active Connections window does not list stopped connections.

The Active Connections window is a function included in the Virtual Private Networking option of AS/400 Operations Navigator.

The Active Connections window opens and displays the running connections and the connections in error. Figure 382 shows an example of the Active Connections window with the default settings applied.

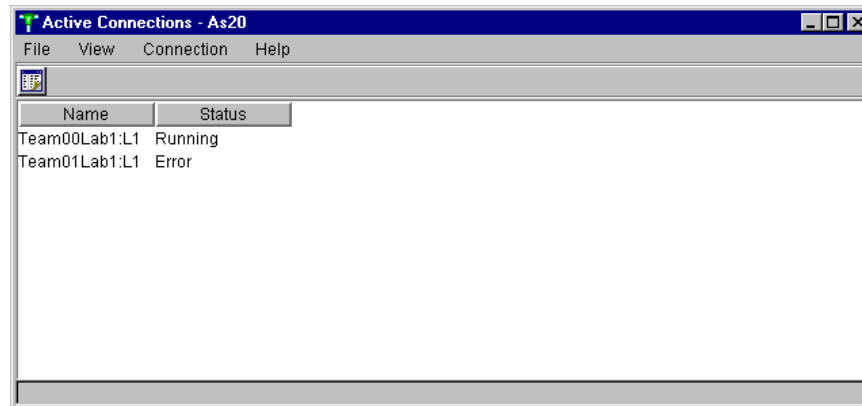


Figure 382. AS/400 - Active connections window

The customizing is performed through the Preferences option of the Active Connections window. You can add various fields to the window in any order. The useful fields are listed below:

- Error Information
- Failed Security Association
- Local Key Server IP Address
- Remote Key Server IP Address
- Local Data Addresses
- Remote Data Addresses

You will see information about each of these fields for each connection as shown in Figure 383.

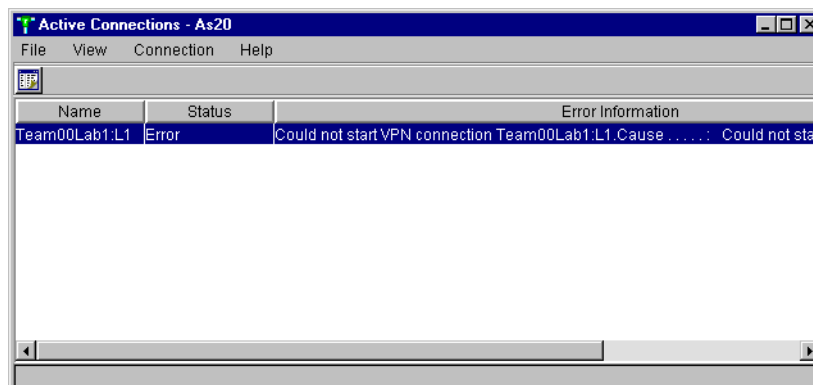


Figure 383. Active Sessions window - error information

Other columns may also be useful to add, depending on the information you want to see or the information you need to isolate a problem. For example, if you define several proposals within one data policy and you don't know which

proposal is actually taken, add the following columns to the Active Connections window:

- Security Protocol
- ESP Authentication
- ESP Encryption
- AH Authentication
- Encapsulation

These columns should allow you to determine which proposal was chosen from the data policy.

16.7.4 Using the QIPFILTER journal

The QIPFILTER journal is located in the QUSRSYS library and contains information about the 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.

16.7.4.1 Enabling the IP Packet Filter journal

Use the IP Packet Security option of AS/400 Operations Navigator to activate the IP Packet Filter journal. You have to enable the logging function for each individual filter rule. There is no function that allows logging for all IP datagrams going into or out of the system.

To enable the IP Packet Filter journal, select the filter rule you want to log and set the journaling option to FULL.

Note

To enable the IP Packet Filter journal, your filters must be deactivated.

If an IP datagram matches the definitions of the changed filter rule, an entry is made into the QIPFILTER journal.

16.7.4.2 Using the IP Packet Filter journal

AS/400 automatically creates the 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 or you can use an outfile.

Figure 384 and Figure 385 are examples from the QIPFILTER journal, that show an IKE request packet being denied.

By copying the journal entries to the 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 outfiles.

The following is an example of the Display Journal (DSPJRN) command:

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTYP((TF)) OUTPUT(*OUTFILE)
OUTFILEMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Use the following steps to copy the IP Packet Filter journal entries to the outfile:

1. Create a copy of the system-supplied outfile QSYS/QATOFIPF into a user library by using the Create Duplicate Object (CRTDUPOBJ) command. The following is an example of 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.

If you copy the DSPJRN into a nonexistent outfile, the system creates a file for you, but this file does not contain the proper field descriptions.

| 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 | | | QTOFJRN | 15:49:58 |
| | 6300 | M | TF | | | QTOFJRN | 15:50:05 |
| | 6301 | M | TF | | | QTOFJRN | 15:50:10 |
| | 6302 | M | TF | | | QTOFJRN | 15:50:12 |
| | 6303 | M | TF | | | QTOFJRN | 15:50:20 |
| | 6304 | M | TF | | | QTOFJRN | 15:50:37 |
| | 6305 | M | TF | | | QTOFJRN | 15:55:12 |
| | 6306 | M | TF | | | QTOFJRN | 15:55:45 |
| | 6307 | M | TF | | | QTOFJRN | 15:56:03 |
| | 6308 | M | TF | | | QTOFJRN | 15:56:03 |
| | 6309 | M | TF | | | QTOFJRN | 15:56:04 |
| | 6310 | M | TF | | | QTOFJRN | 15:56:04 |
| F3=Exit F12=Cancel | | | | | | | |

Figure 384. 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 385. Displaying the QIPFILTER journal - entry specific data

Note

The QIPFILTER journal only contains permit or deny entries for filter rules where the journaling option is set to FULL. For example, if you set up only PERMIT filter rules, IP datagrams that are not explicitly permitted are denied. For those denied datagrams, no entry is added to the journal. For problem analysis you might add a filter rule, which explicitly denies all other traffic and performs FULL journaling. Then, you'll get DENY entries in the journal for all IP datagrams that are denied. Due to performance issues, we do not recommend that you enable journaling for all filter rules. Once your filter sets are tested, reduce the journaling to a useful subset of entries.

Note that there is a second journal for IP Packet Security. This is the QIPNAT journal that contains entries for network address translation (NAT) rules.

16.7.5 Using the QVPN journal

Virtual Private Networks (VPN) use a separate journal to log information about the IP traffic and connections called the QVPN journal. The QVPN is stored in the library QUSRSYS. The journal code is M and the journal type is TS.

16.7.5.1 Enabling the VPN journal

Use the Virtual Private Networking option of AS/400 Operations Navigator to activate the VPN journal. You have to enable the logging function for a single connection group. There is no function that allows logging for all VPN connections.

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 journal logging for a Dynamic Key Group can use one of following options:

| | |
|----------------------------|--|
| 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, etc. as well as IP traffic information are being logged into 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 virtual private network (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. |

Note

Before you can stop journaling, make sure that the connection is inactive. To change the journaling status of a connection group, make sure that there are no active connections associated with that particular group.

16.7.5.2 Using the VPN journal

To view the entry-specific details in the VPN journal, you can display the raw journal entries on the screen or you can use an outfile.

Figure 386 and Figure 387 are examples from the QVPN journal, that show an entry for a dynamic connection.

By copying the journal entries to the 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 outfiles.

The following is an example of the Display Journal (DSPJRN) command:

```
DSPJRN JRN(QVPN) JRNCDE(M) ENTYP((TS)) OUTPUT(*OUTFILE) OUTFILEMT(*TYPE4)
OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Use the following steps to copy the VPN journal entries to the outfile:

1. Create a copy of the system-supplied outfile QSYS/QATOVSOFF into a user library by using the Create Duplicate Object (CRTDUPOBJ) command. The following is an example of 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 created in the previous step.

If you copy the DSPJRN into a nonexistent outfile, the system creates a file for you, but this file does not contain the proper field descriptions.

Note

The model outfile shipped with Version 4 Release 4 Modification 0 is missing some header fields. This will be corrected in Version 4 Release 5 Modification 0. Meanwhile a fixed model outfile is available on the InfoCenter Web site at www.as400.ibm.com.

```
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      Object      Library      Job          Time
      62      M    TS      Object      Library      Job          Time
      63      M    TS      Object      Library      Job          Time
      64      M    TS      Object      Library      Job          Time
      65      M    TS      Object      Library      Job          Time
      66      M    TS      Object      Library      Job          Time
      67      M    TS      Object      Library      Job          Time
      68      M    TS      Object      Library      Job          Time
      69      M    TS      Object      Library      Job          Time
      70      M    TS      Object      Library      Job          Time
      71      M    TS      Object      Library      Job          Time
      72      M    TS      Object      Library      Job          Time
                                         QTOVMAN      18:16:31      +

F3=Exit  F12=Cancel
```

Figure 386. 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 387. Displaying the QVPN journal - entry specific data

16.7.6 The Trace TCP/IP Application (TRCTCPAPP) command

The Trace TCP/IP Application (TRCTCPAPP) command is usually 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, or *SVRMAP)
- Distributed Data Management (DDM)
- Virtual Private Networking (VPN)
- Layer 2 Tunneling Protocol (L2TP)
- Digital Certificate Services

To execute the TRCTCPAPP command, the user profile needs the *SERVICE special authority.

For a given application, there can only be one trace active at a time on the system.

Many error messages issued in the VPN server job logs suggest that you use the TRCTCPAPP command to provide the necessary debug information to the IBM software service. This section focuses on the VPN trace options.

Note

The trace output produced by the TRCTCPAPP command is intended to be used by IBM software support to debug and isolate problems.

16.7.6.1 Start the TCP/IP application trace

The trace information captured by the TRCTCPAPP command is based on the parameter specified during the start of the trace. You have the choice of tracing only the connection manager job, only the key manager job, or both VPN server jobs. Following is an example showing how to start the VPN trace:

```
TRCTCPAPP APP(*VPN) SET(*ON) MAXSTG(*APP) TRCFULL(*WRAP)
```

The parameters for starting the trace are:

- | | |
|---------|---------------------------|
| APP | TCP/IP application |
| SET | Trace option setting |
| MAXSTG | Maximum storage for trace |
| TRCFULL | Trace full action |
- The default value is *WRAP, which means when the trace buffer is full, the trace wraps to the beginning. The second value *STOPTRC lets the trace stop when the trace buffer, specified in the MAXSTG parameter, is full of trace records.
- | | |
|---------|---------------|
| 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. The IBM support personnel will provide the arguments if necessary.

VPNSVR Virtual private network server
Specifies whether the trace information is to be collected for the VPN key manager (*KEYMGR), the VPN connection manager (*CNNMGR), or both. If you leave the parameter empty, both VPN servers are traced.

16.7.6.2 Stop the TCP/IP application trace

If not otherwise directed, the trace is usually stopped as soon as the condition you are tracing has occurred. For example, if you have problems with establishing a VPN connection, stop the trace after you receive an error message.

The following example shows the `TRCTCPAPP` command used to stop a VPN application trace:

```
TRCTCPAPP APP(*VPN) SET(*OFF) TITLE('VPN Trace for connection problems')
```

The parameters for stopping the trace are:

| | |
|--------------|--|
| APP | TCP/IP application The APP parameter defines the TCP/IP application for which you want to stop the trace. |
| SET | Trace option setting *OFF stops the TCP/IP application trace selected in the APP parameter. The trace information is written to the spool file. |
| TITLE | Trace title Give a meaningful title to determine the reason and the circumstances the trace was started. |

For each VPN server job the `TRCTCPAPP` command creates a separate spool file. The printer file used for the trace output is the QPTOCSERVE file.

16.7.6.3 Additional options on the TRCTCPAPP command

There are two more options on `TRCTCPAPP` command which can be also used when tracing VPN servers. The options are specified on the SET parameter. These are:

| | |
|-------------|--|
| *END | This value stops the TCP/IP application trace and deletes all trace data captured. No spool file is created. |
| *CHK | The status of tracing for the specified application is checked. Messages are returned indicating whether or not tracing is active for the specified TCP/IP application, the command parameters specified from the last time that <code>TRCTCPAPP</code> 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 <code>TRCTCPAPP SET(*CHK)</code> command. |

16.7.7 Using job logs for problem determination

In case of a problem, it is always advisable to analyze the AS/400 job logs. There are several job logs that may contain error messages and other information related to a VPN environment.

It is very important that you analyze jobs logs on both side of the connection, that is, if both sides are AS/400 systems.

16.7.7.1 Relevant job logs in virtual private networking

This section introduces the most important jobs in this environment. The following list shows the job names with a brief explanation of what the job is used for:

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

This is the PPP job for dial-out connections.

QTPPPL2TP

Layer-2 Tunneling Protocol (L2TP) manager job. If you have problems setting up a L2TP tunnel, look for messages in this job log.

To work with all QTCP job logs, expand the **Job Management** menu in Operations Navigator. To work with QTOKVPNIKE and QTOVMAN job logs, use the IP Security in Network menu.

16.7.8 Using the AS/400 communications trace

AS/400 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.

16.8 Troubleshooting for OS/390

This section describes the troubleshooting method for VPN features in OS/390.

16.8.1 Using the firewall log to check the tunnel

There are some messages in the firewall log that can help you check the activation of the tunnel, to check if the traffic is flowing through the tunnel, and so on. You can browse the log file using the `OBROWSE` command in a TSO session or using the log viewer in the configuration client. These messages are in the file `/tmp/firewall.all.log` as shown in Figure 388.

```

ICA8233i;507;510; 1
ICA8227i;000000008;192.168.100.100;255.255.255.255;ALL;ALL;192.168.100.150; 2
ICA1073i;TCPIPB;R:p; o; ;192.168.100.100;s; ;192.168.100.100;d; ;192.168.100.150; 3
p; ;icmp;t; ;8;c; ;0;r; ;l;a; ;n;f; ;y;T; ;0000000512:0000000507:0000000510:0000000510:
00000510:0000000510:0000000530:0000000501:000000008"†"*;AH; ;0;ESP; ;0;l; ;284;
ICA1073i;TCPIPB;R:p; i; ;192.168.100.100;s; ;192.168.100.150;d; ;192.168.100.100; 4
p; ;icmp;t; ;0;c; ;0;r; ;l;a; ;n;f; ;y;T; ;0000000512:0000000507:0000000510:0000000510:
0000000510:0000000510:0000000530:0000000501:000000008"†"*;AH; ;0;ESP; ;0;l; ;284;

```

Figure 388. Checking firewall log messages

1 This message indicates that an attempt to create a dynamic connection between the two network objects is in progress. When checking these two network objects in an OMVS shell you will see:

```

GIANCA @ RA03:/u/gianca>fwnwobj cmd=list id=507 format=long
id = 507
type = Host
name = Host.192.168.100.100
desc = Host 192.168.100.100
addr = 192.168.100.100
mask = 255.255.255.255
startaddr =
endaddr =

GIANCA @ RA03:/u/gianca>fwnwobj cmd=list id=510 format=long
id = 510
type = Host
name = Host.192.168.100.150
desc = Host 192.168.100.150
addr = 192.168.100.150
mask = 255.255.255.255
startaddr =
endaddr =

```

Figure 389. Displaying tunnel endpoints network objects

The two network objects are the tunnel endpoints.

2 This message indicates that tunnel ID 8 was created.

3, 4 These messages show a PING (icmp protocol) between the tunnel endpoints. The first icmp message is from an OS/390 host and the second icmp message is from an AS/400 host. These messages also indicate that the traffic is flowing through the tunnel ID 8.

16.9 Troubleshooting for IBM Nways routers

We will show some important commands to troubleshoot problems in the Nways router environment. Note that we give guidelines for the VPN layer only. We do not show commands to handle problems that are specific to other layers in the network.

The following commands are valid for Nways Routers 2210/2212/2216 (MRS / AIS / MAS) unless otherwise noted.

16.9.1 General

Perform the following checks to begin problem determination.

16.9.1.1 Load the encryption package

If you are using the 2212 or 2216, and if you are using encryption within IPsec you have to load the encryption package.

If you are using a 2210 you must ensure that you have an operational code that supports APPN.

Prepacked operational code can be downloaded from the IBM networking home page at <http://www.networking.ibm.com/>.

Select **support > 2210 > download > 2210 operational code**.

The operational code is found at

<http://www.networking.ibm.com/support/code.nsf/2210oper?OpenView>

The encryption package on the 2212 / 2216 can be loaded with the following command:

```
Config (only)>LOAD ADD PACKAGE encryption
encryption package configured successfully
This change requires a reload.
Config (only)>RELOAD y
```

Figure 390. Loading encryption package on the 2212 or 2216

16.9.1.2 Test IP connectivity

Be sure that you have IP connectivity. This is especially important in the case of the layer-2 protocols (L2TP, L2F, PPTP) where IP addresses are dynamically assigned. Ensure that in this case you have the necessary routes defined (either statically or via a routing protocol).

16.9.1.3 Define all necessary tunnels

Ensure that all necessary tunnels are established. For example, in the case of DLsw or TN3270E routers, encapsulate the SNA/APPN/HPR-traffic in IP packets. In these cases the IP addresses of the end-routers are used as source and destination. Therefore the corresponding policies for the internal IP addresses must be applied.

16.9.2 Order of commands while troubleshooting

To perform systematic troubleshooting you should complete the following steps:

- Check the status of IPsec and the policies.
- Disable IPsec and the policies.
- Test all other configuration parameters.
- Enable IPsec and the policies.
- List the IPsec tunnels.
- Check the IPsec traffic flow.

- List the statistics of IPSec and the policies.

16.9.3 Useful commands for Policy and IPSec

Use the following commands for IPSec problem determination.

16.9.3.1 List status of IPSec

The command `LIST STATUS` gives you the current status of IPSec:

```
Center *TALK 6
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPSec config>IPV4
Center IPV4-IPSec config>LIST STATUS
IPSec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
```

Figure 391. List the status of IPSec on a router

16.9.3.2 List Policy Statistics

The command `LIST STATS` gives you important information about the usage of the policy rules.

In the last column the first number per block is the rule count and the second number is the action count.

Before the Security Policy is loaded into the database any rules that are necessary for the different traffic flows we may see are generated. The different traffic flows may share the same action. As a result, there is a rule count and an action count. The action count typically is not the same as the rule count since it could be shared across multiple rules.

```

Center Policy console>
Center Policy console>LIST STATS
+-----+
|Name                                         |Hits |
+-----+
|ike-pre-88.5-102.plout                      |    1|
|   ike-88.5                                (ISAKMP) |    3|
+-----+
|ike-ds-211-211.plout                       |    1|
|   ds-act1                                 (ISAKMP) |    2|
+-----+
|ike-pre-88.5-102.plin                      |    2|
|   ike-88.5                                (ISAKMP) |    3|
+-----+
|ike-pre-100-103-cisco.plin                 |    1|
|   ike-cisco                              (ISAKMP) |    1|
+-----+
|ike-ds-211-211.plin                       |    1|
|   ds-act1                                 (ISAKMP) |    2|
+-----+
|ike-pre-88.5-102.traffic                   |    2|
|                                         tun-88.5-102 (IPSEC) |    2|
+-----+
|ike-ds-211-211.traffic                     |   114|
|                                         tun-101-102-ds (IPSEC) |   227|
+-----+
Center Policy console>

```

Figure 392. Checking the usage of the policy

16.9.3.3 Usage of IPSec

The Command `STATS` tells you the usage of IPSec. Remember that the counters are reset after a restart or reload.

While transferring data over the tunnel you should enter the command several times and see whether the counters increase. You can see whether the IPSec tunnel is really used.

```

Center 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
-----
          387           0           387       386992     193496     193496

Sent:
total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
-----
          359           0           359       42504         0       42504

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

Center IPV4-IPSec>

```

Figure 393. Checking the IPSec statistics of a router

16.9.3.4 List policy

The `LIST POLICY ALL` command provides you with a list of all defined policies and their status (disabled or enabled). You also see the corresponding profile, the validity period, the IPSec action and the ISAKMP action.

You get much more information with the command `list policy complete`.

```

Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>LIST POLICY ALL
Policy Name      = ike-pre-101-102
State:Priority   =Enabled   : 5
Profile          =101.0-to-102.0-pre
Valid Period    =allTheTime
IPSEC Action    =tun-101-102
ISAKMP Action   =ike-act1
.....

```

Figure 394. List the policies on a router

16.9.3.5 List default-policy

In case your policy rules do not match and you see IPSec actions that you did not expect, you should check the default policy of the router:


```

Branch Policy config>LIST DEFAULT-POLICY
Default Policy Rule:                Accept All IP Traffic
Default error handling procedure:    Reset Policy Database to Default Rule
Branch Policy config>

```

Figure 395. List the default policy on a router

16.9.3.6 Test forwarder-query

In the command `TEST FORWARDER-QUERY` you specify an IP packet. The policy database will then be searched for a rule in the policy database that matches the IP packet.

There is no traffic generated on the network.

```

Center Policy console>TEST FORWARDER-QUERY
Enter IPV4 Source Address [0.0.0.0]? 192.168.211.1
Enter IPV4 Destination Address [0.0.0.0]? 192.168.211.2
Enter the value for the Source Port [0]?
Enter the value for the Destination Port [0]?
Enter the value for the IP Protocol ID [0]?
Enter the value for the IP TOS Byte [0]?
No match found
Center Policy console>TEST FORWARDER-QUERY
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.5
Enter IPV4 Destination Address [0.0.0.0]? 192.168.101.7
Enter the value for the Source Port [0]?
Enter the value for the Destination Port [0]?
Enter the value for the IP Protocol ID [0]?
Enter the value for the IP TOS Byte [0]?
Results of Test:
Policy (IPSEC):  ike-pre-101-102.traffic
                  IPSEC Action:  tun-101-102
Center Policy console>

```

Figure 396. Result of the Command test forwarder-query

16.9.3.7 List Tunnel

The command `LIST TUNNELS` provides us with the state of IPSec (enabled or disabled). It also lists all tunnels, including the start and end address, the mode and the state of the tunnel.

```

Li +feature ipsec
Li IPsec>list global

IPsec is ENABLED
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID      Name      Local IP Addr  Remote IP Addr  Mode  State
-----
   1  ESP&AH      192.168.189.1  192.168.189.59  TUNN  Enabled
   2  TRANS-ESP&AH  192.168.189.1  192.168.189.59  TRANS  Enabled

Tunnel Cache:

   ID      Local IP Addr  Remote IP Addr  Mode  Policy  Tunnel Expiration
-----
   2      192.168.189.1  192.168.189.59  TRANS  AH-ESP  16:47 Jun 20 1998
   1      192.168.189.1  192.168.189.59  TUNN   AH-ESP  16:47 Jun 20 1998
Li IPsec>

```

Figure 397. Listing IPsec information

You get more detailed information with the commands `LIST TUNNEL ACTIVE` and `LIST TUNNEL DEFINED`.

16.9.3.8 Disable IPsec and the policies

Be sure you disable IPsec and the policies. If you only disable IPsec, the policies are still active. As soon as a packet matches a policy rule the router tries to perform the corresponding IPsec action, which cannot be done.

The `DISABLE IPSEC STOP` command stops IPsec. The current status of IPsec can be seen with the `LIST STATUS` command.

```

Center *TALK 6
Center Config>FEATURE IPsec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>DISABLE IPSEC STOP

```

Figure 398. Disabling IPsec on a Router

With the `DISABLE POLICY` command you disable the policies:

```

Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>DISABLE POLICY
Enter the Name of the Policy to disable (? for a List)
[?]?
    1: ike-pre-101-102
    2: ike-pre-3-100
    3: ike-pre-211-211
Number of policy [1]?

```

Figure 399. Disabling the policies on a router

16.9.3.9 Enable IPsec and the policies

After verifying the installation you can enable IPsec and the policies again. You use the commands `ENABLE IPSEC` and `ENABLE POLICY`.

16.9.4 Useful Commands for IKE

Use the following commands for IKE problem determination.

16.9.4.1 The status of IKE Phase 1

From `FEATURE IPsec` in talk 5, there are now submenus, one of which is IKE. From this menu you can determine the status of Phase 1 IKE negotiations. The command `LIST ALL` shows the IKE Phase 1 SA. It shows the IP address of the IKE peer, whether the peer is acting as the initiator or the responder, whether Phase 1 occurred in main or aggressive mode, if it occurred at system initialization (Y), the current state of the tunnel, and how authentication occurred - preshared or digital signatures (rsasig). Figure 400 is for two peers that are being authenticated using preshared keys.

```

Center *TALK 5
Center +FEATURE IPsec
Center IPSP>IKE
Center IKE>LIST ALL
Phase 1 ISAKMP Tunnels for IPv4:
-----
Peer Address   I/R  Mode  Auto  State      Auth
-----
192.168.211.2  I    Main  Y     QM_IDLE    pre-shared

```

Figure 400. The status of IKE Phase 1

16.9.4.2 IKE negotiations

You can display IKE negotiations statistics using the `STATS` command from `IKE`, `feature IPsec` in talk 5. If you are trying to debug a problem with IKE this `STATS`

command gives some insight into problems - for example, may be the proposals were invalid or rejected.

```
Center IKE>STATS
Peer address [192.168.211.2]?
Peer IP address.....:    192.168.211.2
Active time (secs)...:    490
                               In           Out
                               ---           ---
Octets.....:              464             540
Packets.....:              4              5
Drop pkts.....:            0              0
Notifys.....:              0              0
Deletes.....:              0              0
Phase 2 Proposals....:      1              1
Invalid Proposals....:      0              0
Rejected Proposals...:      0              0
```

Figure 401. IKE negotiations

16.9.4.3 IKE tunnel display

The `list tunnel` command expands the output of `list all`. This command shows the negotiated encryption algorithms, hash algorithms, Diffie-Hellman group, the lifetime of the Phase 1 SA, the refresh threshold,, and the identity of the peer as shown in Figure 402:

```
Center IKE>LIST TUNNEL
Peer address [192.168.211.2]?
Peer IKE address: 192.168.211.2
Local IKE address: 192.168.211.1
Role: Initiator
Exchange: Main
Autostart: Yes
Oakley State: QM_IDLE
Authentication Method: Pre-shared Key
Encryption algorithm: des
Hash function: md5
Diffie-Hellman group: 1
Refresh threshold: 85
Lifetime (secs): 15000
Peer ID: 192.168.211.2
```

Figure 402. Tunnel display

16.9.5 Useful commands for layer-2 VPNs

For layer-2 commands, use the same names for host/tunnel on both sides.

16.9.5.1 List tunnel profile

The command `LIST TUNNEL-PROFILES` lists all defined tunnel profiles, including the tunnel type, the tunnel endpoint, the name and the corresponding (local) hostname:

```

l2_branch Config>LIST TUNNEL-PROFILES
TunnType Endpoint Tunnel name Hostname
L2TP 192.168.212.1 tocenter l2_branch

1 TUNNEL record displayed.

```

Figure 403. LIST TUNNEL-PROFILES

16.9.5.2 Disable L2TP, PPTP, and L2F

You can disable a layer-2-protocol (L2TP, PPTP, L2F) with the commands `disable L2TP`, `disable PPTP` and `disable L2f`.

16.9.5.3 List layer-2 tunnel state

The command `TUNNEL STATE` lists the tunnels, including the ID, type, peer ID, the state of the tunnel and date:

```

l2_branch *TALK 5
l2_branch Layer-2-Tunneling Console> TUNNEL STATE
Tunnel ID | Type | Peer ID | State | Time Since Chg | # Calls | Flags
62468 | L2TP | 14733 | Established | 0:19:52 | 1 | TL F
l2_branch Layer-2-Tunneling Console>

```

Figure 404. List layer-2 tunnel state

16.9.5.4 List layer-2 tunnel statistics

With the command `TUNNEL STATISTICS` you can check whether your IP traffic is actually going through the tunnel. By using the command several times the corresponding timers should increase.

```

l2_branch Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
62468 | L2TP | 1426 | 84936 | 1438 | 85536 | 6 | 18
l2_branch Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
62468 | L2TP | 1437 | 85588 | 1449 | 86188 | 6 | 18
l2_branch Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
62468 | L2TP | 1448 | 86240 | 1460 | 86840 | 6 | 18
l2_branch Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
62468 | L2TP | 1449 | 86304 | 1461 | 86904 | 6 | 18

```

Figure 405. List layer-2 tunnel statistics

16.9.5.5 List PPP User

The command `LIST PPP-USER` lists all defined PPP users:

```

ISP Config>LIST PPP-USER
List (Name, Verb, User, Addr, VCon, Call, Time, Dial, Encr): [Verb]
  PPP user name: l2_branch
  User IP address: Interface Default
  Netroute Mask: 255.255.255.255
  Hostname: <undefined>
  Virtual Conn: disabled
  Time allotted: Box Default
  Callback type: disabled
  Dial-out: disabled
  Encryption: disabled
  Status: enabled
  Account Expiry: <unlimited>
  Password Expiry: <unlimited>

  PPP user name: wsdial
  User IP address: 192.168.88.5
  Netroute Mask: 255.255.255.255
  Hostname: <undefined>
  Virtual Conn: disabled
  Time allotted: Box Default
  Callback type: disabled
  Dial-out: disabled
  Encryption: disabled
  Status: enabled
  Account Expiry: <unlimited>
  Password Expiry: <unlimited>

2 PPP records displayed.
ISP Config>

```

Figure 406. Listing PPPusers

16.9.5.6 List layer-2 PPP parameters

The command `LIST ALL` in the layer-2 environment gives you a lot of useful information. We can show here only the header of the information blocks:

```

Center Config>
Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>
Center Layer-2-Tunneling Config>ENCAPSULATOR
Point-to-Point user configuration
Center PPP-L2T Config>LIST ALL

Disabled as a Multilink PPP Link
LCP Parameters
...
LCP Options
...
Authentication Options
....
NCP Parameters
...
CCP Options
...
MPPE Options
...
CP Options
...
BCP Options
...
IPCP Options
...
IPv6CP Options
...
Center PPP-L2T Config>

```

Figure 407. Listing layer-2 parameters

16.9.5.7 List layer-2 parameters

The command `LIST` in the layer-2 environment gives us the state of the various layer-2 protocols.

```

Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>LIST
GENERAL ADMINISTRATION
-----
L2TP                               = Enabled
PPTP                               = Disabled
L2F                                = Disabled
Maximum number of tunnels          = 30
Maximum number of calls (total)    = 100
Buffers Requested                  = 200

CONTROL CHANNEL SETTINGS
-----
Tunnel Auth                        = Enabled
Tunnel Rcv Window                  = 4
Retransmit Retries                 = 6
Local Hostname                     = IBM

DATA CHANNEL SETTING
-----
Force CHAP Challenge (extra security) = Disabled
Hiding for PAP Attributes          = Disabled
Hardware Error Polling Period (Sec) = 120
Sequencing                         = Enabled

MISCELLANEOUS
-----
Send Proxy-LCP                     = Enabled
Send Proxy-AUTH                    = Enabled
Fixed UDP source port (1701)       = Disabled

Fixed source IP Address             = Disabled

```

Figure 408. Listing layer-2 parameters

16.9.5.8 List type of address assignment

The command `LIST IP-ADDRESS-ASSIGNMENT` provides an overview of the AAA configuration:

```

Center Config>FEATURE DIALs
Dial-in Access to LANs global configuration
Center DIALs config>LIST IP-ADDRESS-ASSIGNMENT
DIALs client IP address assignment:
Client      : Enabled
UserID     : Enabled
Interface  : Enabled
Pool       : Enabled
DHCP Proxy : Disabled

```

Figure 409. LIST IP-ADDRESS-ASSIGNMENT command

16.9.6 Authentication commands and RADIUS

Use the following commands for RADIUS problem determination.

16.9.6.1 List AAA-configuration

The command `LIST CONFIG` gives an overview of the AAA configuration. You can see whether the authentication, authorization, and accounting for login, ppp, and tunnel are configured locally or remotely (for example, on a RADIUS server):

```
Center *TALK 6
Center AAA Config> LIST CONFIG
ppp authentication      : Radius      mradius
ppp authorization      : Radius      mradius
ppp accounting         : Radius      mradius
tunnel authentication  : locallist
tunnel authorization   : locallist
tunnel accounting      : Disabled
login authentication   : locallist
login authorization    : locallist
login accounting       : Disabled
Center AAA Config>
```

Figure 410. Listing AAA Information

The `LIST LCP` command shows lcp information:

```
Center Config>
Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>ENCAPSULATOR
Point-to-Point user configuration
Center PPP-L2T Config>LIST LCP
LCP Parameters
-----
Config Request Tries:          20  Config Nak Tries:          10
Terminate Tries:              10  Retry Timer:              3000

LCP Options
-----
Max Receive Unit:             2044  Magic Number:             Yes
Peer to Local (RX) ACCM:      A0000
Protocol Field Comp (PFC):    No    Addr/Cntl Field Comp (ACFC): No

Authentication Options
-----
Authenticate remote using:MSCHAP or SPAP or CHAP or PAP[Listed in priority order]
CHAP Rechallenge Interval:    0
MSCHAP Rechallenge Interval:  0
Identify self as:             ibm
Center PPP-L2T Config>EXIT
Center Layer-2-Tunneling Config>
```

Figure 411. Listing lcp Information

Note

It is very important to remember that MSCHAP is not enabled because the N Ways router does not support MSCHAP together with a RADIUS server. That means the above example will not work together with a RADIUS server.

16.9.7 Useful commands for LDAP

Use the following commands for LDAP problem determination.

16.9.7.1 List LDAP definitions

The command `LIST CONFIG` gives an overview of the AAA configuration:

```
Branch Config>
Branch Config>FEATURE Policy
IP Network Policy configuration
Branch Policy config>LIST LDAP
LDAP CONFIGURATION information:
  Primary Server Address:          192.168.100.3
  Secondary Server Address:        0.0.0.0
  Search timeout value:           3 sec(s)
  Retry interval on search failures: 1 min(s)
  Server TCP port number:         389
  Server Version number:          2

  Bind Information:
  Bind Anonymously:               No
  Device Distinguished Name:      cn=root
  Base DN for this device's policies: base cn=policySecureG2toG1
  Search policies from LDAP Directory: Disabled
Branch Policy config>
```

Figure 412. Listing LDAP configuration

16.9.7.2 List LDAP policy definitions

The listing of LDAP-defined policies looks completely different from the listing of router-defined policies:

```
Branch Policy console>LIST POLICY BASIC
1: (Enabled,Valid)    ike-pre-101-102
: (Enabled,Valid)    ike-pre-3-100
: (Enabled,Valid)    ike-pre-211-211
: (Enabled,Valid)    cn=policySecureG2toG1, o=ibm, c=us
Number of Policy to display (0 for All) [0]? 4
Policy Name: cn=policySecureG2toG1, o=ibm, c=us
Loaded from: LDAP Server
State:           Enabled and Valid
Priority:        20
Bits:           0
Profile:        cn=G2toG1, o=ibm, c=us
Validity:       cn=allTheTime, o=ibm, c=us
IPSEC:          cn=secureG2toG1, o=ibm, c=us
ISAKMP:         cn=generalPhase1Action, o=ibm, c=us
```

Listing LDAP policy configuration

16.9.7.3 Test forwarder-query

As in the above case with policies defined on the router you can also use the command `TEST FORWARDER-QUERY` in the LDAP case. Specify an IP packet and the policy database will be searched for a rule in the policy database that matches the IP packet.

There is no traffic generated on the network.

16.9.8 Using ELS subsystems

ELS has been updated with two new subsystems - IKE and PKI (for authentication via digital signatures). IPSP, the subsystem for IPsec, has also been updated. Useful information can also be obtained from the IP and PLCY subsystems.

Configure the ELS to monitor the IKE, PKI and PLCY subsystems. You may want to set these up in talk 6 and restart the router to capture the messages upon startup at talk 2.

```
Center *TALK 6
Gateway user configuration
Centerp Config>EVENT
Event Logging System user configuration
Center ELS config>DISPLAY SUBSYSTEM ipsp all all
Center ELS config>DISPLAY SUBSYSTEM ike all all
Center ELS config>DISPLAY SUBSYSTEM pki all all
Center ELS config>DISPLAY SUBSYSTEM plcy all all
```

Figure 413. Enabling IPsec-related ELS subsystems

16.9.9 Tracing

You can use ELS to trace 221x- traffic.

The command `NODISPLAY SUBSYSTEM ALL ALL` switches off all ELS messages. Afterward you should use the command `DISPLAY SUBSYSTEM subsystem ALL` to enable all ELS messages that are important for your problem.

```
Center ELS>NODISPLAY SUBSYSTEM all all
Complete
Center ELS>DISPLAY SUBSYSTEM l2 all
Center ELS>
```

Figure 414. ELS commands

The following subsystems are important for VPN troubleshooting:

- L2
- AAA
- PPP
- LDAP
- IKE
- PKI
- IPSP (for IPsec)
- IP
- PLCY

Part 4. OEM VPN platforms and interoperability

Chapter 17. Interoperability with Cisco routers

This chapter gives an overview of VPN capabilities of Cisco routers based on Cisco IOS 12.0(5) and shows a few configuration and interoperability examples with IBM VPN solutions.

IP networks at a great number of enterprises and Internet service providers use Cisco routers, and in fact, the majority of routers on the Internet backbone are Cisco machines. It is therefore likely that a Cisco router may be part of a VPN that you want to develop in your own company network. This was the reason for us to include Cisco in our interoperability scenarios.

Because both the number of routers and resources available to us were limited, we keep our Cisco scenarios at a very basic level that does not include all features that Cisco IOS may offer. For a full list of those features as well as product documentation, you may want to consult Cisco's Web site at <http://www.cisco.com>.

17.1 Cisco IOS VPN Capabilities

Depending on your version of IOS and the type of image you have installed on your router, the VPN capabilities may vary. We were using a Cisco 2612 router with IOS 12.0(5)T installed. The type of image we were using was c2600-ik2s-m, which offers the following VPN features:

Table 85. Cisco IOS 12.0(5)T - VPN features

| Feature | |
|----------------------------------|--|
| Tunnel Type | IKE, manual |
| IPSec Header Format | RFCs 24xx, RFC 18xx |
| IKE | |
| Key Management Tunnel (Phase 1) | |
| Negotiation Mode | Main Mode, Aggressive Mode |
| Encryption Algorithm | DES, 3DES |
| Authentication Method | Pre-shared Key, RSA signatures, RSA encryption |
| Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| Diffie-Hellman Group | Group 1, Group 2 |
| Send Phase 1 Delete | Yes |
| On-demand Tunnels | Yes |
| Data Management Tunnel (Phase 2) | |
| Encapsulation Mode | Tunnel Mode, Transport Mode |
| Security Protocol | AH, ESP |
| AH Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| ESP Encryption Algorithm | DES, 3DES, NULL |

| Feature | |
|-------------------------------|--|
| ESP Authentication Algorithm | HMAC-MD5, HMAC-SHA, NULL |
| Multiple SA Proposals | Yes |
| Perfect Forward Secrecy (PFS) | Yes |
| Other | L2TP, L2F, Logging, Wildcard Pre-shared Keys |

For more details about what version of IOS and what type of image supports which VPN features, please see Cisco's product documentation on its Web site.

17.2 Configuring Cisco IOS for IPSec and IKE

The basic configuration steps to set up IKE and IPSec connections are illustrated below, assuming pre-shared keys are used as the method for IKE authentication.

Important

Cisco IOS also supports certificate-based authentication methods for IKE, but that requires a CA that supports Cisco's Certificate Enrollment Protocol (CEP) in order to process a certificate request from the router and to get a certificate back to the router. This is a preferable way of handling certificates in an enterprise environment when you have a CA inhouse. It may be less comfortable if you have to access the Internet from every router in order to reach an external CA, and it may be frustrating for testing. As far as we know, there is no procedure to manually load a certificate into a Cisco router.

If you are using IKE with pre-shared key authentication, be aware that these keys are listed in cleartext when the current configuration is listed using either the `show running` or `write terminal` commands. Pre-shared keys can also be listed with the `crypto show isakmp key` command. You should therefore protect privileged mode commands with an enable password or secret. See Cisco's documentation about how to set passwords for system protection.

17.2.1 IKE configuration using pre-shared key authentication

Before continuing, we assume that you have entered the global configuration mode from either the console or a Telnet host on a local subnet.

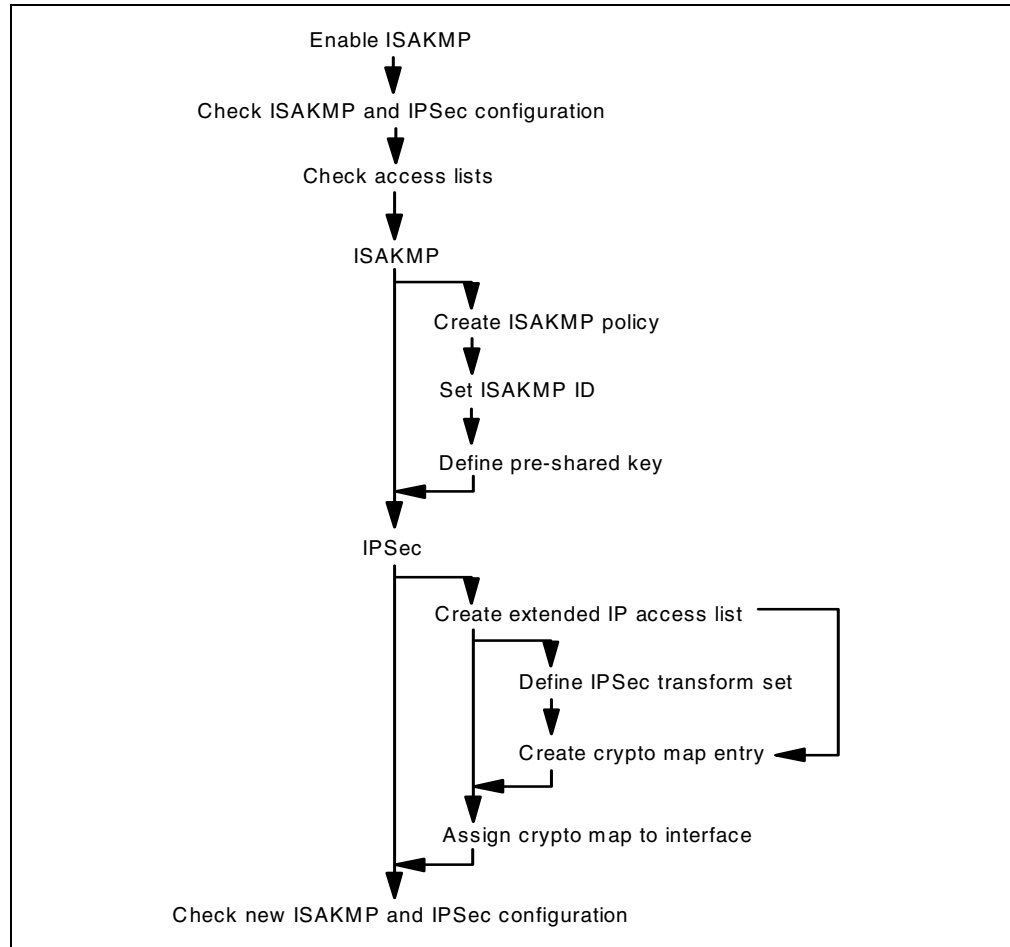


Figure 415. Cisco IKE and IPsec configuration flow - pre-shared keys

The steps illustrated in Figure 415 and explained below describe how to set up a basic configuration for IKE:

1. Enable IKE (enabled by default) and check IKE and the IPsec configuration by issuing the following commands:

```

crypto isakmp enable
crypto isakmp policy
crypto isakmp sa
crypto ipsec sa
  
```

Figure 416. Cisco IKE and IPsec commands

2. Check access lists to ensure that IKE will work. Access lists define what type of IP traffic can reach and pass through the router, which works much the same as IP filtering.

If you have access lists defined for that purpose, you must make sure that you allow IKE (UDP port 500) and IPsec (IP protocols 50, or 0x32, and 51, or 0x33) to flow between your router and the remote system with which you are setting up IKE and IPsec tunnels.

If you do not have any access lists, or if the above has been configured properly, you still need to define IPSec access lists that define which traffic has to be protected by IPSec and directed into the appropriate tunnel.

We do not cover general access lists here, but to check and create an IPSec access list, enter the following commands:

```
show access-list
```

Figure 417. Cisco - show active/defined access lists

3. Create at least one IKE policy to be used for negotiations between your router and the remote system. You can define multiple policies for any given partner which would then be sent as a list of proposals during IKE negotiation. To create a simple policy, enter the following commands:

```
crypto isakmp policy ##
  encryption [alg_encr]
  hash [alg_prf]
  authentication [auth]
  lifetime [#secs]
  group [#group]
```

Figure 418. Cisco - ISAKMP policy command

where ## is the priority number for the policy (lower number means higher priority), alg_encr can be either DES or 3DES (if you have a code image that supports it), alg_prf can be either md5 or sha, auth can be either pre-share, rsa-sig or rsa-key, #secs indicates the time until a Phase 1 SA expires (meaning that keys need to be renegotiated), #group indicates the Diffie-Hellman group, and pfs specifies whether or not PFS should be used with this policy.

A default policy exists that you can use if it suits your security requirements. It will always be listed at the end of all policies you define:

```
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys) .
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

Figure 419. Cisco - display default ISAKMP policy command

To delete an IKE policy (other than the default policy), enter:

```
no crypto isakmp policy ##
```

Figure 420. Cisco - delete ISAKMP policy command

4. Set the identity to be used for IKE during Phase 1. If you use main mode and pre-shared key authentication, the only choice is to use the IP address as the identity.

```
crypto isakmp identity address
```

Figure 421. Cisco - set ISAKMP identity command

If you want to use aggressive mode you may also select an identity in the form of a fully qualified host name (FQDN). In that case, the command would read as follows:

```
crypto isakmp identity hostname
```

Figure 422. Cisco - set ISAKMP identity command

If you are using FQDNs, make sure that a DNS server is always accessible to resolve those names, or add any required name to the router using the `ip host` command.

5. Configure the pre-shared key to be used to authenticate to the remote system during IKE Phase 1.

```
crypto isakmp key [key_string] address [peer_addr]
```

Figure 423. Cisco - set ISAKMP pre-shared key command for address ID

Where `key_string` is the pre-shared key (ASCII format) and `peer_addr` is the IP address of the partner for this IKE connection. For aggressive mode, `peer_fqdn` is the ID you have chosen in the previous step, and the command reads as follows:

```
crypto isakmp key [key_string] hostname [peer_fqdn]
```

Figure 424. Cisco - set ISAKMP pre-shared key command for hostname ID

6. Finally, check your IKE configuration to see if all went well:

```
show crypto isakmp policy
```

Figure 425. Cisco - show active/defined ISAKMP policies command

If you want to check the pre-shared keys, enter the following command or show the current configuration:

```
show crypto isakmp keys
```

Figure 426. Cisco - show running/active configuration command

17.2.2 IKE configuration using RSA signature authentication

Before continuing, we assume that you have entered the global configuration mode from either the console or a Telnet host on a local subnet.

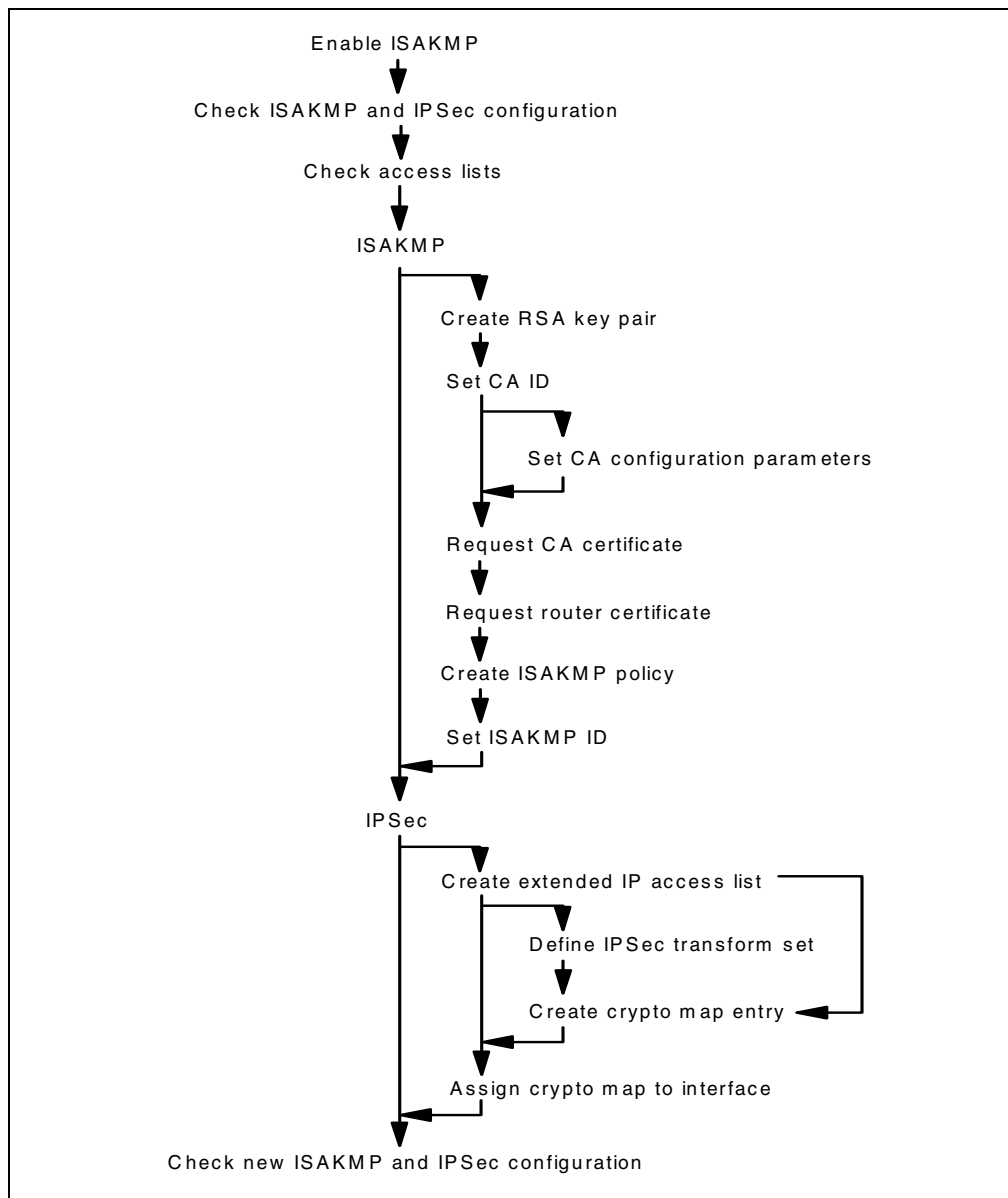


Figure 427. Cisco IKE and IPsec configuration flow - RSA signatures

The steps illustrated in Figure 427 and explained below describe how to set up a basic configuration for IKE:

1. Enable IKE (enabled by default) and check IKE and IPsec configuration.
2. Check access lists to ensure that IKE will work.
3. Generate RSA key pairs to be used to authenticate to the remote system during IKE Phase 1.

```
cry key gen rsa [usage]
```

Figure 428. Cisco - command to generate RSA keys

Where `usage` specifies if you want to create separate keys for signature and encryption operations. If you want to do that, enter the command as shown above which will create two key pairs. Some CAs allow one key pair for both signature and encryption operations and some do not.

Important

You must set the local hostname and domain name using the `ip hostname` and `ip domain-name` commands, otherwise the certificate enrollment process will not work. If you are not using a DNS, or if a DNS is temporarily inaccessible, prevent the router from using DNS with the `no ip domain-lookup` command.

4. Set a name by which the router identifies the certificate authority.

```
cry ca iden [name]
```

Figure 429. Cisco - command to identify a CA

Where `name` is an identifier for your CA. This name is used only by the router and does not have to bear any resemblance to the real name of your CA.

5. Set the configuration parameters pertaining to the software that your CA is using. Following is a configuration example for a CA running Entrust CA with VPN Connector. The router will not check certificate revocation lists (CRLs).

```
enrollment mode ra
enrollment url http://[identifier]
crl optional
```

Figure 430. Cisco - CA configuration parameters

Where `identifier` is the remainder of the URL where your CA listens for CEP requests. This can be either an IP address or a host name, optionally followed by port number and a URL path.

6. Request a CA certificate from your certification authority.

```
cry ca auth [name]
```

Figure 431. Cisco - request CA certificate

Where `name` is the same name that you have previously used to identify your CA.

7. Verify CA certificates.

```
sh cry ca cert
```

Figure 432. Cisco - show available certificates

8. Request certificates for the router.

```
cry ca enroll [name]
```

Figure 433. Cisco - request router certificates

Where `name` is the same name that you have previously used to identify your CA.

9. Verify router and CA certificates.

```
sh cry ca cert
```

Figure 434. Cisco - show available certificates

10. Create at least one IKE policy to be used for negotiations between your router and the remote system.

11. Set the identity to be used for IKE during Phase 1. Irrespective of the mode that IKE is using (main or aggressive), the identity must match the value given for `subject_alternate_name` in the certificate you intend to use. This can be either an IP address or a fully qualified domain name (FQDN).

If you are using FQDNs, make sure that a DNS server is always accessible to resolve those names, or add any required name to the router using the `ip host` command.

12. Finally, check your IKE configuration to see if all went well:

```
show crypto isakmp policy
```

Figure 435. Cisco - Show active/defined ISAKMP policies command

If you want to check certificates, you have to show the current configuration:

```
show running
```

Figure 436. Cisco - Show running/active configuration command

17.2.3 IPSec Configuration

The steps below illustrate and explain how to set up a basic configuration for IPSec:

1. Create a crypto access list for IPSec using the following command:

```
access-list ### [name] permit ip [source_ip] [source_mask]  
[dest_ip] [dest_mask]
```

Figure 437. Cisco - define extended IP access list command

where `###` is the reference number for this access list (use numbers between 100 and 199 or between 2000 and 2699), `source_ip`, and `dest_ip` are the addresses of the destinations for which traffic should be protected by IPSec (it can be hosts, networks, or subnets), and `source_mask` and `dest_mask` are the appropriate subnet masks.

2. Define a transform set for IPSec using the following command:

```
crypto ipsec transform-set [name] [trans_encr] [trans_auth]
```

Figure 438. Cisco - define IPSec transform set command

where `name` is the name of this transform-set, `trans_encr` is the IPSec protocol and transform to be used for encryption, and `trans_auth` is the IPSec protocol and transform to be used for authentication.

To delete a transform set, enter:

```
no crypto ipsec transform-set [name]
```

Figure 439. Cisco - delete transform set command

3. Create a crypto map entry for IPSec and IKE. This step combines an IKE policy with an IPSec access list and transform set to define a set of proposals for IKE negotiations.

```
crypto map [name] ## ipsec-isakmp
  match address [#acc_list]
  set transform-set [ts_name]
  set peer [peer_addr]
  pfs [yes/no]
  set security-association lifetime seconds [#secs]
```

Figure 440. Cisco - define crypto map command

where `##` is the priority number for this map (lower number means higher priority), `name` is the name for this map, `#acc_list` identifies the parties for which IPSec should be used as defined in the appropriate access list above, `ts_name` specifies the IPSec transforms to be used as defined in the appropriate transform-set above, `peer_addr` identifies the IKE peer as defined in the IKE pre-shared key definition above, `pfs` specifies whether or not PFS should be used with this map, and `#secs` indicates the time until a phase 2 SA expires (meaning that keys need to be renegotiated).

To delete a crypto map, enter the following command in global configuration mode:

```
no crypto map [name] [##]
```

Figure 441. Cisco - delete crypto map command

To delete a transform set from a crypto map, enter the following command in crypto map configuration mode:

```
no set transform-set [name]
```

Figure 442. Cisco - delete crypto map command

4. Apply that crypto map entry to an interface using the following command:

```
interface [if_name] crypto map [map_name]
```

Figure 443. Cisco - Add crypto map to interface command

where `if_name` is the name of the interface that this crypto map should be applied to and `map_name` is the name of the crypto map set to be applied.

Important

You can associate only one crypto map set to an interface at any one time. If you need multiple crypto maps on an interface, you have to specify multiple crypto maps into one set of maps by using the same name but different priority numbers for subsequent crypto map definitions.

To remove a crypto map set from an interface, enter the following command in interface configuration mode:

```
no crypto map [name]
```

Figure 444. Cisco - delete crypto map set command

5. Finally, check your IPSec configuration to see if all went well:

```
show crypto transform-set  
show crypto map
```

Figure 445. Cisco - show defined transform sets and crypto map commands

17.2.4 Connection verification

IKE policies are activated as soon as a request for negotiation is received from an IKE peer, or as soon as traffic reaches the router for which IPSec has to be applied and an SA does not already exist. To verify that IKE negotiations have been successful, enter the following command (in enable mode):

```
show crypto isakmp sa
```

Figure 446. Cisco - show active ISAKMP SAs command

To verify that IPSec traffic is being processed as defined, enter the following command:

```
show crypto ipsec sa
```

Figure 447. Cisco - show active IPSec SAs command

To take down an ISAKMP SA, use the connection ID that you got from the `show crypto isakmp sa` command and issue:


```
clear crypto isakmp [ID]
```

Figure 448. Cisco - Delete an ISAKMP SA command

To take down an IPsec SA, use the connection ID that you got from the `show crypto ipsec sa` command and issue:

```
clear crypto sa [peer] [map] [entry] [counters]
```

Figure 449. Cisco - Delete an IPsec SA command

The options of this command are as follows:

- No option specified deletes all IPsec SAs.
- The `peer` option, followed by either an IP address or an FQDN, clears all IPsec SAs between the router and that peer.
- The `map` option, followed by a crypto map set name, clears all IPsec SAs protected by that crypto map set.
- The `entry` option, followed by a destination IP address, an IPsec protocol (AH and ESP) and an SPI number, clears only a particular IPsec SA.

In any case, deleting an IPsec SA also deletes all other IPsec SAs that were established by the same IKE negotiation.

17.3 IBM 2216 to Cisco 2612, gateway-to-gateway

In this scenario, we are presenting one branch office that needs to access the central site network over the Internet. The branch office will access all resources in the central site and will be treated as a part of the network.

17.3.1 Scenario characteristics

- The branch office will access all resources on the central site. Therefore, a gateway-to-gateway VPN tunnel solution is appropriate. With this solution, any host on the central site will be able to access the branch office and any host on the branch office will be able to access the central site using a VPN tunnel secured by the IPsec protocol.
- Both networks are connected to the Internet through routers. The gateway-to-gateway VPN tunnel will be implemented between the central site router and the branch office router.

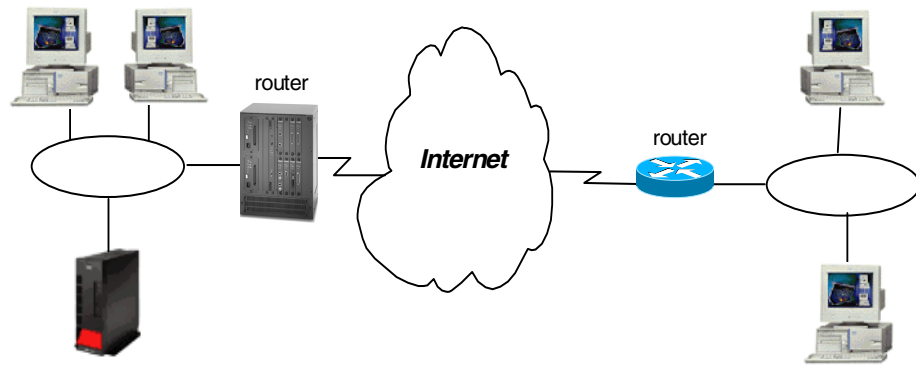


Figure 450. Branch office VPN solutions - small enterprise gateway-to-gateway solution

17.3.1.1 Scenario objectives

The objectives of this scenario are:

- All traffic between the branch office and the central site must be protected by IPSec.
- All the users in the branch office can access all the resources in the central site's network and vice versa.
- The data traffic can flow in the clear in both internal networks behind the VPN gateways. The central site and the branch office belong to the same company.

17.3.1.2 Scenario network configuration

Figure 451 shows our simple network configuration for the gateway-to-gateway VPN tunnel between an IBM 2216 and a Cisco 2612 router.

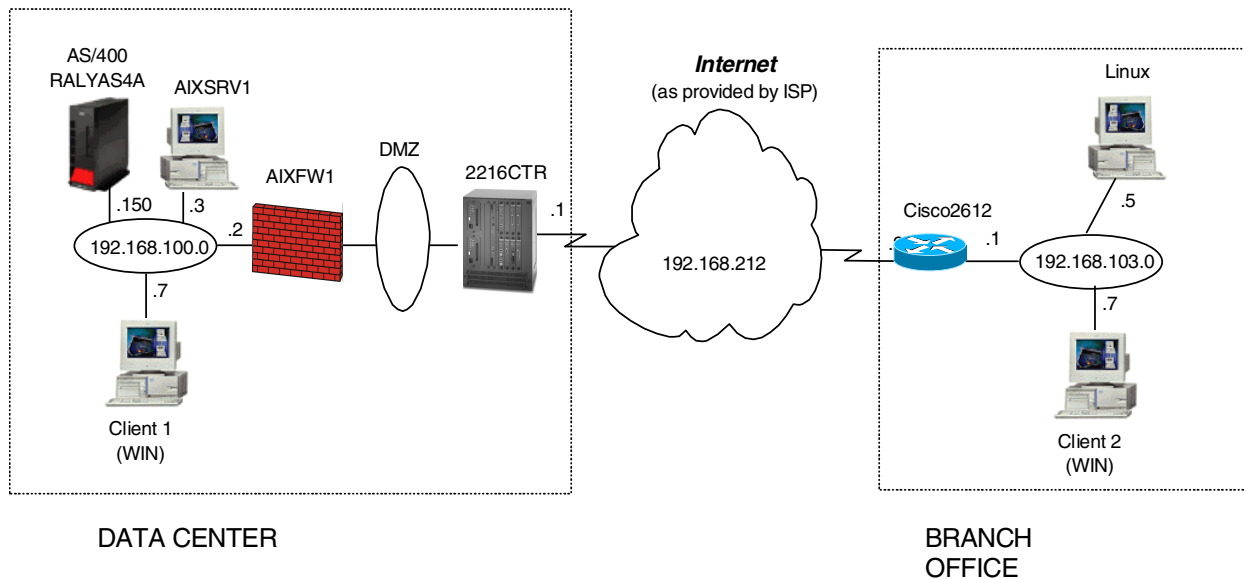


Figure 451. IBM 2216 to Cisco 2612: gateway-to-gateway scenario

17.3.2 Implementation tasks - summary

The following is a summary of 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 the planning worksheets for the two routers.
3. Configure VPN tunnels in the routers.
4. Start the VPN connection.
5. Perform verification tests.

17.3.2.1 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 172.16.3.7
```

2. Repeat the PING in the reverse direction from PC2 at the branch office to PC1 at the data center:

```
PING 192.168.100.7
```

Both tests must succeed before you can continue. In a real Internet environment, there might be routers along the way disallowing the PING command.

17.3.3 Completing the IBM 2216 router planning worksheet

Complete the IBM 2216 router planning worksheets as shown in Table 86 through Table 94. The planning worksheets allow you to gather all the configuration data

before the actual implementation. We completed the planning worksheets from the perspective of central site router in this scenario.

Table 86. IBM 2216 router configuration - Remote user definitions

| Information you need to create your VPN | Center Router |
|--|-------------------------|
| How to identify the remote IKE peer (user): 1: IP address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID | Option 1: IP-address |
| IP Address that distinguishes this user? | 192.168.212.2 |
| Authenticate user with: 1: Pre-shared key? 2: Public certificate? | pre-shared key |
| Mode in which you will enter the pre-shared key: 1: ASCII 2: HEX | Option 1: ASCII |
| Pre-shared key (even number of characters) | 12345678 |

Table 87. Policy definitions

| Information you need to create your VPN | Center Router |
|--|------------------------------|
| Policy name | ike-pre-100-103-cisco |
| Priority of this policy in case of multiple policies | 6 |

Table 88. IBM 2216 router configuration - definition of the policy profile

| Information you need to create your VPN | Center Router |
|--|----------------------------|
| Profile name | 100.0-103.0-pre |
| Source address format 1: NetMask 2: Range 3: Single address | NetMask |
| IPv4 Source address | 192.168.100.0 |
| IPv4 Source Mask (255.255.255.0) | 255.255.255.0 |
| Destination address format 1: NetMask 2: Range 3: Single address | NetMask |
| Destination address | 192.168.103.0 |
| IPv4 Destination Mask (255.255.255.0) | 255.255.255.0 |
| Select the protocol to filter on 1: TCP 2: UDP 3: All protocols 4: Specify range | Option 3: All protocols |
| Starting value for the source port? 0 for all protocols | 0 |

| Information you need to create your VPN | Center Router |
|--|---|
| 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 1: Local tunnel endpoint address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID (any string) | Option 1: local tunnel endpoint address |
| Any user within profile allowed access? | Yes |
| Do you want to limit this profile to specific interface(s)? | No |

Table 89. IBM 2216 router configuration - Definition of Policy validity profile

| Information you need to create your VPN | Center Router |
|--|---------------------|
| Validity profile name | option 1: always |
| Enter the lifetime of this policy yyymmddhhmmss:yyymmddhhmmss or * 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 90. IBM 2216 router configuration - Definition of IPSec action profile Phase 2

| Information you need to create your VPN | Center Router |
|---|----------------|
| IPSec action profile name | tun-212 |
| Select the IPSec security action type: 1: Block 2: Permit | permit |

| Information you need to create your VPN | Center Router |
|---|---------------|
| Should the traffic flow into a secure tunnel or in the clear? 1: Clear 2: Secure tunnel | Secure tunnel |
| What is the tunnel startpoint IP address? | 192.168.212.1 |
| What is the tunnel endpoint IP address? | 192.168.212.2 |
| Does this IPSec tunnel flow within another IPSec tunnel? | No |
| Percentage of SA life-size/lifetime to use as the acceptable minimum? Default is 75% | 75 |
| Security association refresh threshold in percent Default is 85% | 85 |
| Select the option for the DF bit in the outer header 1: Copy 2: Set 3: Clear | Copy |
| Do you want to enable replay prevention? | Disable |
| Do you want to negotiate the security association at system initialization (autostart)? | No |

Table 91. IBM 2216 router configuration - IPSec proposal

| Information you need to create your VPN | Center Router |
|--|----------------|
| What name do you want to give this IPSec proposal? | esp-cisco-prop |
| 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 92. IBM 2216 router configuration - IPSec transform for IKE Phase 2

| Information you need to create your VPN | Center Router |
|---|------------------------|
| IPSec ESP transform name | espTunnelMD5andDES |
| Select the protocol ID: 1: IPSec AH 2: IPSec ESP | Option 2: IPSec ESP |
| Select the encapsulation mode: 1: Tunnel 2: Transport | Option 1: Tunnel |

| Information you need to create your VPN | Center Router |
|---|-----------------------|
| Select the ESP authentication algorithm: 1: HMAC_MD5 2: HMAC_SHA | Option 2: HMAC_MD5 |
| Select the ESP cipher algorithm: 1: ESP DES 2: ESP 3DEC 3: ESP CDMF 4: ESP NULL | Option 1: ESP DES |
| What is the SA life-size, in kilobytes? Default is 50000 kilobytes | 50000 |
| What is the SA lifetime? Default is 3600 sec | 3600 |

Table 93. IBM 2216 router configuration - definitions for ISAKMP action for IKE Phase 1

| Information you need to create your VPN | Center Router |
|--|-------------------|
| ISAKMP action name | ike-cisco |
| Select the ISAKMP exchange mode: 1: Main 2: Aggressive | Option 1: Main |
| Percentage of SA life-size/lifetime to use as the acceptable minimum: Default is 75 % | 75 |
| What is the ISAKMP connection life-size, in kilobytes? Default is 5000 kilobytes | 5000 |
| What is the ISAKMP connection lifetime in seconds? Default is 30000 sec | 28800 |
| Do you want to negotiate the SA at system initialization (autostart)? | Yes |

Table 94. IBM 2216 router configuration - definitions for ISAKMP proposal for IKE Phase 2

| Information you need to create your VPN | Center Router |
|---|-----------------------------|
| ISAKMP proposal name: | ike-cisco-prop |
| Select the authentication method 1: Pre-shared key 2: Digital certificate | Option 1: Pre-shared key |
| Select the hashing algorithm 1: MD5 2: SHA | Option 1: MD5 |
| Select the cipher algorithm 1: DES 2: 3DES | Option 1: DES |

| Information you need to create your VPN | Center Router |
|--|--|
| What is the SA life-size, in kilobytes? Default is 1000 kilobytes | 1000 |
| What is the SA lifetime? Default is 15000 sec | 28800 |
| Select the Diffie-Hellman Group ID 1: Diffie-Hellman Group 1 2: Diffie-Hellman Group 2 | Option 1: Diffie-Hellman Group 1 |
| Do you wish to map a DiffServ Action to this policy? | No |
| What will the status of the policy be? 1: Enabled 2: Disabled | Option 1: Enabled |

17.3.4 Configuring the VPN in the IBM 2216 router

In this section we will give only necessary configuration information for this particular scenario, herein this part. Please refer to 12.2, “Configuring IPsec on an Nways router” on page 309 for more details on IPsec VPN tunnel configuration on IBM Routers.

Perform the following steps to configure a gateway-to-gateway VPN on the central site router. Unless otherwise specified use the default values.

1. Use `add user` command in the policy feature to add a user and use the following values:
 - User identification type: **IP Address**
 - IP address of the user: **192.168.212.2**
 - Pre-shared key: **12345678**
2. If you have not defined a validity period, you can do that using the `add validity-period` command. In all our scenarios, we have defined a period that enables the policy for all times:
 - Validity-period name: **always**
 - Duration: **Forever**
 - Months: **All**
 - Days: **All**
 - Hours: **All Day**
3. Use the `add isakmp-proposal` command in the policy feature to add an isakmp-proposal for the ISAKMP action and use the following values:
 - ISAKMP proposal name: **ike-cisco-prop**
 - Authentication Method: **Pre-shared Key**
 - Hashing Algorithm: **MD5**
 - Cipher Algorithm: **DES**
4. Use the `add isakmp-action` command in the policy feature to add an isakmp-action and use the following values:
 - ISAKMP action name: **ike-cisco**

- ISAKMP action mode: **Main**
 - ISAKMP proposal to be used: **ike-cisco-prop**
5. Use the `add ipsec-transform` command in the policy feature to add an ipsec-transform to be used for IPsec proposal and use the following values:
 - IPsec transform name: **espTunnelMD5andDES**
 - Protocol ID: **IPSEC ESP**
 - Encapsulation Mode: **Tunnel**
 - IPsec Authentication Algorithm: **HMAC-MD5**
 - ESP Cipher Algorithm: **ESP DES**
 - SA Life-size, in Kilobytes: **50000**
 - SA Lifetime: **3600**
 6. Use the `add ipsec-proposal` command in the policy feature to add an IPsec proposal to be used for IPsec action and use the following values:
 - IPsec proposal name: **esp-cisco-prop**
 - Use PFS: **No**
 - Use AH: **No**
 - Use ESP: **Yes**
 - Name of the IPsec transform to be used: **espTunnelMD5andDES**
 7. Use the `add ipsec-action` command in the policy feature to add an IPsec action to be used for the tunnel profile and use the following values:
 - IPsec action name: **tun-212**
 - IPsec security action type: **permit**
 - Traffic flow into a secure tunnel or clear: **Secure Tunnel**
 - Tunnel start point IPv4 address: **192.168.212.1**
 - Tunnel endpoint IPv4 address: **192.168.212.2**
 - Options for DF bit in the outer header: **Copy**
 - Enable replay prevention: **No**
 - Name of the IPsec proposal to be used: **esp-cisco-prop**
 8. Use the `add profile` command in the policy feature to add a profile to be used for the policy pertaining to the tunnel and use the following values:
 - Profile name: **100.0-103.0-pre**
 - Source Address Format: **Netmask**
 - IPv4 Source Address: **192.168.100.0**
 - IPv4 Source Mask: **255.255.255.0**
 - Destination Address Format: **Netmask**
 - IPv4 Destination Address: **192.168.103.0**
 - IPv4 Destination Mask: **255.255.255.0**
 - Protocol IDs: **All Protocols**
 - Configure local and remote IDs for ISAKMP: **Yes**

- Identification to send to remote: **Local Tunnel Endpoint Address**
 - IPSec action to be used for this profile: **tun-212**
9. Use the `add policy` command to define a policy and use the following values:
- Policy name: **ike-pre-100-103-cisco**
 - Profile name to be used for this policy: **100.0-103.0-pre**
 - Validity-period name to be used for this policy: **always**
10. Reload the router for the changes to take effect.

17.3.5 Completing the Cisco router planning worksheet

Complete the Cisco router planning worksheets as shown in Table 95 through Table 101. The planning worksheets allow you to gather all the configuration data before the actual implementation. We completed the planning worksheets from the perspective of a Cisco router in this scenario.

Table 95. Cisco 2612 router configuration - ISAKMP policy definitions

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Priority of this policy in case of multiple policies | 10 |
| Encryption algorithm | DES |
| Hash algorithm | MD5 |
| Authentication mode | pre-share |
| Lifetime | 28800 |
| Diffie-Hellman group | 1 (default) |

Table 96. Cisco 2612 router configuration - ISAKMP identity

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Identity of ISAKMP peer for pre-shared key | IP address |

Table 97. Cisco 2612 router configuration - ISAKMP pre-shared key

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Pre-shared key string | 12345678 |
| ISAKMP peer for which this key will be used | 192.168.212.1 |

Table 98. Cisco 2612 - extended IP access list

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Access-list number | 102 |
| Action | permit |
| Protocols | ip |
| Source address | 192.168.103.0 |

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Source mask | 0.0.0.255 |
| Destination address | 192.168.100.0 |
| Destination mask | 0.0.0.255 |

Note: Cisco interprets subnet masks differently in order to indicate a range of addresses.

Table 99. Cisco 2612 router configuration - IPSec transform set

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Transform set name | center1 |
| IPSec encryption protocol and transform | esp-des |
| IPSec authentication protocol and transform | esp-md5-hmac |
| Mode | tunnel (default) |

Table 100. Cisco 2612 router configuration - crypto map entry

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Priority of this crypto map entry in case of multiple crypto map entries in the same crypto map set | 10 |
| Crypto map set name | Cisco-Center1 |
| Type of security for this crypto map | ipsec-isakmp |
| Access list number against which addresses are mapped for which traffic has to be protected | 102 |
| IPSec transform set to be used with this crypto map entry | center1 |
| ISAKMP peer for which this IPSec protection will be used | 192.168.212.1 |
| SA lifetime (seconds) | 3600 |
| Use PFS? | no (default) |

Table 101. Cisco 2612 router configuration - interface IPSec configuration

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Interface to which crypto map is applied | Ethernet0/0 |
| Crypto map to be applied | Cisco-Center1 |

17.3.6 Configuring the VPN in the Cisco router

Connect to the router using the console. Configure an IKE policy, type of identification, and pre-shared key to be used in conjunction with the IBM 2216:

```

cisco-2612#
cisco-2612#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cisco-2612 (config)#
cisco-2612 (config)#crypto isakmp policy 10
cisco-2612 (config-isakmp)#encryption des
cisco-2612 (config-isakmp)#hash md5
cisco-2612 (config-isakmp)#authentication pre-share
cisco-2612 (config-isakmp)#lifetime 28800
cisco-2612 (config-isakmp)#exit
cisco-2612 (config)#
cisco-2612 (config)#crypto isakmp identity address
cisco-2612 (config)#
cisco-2612 (config)#crypto isakmp key 12345678 address 192.168.212.1
cisco-2612 (config)#

```

Figure 452. Cisco - Add ISAKMP policy

Create the following items for IPsec:

- Access list
- Transform set
- Crypto map

```

cisco-2612 (config)#access-list 102 permit ip 192.168.103.0 0.0.0.255 192.168.100.0 0.0.0.255
cisco-2612 (config)#
cisco-2612 (config)#crypto ipsec transform-set center1 esp-des esp-md5-hmac
cisco-2612 (cfg-crypto-trans)#
cisco-2612 (cfg-crypto-trans)#crypto map Cisco-Center1 10 ipsec-isakmp
cisco-2612 (config-crypto-map)#match address 102
cisco-2612 (config-crypto-map)#set transform-set center1
cisco-2612 (config-crypto-map)#set peer 192.168.212.1
cisco-2612 (config-crypto-map)#set security-association lifetime seconds 3600
cisco-2612 (config-crypto-map)#exit
cisco-2612 (config)#^Z
cisco-2612#

```

Figure 453. Cisco - Add access list, transform set, and crypto map for IPsec

Check that the configuration above is correct.

```

cisco-2612#show access-list

Extended IP access list 102
  permit ip 192.168.103.0 0.0.0.255 192.168.100.0 0.0.0.255
cisco-2612#
cisco-2612#show crypto ipsec transform-set
Transform set center1: { esp-des esp-md5-hmac }
  will negotiate = { Tunnel, },

cisco-2612#
cisco-2612#show crypto map
Crypto Map "Cisco-Center1" 10 ipsec-isakmp
Peer = 192.168.212.1
Extended IP access list 102
  access-list 102 permit ip 192.168.103.0 0.0.0.255 192.168.100.0 0.0.0.255
Current peer: 192.168.212.1
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ center1, }

cisco-2612#

```

Figure 454. Cisco - check new IPSec configuration

Apply the crypto map to an interface, in our case, ethernet0/0:

```

cisco-2612#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cisco-2612(config)#interface ethernet0/0
cisco-2612(config-if)#crypto map Cisco-Center1
cisco-2612(config-if)#exit
cisco-2612(config)#^Z
cisco-2612#

```

Figure 455. Cisco - assign crypto map to interface

At this point, you may want to take a look at the entire router configuration using the `show running` command. If everything is fine, save your configuration.

17.3.7 Connection verification

IKE policies are activated as soon as the configuration is reloaded. To verify that IKE negotiations have been successful, enter the following command in talk 5 mode at the IBM 2216 router:

```
feature ipsec->ipv4->list tunnel active
```

To verify that the IPSec policy is being processed as defined, enter the following command:

```
feature policy->list stats
```

```
Center Policy console>LIST STATS
+-----+
|Name                                         |Hits |
+-----+
|ike-pre-100-103-cisco.plout                |    2|
|   ike-cisco                               |(ISAKMP) |    2|
+-----+
|ike-ds-211-211.plout                       |    1|
|   ds-act1                                 |(ISAKMP) |    2|
+-----+
|ike-ds-211-211.plin                        |    1|
|   ds-act1                                 |(ISAKMP) |    2|
+-----+
|ike-pre-100-103-cisco.traffic              |    34|
|                                         tun-212 (IPSEC) |    66|
+-----+
|ike-ds-211-211.traffic                     |   183|
|                                         tun-101-102-ds (IPSEC) |   365|
+-----+
|ike-pre-100-103-cisco.inBoundTunnel        |    31|
|   ipsecPermitIfInboundTunnel (IPSEC)     |    31|
+-----+
```

Figure 456. 2216 - Verifying IPSec policy

To verify that IPSec traffic is being processed as defined, enter the following command:

```
feature ipsec->ipv4->list stats
```

```
Center 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
-----
          141           0           141       17744       8872       8872

Sent:
total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
-----
          174           0           174       13904           0       13904

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 457. 2216 - Verifying IPSec traffic

To take down an IPSec tunnel, use the tunnel ID that you got from the list tunnel active command and issue:

```
disable tunnel [ID]
```

Use the Cisco router console to verify that the IKE connection is successfully established by entering the command `sh cry isa sa`.

```
cisco-2612#sh cry isa sa
      dst          src          state          conn-id  slot
192.168.212.1  192.168.212.2  QM_IDLE        14       0
cisco-2612#
```

Figure 458. Verifying the VPN connection status on the Cisco router

Use the Cisco router console command `show crypto ipsec sa` to display the VPN tunnel traffic statistics.

17.3.8 Verification tests

Table 102 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 17.3.1.1, “Scenario objectives” on page 514.

Table 102. Verification test - 2216 to Cisco router gateway to gateway scenario

| Direction | TELNET | FTP | PING | TFTP |
|--|--------|-----|------|------|
| From 2216 subnet to Cisco subnet hosts | YES | YES | YES | YES |
| From Cisco subnet hosts to 2216 subnet | YES | YES | YES | YES |

17.4 IBM AS/400 to Cisco 2612, gateway-to-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 at both networks are allowed to access all systems and applications on the remote network. Figure 459 on page 528 represents this scenario.

17.4.1 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 Cisco 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 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 nonsecure interface.

- TOKENRING1 connects the gateway to the internal data center network and represents the secure interface. See Figure 460 on page 529.

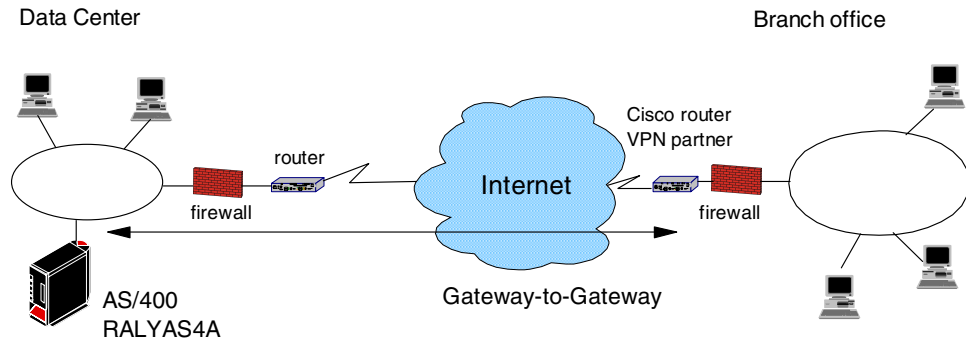


Figure 459. Branch office VPN - gateway-to-gateway AS/400 system to Cisco router

Note

For a higher level of security, the Cisco VPN partner should be placed on the secure side of the firewall at the branch office.

17.4.1.1 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.

17.4.1.2 Scenario network configuration

Figure 460 shows our simple network configuration for the gateway-to-gateway AS/400 system to Cisco router.

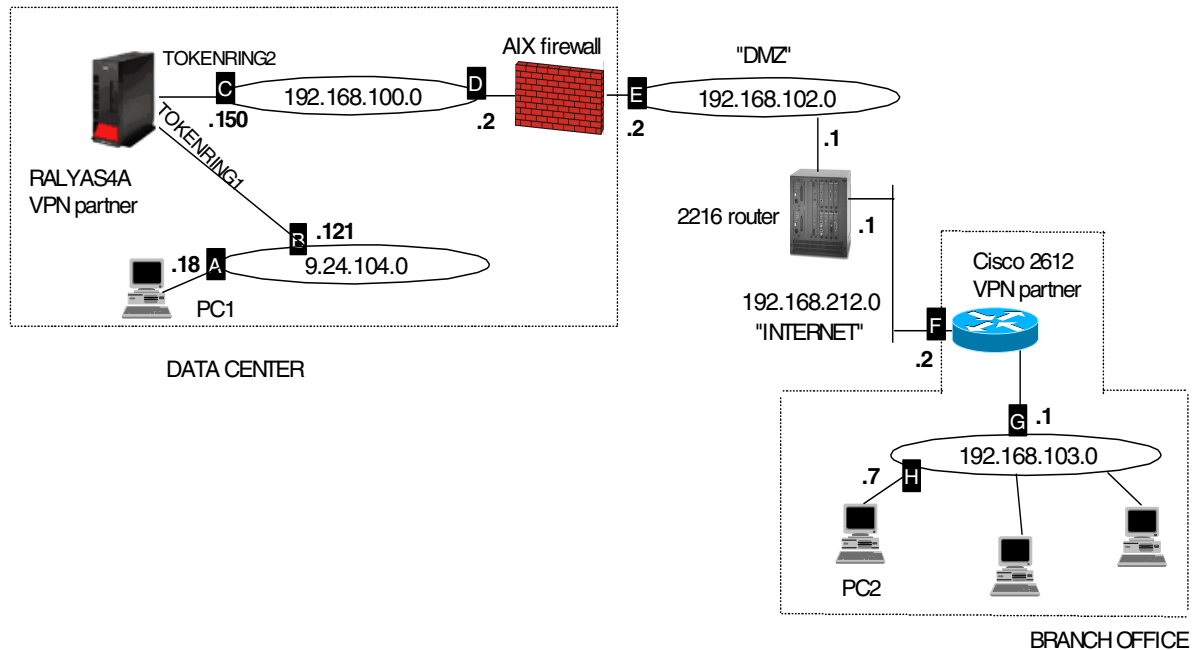


Figure 460. Gateway-to-gateway - OS/400 to Cisco router

17.4.2 Implementation tasks - summary

The following is a summary of 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 the planning worksheets for the Cisco router.
3. Complete the planning worksheets for the AS/400 system.
4. Configure a VPN in the Cisco router.
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.

17.4.2.1 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the data center and the branch office network are correct.

1. From PC1 in the data center network, PING PC2 at the branch office. Enter the following PING command:

```
PING 192.168.103.7
```

2. Repeat the PING in the reverse direction from PC2 at the branch office to PC1 at the data center:

```
PING 9.24.104.18
```

Both tests must succeed before you can continue. In a real Internet environment, there might be routers along the way disallowing the PING command.

17.4.3 Completing the Cisco router planning worksheet

Complete the Cisco router planning worksheets as shown in Table 103 through Table 109. The planning worksheets allow you to gather all the configuration data before the actual implementation. We completed the planning worksheets from the perspective of a Cisco router in this scenario.

Table 103. Cisco 2612 router configuration - ISAKMP policy definitions

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Priority of this policy in case of multiple policies | 10 |
| Encryption algorithm | DES |
| Hash algorithm | MD5 |
| Authentication mode | pre-share |
| Lifetime | 28800 |
| Diffie-Hellman group | 1 (default) |

Table 104. Cisco 2612 router configuration - ISAKMP identity

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Identity of ISAKMP peer for pre-shared key | IP address |

Table 105. Cisco 2612 router configuration - ISAKMP pre-shared key

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Pre-shared key string | 24681012 |
| ISAKMP peer for which this key will be used | 192.168.100.150 |

Table 106. Cisco 2612 - Extended IP access list

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Access list number | 103 |
| Action | permit |
| Protocols | ip |
| Source address | 192.168.103.0 |
| Source mask | 0.0.0.255 |
| Destination address | 9.24.104.0 |
| Destination mask | 0.0.0.255 |

Note that Cisco interprets subnet masks differently in order to indicate a range of addresses.

Table 107. Cisco 2612 router configuration - IPSec transform set

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Transform set name | itso1 |
| IPSec encryption protocol and transform | esp-des |
| IPSec authentication protocol and transform | esp-md5-hmac |
| Mode | tunnel (default) |

Table 108. Cisco 2612 router configuration - crypto map entry

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Priority of this crypto map entry in case of multiple crypto map entries in the same crypto map set | 11 |
| Crypto map set name | Cisco-Center1 |
| Type of security for this crypto map | ipsec-isakmp |
| Access list number against which addresses are mapped for which traffic has to be protected | 103 |
| IPSec transform set to be used with this crypto map entry | itso1 |
| ISAKMP peer for which this IPSec protection will be used | 192.168.100.150 |
| SA lifetime (seconds) | 3600 |
| Use PFS? | no (default) |

Table 109. Cisco 2612 router configuration - interface IPSec configuration

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Interface to which crypto map is applied | Ethernet0/0 |
| Crypto map to be applied | Cisco-Center1 |

17.4.4 Completing the AS/400 system planning worksheet

Complete the AS/400 system planning worksheets as shown in Table 110 and Table 111. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 110. Planning worksheet - New Connection Wizard - RALYAS4A

| This information is 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 | gateway-to-gateway |
| What is the name of the connection group? | AS4AtoCiscoGW |
| 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? | 192.168.212.2 |
| What is the pre-shared key? | 24681012 |
| 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 110) 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 *AS4AtoCiscoGW*, and the pre-shared key is a random string of characters, *24681012*.

Table 111. 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 remote 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 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 address(es)? Use this name as the <i>source address</i> on the IPSEC filter | 9.24.104.0 |
| | 255.255.255.0 |
| | AS4Asubnet |
| If the remote 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 address(es)? Use this name as the <i>destination address</i> on the IPSEC filter | 192.168.103.0 |
| | 255.255.255.0 |
| | Ciscosubnet |
| 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 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 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 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> . | |

We also completed the IP filter rules planning worksheet (Table 111) from the perspective of RALYAS4A. The filter rules allowed traffic between any 9.24.104.* address on the local network and any 192.168.103.* 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 AS4ASubnet and the remote subnet is Ciscosubnet. 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 were activated, they allowed only 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 from and to the internal network since no filter rules are activated on TOKENRING1.

17.4.5 Configuring the VPN in the Cisco router

Connect to the router using the console. Check existing IKE policies and connections. This also verifies that IKE is enabled.

```
cisco-2612>enable
Password:
cisco-2612#show crypto isakmp policy
Default protection suite
encryption algorithm:DES - Data Encryption Standard (56 bit keys) .
hash algorithm:Secure Hash Standard
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#1 (768 bit)
lifetime:86400 seconds, no volume limit
cisco-2612#
cisco-2612#show crypto isakmp sa
      dst          src          state          conn-id  slot
cisco-2612#
```

Figure 461. Cisco - show default IKE (ISAKMP) setup

Configure an IKE policy, type of identification, and pre-shared key to be used in conjunction with RALYAS4A:

```

cisco-2612#
cisco-2612#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cisco-2612(config)#
cisco-2612(config)#crypto isakmp policy 10
cisco-2612(config-isakmp)#encryption des
cisco-2612(config-isakmp)#hash md5
cisco-2612(config-isakmp)#authentication pre-share
cisco-2612(config-isakmp)#lifetime 28800
cisco-2612(config-isakmp)#exit
cisco-2612(config)#
cisco-2612(config)#crypto isakmp identity address
cisco-2612(config)#
cisco-2612(config)#crypto isakmp key 24681012 address 192.168.100.150
cisco-2612(config)#
cisco-2612(config)#exit
cisco-2612#

```

Figure 462. Cisco - add ISAKMP policy

Check your IKE policy configuration:

```

cisco-2612#show crypto isakmp policy
Protection suite of priority 10
encryption algorithm:DES - Data Encryption Standard (56 bit keys).
hash algorithm:Message Digest 5
authentication method:Pre-shared key
Diffie-Hellman group:#1 (768 bit)
lifetime:28800 seconds, no volume limit
Default protection suite
encryption algorithm:DES - Data Encryption Standard (56 bit keys).
hash algorithm:Secure Hash Standard
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#1 (768 bit)
lifetime:86400 seconds, no volume limit
cisco-2612#

```

Figure 463. Cisco - check new IKE (ISAKMP) setup

Create the following items for IPSec:

- Access list
- Transform set
- Crypto map

```

cisco-2612#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cisco-2612(config)#access-list 103 permit ip 192.168.103.0 0.0.0.255 9.24.104.0 0.0.0.255
cisco-2612(config)#
cisco-2612(config)#crypto ipsec transform-set itsol esp-des esp-md5-hmac
cisco-2612(cfg-crypto-trans)#
cisco-2612(cfg-crypto-trans)#crypto map Cisco-Center1 11 ipsec-isakmp
cisco-2612(config-crypto-map)#match address 103
cisco-2612(config-crypto-map)#set transform-set itsol
cisco-2612(config-crypto-map)#set peer 192.168.100.150
cisco-2612(config-crypto-map)#set security-association lifetime seconds 3600
cisco-2612(config-crypto-map)#exit
cisco-2612(config)#^Z
cisco-2612#

```

Figure 464. Cisco - Add access list, transform set, and crypto map for IPSec

In this case, we have used the same crypto map name (Cisco-Center1) that we have used in a previous example, but here we used a different priority, transform set and peer address. In doing so, we can use multiple crypto maps on the nonsecure interface (ethernet0/0).

Check that the configuration above is correct:

```

cisco-2612#show access-list

Extended IP access list 103
  permit ip 192.168.103.0 0.0.0.255 9.24.104.0 0.0.0.255
cisco-2612#
cisco-2612#show crypto ipsec transform-set
Transform set center1: { esp-des esp-md5-hmac }
  will negotiate = { Tunnel, },

Transform set itsol: { esp-des esp-md5-hmac }
  will negotiate = { Tunnel, },

cisco-2612#
cisco-2612#show crypto map
Crypto Map "Cisco-Center1" 10 ipsec-isakmp
Peer = 192.168.212.1
Extended IP access list 102
  access-list 102 permit ip 192.168.103.0 0.0.0.255 192.168.100.0 0.0.0.255
Current peer: 192.168.212.1
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ center1, }

Crypto Map "Cisco-Center1" 11 ipsec-isakmp
Peer = 192.168.100.150
Extended IP access list 103
  access-list 103 permit ip 192.168.103.0 0.0.0.255 9.24.104.0 0.0.0.255
Current peer: 192.168.100.150
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ itsol, }

cisco-2612#

```

Figure 465. Cisco - Check new IPSec configuration

Apply the crypto map to an interface, in our case, ethernet0/0:

```
cisco-2612#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cisco-2612(config)#interface ethernet0/0
cisco-2612(config-if)#crypto map Cisco-Center1
cisco-2612(config-if)#exit
cisco-2612(config)#^Z
cisco-2612#
```

Figure 466. Cisco - assign crypto map to interface

At this point, you may want to take a look at the entire router configuration using the `show running` command.

```
!
crypto isakmp policy 10
  hash md5
  authentication pre-share
  lifetime 28800
crypto isakmp key 12345678 address 192.168.212.1
crypto isakmp key 24681012 address 192.168.100.150
!
!
crypto ipsec transform-set center1 esp-des esp-md5-hmac
crypto ipsec transform-set itsol esp-des esp-md5-hmac
!
!
crypto map Cisco-Center1 10 ipsec-isakmp
  set peer 192.168.212.1
  set transform-set center1
  match address 102
crypto map Cisco-Center1 11 ipsec-isakmp
  set peer 192.168.100.150
  set transform-set itsol
  match address 103
!
!
!
!
interface Ethernet0/0
  ip address 192.168.212.2 255.255.255.0
  no ip directed-broadcast
  no mop enabled
  crypto map Cisco-Center1
!
```

Figure 467. Cisco - show active configuration - IPSec information

If everything is fine, save your configuration using the following command:

```
cisco-2612#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

cisco-2612#
```

Figure 468. Cisco - saving configuration

17.4.6 Configuring the VPN on the AS/400 system (RALYAS4A)

Perform the following steps to configure a gateway-to-gateway VPN on RALYAS4A:

1. Start AS/400 Operations Navigator from the desktop.
2. Expand the AS/400 system, in this case, **RALYAS4A**. Sign on when prompted.
3. Expand **Network**.
4. Double-click **IP Security** to reveal two server names in the right pane: IP Packet Security and Virtual Private Networking. Both functions must be configured, 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 either be Started or Stopped during the following steps.

5. Double-click **Virtual Private Networking** to start the Virtual Private Networking graphical user interface (GUI).
6. Select **File** from the main menu, and then select **New Connection**.
7. Select **Gateway To Gateway** from the drop-down menu. This starts the New Connection Wizard for a gateway-to-gateway connection.
8. Click **Next** after reading the Welcome window.
9. Enter the Name, `AS4AtoCiscoGW`, for the connection group. Recall that `AS4AtoCiscoGW` is the name from the worksheet in Table 110 on page 532. The name specified here is the name for all objects the wizard creates for this particular connection. It is case-sensitive. Also enter a description of the configuration.
10. Click **Next**.
11. In the Key Policy window, 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 worksheet. The wizard chooses the appropriate encryption and authentication algorithms based on the selection made here.
12. Click **Next**.
13. In 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 Cisco router. Referring to the planning worksheet (Table 110 on page 532) and to the network configuration in Figure 460 on page 529, for RALYAS4A, this is **192.168.100.150** (interface C).
14. Click **Next**.
15. Use the Remote Network window 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 Cisco router with IP address 192.168.212.2. This is interface F in Figure 460 on page 529. Refer also to the planning worksheet in Table 110 on page 532. Specify 24681012 in the pre-shared key parameter. Remember, exactly the same pre-shared key must be entered when configuring VPN on the remote Cisco router.

16. Click **Next**.

17. Use the Data Policy window to specify what 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.

18. Click **Next**.

19. The final window 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**.

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.

17.4.7 Matching the Cisco 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 those of the router. The Virtual Private Networking `New Connection Wizard does not provide the option to allow you to customize the key refresh policies.

To customize the key refresh policies, follow these steps:

1. Expand all the subfolders on the VPN Configuration GUI interface.
2. Click **Key Policies** to display a list of key policies configured on your system. 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.
3. Double-click **AS4AtoCiscoGW** 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**.
5. Change the maximum key lifetime parameter value to 480.
6. Click **OK**.
7. Back at the key policy customization window, click **OK**.

8. Click **Data Policies** to display a list of data policies.
9. Double-click **AS4AtoCiscoGW** to view the data policy for this connection.
10. At the data policy Properties window, select the **General** tab. Uncheck the box for Use Diffie-Hellman perfect forward secrecy.
11. Select the **Proposals** tab. Select the data protection proposal you want to change and click **Edit**.
12. At the Data Protection Proposal window, select the **Key Expiration** tab. Leave the Expire after parameter value as 3600.
13. Click **OK**.
14. Back at the data policy properties window, click **OK**.

You have now completed the VPN configuration for RALYAS4A. You will configure AS/400 IP filtering in the next task.

17.4.8 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 to the connection group created by the wizard. Use IP Packet Security in AS/400 Operations Navigator to configure filters.

1. Configure a defined address for the local subnet that is allowed to use the VPN. The TRUSTED subnet behind the AS/400 gateway is 9.24.104.0; the subnet mask is 255.255.255.0. Refer to the planning worksheet for RALYAS4A in Table 111 on page 533 and to Figure 460 on page 529.
2. Configure a defined address for the remote subnet that is allowed to use the VPN. The UNTRUSTED subnet behind the Cisco router gateway is 192.168.103.0; the subnet mask is 255.255.255.0. Refer to the planning worksheet for RALYAS4A in Table 111 on page 533 and to Figure 460 on page 529.
3. Create two filters rules to allow Internet Key Exchange (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.

1. 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 Cisco router address, `192.168.212.2`, 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.

2. 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 Cisco router address, `192.168.212.2`, is the value in the Source address name field, and the local AS/400 system address, `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.

3. Create a filter rule with action IPsec to define the data endpoints that use the secure tunnel.

Use the same filter set name, `VPNIFC`; the Action is IPsec; the Direction is always set to OUTBOUND and grayed out. The corresponding INBOUND IPSEC rule is created implicitly. Specify **AS4Asubnet** for the Source address name parameter; the Destination address name is **Ciscosubnet**. 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 menu to list all the data connections configured in your system and select one of them. In this scenario, select **AS4AtoCiscoGW**.

4. Select the **Services** tab to specify the protocols and ports allowed in the tunnel. In this scenario, select wildcard (*) in the Protocol, Source port and Destination port fields. This allows any protocol using any port through the secure tunnel.
5. 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.
6. Save the filter file in the IFS. In our scenario, we created a subdirectory, VPNRB, under the directory QIBM.

17.4.9 Starting IP filters

Activate the filter rules. At the IP Packet Security window click **File -> Activate**. The syntax is verified and, if correct, the filters are activated.

After activating the filter rules and before starting the VPN connection, verify the IP connectivity again:

1. From PC1 in the data center network (Figure 460 on page 529) PING PC2 in the remote subnet. Enter the following PING command:

```
PING RMTSYS ('192.168.103.7')
```

The ping request fails.

2. Repeat the test from PC2 in the branch office subnet to PC1 in the data center network:

```
PING 9.24.104.18
```

The ping request fails.

17.4.10 Starting the VPN connection

This section explains how to start the VPN connection. Before starting the connection, verify that the IP filters and the VPN servers are started.

To start the AS4AtoCiscoGW connection, perform the following steps:

1. Highlight the **AS4AtoCiscoGW:L1** connection in the right panel and click the green **Start** button to initiate a VPN connection to the Cisco router (Figure 469).

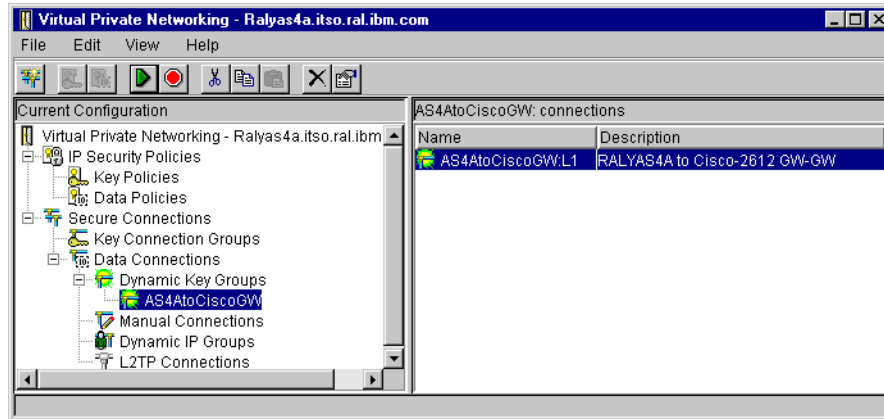


Figure 469. Starting the host-to-gateway connection - AS4AtoCiscoGW

2. Display the connection to verify it is active. At the Virtual Private Networking window, select **View -> Active Connections**.

The Active Connections window is shown in Figure 470:

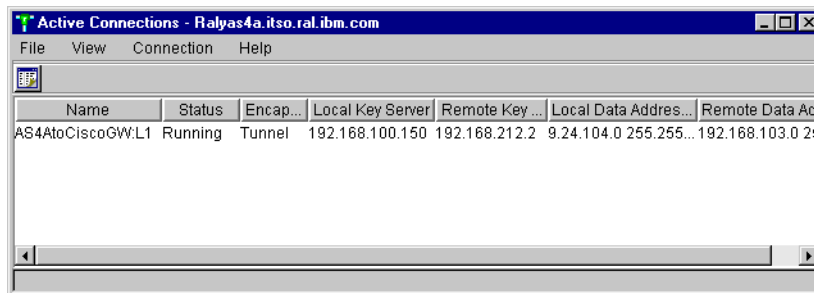


Figure 470. Active Connections window

3. Use the Cisco router console to verify that the IKE connection is successfully established, as shown in Figure 471:

```
cisco-2612#show crypto isakmp sa
      dst          src          state          conn-id  slot
192.168.212.2    192.168.100.150QM_IDLE          127      0
```

Figure 471. Verifying the VPN connection status on the Cisco router

4. Use the Cisco router console command `show crypto ipsec sa` to display the VPN tunnel traffic statistics (see Figure 472).

```

cisco-2612#show cry ipsec sa

interface: Ethernet0/0
  Crypto map tag: Cisco-Center1, local addr. 192.168.212.2

  local ident (addr/mask/prot/port): (192.168.103.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (9.24.104.0/255.255.255.0/0/0)
  current_peer: 192.168.100.150
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 15, #pkts encrypt: 15, #pkts digest 15
    #pkts decaps: 16, #pkts decrypt: 15, #pkts verify 15
    #send errors 0, #recv errors 1

  local crypto endpt.: 192.168.212.2, remote crypto endpt.: 192.168.100.150
  path mtu 1500, media mtu 1500
  current outbound spi: 792BD018

  inbound esp sas:
    spi: 0x162312F0(371397360)
      transform: esp-des esp-md5-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 158, crypto map: Cisco-Center1
      sa timing: remaining key lifetime (k/sec): (4607999/1152)
      IV size: 8 bytes
      replay detection support: Y

  inbound ah sas:

  outbound esp sas:
    spi: 0x792BD018(2032914456)
      transform: esp-des esp-md5-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 159, crypto map: Cisco-Center1
      sa timing: remaining key lifetime (k/sec): (4607999/1143)
      IV size: 8 bytes
      replay detection support: Y

  outbound ah sas:

cisco-2612#

```

Figure 472. Displaying the VPN tunnel traffic statistics on the Cisco router

17.4.11 Verification tests

Table 112 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 17.4.1.1, “Scenario objectives” on page 528.

Table 112. Verification test - OS/400 to Cisco router gateway-to-gateway scenario

| Direction | TELNET | FTP | PING | TFTP |
|--|--------|-----|------|------|
| From AS4A subnet to Cisco subnet hosts | YES | YES | YES | YES |
| From Cisco subnet hosts to RALYAS4A | YES | YES | YES | YES |

17.5 IRE SafeNet VPN Client to Cisco 2612, IPSec over PPP dial-up

This scenario is essentially the same as described in 15.2, “Remote access with IPSec” on page 437. We will focus on the Cisco configuration in this section and

point out the differences in the IPSec client configuration as it pertains to this scenario.

17.5.1 Scenario description

To implement remote access with IPSec, you need a client that supports PPP dial-up and IPSec as well as IKE. Because in most cases the client will get a different IP address from an ISP each time it connects, the IP address cannot be used as the IKE peer identity. Therefore, IKE must either be used in aggressive mode (if pre-shared key authentication has to be used) or with certificate-based authentication (then main mode or aggressive mode can be used). Our environment is based on an IRE SafeNet VPN client dialing into an IBM 2212 router acting as the ISP and then establishing IKE negotiation and IPSec tunnels to a Cisco 2612 router acting as the corporate VPN gateway.

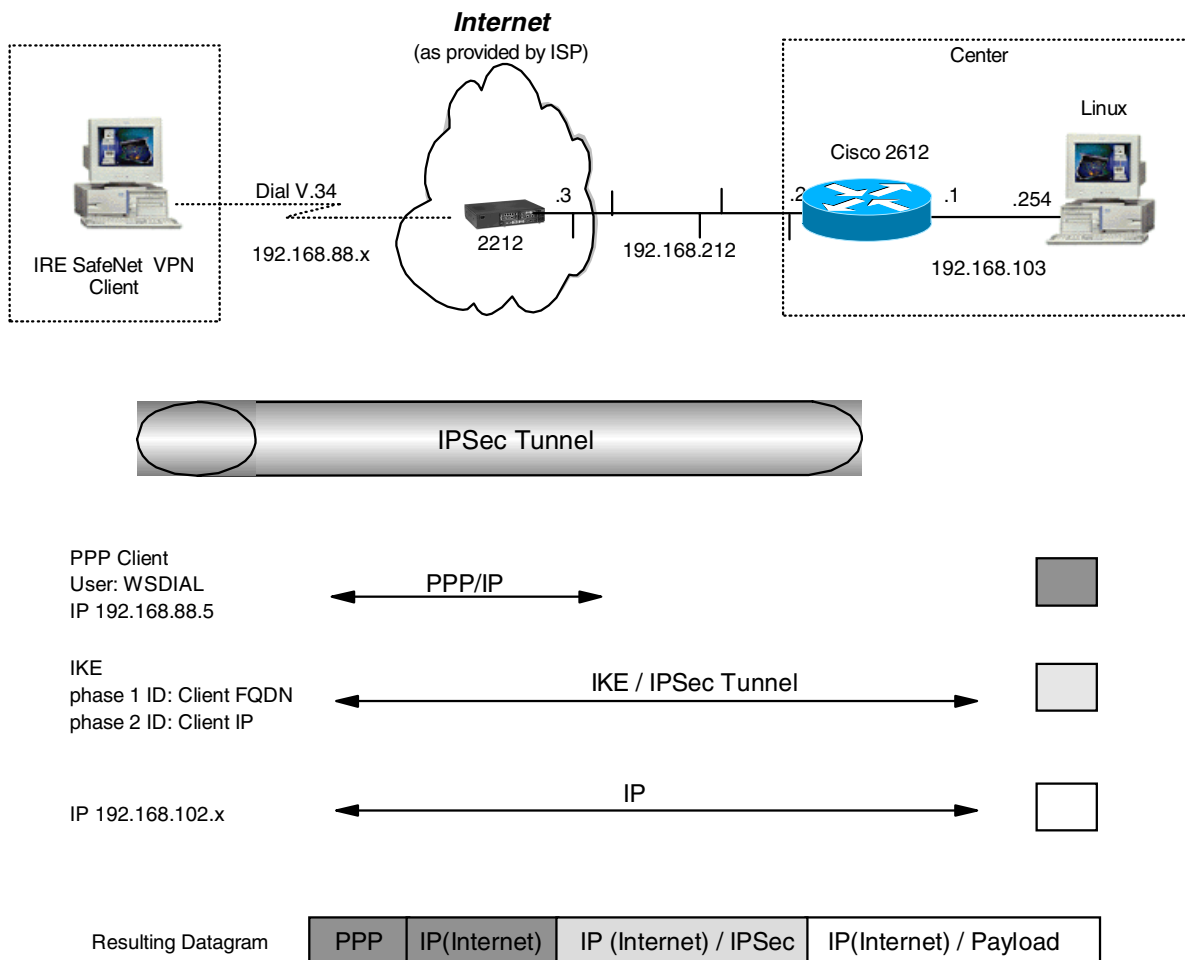


Figure 473. IBM SecureWay VPN client to Cisco router - remote access VPN

In this scenario, the remote client is accessing the secure network with an external IP address. To limit this type of packet on the internal network, we are restricting the client in this scenario to access only one specific server or firewall. In general, access to the whole internal network can be given to a client in this case but it depends on where the VPN gateway is placed relative to the corporate firewall in order to determine how the firewall is to handle this kind of traffic.

Because all client packets arrive via a secure tunnel there is no exposure associated with them other than the general tunnel fear that the client could have been attacked by a cracker and what arrives through the tunnel is malevolent traffic. This is no different from other remote access VPN scenarios.

17.5.2 Configuration of the ISP router

This is the same as described in 15.2.2, “Configuration of the ISP router” on page 439.

17.5.3 Completing the Cisco router planning worksheet

Complete the Cisco router planning worksheets as shown in Table 113 through Table 120. The planning worksheets allow you to gather all the configuration data before the actual implementation. In this scenario we completed the planning worksheets from the perspective of a Cisco router.

Table 113. Cisco 2612 router configuration - ISAKMP policy definitions

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Priority of this policy in case of multiple policies | 10 |
| Encryption algorithm | DES |
| Hash algorithm | MD5 |
| Authentication mode | pre-share |
| Lifetime | 28800 |
| Diffie-Hellman group | 1 (default) |

Table 114. Cisco 2612 router configuration - ISAKMP identity

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Identity of ISAKMP peer for pre-shared key | IP address |

Table 115. Cisco 2612 router configuration - ISAKMP pre-shared key

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Pre-shared key string | 1234567890 |
| ISAKMP peer for which this key will be used | wtr05999 |

Note that using a name rather than an IP address for the ISAKMP peer will force the router to use aggressive mode because of the pre-shared key authentication method.

Table 116. Cisco 2612 - Extended IP access list

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Access list number | 101 |
| Action | permit |
| Protocols | ip |

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Source address | any |
| Destination type | host |
| Destination address | 192.168.103.254 |

Note that since the remote client does not yet have a known IP address but will typically initiate the connection, you have to specify any as the source address for this access list.

Table 117. Cisco 2612 router configuration - IPsec transform set

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Transform set name | ire |
| IPsec encryption protocol and transform | esp-des |
| IPsec authentication protocol and transform | esp-md5-hmac |
| Mode | tunnel (default) |

Table 118. Cisco 2612 router configuration - dynamic crypto map entry

| Information you need to create your VPN | Scenario answers |
|---|------------------|
| Priority of this crypto map entry in case of multiple crypto map entries in the same crypto map set | 10 |
| Dynamic crypto map name | secureint |
| Access list number against which addresses are mapped for which traffic has to be protected | 101 |
| IPsec transform set to be used with this crypto map entry | ire |
| SA lifetime (seconds) | 3600 |
| Use PFS? | no (default) |

A dynamic crypto map is used in this scenario because the IP address of the client is not yet known so a conventional crypto map where the ISAKMP peer has to be specified will not work. However, a crypto map must be defined (see below) because a dynamic map cannot be assigned to an interface directly.

Table 119. Cisco 2612 router configuration - crypto map entry

| Information you need to create your VPN | Scenario answers |
|---|----------------------|
| Priority of this crypto map entry in case of multiple crypto map entries in the same crypto map set | 15 |
| Crypto map set name | secureint |
| Type of security for this crypto map | ipsec-isakmp dynamic |

Table 120. Cisco 2612 router configuration - interface IPSec configuration

| Information you need to create your VPN | Scenario answers |
|--|------------------|
| Interface to which crypto map is applied | Ethernet0/0 |
| Crypto map to be applied | secureint |

17.5.4 Configuring the VPN in the Cisco router

Connect to the router using the console. Configure an IKE policy, type of identification, and pre-shared key to be used in conjunction with the IBM 2216:

```
cisco-2612#
cisco-2612#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cisco-2612(config)#
cisco-2612(config)#crypto isakmp policy 10
cisco-2612(config-isakmp)#encryption des
cisco-2612(config-isakmp)#hash md5
cisco-2612(config-isakmp)#authentication pre-share
cisco-2612(config-isakmp)#lifetime 28800
cisco-2612(config-isakmp)#exit
cisco-2612(config)#
cisco-2612(config)#crypto isakmp identity address
cisco-2612(config)#
cisco-2612(config)#crypto isakmp key 1234567890 hostname wtr05999
cisco-2612(config)#
```

Figure 474. Cisco - add ISAKMP policy

Create the following items for IPSec:

- Access list
- Transform set
- Dynamic crypto map
- Crypto map

```
cisco-2612(config)#access-list 101 permit ip any host 192.168.103.254
cisco-2612(config)#
cisco-2612(config)#crypto ipsec transform-set ire esp-des esp-md5-hmac
cisco-2612(cfg-crypto-trans)#
cisco-2612(cfg-crypto-trans)#crypto dynamic map secureint 10
cisco-2612(config-crypto-map)#match address 101
cisco-2612(config-crypto-map)#set transform-set ire
cisco-2612(config-crypto-map)#set security-association lifetime seconds 3600
cisco-2612(config-crypto-map)#crypto map secureint 15 ipsec-isakmp dynamic secureint
cisco-2612(config-crypto-map)#exit
cisco-2612(config)#^Z
cisco-2612#
```

Figure 475. Cisco - Add access list, transform set, and crypto map for IPSec

Apply the crypto map to an interface, in our case, ethernet0/0:

```
cisco-2612#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cisco-2612 (config)#interface ethernet0/0
cisco-2612 (config-if)#crypto map secureint
cisco-2612 (config-if)#exit
cisco-2612 (config)#^Z
cisco-2612#
```

Figure 476. Cisco - assign crypto map to interface

At this point, you may want to take a look at the entire router configuration using the `show running` command. If everything is fine, save your configuration.

17.5.5 Configuration of the IRE SafeNet VPN Client

This is essentially the same process as described in 15.2.6, “Configuration of the IRE SafeNet VPN Client” on page 449. The only differences are the IP address of the gateway (in this case, the Cisco router’s address is 192.168.212.2) and the value of the pre-shared key.

17.5.6 Testing and verifying the connection

For the VPN client, this is the same process as described in 15.2.7, “Testing and verifying the connection” on page 451.

At the Cisco router, you can use the commands shown in 17.2.4, “Connection verification” on page 512 to verify IKE and IPSec SAs.

17.6 Using digital certificates for IKE authentication

As mentioned before, Cisco routers support IKE authentication based on digital certificates. Those certificates can be requested online from a CA using Cisco’s CEP protocol. We have installed a CA that supports CEP using Entrust CA and VPN Connector. In the example below, we show the necessary commands to request and receive certificates for the router to be used for signatures and encryption. However, we only tested the signature mode with IKE.

Important

To support RSA signature authentication mode with IKE, you must use digital certificates. To support RSA encryption mode with IKE, you do not have to use digital certificates. In that case it is sufficient to create RSA keys and to manually distribute and load them between peers. Though this method offers better security over pre-shared keys and even digital signatures, it has the same scalability problems as the pre-shared key method. We have therefore not tested it in this redbook.

17.6.1 Generating keys and requesting certificates

The steps below explain how to identify the router, the CA, how to generate key pairs, and how to receive a CA certificate:

1. The first step is to specify a local host name and a domain name for the router. If you do not use DNS, you also have to enter a host record for the system where the certificate authority is installed, in our case, 192.168.100.199.

2. Next, you have to create public and private keys, in pairs, to be used for signing and encrypting. You will have to specify the length of the modulus for the keys. Use 512 or 1024 with an Entrust CA.
3. Next, you assign a name to the certificate authority you wish to use. This name has nothing to do with the actual organization name or domain name of the CA; it is merely used as a local identifier by the router. In case of an Entrust CA, you also have to specify additional configuration parameters for the CA, in particular `enrollment mode RA`. You also configure the URL that the router will use to access the CA using CEP, and you specify if you want to use certificate revocation lists with this CA.
4. The next step is to authenticate the CA, which means that you request a CA certificate from it. This certificate is used later to verify certificates from IKE peers during Phase 1 exchanges, provided that those certificates have been issued by the same CA.

The commands for steps 1 to 4 are summarized in Figure 477:

```

Cisco_NAS(config)#hostname Cisco_NAS
Cisco_NAS(config)#ip domain-name itso.ral.ibm.com
Cisco_NAS(config)#ip host ca 192.168.100.199
Cisco_NAS(config)#cry key gen rsa usage
The name for the keys will be: Cisco_NAS.itso.ral.ibm.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  Signature Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]
Choose the size of the key modulus in the range of 360 to 2048 for your
  Encryption Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]

Cisco_NAS(config)#cry ca iden IBM
Cisco_NAS(ca-identity)#enrollment mode ra
Cisco_NAS(ca-identity)#enrollment url http://ca
Cisco_NAS(ca-identity)#crl optional
Cisco_NAS(ca-identity)#exit
Cisco_NAS(config)#cry ca auth IBM
Certificate has the following attributes:
Fingerprint: 46CD5E00 241264A4 7A6EC87A B997603F
% Do you accept this certificate? [yes/no]: y
Cisco_NAS(config)#exit
Cisco_NAS#

```

Figure 477. Cisco - configuration steps for using digital certificates with IKE - part 1

5. It is prudent at this point to check that the CA certificate has arrived properly using the `sh cry ca cert` command. (We are not showing the output of this command at this time.)
6. In the next step you have to request router certificates from the CA. You need to provide information pertaining to the router that you wish to be included in the certificate, such as host name, IP address, and serial number. You also

have to specify a password for the certificate that will be used by the CA administrator if your certificate has to be revoked. The command dialog for this step is shown in Figure 478 on page 550.

Note: Because we are requesting certificates for signing and encryption, we will receive two certificates from the CA.

```
Cisco_NAS(config)#cry ca enroll IBM
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will be: Cisco_NAS.itso.ral.ibm.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 8AC6E50A
% Include an IP address in the subject name? [yes/no]: n
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Cisco_NAS(config)#
  Signing Certificate Reqeust Fingerprint:
    0502E552 1A20FE4A DAD8B8EF 4DF78A84
  Encryption Certificate Request Fingerprint:
    C991DBF3 C2BD73F8 F7E5E99A 0FF97285

2w0d: CRYPTO_PKI: status = 102: certificate request pending

Cisco_NAS(config)#
2w0d: %CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Cisco_NAS(config)#
2w0d: %CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Cisco_NAS(config)#exit
Cisco_NAS#
```

Figure 478. Cisco - configuration steps for using digital certificates with IKE - part 1

7. As illustrated in Figure 479 on page 551 and in Figure 480 on page 552, you can list the certificates that are currently available to the router with the `sh cry ca cert` command. You will see the following certificates for our configuration:

1. A CA certificate
2. A router certificate for signatures
3. A router certificate for encryption (encipherment)
4. An RA certificate for signatures to prove the registration of the router certificate
5. An RA certificate for encryption to prove the registration of the router certificate

```

Cisco NAS#sh cry ca cert
Certificate
  Status: Available
  Certificate Serial Number: 37CFE7CE
  Key Usage: Encryption
  Subject Name
    Name: Cisco_NAS.itso.ral.ibm.com
    Serial Number: 7FFFFFFF
  CRL Distribution Point:
    CN = CRL1, OU = ITSO Raleigh, L = N.C., C = US, O = IBM
  Validity Date:
    start date: 15:51:31 UTC Sep 30 1999
    end   date: 16:21:31 UTC Sep 30 2002

RA Signature Certificate
  Status: Available
  Certificate Serial Number: 37CFE7A6
  Key Usage: Signature
  DN Name
    CN = Martin Murhammer + OID.2.5.4.5 = 21731
    OU = ITSO Raleigh
    L = N.C.
    C = US
    O = IBM
  CRL Distribution Point:
    CN = CRL1, OU = ITSO Raleigh, L = N.C., C = US, O = IBM
  Validity Date:
    start date: 17:45:41 UTC Sep 13 1999
    end   date: 18:15:41 UTC Sep 13 2002

Certificate
  Status: Available
  Certificate Serial Number: 37CFE7CF
  Key Usage: Signature
  Subject Name
    Name: Cisco_NAS.itso.ral.ibm.com
    Serial Number: 7FFFFFFF
  CRL Distribution Point:
    CN = CRL1, OU = ITSO Raleigh, L = N.C., C = US, O = IBM
  Validity Date:
    start date: 15:51:31 UTC Sep 30 1999
    end   date: 16:21:31 UTC Sep 30 2002

```

Figure 479. Cisco - listing digital certificates for use with IKE - part 1

```

CA Certificate
Status: Available
Certificate Serial Number: 37CFE797
Key Usage: Not Set
DN Name
  OU = ITSO Raleigh
  L = N.C.
  C = US
  O = IBM
CRL Distribution Point:
  CN = CRL1, OU = ITSO Raleigh, L = N.C., C = US, O = IBM
Validity Date:
  start date: 14:52:02 UTC Sep 3 1999
  end   date: 15:22:02 UTC Sep 3 2019

RA KeyEncipher Certificate
Status: Available
Certificate Serial Number: 37CFE7A5
Key Usage: Encryption
DN Name
  CN = Martin Murhammer + OID.2.5.4.5 = 21731
  OU = ITSO Raleigh
  L = N.C.
  C = US
  O = IBM
CRL Distribution Point:
  CN = CRL1, OU = ITSO Raleigh, L = N.C., C = US, O = IBM
Validity Date:
  start date: 17:45:42 UTC Sep 13 1999
  end   date: 18:15:42 UTC Sep 13 2002

Cisco_NAS#

```

Figure 480. Cisco - listing digital certificates for use with IKE - part 2

8. If you are satisfied with the certificates, the last step to perform is to save the router configuration, which will also store the certificates in NVRAM. You can do this, for instance, with the `copy run sta` command.

17.6.2 Creating an IKE policy for certificates

An IKE (ISAKMP) policy that uses certificates is not much different from a policy that uses pre-shared keys. However, you have to know what type of IDs are used in the certificates, IP addresses, or fully qualified domain names (FQDN), and you have to set the ISAKMP ID appropriately. You also have to specify that the authentication mode will be RSA signatures instead of pre-shared keys or RSA encryption.

Following is an example of an ISAKMP policy that we were using. The corresponding IRE VPN client configuration can be found in 19.1.5, “Client configuration for certificates” on page 603.


```
cisco-2612(config)#cry isa pol 7
cisco-2612(config-isakmp)#encr des
cisco-2612(config-isakmp)#hash md5
cisco-2612(config-isakmp)#auth rsa-sig
cisco-2612(config-isakmp)#lifetime 28800
cisco-2612(config-isakmp)#exit
cisco-2612(config)#
cisco-2612(config)#cry isa iden addr
cisco-2612(config)#
```

Figure 481. Cisco - ISAKMP policy for RSA signatures

IPSec transform set and crypto maps are defined as usual.

17.7 Windows 2000 to Cisco 2612 using voluntary layer-2 tunneling

Layer-2 tunneling can be deployed between routers to provide multiprotocol support for both leased line as well as dial-up (dial on-demand) connections. Cisco routers offer Cisco's proprietary Layer 2 Forwarding (L2F) as well as the IETF standard (RFC 2661) Layer 2 Tunneling Protocol (L2TP) to facilitate that. However, in a router-to-router configuration, the overhead of PPP over layer-2 tunneling may be greater than that incurred by other techniques such as data link switching when the ultimate goal is merely multiprotocol support.

For the remote client access, however, layer-2 tunneling provides the multiprotocol capability not otherwise available via IPSec dial-up. On the other hand, IPSec can still provide the security for the layer-2 tunnel. Essentially, this combination of VPN technologies offers the customer added functionality at the expense of performance - which may or may not be a problem - without compromising security.

A detailed description of this scenario can be found in 18.4.1, "Scenario characteristics" on page 583, and an illustration of the environment is shown in Figure 510 on page 583.

In this scenario, a Windows 2000 client is dialing into the Cisco_NAS at the ISP and then establishes an L2TP tunnel back to the Cisco_GW corporate gateway, which assigns an IP address to the client out of a pool of internal corporate addresses. IPSec can be used with this scenario in two ways:

- Between the client and the Cisco_GW to protect the L2TP tunnel and all traffic that flows through it. This requires a host-to-host IPSec transport-mode connection and IKE in either aggressive mode (for pre-shared keys) or with digital certificates.
- Between the client and any server in the corporate network to protect end-to-end traffic. Such IPSec connections would be transparent to the router.

For this redbook, we only show the basic L2TP connection.

We are using the configuration as described in 18.4, "Windows 2000 remote access using L2TP" on page 583 for the Windows 2000 system. The only difference is the IP address of the tunnel server, which is 192.168.212.2, in the case of our Cisco router.

Figure 482 lists the configuration for the Cisco router acting as the LNS in this scenario:

```
!  
hostname Cisco_GW  
!  
aaa new-model  
aaa authentication login default local  
aaa authentication ppp default local  
aaa authorization network default local  
enable secret 5 $1$6JFo$G8uRtGnOGz.2RTimQbKBu/  
enable password telnet  
!  
username belmont password 0 belmont  
username cisco password 0 cisco  
username vpnclient@Cisco_GW password 0 vpnclient  
username vpnclient password 0 vpnclient  
!  
ip subnet-zero  
no ip domain-lookup  
!  
vpdn enable  
!  
vpdn-group 1  
! Default L2TP VPDN group  
accept-dialin  
  protocol l2tp  
  virtual-template 1  
local name cisco  
no l2tp tunnel authentication  
!  
interface Serial0/0  
  ip address 9.24.105.168 255.255.255.0  
  no ip directed-broadcast  
  no ip mroute-cache  
!  
interface Ethernet0/0  
  ip address 192.168.103.1 255.255.255.0  
  no ip directed-broadcast  
  no ip mroute-cache  
!  
interface Virtual-Template1  
  ip unnumbered Ethernet0/0  
  no ip directed-broadcast  
  peer default ip address pool test  
  ppp authentication chap  
!  
ip local pool test 192.168.103.150 192.168.103.199  
ip classless  
!
```

Figure 482. Cisco - L2TP configuration with Windows 2000 client

17.8 IBM 2212 to Cisco 2612, L2F dial-up gateway

This scenario involves compulsory layer-2 tunneling using Cisco's Layer 2 Forwarding (L2F) protocol. Upon connection from a client to the ISP, the ISP access router or server determines that this connection should be tunneled back to the corporate network access gateway and establishes the tunnel before effectively extending the PPP connection back to the corporate gateway.

The principles of compulsory tunneling and a scenario using L2F between a Cisco and an IBM router are described in detail in the redbook *A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions*, SG24-5234.

Chapter 18. Interoperability with Windows 2000

This chapter gives an overview of VPN capabilities of Windows 2000 and shows a few configuration and interoperability examples with IBM VPN solutions.

Important

At publication time, Windows 2000 was only available in a beta version. Therefore, the VPN capabilities and configuration screens of the final product may be different from what is described here.

18.1 Windows 2000 VPN capabilities

Windows 2000 supports the following VPN technologies:

1. IP Security Architecture Protocol (IPSec)
2. Layer 2 Tunneling Protocol (L2TP)
3. Point-to-Point Tunneling Protocol (PPTP)
4. RADIUS authentication (Windows 2000 server)
5. Certificate-based authentication for IKE and PPP (EAP)

18.1.1 Windows 2000 IPSec features

Windows 2000 will be available in several different packages ranging from a workstation equivalent to an enterprise server edition. To our observation, Windows 2000 Professional, the workstation edition, only supports IPSec in transport mode, whereas the server editions also support tunnel mode. In this chapter, we will treat Windows 2000 as an IPSec client and IPSec server and not as a gateway.

Note

We also observed that in the pre-release of Windows 2000 we were using for our tests, IKE aggressive mode was not supported or there was no obvious way to configure it.

IPSec is a built-in feature of the Windows 2000 TCP/IP stack. Windows 2000 IPSec implementation offers the following features:

Table 121. Windows 2000 - IPSec VPN features

| Feature | |
|---------------------------------|----------------------|
| Tunnel Type | IKE |
| IPSec Header Format | RFCs 24xx |
| IKE | |
| Key Management Tunnel (Phase 1) | |
| Roles | Initiator, Responder |

| Feature | |
|---|---|
| Negotiation Mode | Main Mode |
| Encryption Algorithm | Triple DES, DES |
| Authentication Method | Digital Signatures (Certificates), Pre-Shared Key Kerberos (non-standard) |
| Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| Diffie-Hellman Group | Group 1, Group 2 export (non-standard) |
| Multiple SA proposals | Yes |
| Send Phase 1 Delete | Yes |
| Data Management Tunnel (Phase 2) | |
| Encapsulation Mode | Transport Mode Tunnel Mode (only on Servers) |
| Security Protocol | AH, ESP |
| AH Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| ESP Encryption Algorithm | DES, Triple DES, NULL |
| ESP Authentication Algorithm | HMAC-MD5, HMAC-SHA, NULL |
| Multiple SA Proposals | Yes |
| Perfect Forward Secrecy (PFS) | Yes |
| On-Demand Outbound Tunnels | Yes |
| On-Demand Inbound Tunnels | Yes |
| Other | Logging, Packet filtering, NAT |

18.1.2 Windows 2000 layer-2 tunneling features

Layer-2 tunneling is provided by the dial-up networking component of Windows 2000 and supports PPTP and L2TP with the following capabilities:

Table 122. Windows 2000 - VPN support using layer-2 tunneling

| Feature | Windows 2000 |
|--------------------------|---------------------|
| Layer-2 Tunneling | |
| Voluntary L2TP | √ |
| L2TP Dial-out | √ |
| PPTP | √ |

| Feature | | Windows 2000 |
|----------------------------------|----------|--------------|
| PPP Authentication | PAP | √ |
| | CHAP | √ |
| | MS-CHAP | √ |
| | SPAP | √ |
| | EAP | √ |
| PPP Encryption | ECP | √ |
| | MPPE | √ |
| Tunnel Authentication | Local | √ |
| | RADIUS | √ |
| | Kerberos | √ |
| PPP Multilink Support | | √ |
| Multiprotocol Support | | √ |
| IPSec Protection for L2TP Tunnel | | √ |

Note

IPSec protection for L2TP tunnels in a remote access environment is only possible when IKE is used with certificate-based authentication because Windows 2000 does not support IKE aggressive mode. We have not tested such a scenario for this redbook.

However, protecting the IP traffic that flows through the L2TP tunnel can be protected with IPSec, and we did test that configuration successfully.

18.2 Configuring IPSec on Windows 2000

The general steps to configure, enable, and use IKE and IPSec on Windows 2000 are as follows:

1. Create and configure an IPSec policy or use a predefined one.
2. Create and configure an IPSec filter rule or use a predefined one.
3. Create and configure an IPSec filter action or use a predefined one.
4. Configure IKE parameters.
5. Assign an IPSec policy to the IPSec policy agent to activate IPSec.
6. Enable IPSec for a network connection.

This section describes each of those steps in turn. We have used a pre-release of the Windows 2000 server edition for this redbook.

18.2.1 IP Security policy management

You may like to add new policies and manage them. You can customize IPSec policies using the IP Security Management snap-in that can be added to the

console tree in any console supported by Microsoft Management Console (MMC). By default, the IP Security Management function is contained in the Local Security Policy console which you can access by clicking **Start -> Settings -> Control Panel -> Administrative Tools -> Local Security Policy**. This console is shown in Figure 483. You may want to create a copy of it to the Windows 2000 desktop for easier access in the future.

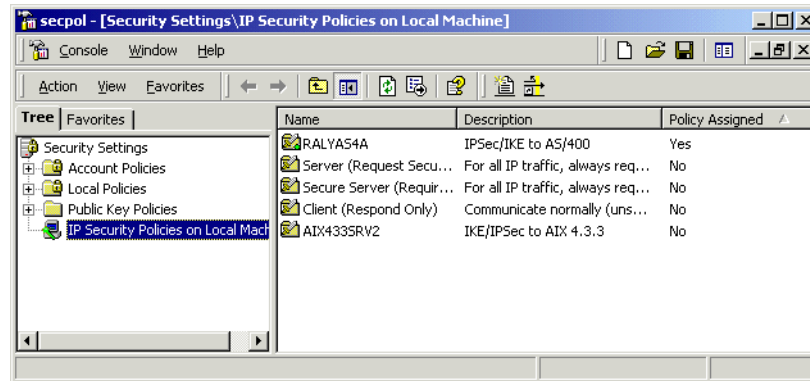


Figure 483. Windows 2000 - Local Security Policy console

To use a particular policy, you must first activate it so that the IP Security Policy Agent service - which must also be active - can use that policy. To activate, highlight a policy, click the right mouse button and select **Assign**. A small green dot on the policy icon will indicate that it is now assigned/active. Only one policy can be active at any given time. You can use a generic policy or define as many rules, actions, and proposals in a policy as you need.

18.2.2 Configuring IPsec and IKE

All IPsec-related tasks can be managed using the IP Security Management console. You can define as many policies as you want but only one can be active at a time.

Unlike other IPsec/IKE implementations, IPsec/IKE configuration is not logically divided into two phases on Windows 2000. IPsec is defined with one policy that applies to any network configuration and all IKE negotiations are done according to this policy. Figure 484 illustrates the policy configuration flow.

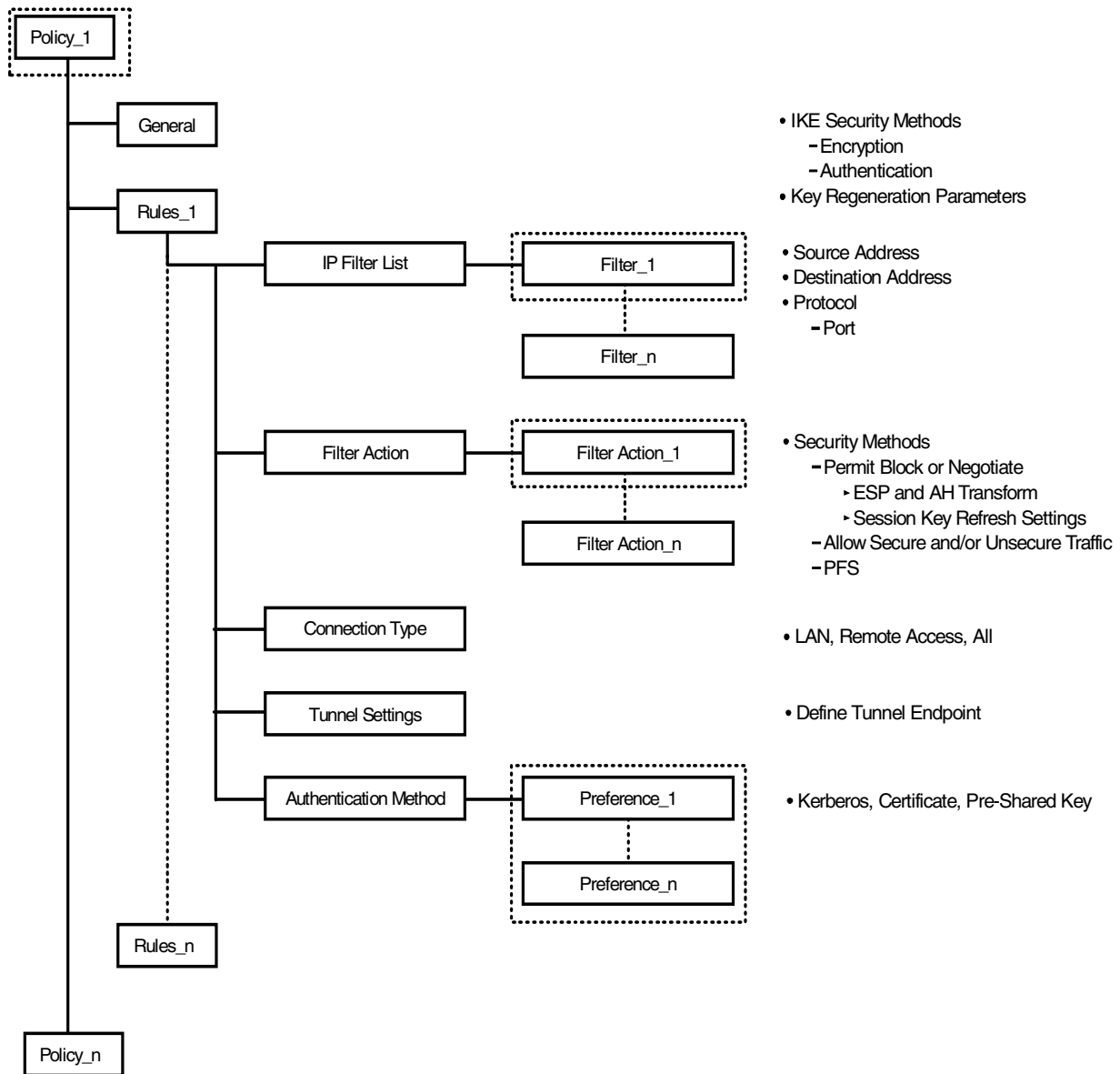


Figure 484. Windows 2000 - IPsec policy configuration

18.2.2.1 Creating an IPsec policy

Please follow the steps below to configure an IPsec policy on Windows 2000:

1. Click **IP Security Policies on Local Machine**.
2. Click the **Action** button and select **Create IP Security Policy**.
This will invoke IP Security Policy Wizard.
3. Click **Next**.
4. Enter a name that can be distinguished easily, for example, local-hostname_remote-hostname and a description for the policy and click **Next** (see Figure 485):

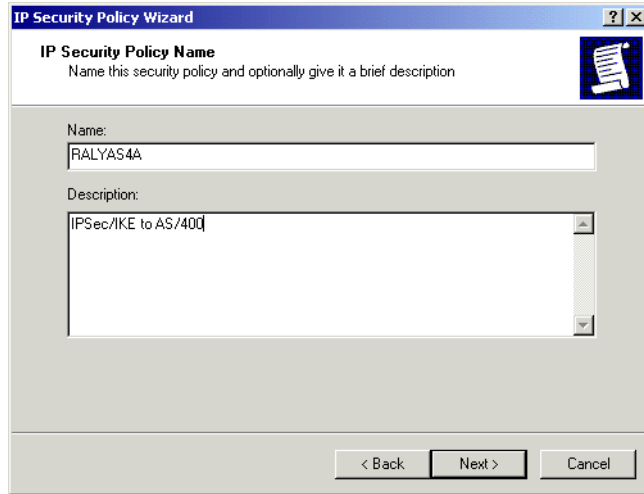


Figure 485. Windows 2000 - IPSec policy configuration: IP Security Policy Name

5. If you do not want to enable the default response rule, uncheck the **Activate the default response rule** option (see Figure 486):

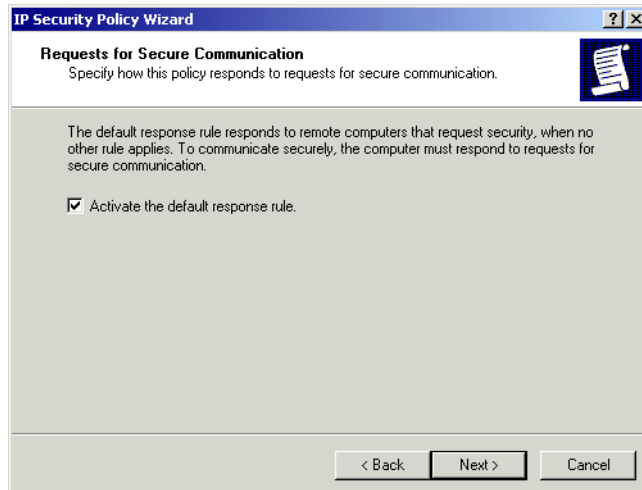


Figure 486. Windows 2000 - IPSec Policy Configuration: Requests for Secure Communication

6. Click **Next**.
7. Select an authentication method; keep in mind that this *must* match the other party. In fact, after completing the basic setup you can add more authentication methods to this policy (see Figure 487).

Select the authentication method from one of the following options:

- Kerberos V5 protocol
This option allows the Windows 2000 machines in a domain or across trusted domains to authenticate each other.
- Public/Private key signatures using certificates
This option allows you to use certificates that are compatible with Microsoft, Entrust, Verisign, and Netscape.
- Pre-shared key

This option allows you to use shared secret between both sides of the IPSec communication.



Figure 487. Windows 2000 - IPSec policy configuration: Default Response Rule Authentication Method

8. Click **Next**.
9. Make sure that **Edit properties** option is checked and click **Finish** (see Figure 488):

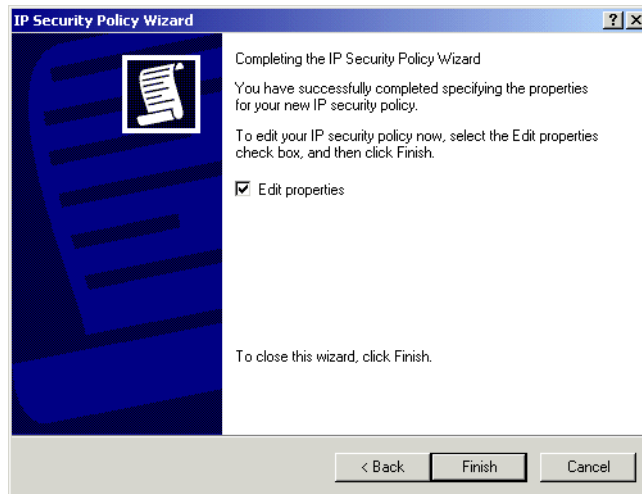


Figure 488. Windows 2000 - IPSec Policy Configuration: Completing the IP Security Policy Wizard

You have completed the basic setup using IP Security Policy Wizard. Now you can customize the rules and actions of the policy that has been created by the wizard.

18.2.2.2 Configuring an IPSec rule

For each policy a Dynamic Default Response rule is automatically created if you selected that option during the policy creation. This rule does not define the tunnel endpoint, therefore, any host can make an IPSec tunnel if the parameters match. If you want to define a tunnel endpoint and apply further security rules you may want to add a new security rule.

Perform the following steps to add a new IPSec rule:

1. In the policy properties window, make sure the **Use Add Wizard** box is checked, then click the **Add** button (see Figure 489) to bring up the Security Rule Wizard.

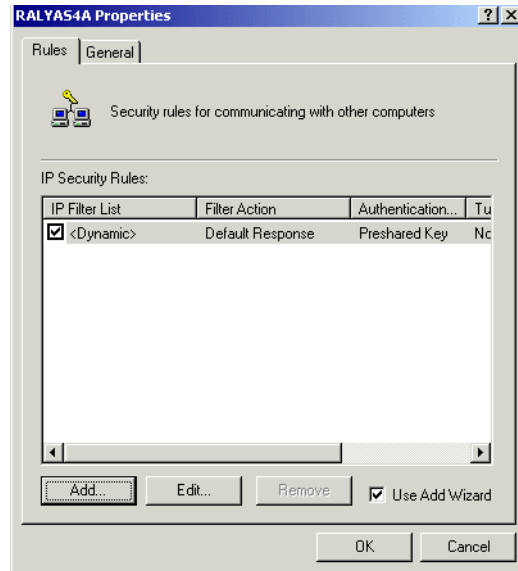


Figure 489. Windows 2000 - IPSec policy configuration - policy properties

2. Click **Next**.
3. Select the tunnel endpoint specification type from one of the following options:
 - This rule does not specify a tunnel.
 - The tunnel endpoint is specified by this DNS name.
 - The tunnel endpoint is specified by this IP address.

If you have selected IP address, type the IP address of the remote endpoint where the tunnel terminates.

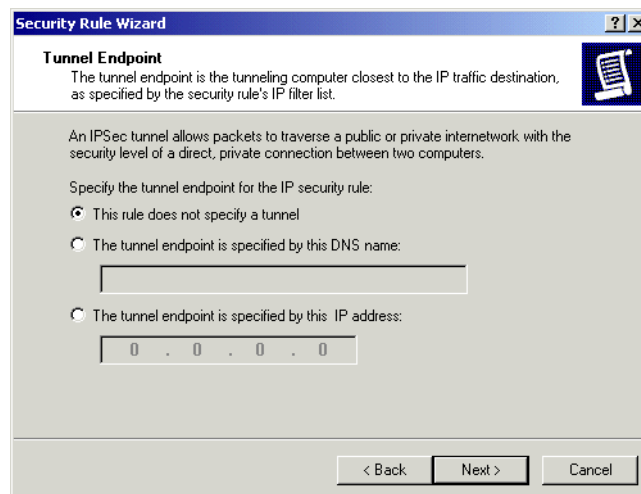


Figure 490. Windows 2000 - IPSec policy configuration: Tunnel Endpoint

4. Click **Next**.
5. Select the network type from one of the following options:
 - All network connections
 - Local area network (LAN)
 - Remote access

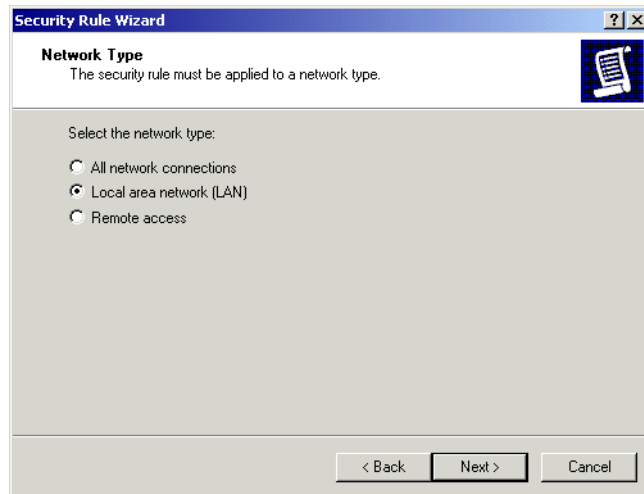


Figure 491. Windows 2000 - IPSec policy configuration: Network Type

6. Click **Next**.
7. Select the authentication method from one of the following options:
 - Kerberos V5 protocol
 - Public/Private key signatures using certificates
 - Pre-shared key
8. Click **Next**.
9. Select the IP filter of your choice for this IP Security rule or create a new one.

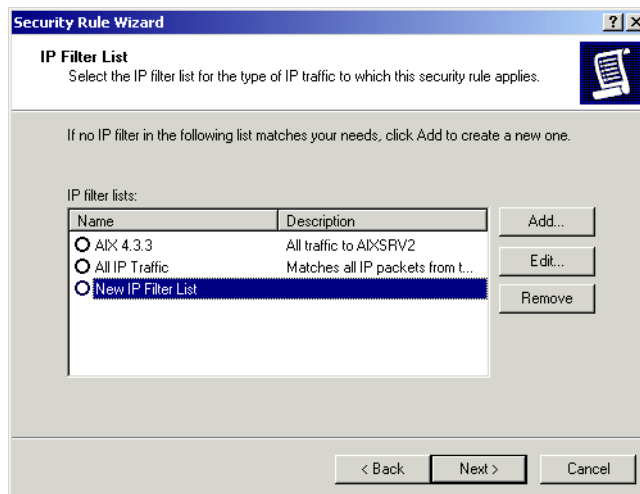


Figure 492. Windows 2000 - IPSec policy configuration: IP Filter List

To create an IPSec filter list proceed to the following section.

18.2.2.3 Configuring an IPSec filter list

When IP packets are being sent outbound or inbound, they are matched against filters to determine whether the packet will be secured, permitted, or discarded.

Windows 2000 IPSec implementation does not secure the following IP traffic:

- Broadcast
- Multicast
- RSVP
- Kerberos
- IKE
- LDAP

To secure IP traffic, two ways of filtering rules must be generated. Thus, the inbound and outbound traffic will be secured. You can achieve this by selecting the **mirrored** option of a particular filter properties window.

Perform the following steps to configure an IP filter list:

1. On the IP Filter List window, click **Add**. This will bring up a list of IP filters (see Figure 493).
2. Enter a name that can be distinguished easily and a description for the filter list.
3. Make sure that **Use Add Wizard** is checked and click **Add** (see Figure 493).

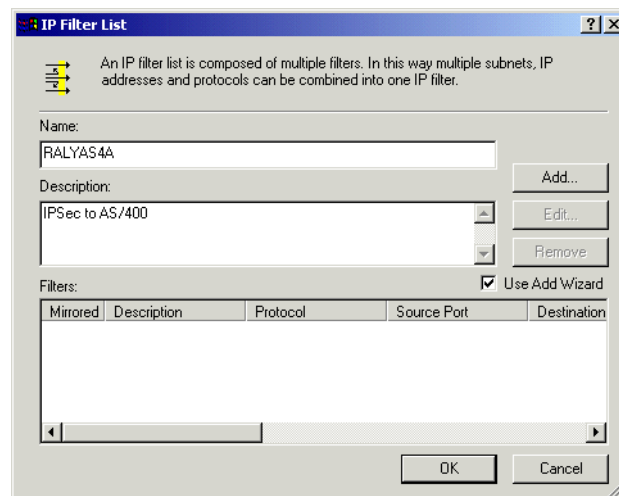


Figure 493. Windows 2000 - IPSec policy configuration - adding new IP filter list

4. Click **Next**.
5. You can select the following options for Source address in the IP Traffic Source window:
 - My IP Address
 - Any IP Address
 - A specific DNS Name
 - A specific IP Address
 - A specific IP Subnet

If you want to create a host-to-host connection, you may choose the **My IP Address** option.

6. You will be prompted to enter source address information depending on your selection of source address type.

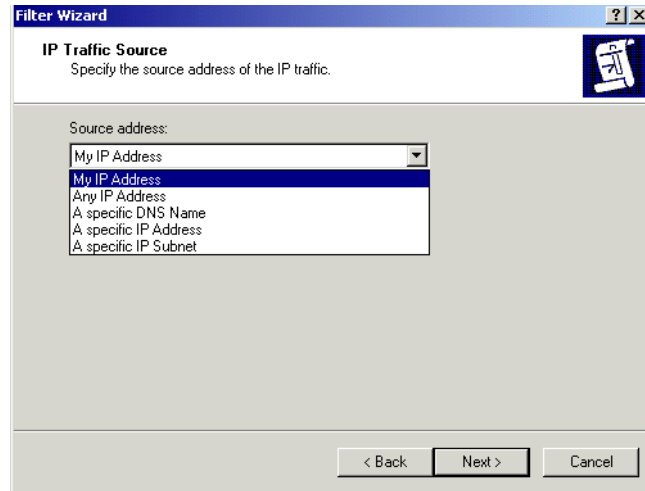


Figure 494. Windows 2000 - IPSec policy configuration: IP Traffic Source

7. Click **Next** if you have entered an address.
8. Select the appropriate destination address definition and click **Next**.
9. You will be prompted to enter destination address information, depending on your selection of destination address type.

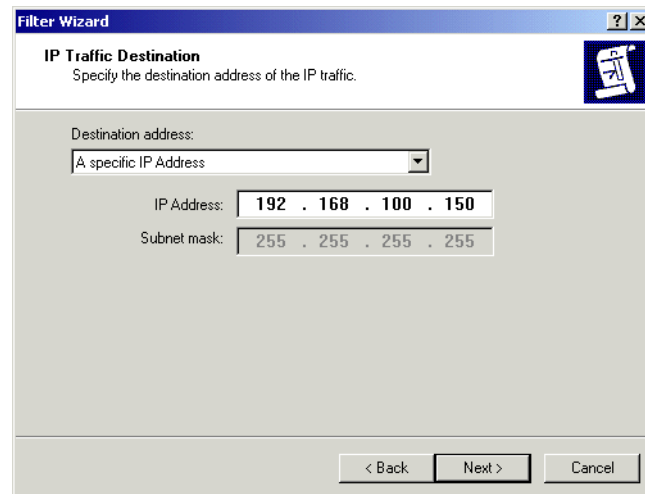


Figure 495. Windows 2000 - IPSec policy configuration: IP Traffic Destination

10. Click **Next** if you have entered an address (see Figure 495).
11. Select the protocol type to be protected by IPSec. You can choose from the following options:
 - Any
 - EGP
 - HMP

- ICMP
- Other
- RAW
- RDP
- TCP
- UDP
- XNS-IDP

12. Click **Next**.

13. Click **Finish**, then click **Close** to return to the Rule Wizard.

You have now configured an IP filter list.

18.2.2.4 Configuring an IPSec filter action

An IPSec filter action defines whether a specific filter list will be permitted, denied or secured. It also defines the IKE data management tunnel parameters that will be negotiated in Phase 2. You can either use the predefined IPSec filter actions or you can create your own.

There are two methods for non-IPSec computers:

- For non-IPSec computers to communicate with Windows 2000, you can define an IPSec filtering list. Then you select permit for this filter rule in the IPSec filter action definition. This will allow the particular computer to access Windows 2000 as you defined in the IPSec filter list.
- If you select the **Fall back to unsecured communication** option, Windows 2000 will first try to negotiate an IPSec tunnel. If the remote endpoint does not respond to the IKE negotiation request, it will fall back to clear communication. If the remote endpoint replies to the IKE negotiation request, it will continue with the IKE negotiation and try to establish an IPSec connection. If the partner does not reply to the IKE negotiation request, all packets will be discarded in one minute, and Windows 2000 falls back to unsecured communication.

Perform the following steps to configure an IPSec filter action:

1. On the Filter Action panel, make sure that **Use Add Wizard** is checked and then click **Add**, which brings up the Filter Action Wizard.
2. Fill in a name and description for this IPSec filter action, then click **Next**.
3. Select **Negotiate security** and then click **Next**.

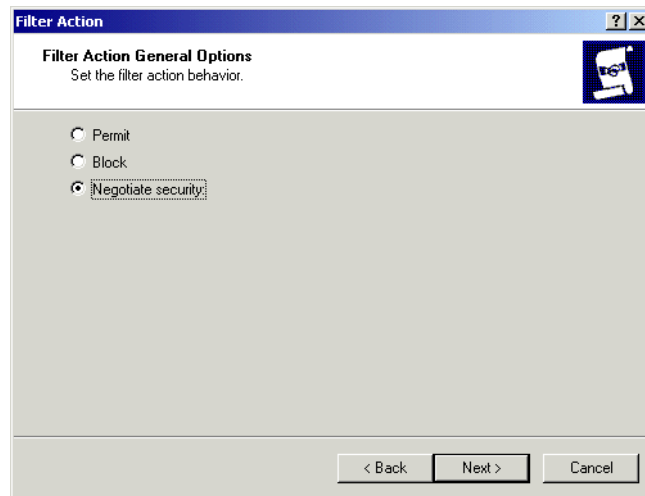


Figure 496. Windows 2000 - IPSec policy configuration: Filter Action

4. Click **Do not communicate with computers that do not support IPSec** and click **Next**.

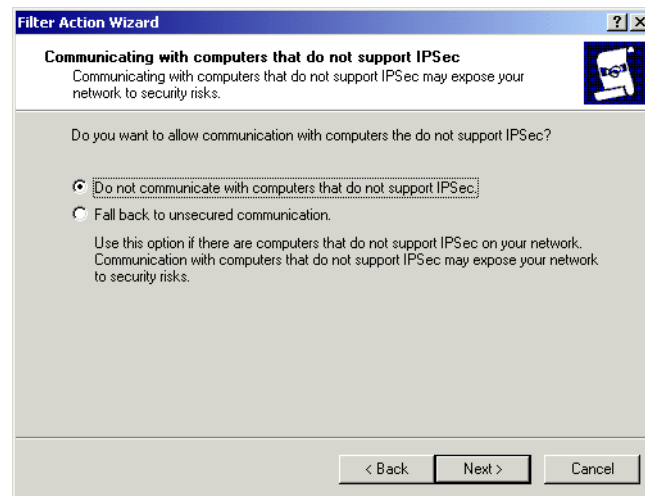


Figure 497. Windows 2000 - IPSec policy configuration - communication settings

5. Select one of the following security methods (see Figure 498):
 - High
 - Medium
 - Custom

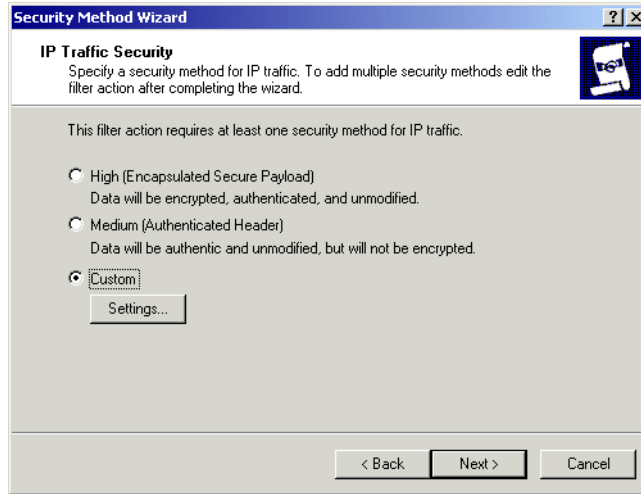


Figure 498. Windows 2000 - IPSec policy configuration: IP Traffic Security

Table 123 shows the parameters used for the two predefined security methods:

Table 123. Predefined Security Methods

| Security methods | High | Medium |
|---------------------|------|--------|
| AH Integrity | None | MD5 |
| ESP Confidentiality | DES | None |
| ESP Integrity | MD5 | None |

If the predefined security methods do not fit your requirements, you can create your own security methods following the steps below:

1. Select **Custom**, then click **Settings**.

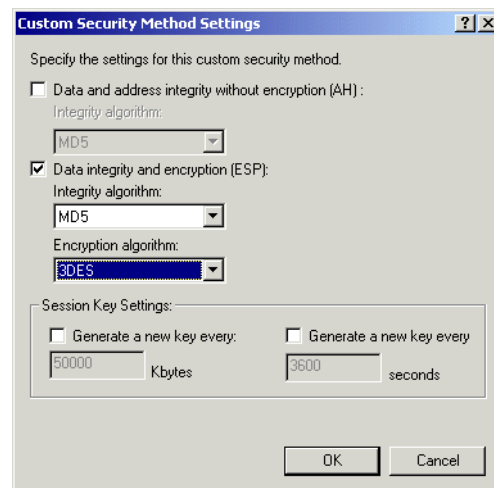


Figure 499. Windows 2000 - IPSec policy configuration - adding new security method

2. Define your security method, then click **OK**.
6. Click **Next** and click **Finish** to return to the Security Rule Wizard.

7. Select the filter you have just created, then click **Next->Finish** to return to the IPsec policy Properties window.

You have now configured the IPsec filter rule and filter action definition.

18.2.2.5 Configuring key exchange settings

Key exchange settings apply to key management tunnel and are negotiated during Phase 1. These parameters are unique to each policy.

To configure key exchange settings, perform the following steps:

1. Double-click the policy you have created on the IP Security Policy Management console.
2. Click the **General** tab (see Figure 489 on page 564).

You can set the time period for detecting policy changes. The default value is 180 minutes.

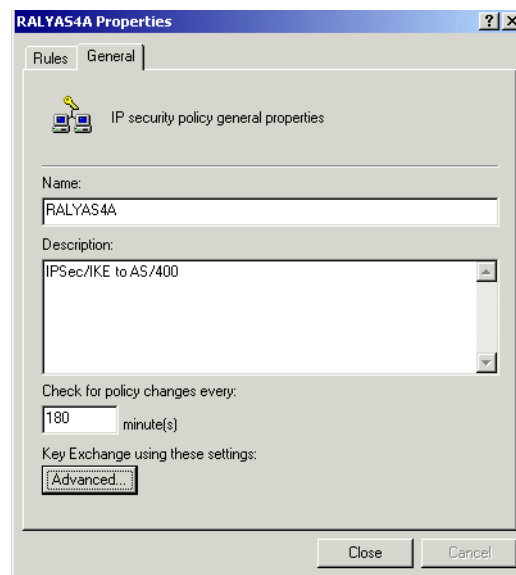


Figure 500. Windows 2000 - IPsec Policy Configuration: General policy properties

3. Click the **Advanced** button.

The options on the Key Exchange Settings configuration panel determines the IKE Phase 1 security methods (see Figure 501).

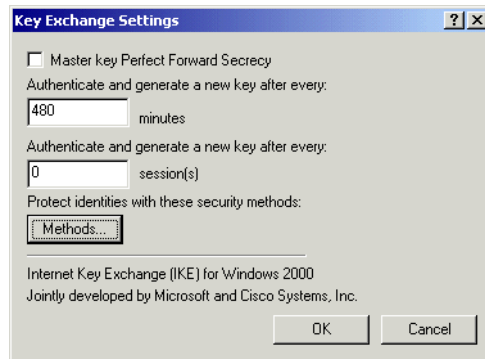


Figure 501. Windows 2000 - IPSec Policy Configuration: Key Exchange Settings

4. Place a check mark beside the **Master key Perfect Forward Secrecy** option if you want additional exponentiation on the master key. Keep in mind that this option must match the other party.
5. You can set key generation values in two ways:
 - A time period in minutes
 - Number of sessions (Phase 2 SAs)
6. Click the **Methods** button.

There are two predefined security methods in Windows 2000, as shown in the table below:

Table 124. Predefined security methods

| Key exchange security methods | | |
|-------------------------------|---------------|------------------|
| Type | IKE | IKE |
| Encryption Algorithm | DES | 3DES |
| Integrity | MD5 | MD5 |
| Diffie-Hellman | Low (Group 1) | Medium (Group 2) |

If the predefined security methods do not meet your requirements, you can create or customize your own security method.

7. Click the **Add** button to add a new key exchange security method.

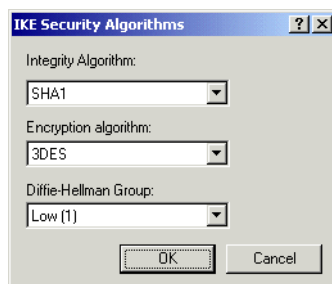


Figure 502. Windows 2000 - IPSec policy configuration: IKE Security Algorithms

8. Select the **Integrity Algorithm** from the following values:

- MD5
 - SHA
9. Select the **Encryption algorithm** from the following values:
 - 3DES
 - DES
 10. Select the **Diffie-Hellman Group** from the following values:
 - Low (1)
 - Medium (2)
 - Export (non-standard)
 11. Click **OK** twice, then click **Close** to return to the security policy Properties window.

18.2.3 Enable IPsec for a network connection

You should perform the following steps in order to use an IPsec policy for a particular network connection.

1. Click **Start->Settings->Control Panel->Network and Dial-up Connections**.
2. Right-click the network connection you want to use with IPsec and click **Properties**.
3. Highlight **Internet Protocol (TCP/IP)** and click the **Properties** button (see Figure 503):

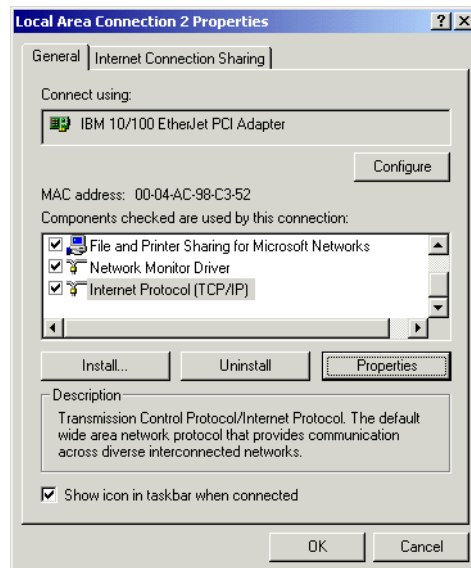


Figure 503. Windows 2000 - IPsec configuration - network connection configuration panel

4. Click the **Advanced** button (see Figure 504).

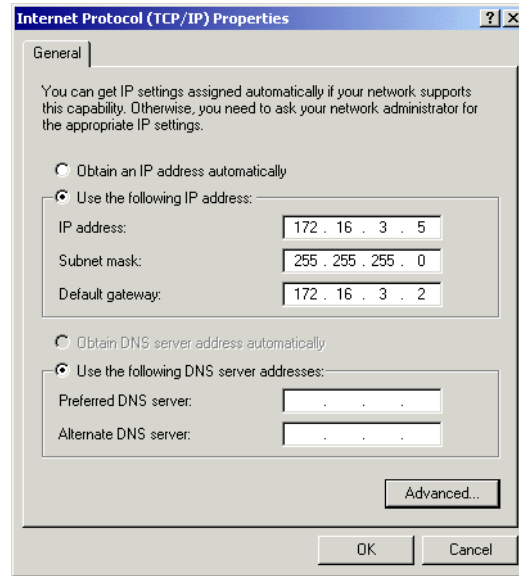


Figure 504. Windows 2000 - IPsec configuration: TCP/IP configuration panel

5. Click the **Options** tab (see Figure 505):

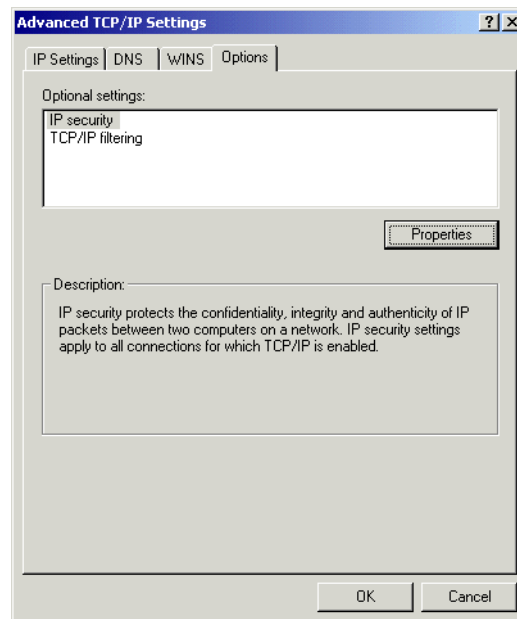


Figure 505. Windows 2000 - IPsec configuration: Options

6. Highlight **IP security** and click **Properties**.

7. Click **Use this IP security policy** and select the policy that you want to use for this network connection (See Figure 506):

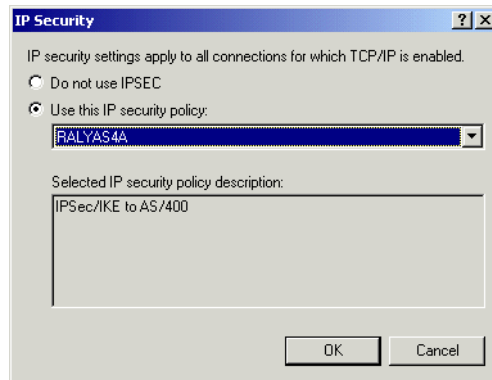


Figure 506. Windows 2000 - IPSec configuration: IP Security

There are three default policies defined:

1. Client (Respond Only)

This option enables a Windows 2000 machine to respond to any IPSec request from outside. If the IPSec parameters match, a VPN connection will be established. Since no remote endpoints are defined by this policy, this option allows Windows 2000 only to respond to IPSec connection requests.

2. Server (Request Security)

This option enables Windows 2000 to establish unsecured connections, but it first attempts to create IPSec connections with the remote computer. That way Windows 2000 will allow an unsecured connection if the remote computer does not support IPSec.

3. Secure Server (Require Security)

This option only accepts connections from remote computers if they use IPSec/IKE negotiation requests. All other traffic is dropped off.

Note

You must have administrator privileges to set IPSec policies.

18.2.4 Starting IPSec connections

If you have defined an IP Security Rule with a tunnel endpoint definition, you should start communication to initiate the negotiation. Basically, you can ping that particular system, or use any other application for which a matching policy has been defined. With ping, you will see Negotiating IP Security as a reply. If the negotiation is successful you should get a response from the remote endpoint. This concept of traffic-initiated IPSec connections is essentially the same as the on-demand tunnels implemented by IBM AIX 4.3.3 and IBM routers.

18.2.5 Using the IP Security Monitor

To verify that IPSec is used as desired, use the IP Security Monitor application. Enter `ipsecmon` from a command prompt to start the monitor. Figure 507 shows an example of the IP Security Monitor.

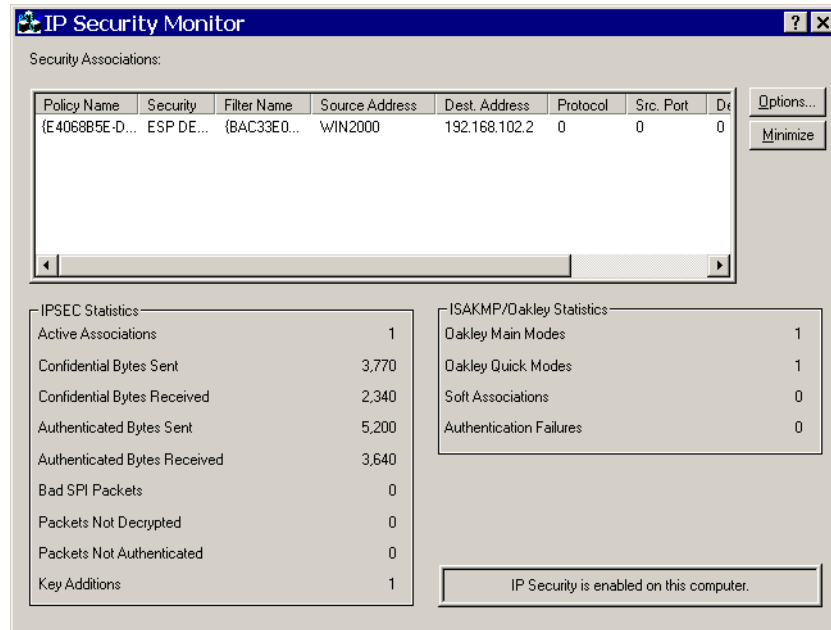


Figure 507. Windows 2000 - IP Security Monitor

18.3 Windows 2000 to AIX 4.3.2, host-to-host

In this scenario, we are presenting 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 and therefore, they want to ensure the connection is protected by IPsec protocols to the very hosts they want to connect. Figure 498 on page 570 represents this scenario.

18.3.1 Scenario characteristics

- Both networks, the distributor's and the manufacturer's, 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 hosts' VPN partners.

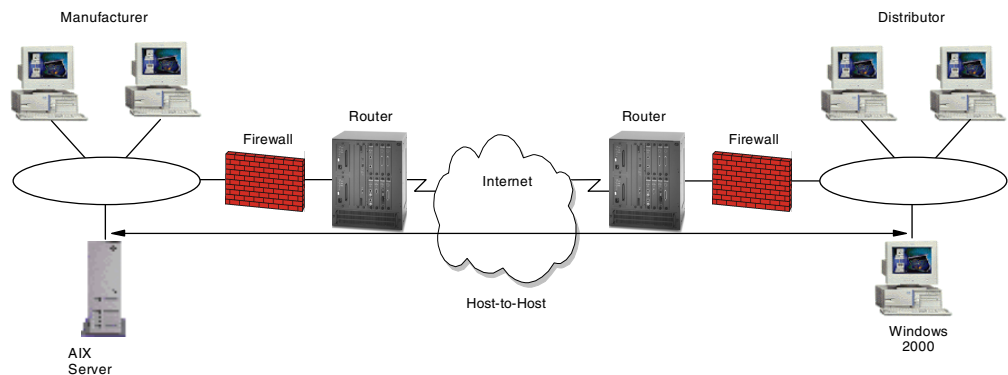


Figure 508. Business partners VPN - host-to-host Windows 2000 server to AIX server

18.3.1.1 Scenario objectives

The objectives of this scenario are:

- All traffic between WIN2000 and AIXSRV1 must be protected by IPSec.
- Only AIXSRV1 in the manufacturer's network can access WIN2000 in the distributor's network and vice versa.
- Only Telnet from the distributor (WIN2000) to the manufacturer (AIXSRV1) is allowed over the VPN.
- Only the distributor (WIN2000) is allowed to initiate the VPN connection.

18.3.1.2 Scenario network configuration

Figure 509 on page 577 shows our simple network configuration for the host-to-host Windows 2000 server to AIX server.

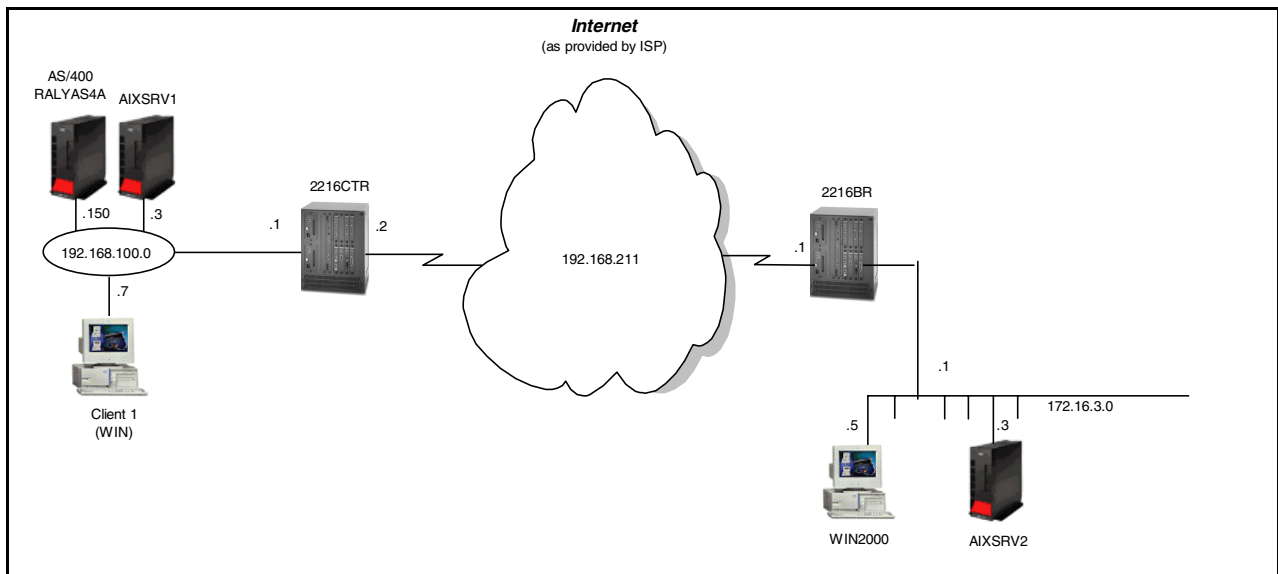


Figure 509. Business partners VPN - host-to-host scenario

18.3.2 Implementation tasks - summary

The following is a summary of tasks used to implement this VPN host-to-host environment:

1. Verify connectivity. Before you start configuring VPN and security policies, you must be sure that the underlying TCP/IP network is properly configured and working.
2. Complete the planning worksheets for both systems.
3. Configure VPN tunnels in Windows 2000.
4. Configure VPN tunnels in the AIX server.
5. Start the VPN connection.
6. Perform verification tests.

18.3.2.1 Verifying initial connectivity

Before starting the VPN configuration, verify that connectivity and routing between the two hosts is working properly.

1. From WIN2000 server, PING AIXSRV1. Enter the following PING command:

PING 192.168.100.3

2. Repeat the PING in the reverse direction from AIXSRV1 to WIN2000:

PING 172.16.3.5

Both tests must succeed before you can continue. In a real Internet environment, there might be routers along the way disallowing the PING command.

18.3.3 Completing the Windows 2000 server planning worksheet

Complete the Windows 2000 planning worksheet as shown in Table 125. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 125. Windows 2000 planning worksheet

| Information you need to configure VPN in the Windows 2000 Server | Scenario answers |
|--|------------------|
| Policy name | WIN2000_AIXSRV1 |
| Tunnel endpoint address | 192.168.100.3 |
| Role | Initiator |
| Pre-shared key | 12345678 |
| Key Exchange Security Methods | |
| Integrity Algorithm | DES |
| Encryption Algorithm | MD5 |
| Diffie-Hellman Group | Group 1 |
| IP Filters | |
| Source address | 172.16.3.5 |
| Destination address | 192.168.100.3 |
| Protocol type | Any |
| Port | N/A |
| Filter Action | |
| AH Transform | MD5 |
| ESP Integrity | MD5 |
| ESP Authentication | DEs |
| New key regeneration period (seconds/KBs) | 28800 seconds |
| Perfect Forward Secrecy (PFS) | No |

18.3.4 Completing the AIX server planning worksheet

Complete the AIX planning worksheet as shown in Table 126. The planning worksheet allows you to gather all the configuration data before the actual implementation.

Table 126. 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 | AIXSVR1 | |
| IP address | 192.168.100.3 | |
| Role | Responder | |
| Key Management Tunnel (Phase 1) | | |
| Mode | Main | |
| Encryption | DES | |
| Authentication Algorithm | MD5 | |
| Key Exchange Group | 1 | |
| Key Life Time | 28800 sec (default) | |
| Negotiation ID | IP Address | |
| Pre-Shared Key | 3132333435363738 (HEX of 12345677) | |
| 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 Life Time | 30 min | |

18.3.5 Configuring a host-to-host VPN in the Windows 2000 server

Perform the following steps to configure a host-to-host VPN on Windows 2000 using the IP Security Policy Management console:

1. Start the IP Security Policy Management console.
2. Click **IP Security Policies on Local Machine**.
3. Click the **Action** button and select **Create IP Security Policy**.

This will invoke IP Security Policy Wizard:

4. Click **Next**.
5. Enter **WIN2000_AIXSRV1** and **Host-to-host** for the description and click **Next**.

6. Uncheck the **Activate the default response rule** option.
7. Click **Next**.
8. Select the **Use this string to protect the key exchange (pre-shared key)** option and enter **12345678** for the pre-shared key.
9. Make sure that the **Edit Properties** option is checked and click **Finish**.
10. Click the **General** tab.
11. Click the **Advanced** button.

The options on the Key Exchange Settings configuration panel determines the IKE Phase 1 security methods.

12. Make sure that there is no check mark for the **Master key Perfect Forward Secrecy** option. Keep in mind that this option must match the other party.
13. Click the **Methods** button.
14. Click the **Add** button to add a new key exchange security method.
15. Select **MD5** for the **Integrity Algorithm** option.
16. Select **DES** for the **Encryption algorithm** option.
17. Select **Low (1)** for the **Diffie-Hellman Group** option.
18. Click the **OK** buttons till you get back to the WIN2000_AIXSRV1 policy properties window.
19. Click the **Rules** tab.
20. Make sure that **<Dynamic>** IP Security Rule is not checked.
21. In the policy properties window click the **Add** button.
22. Click **Next**.
23. Select **The tunnel endpoint is specified by this IP address** and enter **192.168.100.3**.
24. Click **Next**.
25. Select **Local area network (LAN)** for the network type Remote access.
26. Click **Next**.
27. Select the **Use this string to protect the key exchange (pre-shared key)** option and enter **12345678** for the pre-shared key.
28. Select the IP filter of your choice for this IP Security rule or create a new one.
To create an IPSec filter list proceed to the following steps:
29. On the IP Filter List window, click **Add**. This will bring up a list of IP filters.
30. Enter **3.5-to-100.3** for the name.
31. Make sure that Use Add Wizard is checked and click **Add**.
32. Click **Next**.
33. Select the **My IP Address** option for Source address and click **Next**.
34. Select the **A Specific IP Address** option for the destination address.
35. Enter **192.168.100.3** for the IP address and click **Next**.
36. Click **Next**.
37. Click **Finish**.

You have now configured an IP filter list.

Perform the following steps to configure an IPSec filter action:

38. On the Filter Action panel, make sure that **Use Add Wizard** is checked and then click **Add**.
39. Click **Next**.
40. Select **Negotiate security** and then click **Next**.
41. Click **Do not communicate with computers that do not support IPSec** and click **Next**.
42. Select **High** for the security methods.
43. Click **Next** and click **Finish**.

You have now configured the IPSec VPN tunnel definition on Windows 2000.

18.3.6 Configuring a host-to-host VPN in the AIX server

Perform the following steps to configure a host-to-host VPN on AIXSRV1 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 to open the Internet Key Management (IKE) Tunnel configuration panel.
5. Select **Tunnel -> New Key Management Tunnel** to open the Key Management (Phase 1) Tunnel Properties window.
6. On the Identification panel, enter the key management tunnel name. In this scenario, it is WIN2000_AIXSRV1.
7. Select **IP address** as Host Identity type for the local and remote endpoints for the tunnel and enter the IP addresses of the local and remote hosts:
 - Local Host Identity: 192.168.100.3
 - Remote Host Identity: 172.16.3.5
8. Select the **Key (Phase 1) Policy** window. The Key Management (Phase 1) Tunnel Properties panel is displayed.
9. Select the **BOTH_MAIN_DES_MD5** policy from Defined key management (phase 1) policies and click **Associate**.
10. Select **Key**. The Key Management (Phase I) Tunnel Properties is displayed.
11. Enter the pre-shared key. Use a hexadecimal notation, for example, Hex 31, 32 is equivalent to the ASCII decimal value 1, 2... entered on the Windows 2000 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 Management Tunnel** on the Internet Key Exchange (IKE) Tunnels configuration panel or open the Data Management (Phase 2) Tunnel Properties window.
14. On the Identification panel, enter the data management tunnel name. In this scenario, it is WIN2000_AIXSRV1.
15. Select the key management tunnel that should be associated with this data management tunnel; in this scenario, it is WIN2000_AIXSRV1. Click **Associate**.

Note

Do not check Automatic data management tunnel if your side is the responder or you do not want to establish data management tunnel at system restart.

16. Click **Endpoints**. The Data Management (Phase 2) Tunnel Properties window is displayed.
17. For Local data endpoint enter:
 - Endpoint type: **Host** (this is a host-to-host scenario)
 - Host ID: **192.168.100.3**
 - Port: **23** (only Telnet from WIN2000 to AIXSVR1 is allowed)
 - Protocol: **TCP** (only Telnet from WIN2000 to AIXSVR1 is allowed)
18. For Remote data endpoint enter:
 - Endpoint type: **Host** (this is a host-to-host scenario)
 - Host ID: **172.16.3.5**
 - Port: **0** (Telnet client in WIN2000 is coming from an ephemeral port)
 - Protocol: **TCP** (only Telnet from WIN2000 to AIXSVR1 is allowed)
19. Click **Data (Phase 2) Policy**. The Data Management (Phase 2) Tunnel Properties panel is displayed.
20. Select **ESP_DES_MD5_TRANSPORT_NO_PFS** policy from Defined data management (phase 2) policies and click **Associate**.
21. Click **OK**.

Now the data management tunnel is configured. Wait for the tunnel creation request from the Windows 2000 server.

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 pane.

18.3.7 Starting the VPN connection

Start a Telnet session from WIN2000 to AIX:

```
Telnet 192.168.100.3
```

Use the IP Security Monitor (see 18.2.5, "Using the IP Security Monitor" on page 575) to determine that IPSec is properly used to secure this connection.

18.4 Windows 2000 remote access using L2TP

Windows 2000 supports both the Microsoft proprietary PPTP protocol and the IETF standard L2TP protocol to facilitate layer-2 tunneling VPN connections. PPTP is commonly available on Windows 95, Windows 98, and Windows NT systems for that purpose, but L2TP is the chosen industry standard for this type of VPN.

18.4.1 Scenario characteristics

This scenario assumes that the client accesses the Internet using whatever ISP is available. The client will then build an L2TP tunnel to a corporate gateway so that it will get an IP address in the intranet. The client will use the standard dial-up networking and L2TP VPN support that comes with Windows 2000.

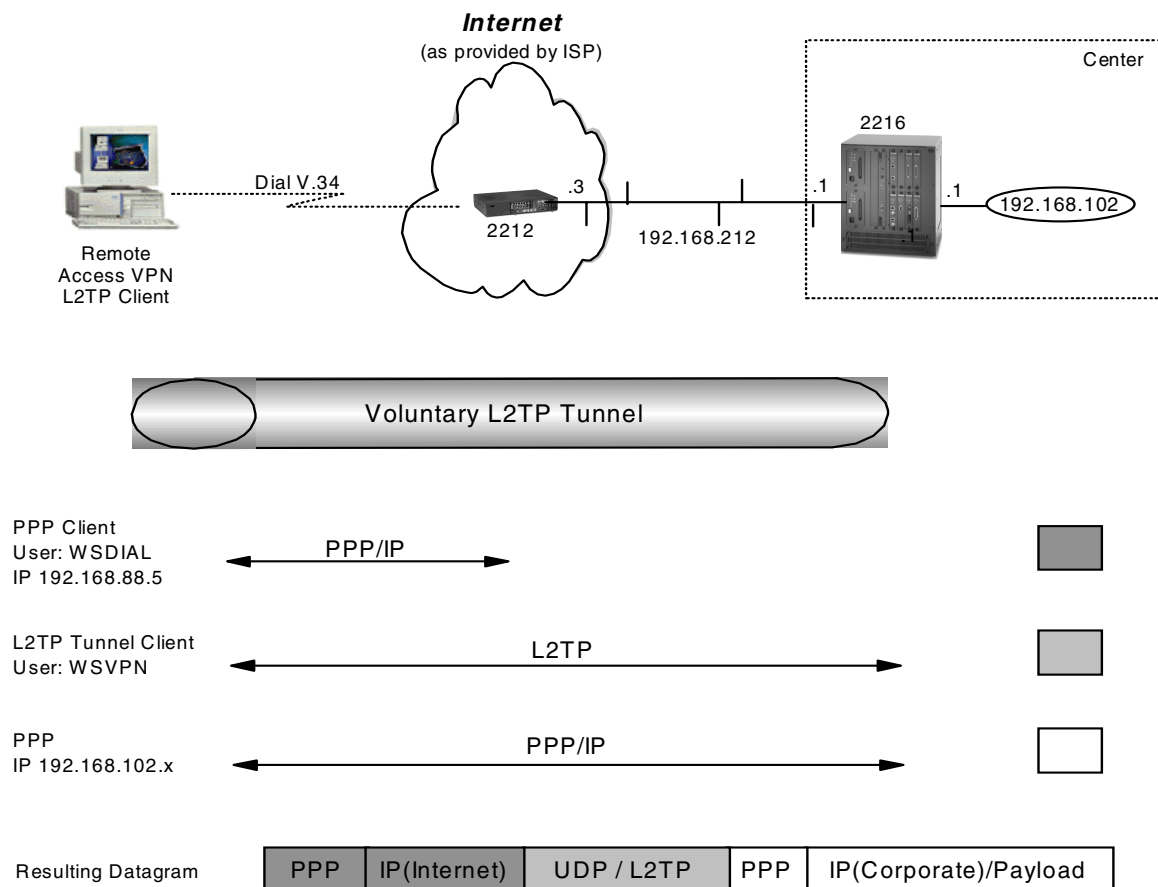


Figure 510. Creating an L2TP connection

In this scenario, the client will be assigned two IP addresses, one from the ISP and one from the corporate gateway, so the client will effectively have access to the Internet and the corporate network at the same time. This speeds up Internet access for the client but may be a security exposure to the corporate network in case the client is attacked and the L2TP tunnel is used as a backdoor by a hacker. For traveling users who need occasional access to corporate servers that cannot be accessed externally or by a Web browser but who do most of their other work over the Internet, this is certainly acceptable. For remote users who do

most of their work online to corporate servers, we recommend using PPP encryption.

18.4.1.1 Verifying initial connectivity

To make sure that you can reach your corporate VPN gateway or access server, start the ISP dial-up connection and try to ping the IP address of the server. If that is successful, chances are good that the L2TP tunnel initialization request and subsequent traffic through the tunnel will also reach the server.

18.4.2 Configuring the ISP router

This is the same as described in 15.2.2, “Configuration of the ISP router” on page 439.

18.4.3 Configuring the center router

For the configuration of the 2216 in the center we have to perform the following steps:

- Preparation.
- Enable L2TP and add layer-2 nets.
- Add a PPP user to the dial-in workstation.
- Add a default route to the Internet and enable ARP-subnet-routing.
- Activate the definitions on the center router.

18.4.3.1 Preparation

We assume that the permanent Ethernet connection to the ISP is already established. Therefore, we can concentrate on the dial-in features of this connection.

18.4.3.2 Configure L2TP

You now have to define the layer-2 tunnel. Tunnel authentication is disabled because the client has not been enabled to do this. If it has been enabled on the client you must leave it enabled here and define the tunnel through the `ADD TUNNEL-PROFILE` command.


```

Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets: [0]? 1
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 4
Defaulting data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.

Center Layer-2-Tunneling Config>ENABLE L2TP

Restart system for changes to take effect.
Center Layer-2-Tunneling Config>ENABLE FIXED-UDP-SOURCE-PORT
Center Layer-2-Tunneling Config>DISABLE TUNNEL-AUTH
Center Layer-2-Tunneling Config>LIST all
GENERAL ADMINISTRATION
-----
L2TP                               = Enabled
PPTP                               = Disabled
L2F                                 = Disabled
Maximum number of tunnels          = 30
Maximum number of calls (total)    = 100
Buffers Requested                   = 200

CONTROL CHANNEL SETTINGS
-----
Tunnel Auth                         = Disabled
Tunnel Rcv Window                   = 4
Retransmit Retries                  = 6
Local Hostname                      = IBM

DATA CHANNEL SETTINGS
-----
Force CHAP Challenge (extra security)= Disabled
Hiding for PAP Attributes            = Disabled
Hardware Error Polling Period (Sec) = 120
Sequencing                           = Enabled

MISCELLANEOUS
-----
Send Proxy-LCP                      = Enabled
Send Proxy-AUTH                     = Enabled
Fixed UDP source port (1701)        = Enabled
Fixed source IP Address              = Disabled

```

Figure 511. Center router L2TP configuration for L2TP + IPsec

18.4.3.3 Add PPP user

The next step is to define the PPP user and to reload the router. The IP address handed out to this PPP user is given out from a pool of corporate IP addresses and can also be assigned using DHCP or RADIUS. To systems inside the corporate network the remote client will thus appear to also be inside the corporate network.

```

Center Config>ADD PPP-USER
Enter name: []? vpnclient
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALS' user? (Yes, No): [Yes]
Type of route? (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]? 192.168.102.110
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]

      PPP user name: vpnclient
      User IP address: 192.168.102.110
      Netroute Mask: 255.255.255.255
      Hostname: <undefined>
      Virtual Conn: disabled
      Time allotted: Box Default
      Callback type: disabled
      Encryption: disabled
      Status: enabled
      Account Expiry: <unlimited>
      Password Expiry: <unlimited>

Is information correct? (Yes, No, Quit): [Yes] y

```

Figure 512. Center router PPP user configuration for L2TP + IPsec

18.4.3.4 Add default route and enable ARP-subnet-routing

These steps and the reasons for performing them are the same as described in 19.4.2.9, “Add default route and enable ARP subnet routing” on page 635 for the PPTP scenario.

18.4.3.5 Activate the definitions on the center router

You activate the definitions on the center router with the command `restart` (Figure 513):

```

Center Config>WRITE
Config Save: Using bank B and config number 3
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y

```

Figure 513. Reloading the center router

18.4.4 Configuring the Windows 2000 client

To use a remote access VPN connection with L2TP or PPTP, you have to define two dial-up networking profiles, one for the PPP connection to your ISP, another for the actual layer-2 tunnel.

18.4.4.1 Configuring a dial-up connection to the ISP

Follow the steps below to create a PPP connection profile to dial to our ISP:

1. Click **Start -> Settings -> Control Panel -> Network and Dial-up Connections -> Make New Connection**. This brings up the Connection Wizard.
2. Click **Next** and select **Dial-up to the Internet**.

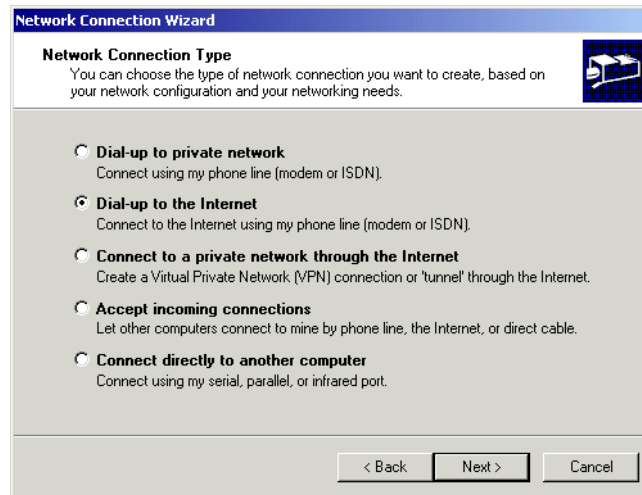


Figure 514. Windows 2000 dial-up connection - ISP

3. Click **Next** and select **Manually define connection**.

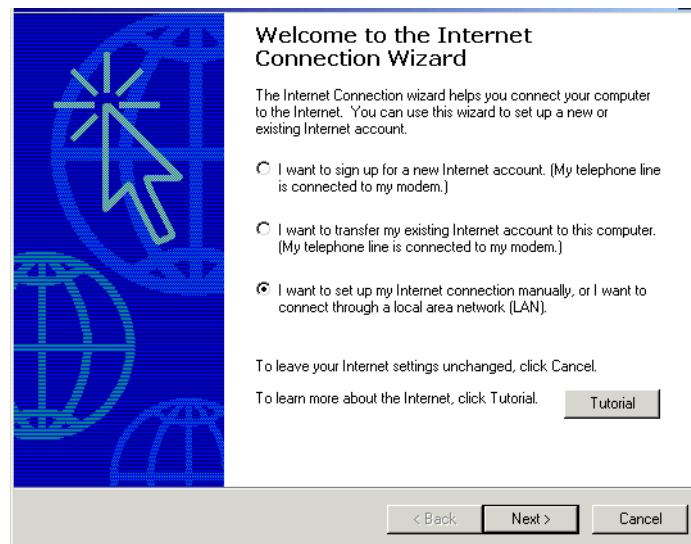


Figure 515. Windows 2000 dial-up connection - Internet Connection

4. Click **Next** and select **Connect through a modem**.

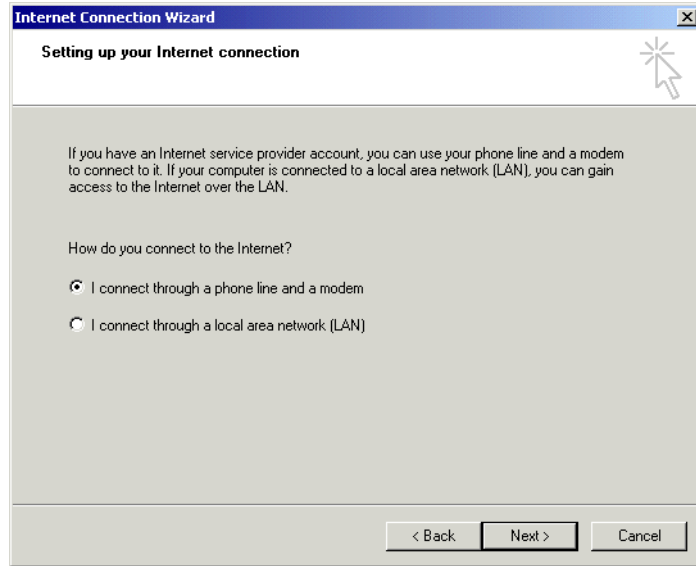


Figure 516. Windows 2000 dial-up connection - modem connection

5. Click **Next** and fill in the necessary parameters on the connection information step 1 of 3 window:

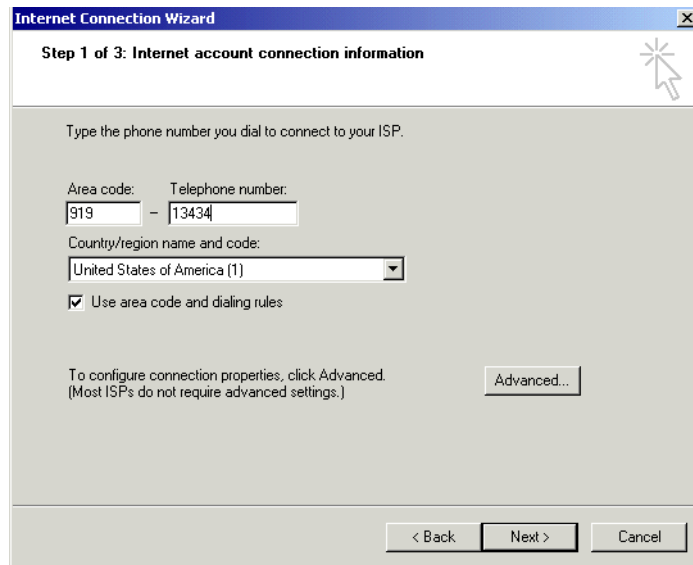


Figure 517. Windows 2000 dial-up connection - calling parameters

6. Click **Advanced** to configure additional settings pertaining to your connection.

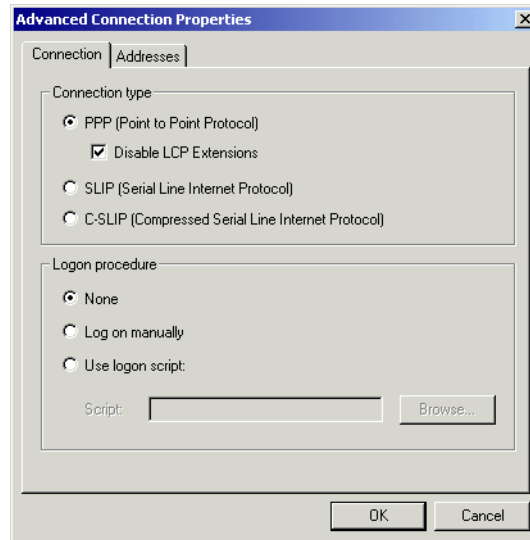


Figure 518. Windows 2000 dial-up connection - advanced settings

7. Click **Next** and enter the user ID and password for this connection, in our case, `wsdial` and `wsdial`.
8. Click **Next** and enter a name for this dial-up connection entry.
9. Select **No** to not set up an Internet account at this time and click **Next**.
10. If you want to test the connection, leave the check box at the default and click **Finish**; otherwise, select not to connect at this time and click **Finish**.
11. If you do not want to be prompted to enter a user ID and password for the ISP connection every time, highlight the dial-up entry, click the right mouse button and select **Properties** -> **Options**. Uncheck the box to prompt for a user ID.

18.4.4.2 Configuring an L2TP VPN connection

Follow the steps below to create a VPN connection profile to a corporate access server using L2TP:

1. Click **Start** -> **Settings** -> **Control Panel** -> **Network and Dial-up Connections** -> **Make New Connection**. This brings up the Connection Wizard.
2. Click **Next** and select **Connect to private network through the Internet**.

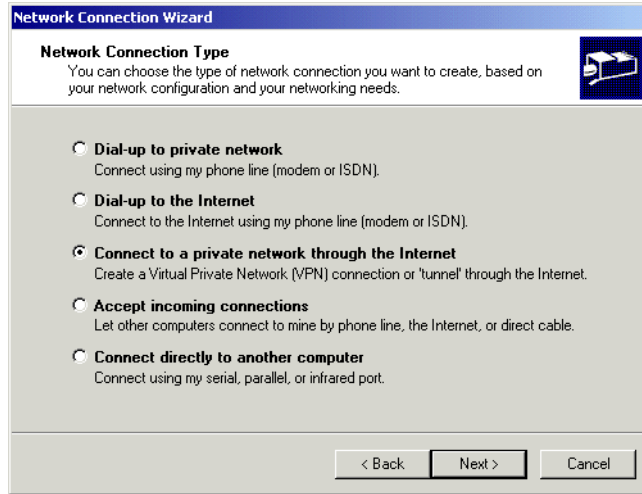


Figure 519. Windows 2000 VPN connection

3. Click **Next**. Check **Automatically dial this initial connection** and select the previously defined dial-up entry. This will invoke the dial-up to the ISP before the L2TP tunnel will be started.

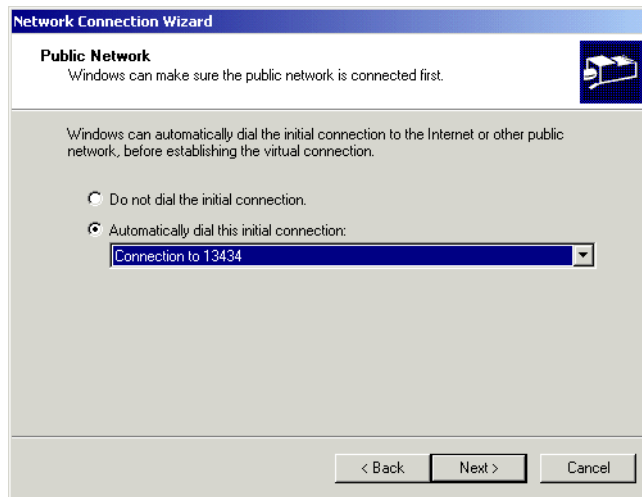


Figure 520. Windows 2000 VPN connection - ISP profile

4. Click **Next** and enter the IP address of the tunnel server.

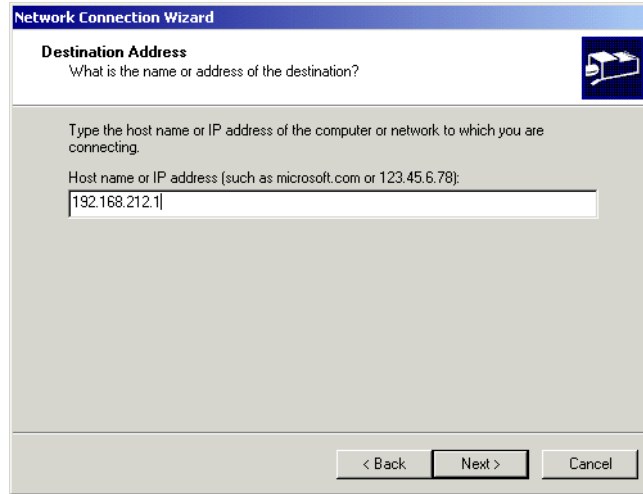


Figure 521. Windows 2000 dial-up connection - tunnel server

5. Click **Next** and select if this connection is to be available to all users or just to yourself.
6. Click **Next** and specify if you want to share this Internet connection with other computers on the local LAN. This will effectively turn your computer into a VPN gateway to connect a remote LAN to a corporate network.
7. Click **Next** and enter a name for this VPN connection, then click **Finish**.
8. To specify that this VPN connection should use L2TP, highlight the dial-up entry, click the right mouse button and select **Properties -> Networking -> Type of Server** and select **L2TP**.

Note

By default, the server type is set to Automatic, which allows Windows 2000 to determine whether to use L2TP or PPTP.

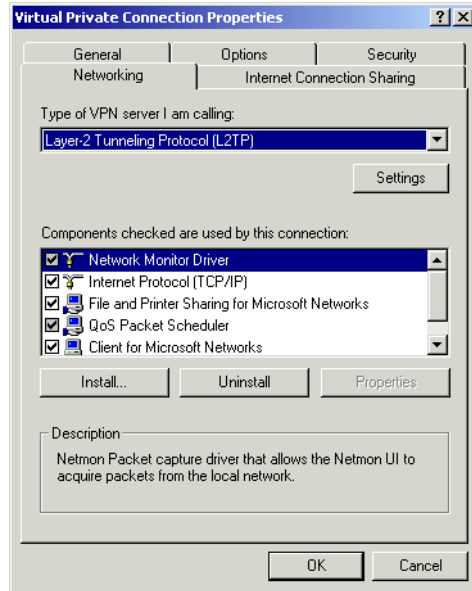


Figure 522. Windows 2000 dial-up connection - L2TP

9. Click **Settings** to specify additional options pertaining to your connection.

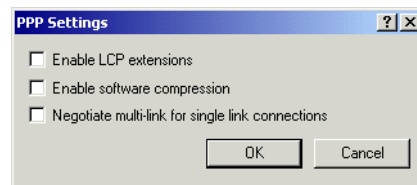


Figure 523. Windows 2000 dial-up connection - advanced PPP settings

10. If you do not want to be prompted to enter a user ID and password for the ISP connection every time, highlight the dial-up entry, click the right mouse button and select **Properties -> Options**. Uncheck the box to prompt for a user ID.

18.4.5 Starting the VPN connection

From the Network and Dial-up Connections window shown in Figure 518 on page 589, double-click the VPN connection to start it. If configured properly, it will first dial the ISP connection and then establish the L2TP tunnel to the corporate access server.

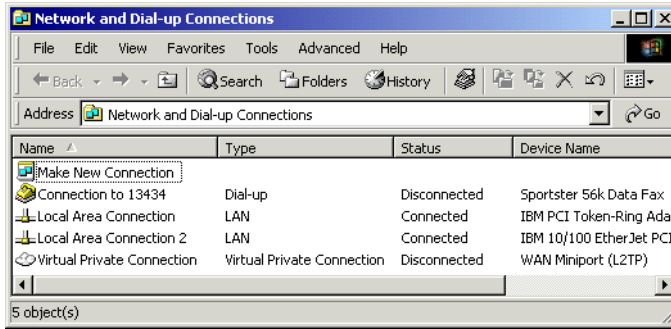


Figure 524. Windows 2000 dial-up connection - ISP

Note

When you start the ISP connection implicitly via the VPN connection, it will also be terminated when you close the VPN connection.

If you start the ISP connection and VPN connection separately, you can also terminate them separately. In that case, do not configure the VPN connection to automatically start the ISP connection.

18.4.6 Verification tests

Once the ISP and VPN connections have been established, an icon for each of them will be placed on the Windows task bar by default. Double-click the VPN connection icon to bring up the connection status window.

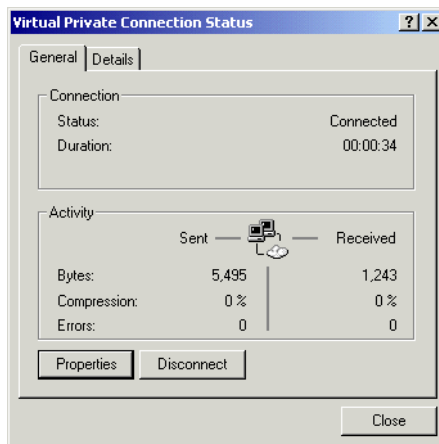


Figure 525. Windows 2000 VPN connection - status

Click **Properties** and select the **Details** tab to find out if the L2TP tunnel parameters have been properly configured by the LNS, in particular, the IP address that has been assigned to this system from the corporate address pool.

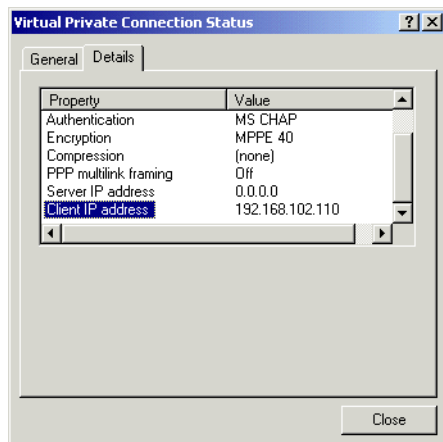


Figure 526. Windows 2000 VPN connection - details

Verify the routing table to see if all traffic is defaulted into the L2TP tunnel using the command shown below:

```

=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 04 ac 98 c3 52 ..... IBM 10/100 EtherJet PCI Adapter
0x3 ...00 06 29 b3 20 ae ..... IBM Token-Ring PCI Family Adapter
0x8000005 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
0xd000006 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
=====

Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          192.168.88.5     192.168.88.5     2
0.0.0.0                    0.0.0.0          192.168.102.110 192.168.102.110 1
0.0.0.0                    0.0.0.0          172.16.3.2       172.16.3.5       3
0.0.0.0                    0.0.0.0          192.168.103.1    192.168.103.5    3
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1        1
172.16.3.0                 255.255.255.0    172.16.3.5       172.16.3.5       1
172.16.3.5                 255.255.255.255  127.0.0.1        127.0.0.1        1
172.16.255.255            255.255.255.255  172.16.3.5       172.16.3.5       1
192.168.88.5              255.255.255.255  127.0.0.1        127.0.0.1        1
192.168.88.255            255.255.255.255  192.168.88.5     192.168.88.5     1
192.168.102.110           255.255.255.255  127.0.0.1        127.0.0.1        1
192.168.102.255           255.255.255.255  192.168.102.110 192.168.102.110 1
192.168.103.0             255.255.255.0    192.168.103.5    192.168.103.5    1
192.168.103.5             255.255.255.255  127.0.0.1        127.0.0.1        1
192.168.103.255           255.255.255.255  192.168.103.5    192.168.103.5    1
192.168.212.1             255.255.255.255  192.168.88.5     192.168.88.5     1
224.0.0.0                 224.0.0.0        172.16.3.5       172.16.3.5       1
224.0.0.0                 224.0.0.0        192.168.88.5     192.168.88.5     1
224.0.0.0                 224.0.0.0        192.168.102.110 192.168.102.110 1
224.0.0.0                 224.0.0.0        192.168.103.5    192.168.103.5    1
255.255.255.255          255.255.255.255  172.16.3.5       172.16.3.5       1
Default Gateway:         192.168.102.110
=====

Persistent Routes:
None
=====

```

Figure 527. Windows 2000 - verifying routing tables for L2TP connection

Note

Our Windows 2000 server had a token-ring and an Ethernet adapter installed in addition to the dial-up connection. Therefore, you see more routes in the screen above than you would in a pure dial-up environment.

On the center router, check that the L2TP tunnel is up and that the PPP user is authenticated using the commands shown below:

```
Center *TALK 5

Center +FEATURE Layer-2-Tunneling
Layer-2-Tunneling Information
Center Layer-2-Tunneling Console> TUNNEL STATE
Tunnel ID | Type | Peer ID | State | Time Since Chg | # Calls | Flags
24533 | L2TP | 11 | Established | 1: 3:47 | 1 | TL F
Center Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
24533 | L2TP | 761 | 100945 | 868 | 58429 | 7 | 19
Center Layer-2-Tunneling Console> TUNNEL TRANSPORT
Tunnel ID | Type | Peer IP Address | UDP Src | UDP Dest
24533 | L2TP | 192.168.88.5 | 1701 | 1701
Center Layer-2-Tunneling Console> EXIT
Center +FEATURE AUTH
AAA Information
Center AAA Console> LIST ONLINE USERS PPP
List (Name, Verb, Addr, VCon, Call, Time, Encr): [Verb]
Active PPP entities:
    Net: 5
    PPP user name: vpnclient
    User IP address: 192.168.102.110
    Netroute Mask: 255.255.255.255
    Hostname: <undefined>
    Virtual Conn: disabled
    Time allotted: Unlimited
    TimeConnected: 01:05:13
    TimeRemaining: Unlimited
    Callback type: disabled
    Encryption: disabled
    Status: enabled
    Account Expiry: <unlimited>
    Password Expiry: <unlimited>

1 PPP record displayed.

Center AAA Console>
```

Figure 528. Windows 2000 - verifying L2TP status at the LNS

18.4.7 Using IPSec inside an L2TP tunnel

As mentioned in 18.1, “Windows 2000 VPN capabilities” on page 557, IP traffic that flows through a layer-2 tunnel can be protected by IPSec even though the layer-2 tunnel itself is not IPSec protected. This will be sufficient if IP is the only protocol that uses the layer-2 tunnel.

The protocols used in this scenario are illustrated in Figure 529, which is a slight modification from the scenario shown in Figure 17 on page 30.

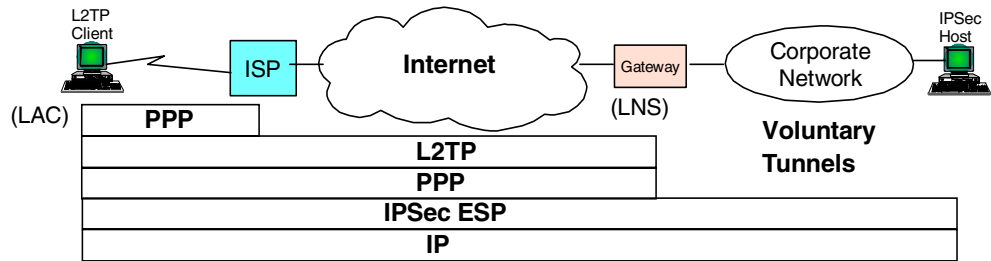


Figure 529. Windows 2000 - IPsec over L2TP

We have tested this configuration successfully but do not describe it here in detail. It is basically a combination of the two scenarios described in 18.3, “Windows 2000 to AIX 4.3.2, host-to-host” on page 576 and 18.4, “Windows 2000 remote access using L2TP” on page 583. The difference is that the IPsec connection on the Windows 2000 side uses the IP address received from the LNS.

Chapter 19. Interoperability with OEM VPN products

This chapter describes interoperability scenarios between the aforementioned IBM VPN solutions and VPN clients developed by other companies. Because of the extensive list of such clients, we have limited our tests to just a few. This does not mean that the others will not work with an IBM VPN product.

Some vendors do not sell their VPN technology commercially but make them available to other companies to include in their products. We have chosen VPN clients that were, at the time of writing, commercially available from their manufacturers so that you can purchase them if they fit your VPN requirements.

Caveat

Many VPN client products we have tested - with the exception of Windows 2000, which is not yet released - do not, at the time of writing, support token-ring. In fact, if you are using some VPN clients on a system that has a token-ring adapter installed, chances are that the system may crash as soon as you enable an IPsec policy. We suggest that you perform careful and rigid testing of any VPN client that you want to use on Windows systems equipped with token-ring network adapters.

19.1 IRE SafeNet VPN client

Information Resource Engineering, Inc. (IRE) is a company that develops software for other vendors to include in their products. Cisco Systems, Inc., for example, has licensed SafeNet as its client solution for VPNs. IRE also distributes some of their products commercially. The generally available version of the IRE VPN client is called SafeNet/Soft-PK. We used Version 2.0.7, build 18, of SafeNet (we will use this shortened name throughout this redbook) for our interoperability scenarios. To find more information about SafeNet and how you can purchase it, please access the URL below:

<http://www.ire.com>

19.1.1 SafeNet VPN client capabilities

The IRE VPN client offers one of the richest sets of VPN features available in the market today, ranging from manual IPsec tunnels to IKE support with digital certificates and online CA support to remote access capability with a private IP address. We have therefore chosen this client for several scenarios in this redbook. In particular, we have successfully tested the IRE SafeNet VPN client in combination with the following VPN platforms:

- IBM AIX
- IBM OS/400
- IBM routers
- Cisco routers
- Windows 2000

This section briefly lists the VPN capabilities of the IRE VPN client:

Table 127. SafeNet VPN Client 2.0.7 - VPN features

| Feature | |
|----------------------------------|---|
| Tunnel Type | IKE, manual |
| IPSec Header Format | RFCs 24xx |
| Operating Systems Supported | Windows NT, Windows 98, Windows 95 |
| Interfaces Supported | Ethernet, Dial-up |
| IKE | |
| Key Management Tunnel (Phase 1) | |
| Negotiation Mode | Main Mode, Aggressive Mode |
| Encryption Algorithm | DES, 3DES |
| Authentication Method | Pre-Shared Key, RSA Signatures |
| Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| Diffie-Hellman Group | Group 1, Group 2 |
| Send Phase 1 Delete | Yes |
| On-demand Tunnels | Yes |
| Data Management Tunnel (Phase 2) | |
| Encapsulation Mode | Tunnel Mode, Transport Mode |
| Security Protocol | AH, ESP (not both in beta version) |
| AH Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| ESP Encryption Algorithm | DES, 3DES |
| ESP Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| Multiple SA Proposals | Yes |
| Perfect Forward Secrecy (PFS) | Yes |
| Other | Logging, Certificates, Private (Virtual) IP Address |

We used an IBM PC 750 with Windows 98 as a client workstation for this scenario.

Configuration of the IRE client for LAN connections and digital certificates is discussed in this chapter. Configuration for remote access is shown in 15.2.6, "Configuration of the IRE SafeNet VPN Client" on page 449.

19.1.2 Client installation

For remote access VPNs, SafeNet VPN client requires Microsoft Dial-Up Networking 1.2 or higher on Windows 95.

To install SafeNet, click **Setup** in the directory in which the software has been unpacked, then follow the instructions on the screen. Once the setup procedure has finished, reboot your system.

19.1.3 Client configuration for LAN connections

After the system has been rebooted, SafeNet starts automatically and minimizes itself to the task bar.

1. Right mouse click the task bar icon and select **Security Policy Editor** from the context menu.



Figure 530. IRE SafeNet - task bar icon context menu

2. Create a new connection via **File -> New Connection**.

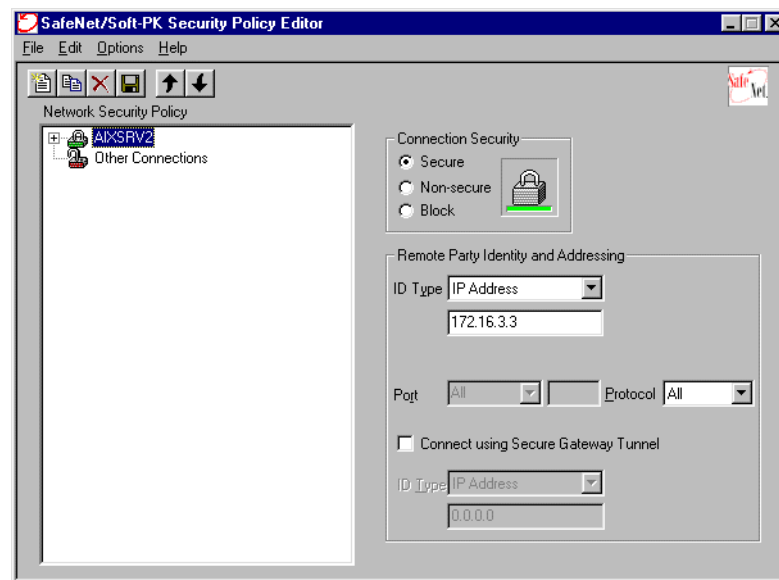


Figure 531. IRE SafeNet - Security Policy Editor

3. Mark **Secure** to protect this connection with IPsec. Select **IP address** as the ID Type and enter the remote party's IP address, which in our case is the AIXSRV2 server at 172.16.3.3. Do not check Connect using Secure Gateway Tunnel because you are building an end-to-end connection in this scenario.
4. Expand all objects in the connection tree by clicking the **(+)** signs next to them, then click **My Identity**.

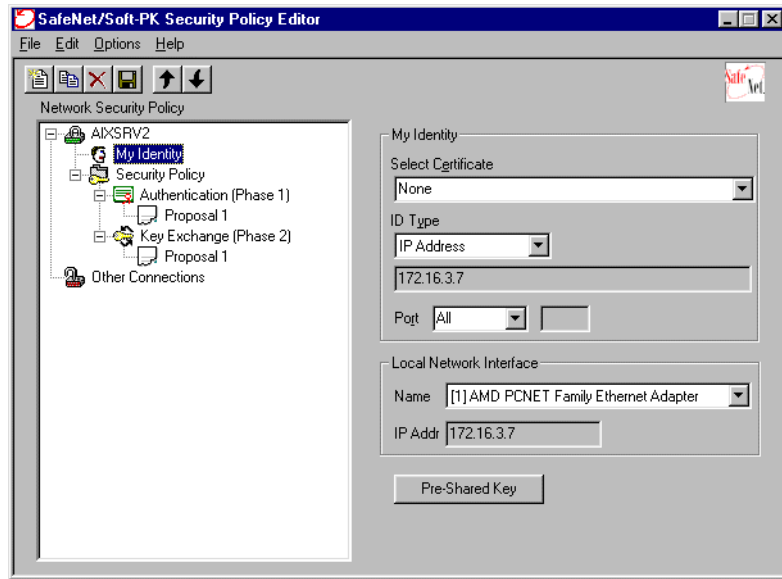


Figure 532. IRE SafeNet - client IKE identity

5. Select **IP address** as the ID type and then choose a Local Network Interface, which will insert the appropriate IP address that is configured for that interface, in our case, Ethernet and 172.16.3.7. If you were using certificates, you would have to select one that you have previously requested and received using the Certificate Manager.
6. Click the **Pre-Shared Key** button, then click **Enter Key** and enter the value for the pre-shared key. Click **OK** when done.

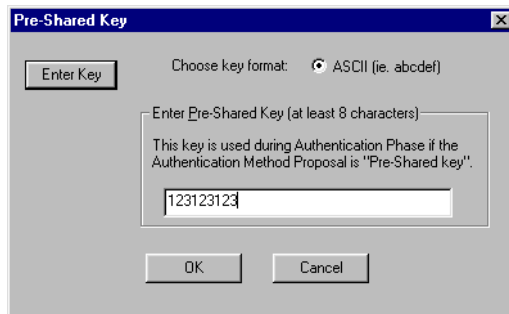


Figure 533. IRE SafeNet - Pre-Shared Key

7. Click **Security Policy** and select **Main Mode**. Note that replay protection is enabled by default but can be disabled if you do not want to use it. Do not check PFS.

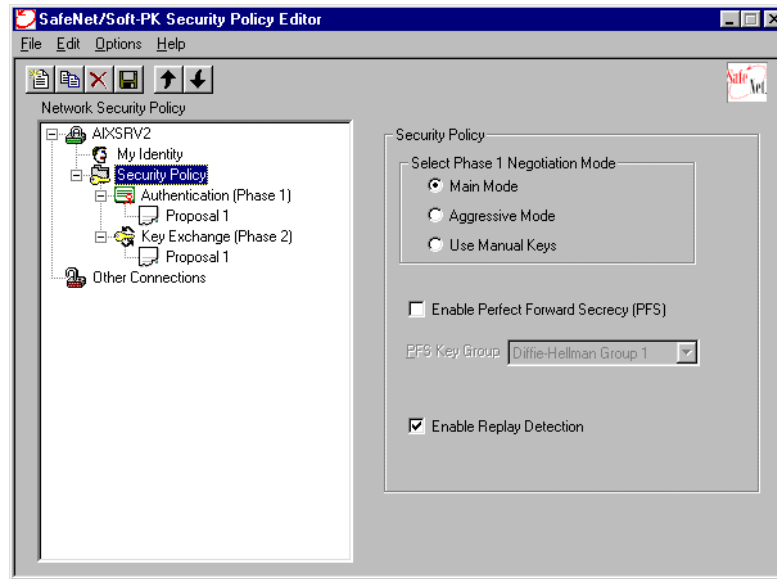


Figure 534. IRE SafeNet - security policy

8. Click **Proposal 1** under Authentication (Phase 1) to see the default phase 1 proposal. You can edit this proposal or add new proposals if you wish. We decided to modify the proposal as shown in Figure 535:

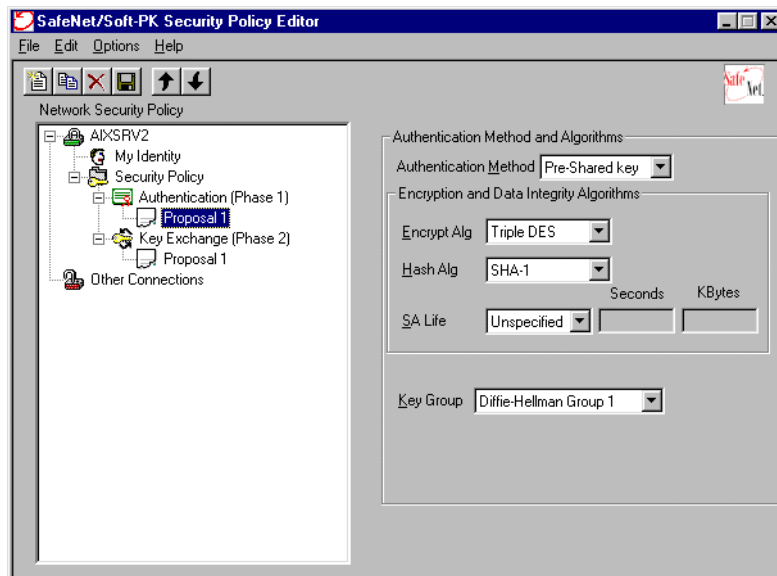


Figure 535. IRE SafeNet - phase 1 proposal

9. Click **Proposal 1** under Key Exchange (Phase 2) to see the default phase 2 proposal. You can edit this proposal or add new proposals if you wish. We decided to modify the proposal as shown in Figure 536 on page 602.

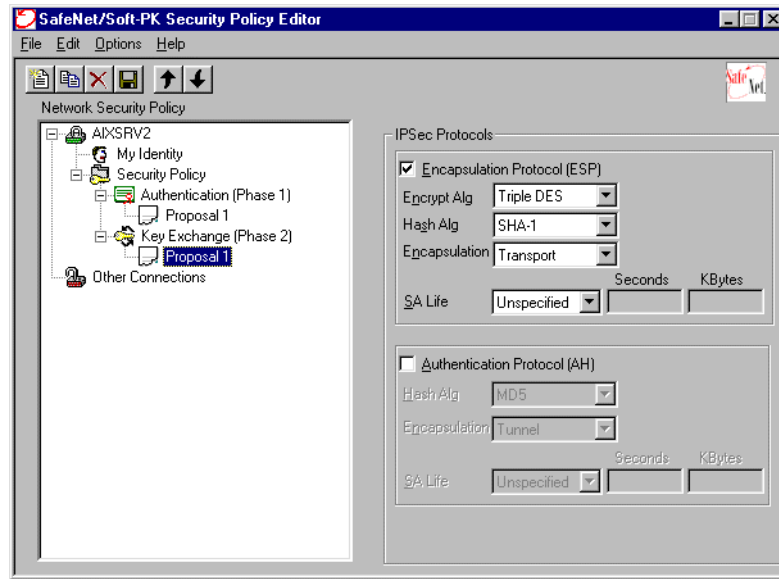


Figure 536. IRE SafeNet - security policy phase 2

10. Click **File->Save** to save the policy and then select **Reload Policy** from the task bar icon context menu.

19.1.4 Building a LAN connection

Once the policy has been reloaded, the SafeNet VPN client is checking any outgoing packet to see if it matches a secure traffic profile. If it does, then IKE negotiations are started as defined in the security policy. If successful, matching traffic will be secured with IPSec as defined in the security policy.

Likewise, any incoming packet is checked to see if it matches a secure traffic profile. If it does, IPSec will be used as defined in the security policy, or, in case of IKE packets, appropriate IKE response messages will be sent to negotiate new SAs for that traffic. If successful, matching traffic will be secured with IPSec as defined in the security policy.

This resembles exactly the behavior described in 3.3.1, “Outbound IPSec processing for host systems” on page 69.

From the context menu, select **Log Viewer** to determine if everything goes as it should. To initiate IKE negotiations, simply access AIXSRV2 for which a security policy has been defined. Provided the partner is ready to respond, you see in the log that IKE main mode and quick mode are completed successfully and SAs are established to protect traffic with IPSec.

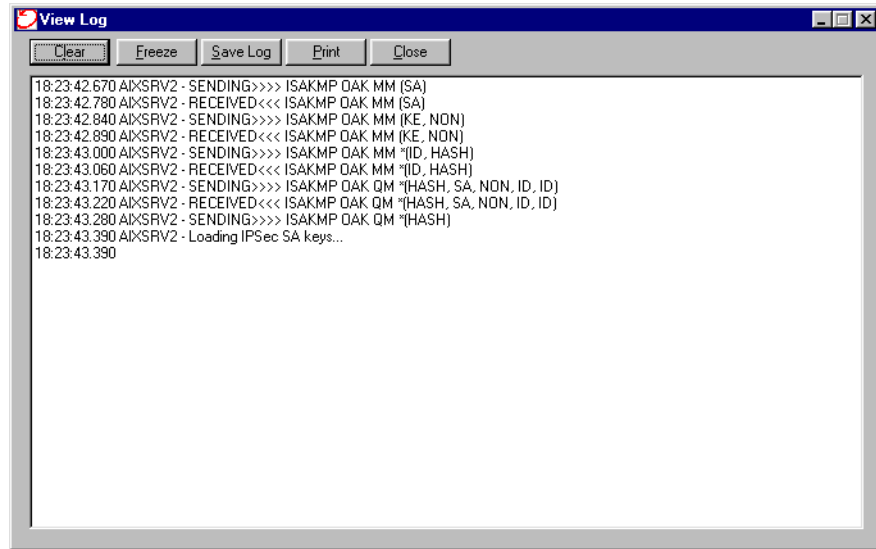


Figure 537. IRE SafeNet - Log viewer for LAN connection

To act as a responder, just ping the client from AIXSRV2 and check the log for details.

19.1.5 Client configuration for certificates

The IRE SafeNet VPN client supports manual and online requests of certificates and supports a variety of CA products, such as Verisign, Netscape and Microsoft. Because the CA we have built internally uses software from Entrust, we had to follow the manual process to request and receive the CA certificate and the client's VPN certificate. IRE and Entrust are currently working on improving this situation.

In the example below, we perform the following steps to obtain a client and a CA certificate that will be used by the client to authenticate IKE exchanges to a Cisco router. The corresponding Cisco configuration is shown in 17.6, "Using digital certificates for IKE authentication" on page 548.

1. From the SafeNet task bar icon, select **Certificate Manager**.
2. On the My Certificates panel (see Figure 538), click **Request Certificate**.

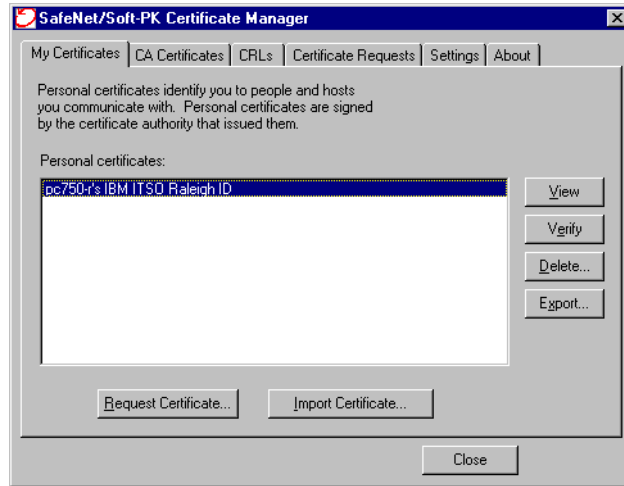


Figure 538. IRE SafeNet - Certificate Manager

Fill in the certificate request form and select the **File** option for the Enrollment method, as shown in Figure 539:

Figure 539. IRE SafeNet - Certificate Request form

3. Click **OK**. This will generate a private and public key pair and a PKCS#10 certificate request file in the directory and with the name you have specified. This file is shown in Figure 540 on page 605:

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB0zCCATwCAQAwSzELMAkGA1UEBhMCVVMxDTALBgNVBAGTBE4uQy4xDDAKBgNV
BAoTA01CTTENMAsgA1UECxmESVRITzEQMA4GA1UEAxMHcGM3NTAtc jCBnzANBgkq
hkIG9w0BAQEFAAOBjQAwYkCgYEAz5jIPsbpJ1Cn2Ux19si60CFQqpUYGKIEBZg/
HRoghEwOi/51jYV0SLiXD86WYliQx6rVtLBYLhwZUlbiThjJcYmyZ6sMMndX30igB
hKogJkGQF+7v6OxmxCXYR4ng+Pod04m1K0siGgX7s8AYsC9qR2sjGAz1vjXkD0qa
/VwqLSkCAwEAAaBIMEYGCsGSIb3DQEJJDjE5MDcwNQYDVR0RBC4wLlIcErBADB4ES
cGM3NTAtckB1cy5pYm0uY29tghBpdHNvLnJhbC5pYm0uY29tMA0GCSqGSIb3DQEB
BAUAA4GBADDk31RQma1sIJmDi63bhTZ57W1eaXCf4/d5YuyZzp5gjsWTozP0zohy
F+ZVCnamLWLE7Iv0+3eL/iPpVUJb8ysGAM89AZUqhwR58ITblSetFeT41WljNcU
p1UhD7M9peEw9mWZPaqWDE9NCPccAZn4G1NSK6gUgiuEv+5ACUk6
-----END NEW CERTIFICATE REQUEST-----

```

Figure 540. IRE SafeNet - certificate request

4. Send this certificate to your CA in a secure manner. Some CAs support secure HTTP over SSL, some support secure e-mail. Remember, we cannot yet use an online protocol such as CEP with the IRE client and an Entrust CA. Because our CA was local, though, this was a relatively easy step.
5. Once your certificate has been processed by your CA, you should receive a client certificate (shown in Figure 541) and a CA certificate (shown in Figure 542 on page 606).

```

MIIDLzCCApiGAWIBAgIEN8/n0jANBgkqhkiG9w0BAQUFADBBMQwwCgYDVQQKEwNj
Qk0xCzAJBgNVBAYTAlVIMQ0wCwYDVQQHEwR0LkMuMRUwEwYDVQQLEwxiJVFNPiFJh
bGVpZ2gwHhcNOTkwOTMwMTkxMTE3WhcNMDIwOTMwMTkxMTE3WjBTMQwwCgYDVQQK
EwNjQk0xCzAJBgNVBAYTAlVIMQ0wCwYDVQQHEwR0LkMuMRUwEwYDVQQLEwxiJVFNP
iFJhbGVpZ2gxEDA0BjQAwYkCgYEAz5jIPsbpJ1Cn2Ux19si60CFQqpUYGKIEBZg/
HRoghEwOi/51jYV0SLiXD86WYliQx6rVtLBYLhwZUlbiThjJcYmyZ6sMMndX30igB
hKogJkGQF+7v6OxmxCXYR4ng+Pod04m1K0siGgX7s8AYsC9qR2sjGAz1vjXkD0qa
/VwqLSkCAwEAAaBIMEYGCsGSIb3DQEJJDjE5MDcwNQYDVR0RBC4wLlIcErBADB4ES
cGM3NTAtckB1cy5pYm0uY29tghBpdHNvLnJhbC5pYm0uY29tMA0GCSqGSIb3DQEB
BAUAA4GBADDk31RQma1sIJmDi63bhTZ57W1eaXCf4/d5YuyZzp5gjsWTozP0zohy
F+ZVCnamLWLE7Iv0+3eL/iPpVUJb8ysGAM89AZUqhwR58ITblSetFeT41WljNcU
p1UhD7M9peEw9mWZPaqWDE9NCPccAZn4G1NSK6gUgiuEv+5ACUk6
-----END NEW CERTIFICATE REQUEST-----

```

Figure 541. IRE SafeNet - client certificate

```

-----BEGIN CERTIFICATE-----
MIIDGjCCAoOgAwIBAgIEN8/n1zANBgkqhkiG9w0BAQUFADBBMQwwCgYDVQQKEwNj
Qk0xCzAJBgNVBAYTAlVIMQ0wCwYDVQQHEwRlkmUMRUwEwYDVQQLEwxiJVFNPIFJh
bGVpZ2gwHhcNOTkwOTAzMTQ1MjAyWWhcNMTkwOTAzMTUyMjAyWjBBMQwwCgYDVQQK
EwNjQk0xCzAJBgNVBAYTAlVIMQ0wCwYDVQQHEwRlkmUMRUwEwYDVQQLEwxiJVFNPI
IFJhbGVpZ2gwZ2gZ0wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBAL1gbf2uLLbtDgUy
VsEZ9wLxpmMbKk5V6iQ4IFTCAUGVre6vx/fbh1C0n3XugjcBgKEBppsO0DE4tF3p
kP1SKU6cNO5U2X6Y+B00g70UMeDwGjmPzA3awc1dkbKhePr0No9myi.2vh0at8GGw
/IvPVF3DqeTdw44nEQjwGdLZ7RODagEo4IBHzCCARsweQYJYIZIAYb4QgEBBAQD
AgAHMGMGA1UdHwRcMFowWKEwoFskUjBQMqwwCgYDVQQKEwNjQk0xCzAJBgNVBAYT
AlVIMQ0wCwYDVQQHEwRlkmUMRUwEwYDVQQLEwxiJVFNPIFJhbGVpZ2gxDTALBgNV
BAMTBENSTDEwKwYDVROQBQcWIoAPMTk5OTA5MDMxNDUyMDJagQ8yMDE5MDkwMzE0
NTIwM1owCwYDVROPBAAQDAgEGMB8GA1UdIwQYMBaAFTXmk13C8I+vIyk/pVOvc6q9
OggzMB0GA1UdDgQWBBSF5pNdwvCPryMpP6VTr3OqvdIIMzAMBgnVHRMEBTADAQH/
MBkGCSqGSIb3fQdBAQMMAobBFY0LjADAgSQMA0GCSqGSIb3DQEBBQUAA4GBALdQ
Gm2rPTkKZ5r/Ghy7WZJD/41exm5NY24CnCrFecTMPDN3x5RHAMwOeIBCnjNGeGeH
QBALU17govD2AQ1AeMVV/7+MvLVsNmAPTshYaaF90PfF31grKJ+duxqMmOJdz/bj
cDtgcufvxOhlZXqUfjxi87KM7cC/Cu2NeIKbhXoT
-----END CERTIFICATE-----

```

Figure 542. IRE SafeNet - CA certificate

6. On the CA Certificates panel, click **Import Certificate**, as shown in Figure 543. Select the file that holds your CA certificate.

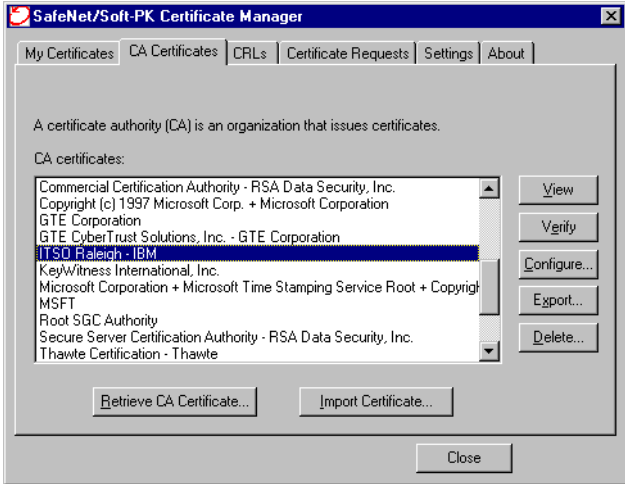


Figure 543. IRE SafeNet - import CA certificate

7. On the My Certificates panel (see Figure 538 on page 604), select **Import Certificate**. Select the file that holds your client certificate.
8. Highlight the new certificate and click **Verify**. This is a test to see if the client certificate was indeed issued by your CA.
9. Click **Close** to exit from Certificate Manager.
10. In the Security Policy Editor (see Figure 544 on page 607), create a new policy and choose **Domain Name** as the ID type of the remote system because that is the ID contained in the certificate (see 17.6.1, “Generating keys and requesting certificates” on page 548).

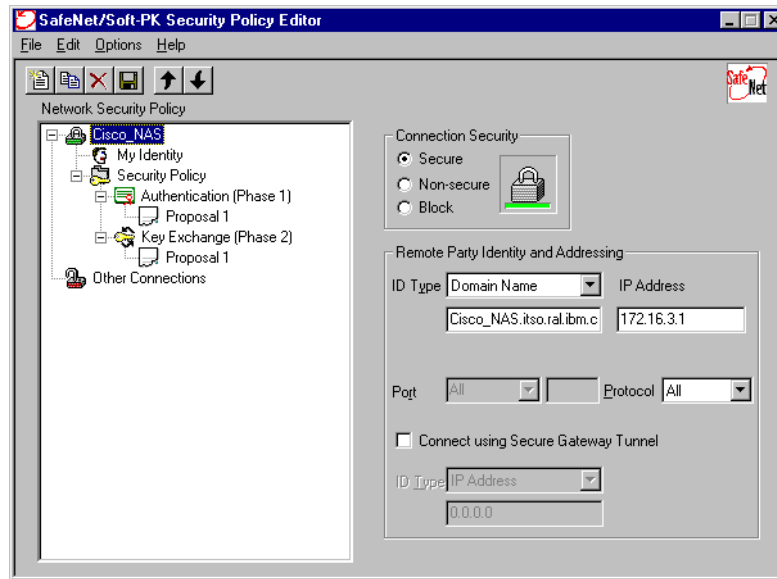


Figure 544. IRE SafeNet - Remote ID using a certificate

11. Click **My Identity** and select the client certificate that you have previously received. As ID type, select **E-mail Address** because that is where the client ID is stored in the VPN certificate with this release of the IRE client and when you are using an Entrust CA. You will see (Figure 545) that the name contained in this field is not an e-mail address but the value that your CA administrator has entered as `subject_alternate_name` in the VPN certificate.

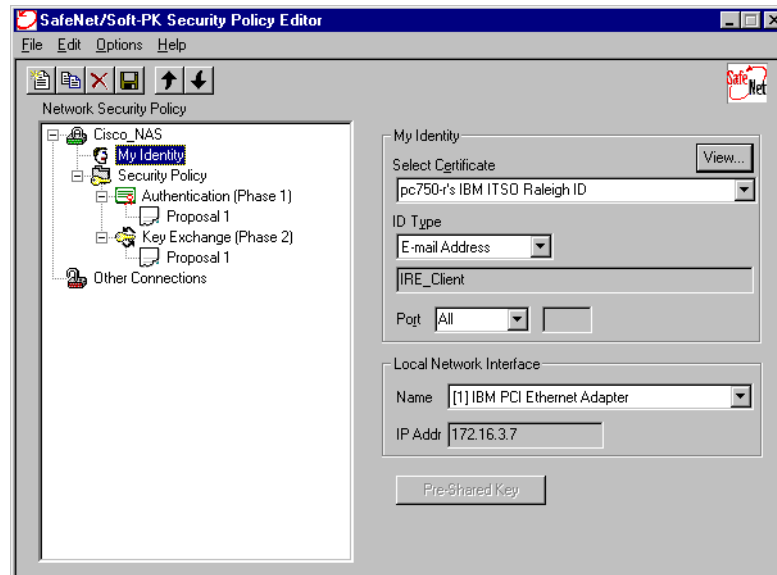


Figure 545. IRE SafeNet - local identity using a certificate

12. In the Phase 1 Policy (see Figure 546 on page 608), select **RSA Signatures** as the Authentication Method.

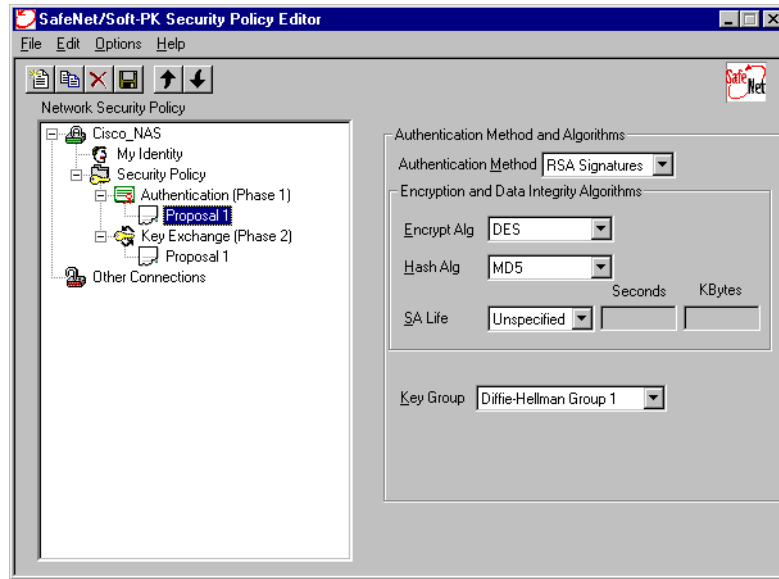


Figure 546. IRE SafeNet - certificate manager

13. Save the policy and exit Security Policy Manager.

19.1.5.1 Testing and verifying the connection

As in the previous scenario, it is sufficient to initiate traffic that matches the new policy to kick off IKE negotiations. A successful IKE negotiation using digital certificates and RSA signature authentication is shown in Figure 547. Note how the messages are different from the pre-shared key exchange shown in Figure 537 on page 603.

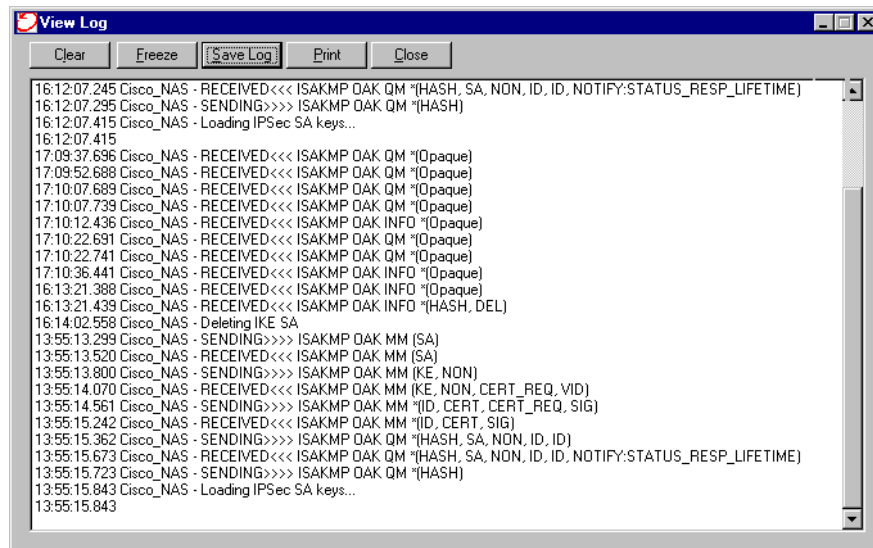


Figure 547. IRE SafeNet - log viewer shown in IKE negotiation with digital signatures

19.1.6 Configuring manual IPsec tunnels

Apart from supporting the dynamic creation and refresh of keys for IPsec connections using IKE, the SafeNet VPN client also supports manual IPsec

tunnels. This means that the keys and SPI values must be entered by a user based on corresponding values provided by a user at a remote system with which secure communication is desired. There are several problems involved with manual tunnels:

1. The keys must be transferred by way of e-mail, file transfer, diskettes, telephone, or other means, all of which involve out-of-band handling and constitute security exposures.
2. The manual keying method does not scale beyond a few systems until it becomes impractical and unmanageable.
3. The manual keying method does not provide key refresh. Tunnels must usually be deleted and recreated, which causes traffic delay and administrative overhead.

However, for testing purposes and for interoperability with certain IPSec implementations that do not support IKE, manual tunnels can be used.

Follow the steps below to configure manual IPSec tunnels for the SafeNet VPN client. A matching AIX configuration for this scenario is described in 9.2.5, “Manual tunnel configuration using WebSM” on page 166.

1. Create a new connection with the Security Policy editor and expand all subtrees by clicking the (+) signs.
2. Specify the IP address of the remote system, as shown in Figure 548:

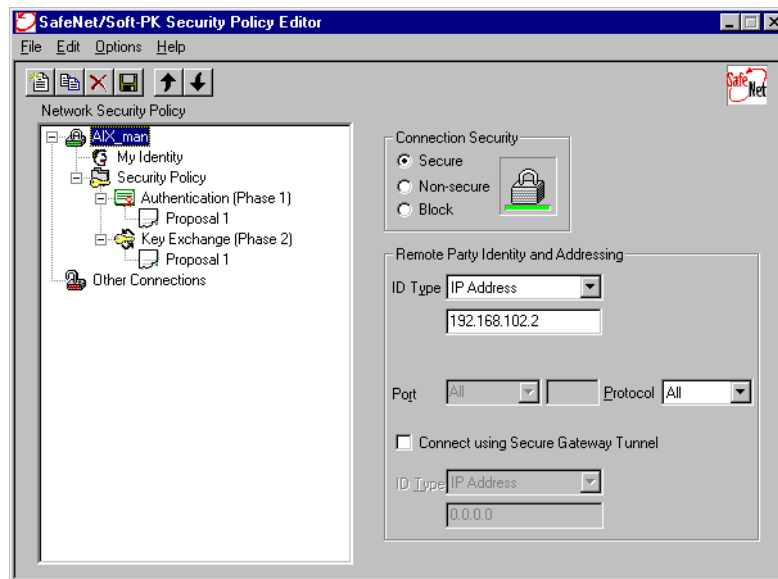


Figure 548. IRE SafeNet - manual tunnel connection

3. Click **My Identity** in the configuration tree and select a local interface and IP address as identifier (see Figure 549 on page 610).

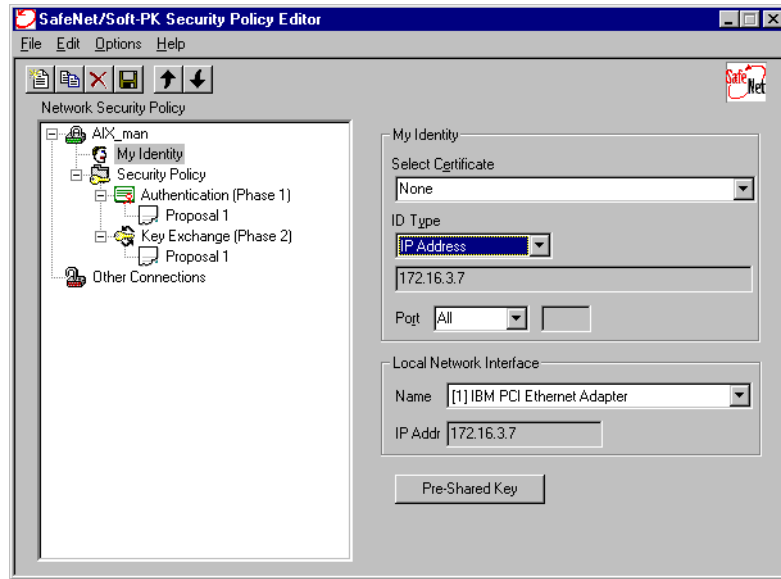


Figure 549. IRE SafeNet - manual tunnel ID and interface

4. Click **Security Policy** and select **Use Manual Keys** in the Security Policy pane (see Figure 550):

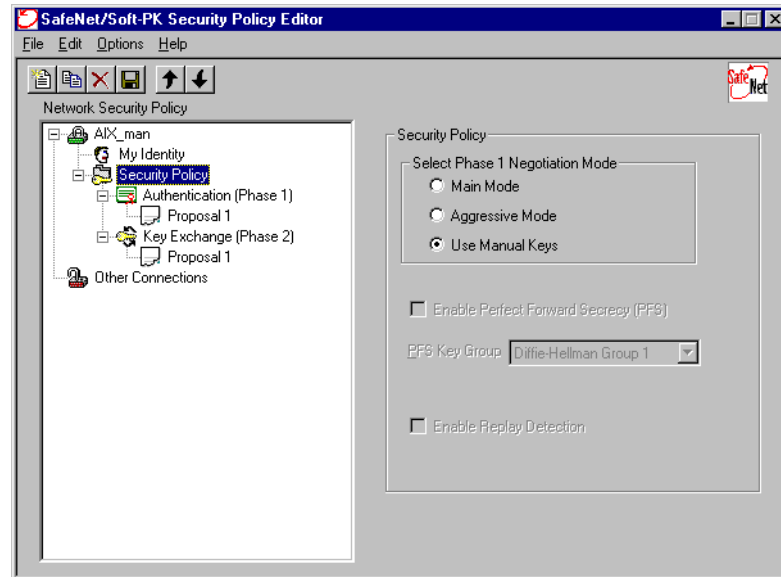


Figure 550. IRE SafeNet - manual key security policy

5. Click **Proposal 1** under Key Exchange (Phase 2) and specify the IPSec protocol(s), transforms, and mode to be used for this manual connection. This is shown in Figure 551 on page 611.

Note: No Phase 1 proposals need to be configured for manual tunnels; they will be ignored because IKE is not used in this case.

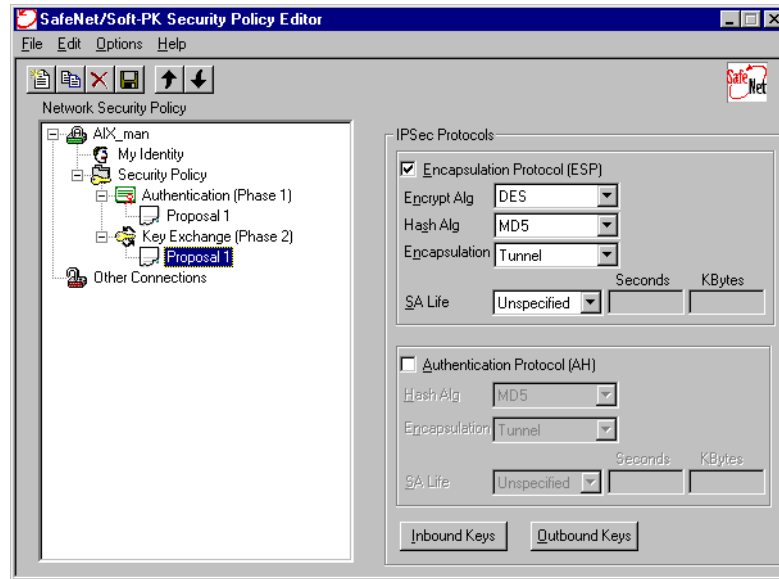


Figure 551. IRE SafeNet - manual tunnel IPSec proposal

6. Click **Inbound Keys**.
7. Click **Enter Key** and fill in the values of the keys as required by the previously selected transforms. These key values are given to you by the administrator of the remote system. An example is shown in Figure 552. When done, click **OK** to return to the previous menu.

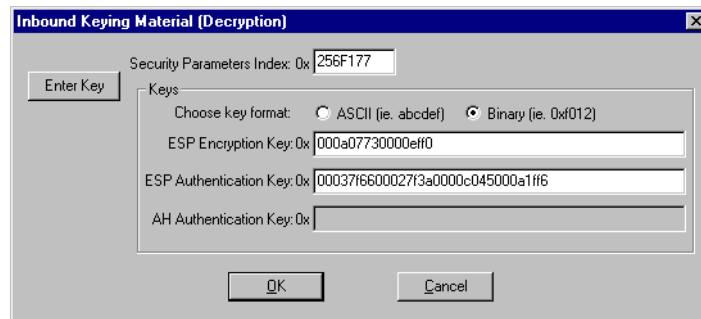


Figure 552. IRE SafeNet - manual tunnel inbound keys and SPI

8. Click **Outbound Keys**.
9. Click **Enter Key** and fill in the values of the keys as required by the previously selected transforms. These key values are used by the local system. An example is shown in Figure 553 on page 612. When done, click **OK** to return to the previous menu.

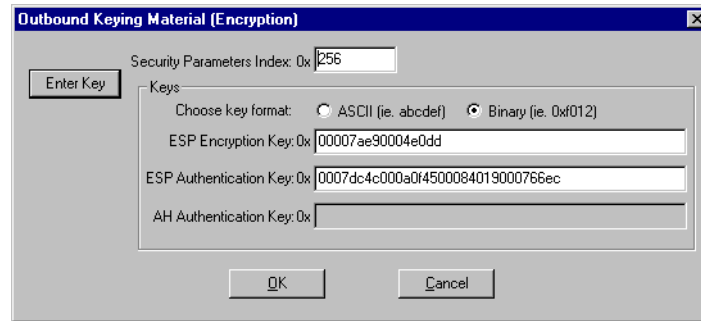


Figure 553. IRE SafeNet - manual tunnel outbound keys and SPI

Important

We experienced problems with the SPI values between a SafeNet VPN client and an AIX 4.3.3 server. It must be observed that AIX requires SPI values to be in decimal form while IRE requires hexadecimal form. On top of that, IRE did not accept the SPI value of 256 that we entered but generated a value of its own. Unfortunately, the version of SafeNet we used did not show the SPI value chosen by the client in the Inbound Keys panel. We finally used the `tcpdump` command on AIX to determine the SPI values that IRE expected and changed the AIX configuration accordingly.

10. Before you can use this policy to protect traffic, you have to save the security policy. This will automatically activate the policy.

19.2 WinVPN client from Wind River Systems

Wind River Systems (WRS) develops OEM networking software (for other vendors to include in their products) and other commercial products through its business division, Wind River Networks, located at Newport Beach. This division provides Windows-based products to Internet service providers, corporations, remote offices and home users with standards-based network access solutions. The commercial products include a VPN client, VPN server, and NAT gateway running on Windows 95, Windows 98, and Windows NT. These solutions support major and emerging protocol standards including NAT, PPTP, L2F, L2TP, IPSec, PPP over Ethernet, and more. To find more information on WinVPN Client and how you can purchase it, please access the URL below:

<http://www.ivation.com>

We were using Version 1.2 of the WinVPN client for the scenarios in this redbook. In particular, we have successfully tested the WinVPN client in combination with the following VPN platforms:

- IBM OS/400
- IBM routers

Important

Please be aware also that the WinVPN client requires Microsoft Internet Explorer 5.0 or it will not install.

19.2.1 WinVPN client capabilities

In this section we briefly list the VPN capabilities of the WinVPN client from WRS:

Table 128. WinVPN Client Version 1.2 from WRS - VPN features

| Feature | |
|----------------------------------|--------------------------------|
| Tunnel Type | IKE |
| IPSec Header Format | RFCs 24xx |
| IKE | |
| Key Management Tunnel (Phase 1) | |
| Negotiation Mode | Main Mode, Aggressive Mode |
| Encryption Algorithm | DES, 3DES |
| Authentication Method | Pre-Shared Key, RSA Signatures |
| Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| Diffie-Hellman Group | Group 1, Group 2 |
| Send Phase 1 Delete | No |
| On-demand Tunnels | No |
| Data Management Tunnel (Phase 2) | |
| Encapsulation Mode | Transport Mode |
| Security Protocol | ESP |
| ESP Encryption Algorithm | DES, 3DES |
| ESP Authentication Algorithm | HMAC-MD5, HMAC-SHA |
| Multiple SA Proposals | Yes |
| Perfect Forward Secrecy (PFS) | Yes |
| Other | Voluntary L2TP, Logging |

We used an IBM Thinkpad with Windows 95 and an IBM PC 750 with Windows NT as client workstations for this scenario.

19.2.2 Client installation

The WinVPN client requires Microsoft Dial-Up Networking 1.2 or higher on Windows 95. The Windows 95 CD-ROM is also required to complete the installation on Windows 95.

To install the WinVPN client, click **Setup** in the directory where the software has been unpacked, then follow the instructions on the screen. During the installation, two iVasion VPNic virtual adapters will be added to your network configuration. The installation procedure also creates and stores in the registry a private/public key pair if you later want to use IKE with certificate-based authentication. New keys can be created at a later time. Once the setup procedure has finished, reboot your system.

Windows NT note

If you install WinVPN on Windows NT, setup will display a message that the installation could not complete because no VPN adapter could be found. You have to manually add that adapter following the steps in the Troubleshooting guide, which is provided electronically with the software. That procedure will then invoke the RAS setup so that you can add the iVasion VPNic as a RAS port for L2TP tunnels.

19.2.3 Client configuration

Once the system has been rebooted, the WinVPN client is added as an icon to the task bar. Use the left mouse button on that icon to invoke the configuration menu as shown in Figure 554:

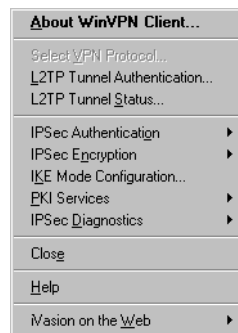


Figure 554. WinVPN client configuration menu

You have to configure the following settings to make this scenario work:

IPSec authentication

Here you can specify if you want to use pre-shared keys or certificates for IKE Phase 1 authentication. We used pre-shared keys. Certificates are supported in a copy-and-paste manner, meaning you have to manually create a certificate request, copy and paste it into a Web browser, send it to a CA, and copy and paste the certificate and the CA certificate back into the VPN client.

Important

When you switch from pre-shared key authentication to certificate-based authentication, all pre-shared key definitions will be lost.

IPSec encryption

Choose either DES or 3DES. The client will send all possible proposals for both DES and 3DES during Phase 1 and Phase 2 negotiations. This option only tells the client which transforms should be offered first. This feature is very practical in that it allows a VPN gateway to pick the appropriate proposal. It is left to the VPN gateway to enforce (that is, require) the security transform of choice. The VPN gateway may even be configured to offer or support only one transform during negotiations.

IKE mode

Select either main or aggressive mode. Because the client in our scenario is assigned a dynamic IP address from an ISP we have to use aggressive mode. As the ID we are using the fully qualified domain name (FQDN) vpnclient.corporate.com, which has to be matched by the VPN gateway configuration as described in 19.4.2.6, “Configure ISAKMP action and proposal” on page 632. Main mode can be used with dynamic IP addresses and certificates.

L2TP tunnel authentication

Enter the user ID for the LNS if L2TP tunnel authentication is enabled at the server. For our scenario we did not use it because the client was already authenticated using IKE.

Next, you have to create dial-up entries for the ISP and the corporate gateway (L2TP tunnel server). You have to use the iVasion VPNic (#1 or #2) adapter as a device for the entry that describes the tunnel server, as shown in Figure 555 for a Windows 95 system:

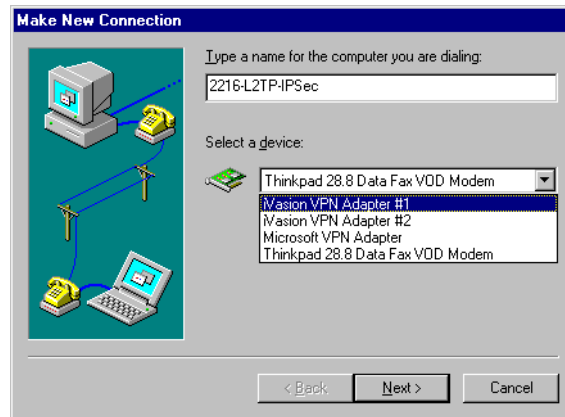


Figure 555. Dial-up networking entry for L2TP server using WinVPN client from WRS on Windows 95

The configuration on Windows NT is similarly performed by adding an entry for the ISP and another entry for the LNS, as shown in Figure 556:

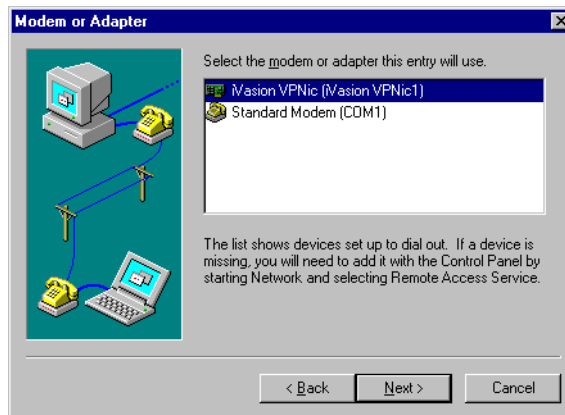


Figure 556. Dial-up networking entry for L2TP server using WinVPN client from WRS on Windows NT

19.2.4 Building the connection

To establish an L2TP tunnel using the WinVPN client you need to use two DUN sessions: The first one (DUN1) to the Internet (in our case, to the ISP's router) and the second one (DUN2) to the center router.

19.2.4.1 Dialing to ISP router

We launch the PPP dial-up connection which establishes the Internet connection and log on with the user ID `wsdial`.

At this time, you would assume that you have full Internet connectivity as is normally the case with PPP access. However, the WinVPN Client software hides that connectivity from the user and all applications until the L2TP tunnel is established and secured with IPsec.

19.2.4.2 Controlling traffic through the VPN tunnel

If the box, Use default gateway on remote network, located under **My Computer->Dial-Up Networking->DUN2->Properties->Server Types->TCP/IP Settings**, is checked, then all traffic from the client is forced into the DUN2 connection and hence into the tunnel to the corporate network.

If the box, Use default gateway on remote network, is unchecked, then only traffic bound to the corporate network goes through the tunnel.

WinVPN client does not support simultaneous direct Internet access (outside the tunnel) and VPN access (through the tunnel) on the same network interface. That is, it does not support concurrent use (or sharing) of a network interface. If another network interface (say using cable or DSL) is available, direct Internet access is possible through the provider of such broadband service.

If direct access to the Internet is required (and no VPN), you only need to do the following:

1. Disconnect from the ISP, if the dial-up connection is up.
2. Shut down the WinVPN client, if it is running.
3. Connect to the ISP.

At this time, direct Internet access is available.

When connection to the corporate network (VPN) is required, you need to do the following:

1. Disconnect from the ISP if the dial-up connection is up.
2. Start the WinVPN Client again by clicking **Start->Programs->StartUp->WinVPN Client**.
3. Connect to the ISP.
4. Connect to the corporate VPN gateway.

At this time, the client is logged on to the corporate intranet.

The routes on the Windows NT workstation look like the following (`netstat -r`). See Figure 557:


```
Active Routes:
Network Destination      Netmask          Gateway          Interface        Metric
127.0.0.0                255.0.0.0       127.0.0.1       127.0.0.1        1
192.168.88.5             255.255.255.255 127.0.0.1       127.0.0.1        1
192.168.88.255           255.255.255.255 192.168.88.5    192.168.88.5     1
224.0.0.0                224.0.0.0       192.168.88.5    192.168.88.5     1
255.255.255.255         255.255.255.255 192.168.88.5    192.168.88.5     1
```

Figure 557. Routes on the workstation after logon to the ISP

Of course WinVPN client has to allow IKE negotiations and the IPSec-protected L2TP tunnel traffic to flow back to the corporate network, but it completely hides that from the user.

You can, however, determine your actual ISP-assigned IP configuration by selecting **IPSec Diagnostics -> Network Status** from the WinVPN context menu of the task bar icon.

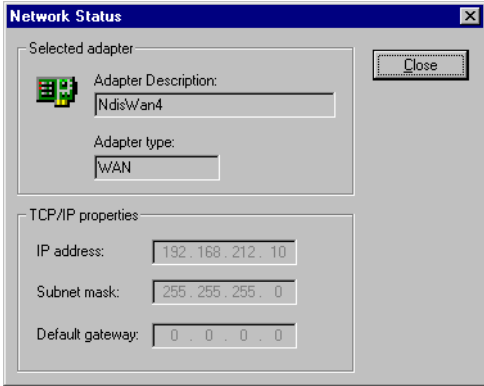


Figure 558. Verifying ISP connectivity with WinVPN client

Address information for both the ISP dial-up connection and L2TP tunnel can also be obtained from the Dial-up Monitor on Windows NT.

19.2.4.3 Dialing to center router through tunnel

Launch the L2TP connection to create the tunnel to the center router with the user ID `wsvpn`.

This will first kick off an IKE negotiation between the WinVPN client and the router that will be used to protect the L2TP tunnel. When that is successful, the L2TP tunnel itself will be established. Once the tunnel is in place, you can ping all hosts on the center intranet. The command `netstat -r` shows the updated routing table on the workstation (see Figure 559):

```
Active Routes:
Network Destination      Netmask          Gateway          Interface        Metric
0.0.0.0                  0.0.0.0         192.168.102.110 192.168.102.110 1
127.0.0.0                255.0.0.0       127.0.0.1       127.0.0.1       1
192.168.102.0            255.255.255.0   192.168.102.110 192.168.102.110 1
192.168.102.110         255.255.255.255 127.0.0.1       127.0.0.1       1
192.168.102.255         255.255.255.255 192.168.102.110 192.168.102.110 1
192.168.88.5            255.255.255.255 127.0.0.1       127.0.0.1       1
192.168.88.255          255.255.255.255 192.168.88.5    192.168.88.5    1
224.0.0.0                224.0.0.0       192.168.102.110 192.168.102.110 1
224.0.0.0                224.0.0.0       192.168.88.5    192.168.88.5    1
255.255.255.255         255.255.255.255 192.168.88.5    192.168.88.5    1
```

Figure 559. Routes on the workstation after building the L2TP and IPSec connections

To display L2TP tunnel status, select that option from the WinVPN task bar icon menu:

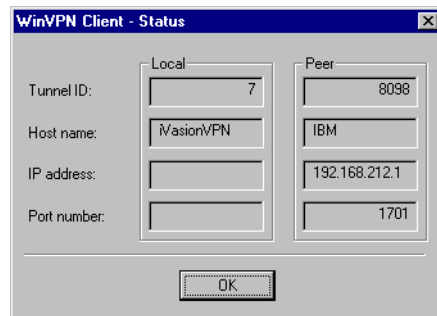


Figure 560. L2TP tunnel status for WinVPN client

By selecting **IPSec Diagnostics -> View Log** from the WinVPN task bar icon menu, you can access the client log file where information about successfully established IKE and L2TP sessions is displayed. Under Windows 95 this is a flat file, under Windows NT these messages are logged to the application log of the Windows NT Event Log.

19.3 Network TeleSystems TunnelBuilder

Network TeleSystems (NTS) is a company that develops software for a variety of tasks in the IP environment, including IP address and NetBIOS name management and VPN remote access. One of its products, TunnelBuilder, is a remote access VPN client that implements PPTP, L2TP, and PPP over Ethernet (PPPoE) for cable modem and xDSL access. TunnelMaster is the server software for TunnelBuilder, but the client is designed to work with any VPN gateway that implements standard protocols. TunnelBuilder is available for Windows 95, Windows 98, and Windows NT. NTS also offers remote access software for Macintosh, Linux, and older versions of Windows.

To find more information about TunnelBuilder and how you can purchase it, please access the URL below:

<http://www.nts.com>

Important

The version of TunnelBuilder that we used for this scenario was a pre-release, so the description and screenshots shown in this redbook may vary from the software you may have purchased.

We have successfully tested the TunnelBuilder client in combination with IBM routers.

19.3.1 NTS TunnelBuilder capabilities

In this section we briefly list the VPN capabilities of the TunnelBuilder client:

Table 129. NTS TunnelBuilder - VPN features

| Feature | |
|----------------|-------------------------|
| Tunnel Type | L2TP Voluntary, PPTP |
| Encryption | MPPE |
| Authentication | PAP, CHAP, MS-CHAP (V1) |
| Other | Logging |

We used an IBM PC 750 with Windows 98 as a client workstation for this scenario.

19.3.2 Client installation

NTS TunnelBuilder requires Microsoft Dial-Up Networking 1.2 or higher on Windows 95. The Windows CD-ROM is also required to complete the installation on Windows 95 and Windows 98.

To install TunnelBuilder, click **Setup** in the directory where the software has been unpacked, then follow the instructions on the screen. During the installation, an NTS VPN virtual adapter will be added to your network configuration.

Windows NT note

If you install TunnelBuilder on Windows NT, setup will display a Notepad window with instructions on how to install the NTS VPN adapter. You have to manually add that adapter following the steps in this window. That procedure will then invoke RAS setup so that you can add the NTS VPN adapter as a RAS port for L2TP and PPTP tunnels. Finally, select not to reboot after you finish the networking configuration and exit the Notepad window as instructed to allow setup to finish, then let it reboot the system.

19.3.2.1 Configure a dial-up connection to the ISP

Before you can use TunnelBuilder you have to create a dial-up networking configuration to access your ISP. The L2TP tunnel will be established over this connection so it needs to be defined first. This step is essentially the same as described in 19.2.3, "Client configuration" on page 614 for creating a DUN entry for the ISP. The difference is that in the case of TunnelBuilder you do not have to

create a second DUN entry but perform that step from the TunnelBuilder Profile window, which is described in the following section.

19.3.3 Client configuration

Once the system has been rebooted, the TunnelBuilder client is added as an icon to the desktop. Double-click that icon to open the Profiles configuration window.

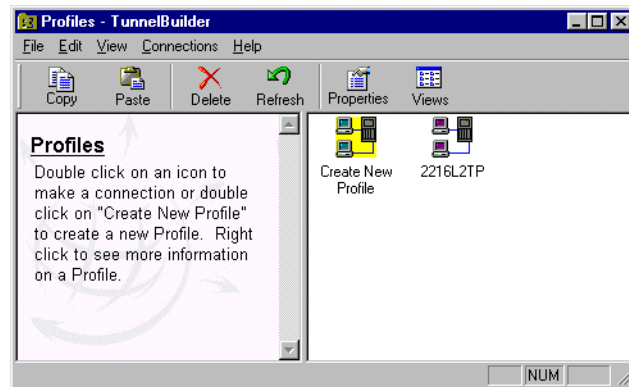


Figure 561. NTS TunnelBuilder - configuration window

Create a new configuration by double-clicking the **Create New Profile** icon. Enter a name for this configuration and a user ID and password on the following screens, then click **Finish**. This is the user ID and password to connect to the corporate gateway so it has to match whatever is defined there, as described in 19.4.2.8, "Add PPP User" on page 635. An icon for the new configuration will be placed in the profile window, as shown in Figure 561.

This new profile is rather generic and requires some fine-tuning. Highlight the new configuration and click the **Properties** button to invoke the Properties window shown in Figure 562 on page 621.

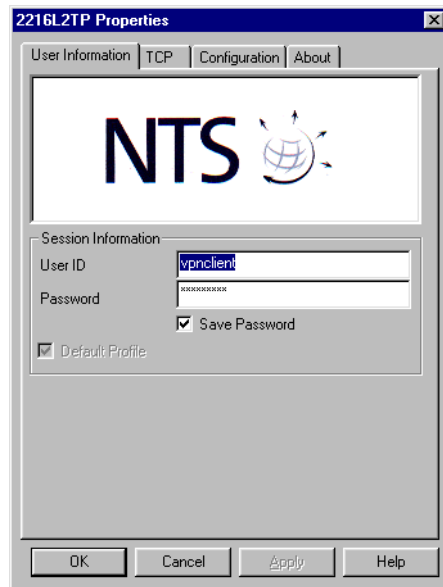


Figure 562. NTS TunnelBuilder - connection properties

Check **Save Password** if you do not want to be prompted for a password every time this connection is started, then click the **TCP** tab to specify TCP/IP configuration parameters for this connection. This is shown in Figure 563:

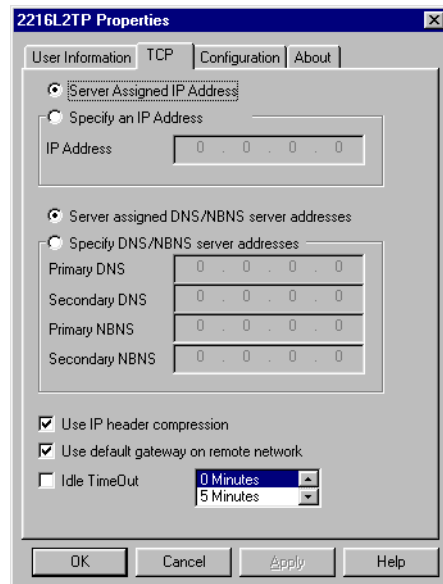


Figure 563. NTS TunnelBuilder - TCP/IP properties

Select to obtain all IP information from the server and optionally choose **Use IP header compression**. Also check **Use default gateway on remote network** to make the L2TP tunnel the default route for client traffic. Then click the **Configuration** tab to access the protocol configuration window shown in Figure 564 on page 622.

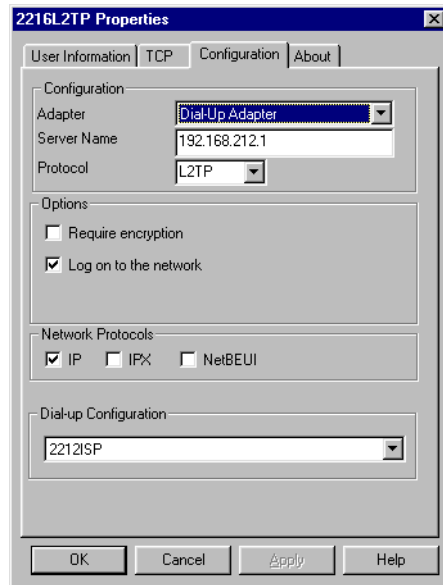


Figure 564. NTS TunnelBuilder - protocol properties

In this window you specify which tunnel protocol (L2TP, PPTP, PPPoE) you want to use over which adapter, which gateway to connect to, and which protocols to run over the tunnel.

1. In the Protocol field, select **L2TP**.

Note

The default is PPPoE and Ethernet Adapter if any is installed, so you have to select the protocol first to be able to select a dial-up adapter.

2. In the Adapter field, select **Dial-Up Adapter**.
3. In the Server Name field, enter the IP address of the corporate gateway, in our case, the 2216 center router at **192.168.212.1**.
4. You must check **Log on to the network** for the PPP connection to be established over the L2TP tunnel. Check **Require encryption** if you want to protect the traffic in the tunnel and the corporate gateway supports it.
5. Select the network protocols you want to use over the tunnel, then in the Dial-up Configuration window, select the dial-up connection you have previously created to access the ISP. TunnelBuilder will automatically establish that connection before starting the tunnel so you do not have to start two separate DUN sessions. Unfortunately, when you end a TunnelBuilder session it does not also take down the ISP session. This may not be viewed as a disadvantage as long as you remember to do it yourself because local telephone calls are free in very few countries.

Click **OK** to finish the configuration.

19.3.4 Building the connection

To establish an L2TP tunnel using TunnelBuilder you need to use two DUN sessions: The first one to the Internet (in our case, to the ISP's router) and the second one to the center router.

19.3.4.1 Dialing to ISP router

Launch the PPP dial-up connection which establishes the Internet connection and also the L2TP tunnel by double-clicking the connection profile in the TunnelBuilder window and clicking **Connect**.

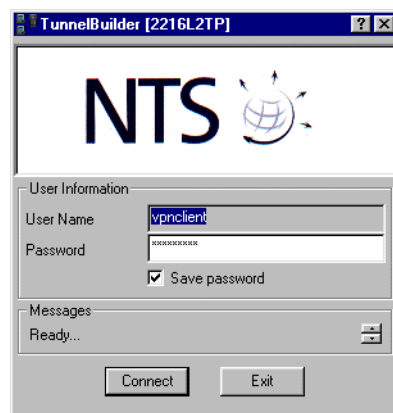


Figure 565. NTS TunnelBuilder - start connection

TunnelBuilder now invokes the Dial-Up Networking entry you specified to access the ISP and places a dial-up session icon on the task bar. Next, TunnelBuilder starts the L2TP tunnel to the corporate gateway and establishes a PPP connection to it. If that is successful, another icon is placed on the task bar for the TunnelBuilder connection. Right-click that icon to access its context menu, as shown in Figure 566:



Figure 566. NTS TunnelBuilder - session context menu

Select **Connection Details** to obtain information on the L2TP tunnel, which is shown in Figure 567 on page 624.

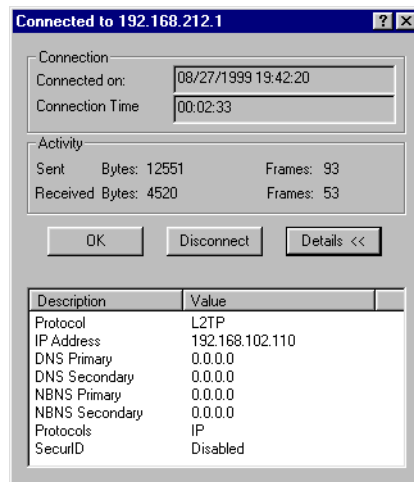


Figure 567. NTS TunnelBuilder - connection details

From the session context menu, select **Advanced** to obtain a full range of information on the system's present IP configuration, including interfaces, drivers, and protocols as well as a message log which is shown below:

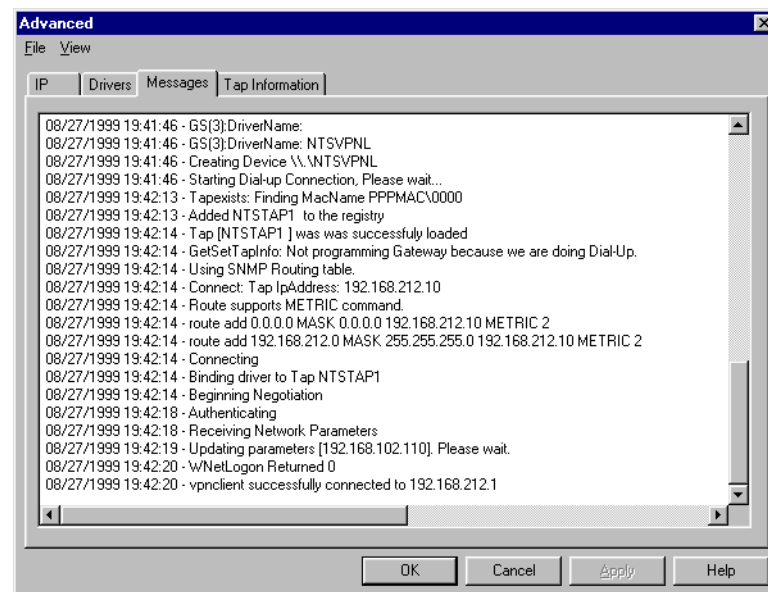


Figure 568. NTS TunnelBuilder - advanced connection information

You can look at the IP routing table in the Advanced information window shown above, or use the `netstat -r` command which produces the output shown in Figure 569 on page 625. The first statement shows a default route to the dial-up interface to direct all traffic over the ISP connection. The next statement shows a default route to the virtual PPP interface to direct all traffic over the L2TP tunnel to the corporate network.

Note

Our Windows 98 system has an Ethernet adapter with IP address 172.16.3.7 in addition to the dial-up adapter, so there are some routes listed in Figure 563 that you may not see on a dial-up only system.

Active Routes:

| Network Address | Netmask | Gateway Address | Interface | Metric |
|-----------------|-----------------|-----------------|-----------------|--------|
| 0.0.0.0 | 0.0.0.0 | 192.168.88.5 | 192.168.88.5 | 2 |
| 0.0.0.0 | 0.0.0.0 | 192.168.102.110 | 192.168.102.110 | 1 |
| 0.0.0.0 | 0.0.0.0 | 172.16.3.2 | 172.16.3.7 | 2 |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |
| 172.16.3.0 | 255.255.255.0 | 172.16.3.7 | 172.16.3.7 | 2 |
| 172.16.3.7 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 |
| 172.16.255.255 | 255.255.255.255 | 172.16.3.7 | 172.16.3.7 | 1 |
| 192.168.102.0 | 255.255.255.0 | 192.168.102.110 | 192.168.102.110 | 1 |
| 192.168.102.110 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 |
| 192.168.88.0 | 255.255.255.0 | 192.168.88.5 | 192.168.88.5 | 2 |
| 192.168.88.5 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 |
| 224.0.0.0 | 224.0.0.0 | 172.16.3.7 | 172.16.3.7 | 1 |
| 224.0.0.0 | 224.0.0.0 | 192.168.102.110 | 192.168.102.110 | 1 |
| 224.0.0.0 | 224.0.0.0 | 192.168.88.5 | 192.168.88.5 | 1 |
| 255.255.255.255 | 255.255.255.255 | 192.168.88.5 | 192.168.88.5 | 1 |

Figure 569. Routing table for L2TP connection with NTS

You can use the same router commands as described in 16.9.5, “Useful commands for layer-2 VPNs” on page 492 to verify that the L2TP connection has been successfully established and that the client PPP session is active.

To verify the connection from the client, try to ping a system in the corporate network, for instance, 192.168.100.3, and check the dial-up session details for increasing byte and packet counts. We have also verified this connection using Telnet and FTP between the client and a server in the corporate network, as well as using a packet sniffer in the Internet segment.

19.4 IBM router configuration for the OEM VPN client scenarios

This section provides a brief summary of the configuration steps for the ISP and center router that correspond to the three client configurations shown in 19.2, “WinVPN client from Wind River Systems” on page 612 and 19.3, “Network TeleSystems TunnelBuilder” on page 618.

19.4.1 ISP router

To configure the ISP router for this scenario follow the steps described in 15.2.2, “Configuration of the ISP router” on page 439.

19.4.2 Center router

There are three configuration scenarios for this router, which require the following steps:

1. L2TP configuration for NTS and WinVPN clients

- This configuration is already described in 18.4.3, “Configuring the center router” on page 584.
2. IPsec configuration for WinVPN client
 3. IPsec configuration for IRE client
 - This configuration is already described in 15.2.3, “Configuration of the VPN Gateway (Center 2216 Router)” on page 442.

We therefore describe the L2TP and IPsec configuration steps necessary to complete the WinVPN client scenario.

19.4.2.1 Center router IPsec configuration

For the configuration of the 2216 in the center we have to perform the following steps:

- Preparation
- Configure policy and validity period for IPsec and IKE
- Configure IPsec action and proposal
- Configure ISAKMP action and proposal
- Enable L2TP and add layer 2 nets
- Add PPP user for the dial-in workstation
- Add default route to the Internet and enable ARP-subnet-routing
- Activate the definitions on the center router

19.4.2.2 Preparation

We assume that the permanent Ethernet connection to the ISP is already established. Therefore, we can concentrate on the dial-in features of this connection.

19.4.2.3 Configure policy profile for IPsec and IKE

The first step is to configure a policy that will encapsulate L2TP traffic in an IPsec tunnel. When configuring the profile it is important that you select an address range rather than a netmask or single IP address. This is because if you use netmask the ID comparisons will fail because the netmask is of a subnet type while the ID type that will be received by the client would be an IP address type. Of course you cannot use a single IP address because you do not know what IP address the client will get from the ISP.

Additionally you also have to build the profile such that it traps UDP port 1701, which is the L2TP port.

```

Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? routerware
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

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 []? routerware
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]? 192.168.212.1
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 2
Enter IPV4 Starting Destination Address [0.0.0.0]?
Enter IPV4 Ending Destination Address [0.0.0.0]? 255.255.255.255

Protocol IDs:
    1) TCP
    2) UDP
    3) All Protocols
    4) Specify Range

Select the protocol to filter on (1-4) [3]? 2
Enter the Starting value for the Source Port [0]? 1701
Enter the Ending value for the Source Port [65535]? 1701
Enter the Starting value for the Destination Port [0]? 1701
Enter the Ending value for the Destination Port [65535]? 1701
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]?
Configure local and remote ID's for ISAKMP? [No]: y
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]? 1
Any user within profile definition allowed access? [Yes]:
The Source and/or Destination Address information you specified
includes all addresses. You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy. The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]:

```

Figure 570. Center router IKE policy configuration for L2TP + IPSec

```

Here is the Profile you specified...

Profile Name      = routerware
sAddr            = 192.168.212.1 : sPort= 1701 : 1701
dAddr:End       = 0.0.0.0 : 255.255.255.255 dPort= 1701 : 1701
proto           = 17 : 17
TOS             = x00 : x00
Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
0: New Profile
1: routerware

Enter number of the profile for this policy [1]?

```

Figure 571. Center router profile configuration for L2TP + IPSec

19.4.2.4 Configure validity period

The next step is to define a validity period.

```

List of Validity Periods:
0: New Validity Period

Enter number of the validity period for this policy [0]? 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)
[*]?

```

Figure 572. Center router validity period configuration for L2TP + IPSec - Part 1

```
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 573. Center router validity period configuration for L2TP + IPSec - part 2

19.4.2.5 Configure IPSec action and proposal

The next step is to define the IPSec action and proposal. You should note that you do not know the tunnel endpoint so 0.0.0.0 is entered as the destination tunnel endpoint.

```

Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
    0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
Enter a Name (1-29 characters) for this IPsec Action []? routerware
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
[192.168.102.1]? 192.168.212.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
[0.0.0.0]?
Percentage of SA lifesize/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]?
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 []? routerware
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:

```

Figure 574. Center router IPSEC policy configuration for L2TP + IPsec - part 1

Also take note of the SA lifesize and lifetime. These are the values used by the WinVPN client which are significantly less than the default values in the router. If these are not changed the tunnel will not come up, since the router's acceptable minimum is 75% of the configured value. Of course the router's minimum tolerance percentage level could have been changed instead.

Tip

How do you find out what transforms and lifetimes a client proposes in order to match a configuration on a VPN gateway? Well, normally a client allows you to modify those settings but the WinVPN Client is different in that it allows the user very little to configure which is not a bad thing. In this case you need to run the client against a system that supports IKE and also provides extensive output for debugging. We have used IBM AIX 4.3.2 for that purpose.

```

Do you wish to enter any ESP transforms for this proposal? [No]: y
List of ESP Transforms:
    0: New Transform

Enter the Number of the ESP transform [0]? 0
Enter a Name (1-29 characters) for this IPsec Transform []? routerware
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]? 2
List of IPsec Authentication Algorithms:
    0) None
    1) HMAC-MD5
    2) HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]?
List of ESP Cipher Algorithms:
    1) ESP DES
    3) ESP CDMF
    4) ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]?
Security Association Lifesize, in kilobytes (1024-2147483647) [50000]? 10240
Security Association Lifetime, in seconds (120-2147483647) [3600]? 300

Here is the IPsec transform you specified...

Transform Name = routerware
    Type =ESP   Mode =Transport   LifeSize=   10240   LifeTime=   300
    Auth =SHA   Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
    0: New Transform
    1: routerware

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [No]:

Here is the IPsec proposal you specified...

Name = routerware
    Pfs = N
    ESP Transforms:
        routerware
Is this correct? [Yes]:
List of IPSEC Proposals:
    0: New Proposal
    1: routerware

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:

```

Figure 575. Center router IPsec policy configuration for L2TP + IPsec - part 2

```

Here is the IPsec Action you specified...

IPSECAction Name = routerware
  Tunnel Start:End      = 192.168.212.1 : 0.0.0.0
  Min Percent of SA Life =          75
  Refresh Threshold     =          85 %
  Autostart             =          No
  DF Bit                =          COPY
  Replay Prevention     =          Disabled
  IPSEC Proposals:
    routerware
Is this correct? [Yes]:
IPSEC Actions:
  0: New IPSEC Action
  1: routerware

Enter the Number of the IPSEC Action [1]?

```

Figure 576. Center router IPsec action configuration for L2TP + IPsec

19.4.2.6 Configure ISAKMP action and proposal

Once the IPsec action and proposal have been fully defined the next step is to define the ISAKMP action/proposal. The main point in this step is that aggressive mode must be used because the IP address of the client will not be known. In main mode the IDs are exchanged in messages 5 and 6, however, the keys must be known before then to encrypt messages 5 and 6 themselves. In aggressive mode the IDs are exchanged during the beginning of the exchange so the keys to be used can be determined at that time. In addition, encryption the last message of an aggressive mode exchange is optional.

```

ISAKMP Actions:
  0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
Enter a Name (1-29 characters) for this ISAKMP Action []? routerware

List of ISAKMP Exchange Modes:
  1) Main
  2) Aggressive

Enter Exchange Mode (1-2) [1]? 2
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, 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]:

```

Figure 577. Center router ISAKMP action configuration for L2TP + IPsec - part 1

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 []? **routerware**

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]? **2**

List of Cipher Algorithms:

- 1) DES

Select the Cipher Algorithm (1-2) [1]?

Security Association Lifesize, in kilobytes (100-2147483647) [1000]?

Security Association Lifetime, in seconds (120-2147483647) [15000]?

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]?

Here is the ISAKMP Proposal you specified...

Name = routerware

AuthMethod = Pre-Shared Key

LifeSize = 1000

LifeTime = 15000

DHGroupID = 1

Hash Algo = SHA

Encr Algo = DES CBC

Is this correct? [Yes]:

List of ISAKMP Proposals:

0: New Proposal

1: routerware

Enter the Number of the ISAKMP Proposal [1]?

Are there any more Proposal definitions for this ISAKMP Action? [No]:

Figure 578. Center router ISAKMP action configuration for L2TP + IPSec - part 2

```

Here is the ISAKMP Action you specified...

ISAKMP Name      = routerware
  Mode           =          Aggressive
  Min Percent of SA Life =          75
  Conn LifeSize:LifeTime =          5000 : 30000
  Autostart      =          Yes
  ISAKMP Proposals:
    routerware
Is this correct? [Yes]:
ISAKMP Actions:
  0: New ISAKMP Action
  1: routerware

Enter the Number of the ISAKMP Action [1]?
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      = routerware
  State:Priority =Enabled   : 5
  Profile        =routerware
  Valid Period   =always
  IPSEC Action   =routerware
  ISAKMP Action  =routerware
Is this correct? [Yes]:

```

Figure 579. Center router ISAKMP action configuration for L2TP + IPsec - part 3

The last step of the policy definition is to enter the user as a fully qualified domain name (FQDN). This is the ID type that must be used because IP addresses are not known.

```

To authenticate the ISAKMP Peer with Pre-Shared Key a User
must be added. Add a USER now? [Yes]: y
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]? 2
Enter the FQDN to distinguish this user (No spaces allowed) []? vpnclient.corporate.com
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):
Enter the Pre-Shared Key again (8 characters) in ascii:

Here is the User Information you specified...

Name      = vpnclient.corporate.com
  Type     = FQDN
  Group    =
  Auth Mode =Pre-Shared Key
Is this correct? [Yes]:

```

Figure 580. Center router ISAKMP ID configuration for L2TP + IPsec

The FQDN configured in Figure 580 on page 634 must match the FQDN that was specified at the client as described in 19.2.3, “Client configuration” on page 614.

19.4.2.7 Configure L2TP

These steps and the reasons for performing them are the same as described in 18.4.3, “Configuring the center router” on page 584.

19.4.2.8 Add PPP User

These steps and the reasons for performing them are the same as described in 18.4.3, “Configuring the center router” on page 584.

19.4.2.9 Add default route and enable ARP subnet routing

These steps and the reasons for performing them are the same as described in 18.4.3, “Configuring the center router” on page 584.

19.4.2.10 Activate the definitions on the center router

You activate the definitions on the Center router with the command `restart` (Figure 581 on page 635):

```
Center Config>WRITE
Config Save: Using bank B and config number 3
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 581. Reloading the Center Router

19.4.3 Switching between configurations

Once you have completed all the configuration steps for the various OEM VPN clients (IRE, Windows 2000, WinVPN and NTS) you can selectively switch between them in the following way:

- Leave L2TP enabled (see “Configure L2TP” on page 584) all the time and disable all IPSec policies to support NTS and Windows 2000 L2TP clients.
- Enable the IPSec policy called ire (see 20.3.2 “Configure policy profile for IPSec and IKE” of *A Comprehensive Guide to Virtual Private Networks, Volume II: BM Nways Router Solutions*, SG24-5234) to support the IRE SafeNet client using IPSec.
- Disable the IPSec policy called ire and enable the IPSec policy called routerware (see 19.4.2.3, “Configure policy profile for IPSec and IKE” on page 626) to support the WinVPN client using IPSec and L2TP.

19.5 IBM server configuration for the OEM VPN client scenarios

The only configuration required on a non-router system for this scenario is the AIXSRV2 server setup for the IRE client scenario.

This is essentially the same as an AIX host-to-host connection as described in 9.3, “Creating a VPN host-to-host connection” on page 180. We are not repeating these steps here.

19.6 VPN solutions for Linux and OS/2

For your reference, we include some VPN implementations on the Linux and OS/2 operating systems in this section. However, we have not performed any interoperability tests during our projects and therefore cannot include any scenario documentations in this redbook. Nonetheless, you may have a business need for a VPN solution on Linux or OS/2 and therefore appreciate this information to get started.

19.6.1 Linux VPN implementations

At the time of writing this book, no Linux distribution nor any otherwise available Linux kernel was actually ready for VPNs. The latest kernel that we could find, 2.2.10, seemed to be prepared for IPsec but did not actually contain the necessary code that would implement it. Therefore, we had to turn to the Internet to find suitable implementations of VPN technology for Linux, and we found the following which we consider a non-exhaustive list:

FreeS/WAN: A free source package including kernel IPsec function for 2.0.36 kernels and an IKE daemon. FreeS/WAN (<http://www.xs4all.nl/~freeswan/>) is based upon the Secure WAN (S/WAN) initiative started by RSA Data Security to foster interoperability between IPsec implementations from different vendors (<http://www.rsa.com/rsa/SWAN/>). FreeS/WAN is an IPsec/IKE reference implementation being developed outside the United States and is therefore not subject to U.S. export regulations regarding cryptography. For more details on legal implications, especially the exclusion from development contributions for U.S. residents, please check out the following URL:

http://www.xs4all.nl/~freeswan/freeswan_trees/freeswan-1.00/doc/exportlaws.html.

Paktronix GuardianLinux VPN and Firewall: A custom-built firewall system based on Linux 2.2 kernel features plus add-on VPN support with hardware crypto-assist. For more information, please check <http://www.guardianlinux.com/products/glvpn.html>.

RedCreek IPsec VPN Card: A Linux device driver for 2.0 and 2.2 kernels that supports a hardware VPN implementation. For more information, please check <http://www.redcreek.com/products/shareware.html>.

Network TeleSystems EnterNet VPN: Source code (not free) for a driver that supports attachment to xDSL lines via PPP over Ethernet and also offers VPN capabilities. For more information, please check <http://www.nts.com/>.

The basic Linux kernel also includes other IP security features that you may want to or may have to combine with any VPN-specific functionality that you are adding to your system, such as the following:

- IP packet filtering (firewall)
- IP masquerading (similar to network address translation)
- Transparent proxy support

Installation and customization of those features is beyond the scope of this appendix, but we will include specific information as it pertains to the scenarios that we provide here.

19.6.2 OS/2 VPN implementations

At the time of writing, we were aware of only two VPN implementations on the OS/2 platform:

IBM TCP/IP V4.2 for OS/2: This level of the operating system's TCP/IP stack, an add-on feature to OS/2 Warp V3.1 and higher, implements IPsec based on RFCs 1825-27 and the concept of manual tunnels. In addition, TCP/IP V4.2 offers remote VPN dial-up to an IBM eNetwork Firewall.

Scenarios including these OS/2 VPN features are described in the redbook *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions*, SG24-5201.

Currently, IBM has no plans to further enhance the IPsec and VPN capabilities of OS/2.

F/X Communications InJoy Firewall for OS/2: Because OS/2 is still a common platform with many European large account customers, F/X Communications, a software vendor in Denmark who specializes on OS/2 networking software, caters to the need of those customers in areas where IBM has stopped rolling out new features for OS/2.

InJoy Firewall for OS/2 offers, among other firewall features such as IP filtering and NAT, an IPsec implementation based on the new RFC standards and the concepts of manual tunnels. In addition, F/X Communications offers IKE support on top which is a port of the IKE implementation called Pluto from the Linux FreeS/WAN project.

F/X Communications also offers products for remote VPN dial-up access. For more information, please contact

<http://www.fx.dk/products.html>.

Appendix A. Special notices

This publication is intended to help network security consultants, network designers and networking engineers to implement virtual private networks. The information in this publication is not intended as the specification of any programming interfaces that are provided by the products used throughout this redbook. See the PUBLICATIONS section of the IBM Programming Announcement for the following products for more information about what publications are considered to be product documentation:

- AIX V4.3.2 and V4.3.3
- OS/400 V4R4
- Communications Server and Security Server for OS/390 V2R8
- Nways 2210, 2212, 2216 Routers using MRS/AIS/MAS V3.3
- Nways Manager V2

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 USA.

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.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

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:

| | |
|--------------------|------------------------|
| AFP | AIX |
| AIX/6000 | Application System/400 |
| APPN | AS/400 |
| CICS | DB2 |
| eNetwork | ESCON |
| EtherJet | FAA |
| IBM Global Network | IBM |
| IMS | MQ |
| Netfinity | NetView |
| Nways | Operating System/2 |
| OS/2 | OS/390 |
| OS/400 | RACF |
| RISC System/6000 | RS/6000 |
| S/390 | SecureWay |
| SP | SP1 |
| System/390 | VTAM |
| XT | |

The following terms are trademarks of other companies:

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/or other countries licensed exclusively through X/Open Company Limited.

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

For information on ordering these ITSO publications see “How to get IBM Redbooks” on page 647.

VPN

- *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions*, SG24-5201
- *A Comprehensive Guide to Virtual Private Networks, Volume II: BM Nways Router Solutions*, SG24-5234
- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404
- *SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements*, SG24-5631

TCP/IP

- *TCP/IP Tutorial and Technical Overview*, GG24-3376-05
- *IP Network Design Guide*, SG24-2580-01
- *Stay Cool on OS/390: Installing Firewall Technology*, SG24-2046

LDAP

- *Understanding LDAP*, SG24-4986
- *LDAP Implementation Cookbook*, SG24-5110

B.2 Redbooks on CD-ROMs

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 publications

These publications are also relevant as further information sources:

B.3.1 IBM publications

- *OS/390 Firewall Technologies Guide and Reference*, SC24-5835
- *OS/390 SecureWay Communications Server IP Configuration*, SC31-8513
- *OS/390 MVS Initialization and Tuning Reference*, SC28-1752
- *OS/390 Security Server (RACF) Command Language Reference*, SC28-1919
- *Open Cryptographic Services Facility Application Developer's Guide and Reference*, SC24-5875
- *OS/390 Security Server Open Cryptographic Enhanced Plug-ins Guide and Reference*, SA22-7429
- *OS/390 UNIX System Services Command Reference*, SC28-1892
- *OS/390 UNIX System Services Planning*, SC28-1890
- *OS/390 Cryptographic Services System Secure Sockets Layer Programming Guide and Reference*, SC24-5877
- *OS/390 UNIX System Services User's Guide*, SC28-1891

B.3.2 Internet standards and drafts

IPSec

- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2402: IP Authentication Header
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405: The ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2406: IP Encapsulating Security Payload (ESP)
- RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2411: IP Security Document Roadmap
- RFC 2412: The OAKLEY Key Determination Protocol
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- draft-ietf-ipsec-pki-req-03.txt: PKI Requirements for IP Security

L2TP

- RFC 2661: Layer Two Tunneling Protocol "L2TP"
- draft-ietf-pppext-l2tp-security-04.txt: Securing L2TP using IPSEC

PPTP

- RFC 2637: Point-to-Point Tunneling Protocol (PPTP)

L2F

- RFC 2341: Cisco Layer Two Forwarding (Protocol) "L2F"

LDAP

- RFC1777 : Lightweight Directory Access Protocol
- RFC2251: Lightweight Directory Access Protocol (v3)
- RFC2252: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
- draft-rajan-policy-qoschema : Schema for Differentiated Services and Integrated Services in Networks
- draft-good-ldap-ldif: The LDAP Data Interchange Format (LDIF) - Technical Specification

RADIUS

- RFC 2138: Remote Authentication Dial In User Service (RADIUS)
- RFC 2139: RADIUS Accounting

Public key infrastructure

- RFC 2437: PKCS #1: RSA Cryptography Specifications Version 2.0
- RFC 2315: PKCS #7: Cryptographic Message Syntax Version 1.5
- RFC 2314: PKCS #10: Certification Request Syntax Version 1.5
- RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 2510: Internet X.509 Public Key Infrastructure Certificate Management Protocols
- RFC 2511: Internet X.509 Certificate Request Message Format
- RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC 2528: Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates
- RFC 2559: Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2
- RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- RFC 2585: Internet X.509 Public Key Infrastructure Operational Protocols - FTP and HTTP
- RFC 2587: Internet X.509 Public Key Infrastructure LDAPv2 Schema

B.3.3 Further reading

Security and VPN

- *Applied Cryptography*, Second Edition, John Wiley & Sons, Inc., 1996, by Bruce Schneier; ISBN 0-471-11709-9.

- *Network Security: Private Communication in a Public World*, PTR Prentice Hall, 1995, by Charlie Kaufman, Radia Perlman, and Mike Speciner; ISBN 0-13-061466-1.
- *Designing Network Security*, Cisco Press, 1999, by Merike Kaeo; ISBN 1-57870-043-4
- *Enhanced IP Services for Cisco Networks*, Cisco Press, 1999, by Donald C. Lee; ISBN 1-57870-106-6
- *IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks*, PTR Prentice Hall, 1999, by Naganand Doraswamy and Dan Harkins; ISBN 0-13-011898-2
- *L2TP: Implementation and Operation*, Addison-Wesley, 1999, by Richard Shea; ISBN 0-201-60448-5
- *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*, Second Edition, Sam's Publishing, 1998, by anonymous; ISBN 0-67231-341-3
- *Intrusion Detection: Network Security Beyond the Firewall*, John Wiley & Sons, Inc., 1998, by Terry Escamilla; ISBN: 0-47129-000-9

B.3.4 Referenced Web sites

Internet standards and drafts

- <http://www.ietf.org>

Public key infrastructure

- <http://www.rsa.com>

IBM VPN solutions

- <http://www.networking.ibm.com/vpn/vpnprod.html>

IBM Security

- <http://www.ibm.com/security>

Cisco Systems, Inc.

- <http://www.cisco.com>

Microsoft Windows 2000

- <http://www.microsoft.com/windows/professional/>
- <http://www.microsoft.com/windows/server/>

IRE SafeNet VPN client

- http://www.ire.com/Products/VPN/soft_pk.htm

Network TeleSystems TunnelBuilder VPN client

- http://www.nts.com/products/prod_client.html

Wind River Networks WinVPN client

- http://www.ivation.com/winvpn_client/vpnclient_overview.htm

RADIUS

- <http://www.livingston.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.

List of abbreviations

| | | | |
|---------------|--|----------------|--|
| AAA | Authentication, Authorization and Accounting | CERN | Conseil Européen pour la Recherche Nucléaire |
| AAL | ATM Adaptation Layer | CGI | Common Gateway Interface |
| ACL | access control list | CHAP | Challenge Handshake Authentication Protocol |
| AFS | Andrews File System | CICS | Customer Information Control System |
| AH | Authentication Header | CIDR | Classless Inter-Domain Routing |
| AIX | Advanced Interactive Executive Operating System | CIX | Commercial Internet Exchange |
| API | Application Programming Interface | CLNP | Connectionless Network Protocol |
| APPN | Advanced Peer-to-Peer Networking | CORBA | Common Object Request Broker Architecture |
| ARP | Address Resolution Protocol | COS | Class of Service |
| ARPA | Advanced Research Projects Agency | CPCS | Common Part Convergence Sublayer |
| AS | Autonomous System | CPU | central processing unit |
| ASCII | American Standard Code for Information Interchange | CSMA/CD | Carrier Sense Multiple Access with Collision Detection |
| ASN.1 | Abstract Syntax Notation 1 | DARPA | Defense Advanced Research Projects Agency |
| AS/400 | Application System/400 | DCE | Distributed Computing Environment |
| ATM | Asynchronous Transfer Mode | DCE | Data Circuit-terminating Equipment |
| BGP | Border Gateway Protocol | DDN | Defense Data Network |
| BIND | Berkeley Internet Name Domain | DDNS | Dynamic Domain Name System |
| BNF | Backus-Naur Form | DEN | Directory-Enabled Networking |
| BRI | Basic Rate Interface | DES | Digital Encryption Standard |
| BSD | Berkeley Software Distribution | DFS | Distributed File Service |
| CA | Certification Authority | DHCP | Dynamic Host Configuration Protocol |
| CBC | Cipher Block Chaining | DLC | Data Link Control |
| CCITT | Comité Consultatif International Télégraphique et Téléphonique (now ITU-T) | DLCI | Data Link Connection Identifier |
| CDMF | Commercial Data Masking Facility | | |

| | | | |
|---------------|---|-------------|---|
| DLL | Dynamic Link Library | GUI | Graphical User Interface |
| DLSw | data link switching | HDLC | High-level Data Link Control |
| DLUR | dependent LU requester | HMAC | Hashed Message Authentication Code |
| DLUS | Dependent LU Server | HPR | High Performance Routing |
| DME | Distributed Management Environment | HTML | Hypertext Markup Language |
| DMI | Desktop Management Interface | HTTP | Hypertext Transfer Protocol |
| DMTF | Desktop Management Task Force | IAB | Internet Activities Board |
| DMZ | demilitarized zone | IAC | Interpret As Command |
| DNS | Domain Name System | IANA | Internet Assigned Numbers Authority |
| DOD | U.S. Department of Defense | IBM | International Business Machines Corporation |
| DOI | Domain of Interpretation | ICMP | Internet Control Message Protocol |
| DOS | Disk Operating System | ICSS | Internet Connection Secure Server |
| DSA | Digital Signature Algorithm | ICV | Integrity Check Value |
| DSAP | Destination Service Access Point | IDEA | International Data Encryption Algorithm |
| DSS | Digital Signature Standard | IDLC | Integrated Data Link Control |
| DTE | Data Terminal Equipment | IDRP | Inter-Domain Routing Protocol |
| DTP | Data Transfer Process | IEEE | Institute of Electrical and Electronics Engineers |
| DVMRP | Distance Vector Multicast Routing Protocol | IESG | Internet Engineering Steering Group |
| EBCDIC | Extended Binary Communication Data Interchange Code | IETF | Internet Engineering Task Force |
| EGP | Exterior Gateway Protocol | IGMP | Internet Group Management Protocol |
| ESCON | Enterprise Systems Connection | IGN | IBM Global Network |
| ESP | Encapsulating Security Payload | IGP | Interior Gateway Protocol |
| FDDI | Fiber Distributed Data Interface | IIOF | Internet Inter-ORB Protocol |
| FQDN | Fully Qualified Domain Name | IKE | Internet Key Exchange |
| FR | frame relay | IMAP | Internet Message Access Protocol |
| FTP | File Transfer Protocol | | |
| GGP | Gateway-to-Gateway Protocol | | |
| GMT | Greenwich Mean Time | | |
| GSM | Group Special Mobile | | |

| | | | |
|---------------|--|----------------|---|
| IMS | Information Management System | LDAP | Lightweight Directory Access Protocol |
| IP | Internet Protocol | LE | LAN Emulation (ATM) |
| IPC | Interprocess Communication | LLC | Logical Link Layer |
| IPSec | IP Security Architecture | LNS | L2TP Network Server |
| IPv4 | Internet Protocol Version 4 | LPD | Line Printer Daemon |
| IPv6 | Internet Protocol Version 6 | LPR | Line Printer Requester |
| IPX | Internetwork Packet Exchange | LSAP | Link Service Access Point |
| IRFT | Internet Research Task Force | L2F | Layer 2 Forwarding |
| ISAKMP | Internet Security Association and Key Management Protocol | L2TP | Layer 2 Tunneling Protocol |
| ISDN | Integrated Services Digital Network | MAC | Message Authentication Code |
| ISO | International Organization for Standardization | MAC | Medium Access Control |
| ISP | Internet service provider | MD2 | RSA Message Digest 2 Algorithm |
| ITSO | International Technical Support Organization | MD5 | RSA Message Digest 5 Algorithm |
| ITU-T | International Telecommunication Union - Telecommunication Standardization Sector (was CCITT) | MIB | Management Information Base |
| IV | Initialization Vector | MILNET | Military Network |
| JDBC | Java Database Connectivity | MIME | Multipurpose Internet Mail Extensions |
| JDK | Java Development Toolkit | MLD | Multicast Listener Discovery |
| JES | Job Entry System | MOSPF | Multicast Open Shortest Path First |
| JIT | Java Just-in-Time Compiler | MPC | multipath channel |
| JMAPI | Java Management API | MPEG | Moving Pictures Experts Group |
| JVM | Java Virtual Machine | MPLS | Multiprotocol Label Switching |
| JPEG | Joint Photographic Experts Group | MPOA | Multiprotocol over ATM |
| LAC | L2TP Access Concentrator | MPTN | Multiprotocol Transport Network |
| LAN | local area network | MS-CHAP | Microsoft Challenge Handshake Authentication Protocol |
| LAPB | Link Access Protocol Balanced | MTA | Message Transfer Agent |
| LCP | Link Control Protocol | MTU | maximum transmission unit |
| | | MVS | Multiple Virtual Storage Operating System |
| | | NAS | Network Access Server |

| | | | |
|----------------|--|---------------|--|
| NAT | network address translation | OSI | Open Systems Interconnect |
| NBDD | NetBIOS Datagram Distributor | OSF | Open Software Foundation |
| NBNS | NetBIOS Name Server | OSPF | Open Shortest Path First |
| NCF | Network Computing Framework | OS/2 | Operating System/2 |
| NCP | Network Control Protocol | OS/390 | Operating System for the System/390 platform |
| NCSA | National Computer Security Association | OS/400 | Operating System for the AS/400 platform |
| NDIS | Network Driver Interface Specification | PAD | Packet Assembler/Disassembler |
| NetBIOS | Network Basic Input/Output System | PAP | Password Authentication Protocol |
| NFS | Network File System | PDU | Protocol Data Unit |
| NIC | Network Information Center | PGP | Pretty Good Privacy |
| NIS | Network Information Systems | PI | Protocol Interpreter |
| NIST | National Institute of Standards and Technology | PIM | Protocol Independent Multicast |
| NMS | Network Management Station | PKCS | Public Key Cryptosystem |
| NNTP | Network News Transfer Protocol | PKI | Public Key Infrastructure |
| NRZ | Non-Return-to-Zero | PNNI | Private Network-to-Network Interface |
| NRZI | Non-Return-to-Zero Inverted | POP | Post Office Protocol |
| NSA | National Security Agency | POP | point of presence |
| NSAP | Network Service Access Point | PPP | Point-to-Point Protocol |
| NSF | National Science Foundation | PPTP | Point-to-Point Tunneling Protocol |
| NTP | Network Time Protocol | PRI | Primary Rate Interface |
| NVT | Network Virtual Terminal | PSDN | Packet Switching Data Network |
| ODBC | Open Database Connectivity | PSTN | Public Switched Telephone Network |
| ODI | Open Datalink Interface | PVC | Permanent Virtual Circuit |
| OEM | Original Equipment Manufacturer | QLLC | Qualified Logical Link Control |
| ONC | Open Network Computing | QOS | Quality of Service |
| ORB | object request broker | RACF | Resource Access Control Facility |
| OSA | Open Systems Adapter | RADIUS | Remote Authentication Dial-In User Service |
| | | RAM | random access memory |

| | | | |
|----------------|--------------------------------------|---------------|--|
| RARP | Reverse Address Resolution Protocol | S-MIME | Secure Multipurpose Internet Mail Extension |
| RAS | Remote Access Service | SMTP | Simple Mail Transfer Protocol |
| RC2 | RSA Rivest Cipher 2 Algorithm | SNA | System Network Architecture |
| RC4 | RSA Rivest Cipher 4 Algorithm | SNAP | Subnetwork Access Protocol |
| REXEC | Remote Execution Command Protocol | SNG | Secured Network Gateway (former product name of the IBM eNetwork Firewall) |
| RFC | Request for Comments | SNMP | Simple Network Management Protocol |
| RIP | Routing Information Protocol | SOA | Start of Authority |
| RIPE | Réseaux IP Européens | SONET | Synchronous Optical Network |
| RISC | Reduced Instruction-Set Computer | SOCKS | SOCK-et-S (An internal NEC development name that remained after release) |
| ROM | Read-only Memory | SPI | Security Parameter Index |
| RPC | Remote Procedure Call | SSL | Secure Sockets Layer |
| RSH | Remote Shell | SSAP | Source Service Access Point |
| RSVP | Resource Reservation Protocol | SSP | Switch-to-Switch Protocol |
| RS/6000 | IBM RISC System/6000 | SSRC | Synchronization Source |
| RTCP | Realtime Control Protocol | SVC | Switched Virtual Circuit |
| RTP | Realtime Protocol | TACACS | Terminal Access Controller Access Control System |
| SA | security association | TCP | Transmission Control Protocol |
| SAP | Service Access Point | TCP/IP | Transmission Control Protocol/Internet Protocol |
| SDH | Synchronous Digital Hierarchy | TFTP | Trivial File Transfer Protocol |
| SDLC | Synchronous Data Link Control | TLPB | Transport-Layer Protocol Boundary |
| SET | Secure Electronic Transaction | TLS | Transport Layer Security |
| SGML | Standard Generalized Markup Language | TOS | Type of Service |
| SHA | Secure Hash Algorithm | TRD | Transit Routing Domain |
| S-HTTP | Secure Hypertext Transfer Protocol | TTL | time to live |
| SLA | service level agreement | UDP | User Datagram Protocol |
| SLIP | Serial Line Internet Protocol | UID | Unique Identifier |
| SMI | Structure of Management Information | | |

| | |
|--------------|---|
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UT | Universal Time |
| VC | Virtual Circuit |
| VM | Virtual Machine Operating System |
| VPN | Virtual Private Network |
| VRML | Virtual Reality Modeling Language |
| VRRP | Virtual Router Redundancy Protocol |
| VTAM | Virtual Telecommunications Access Method |
| WAN | wide area network |
| WWW | World Wide Web |
| XDR | External Data Representation |
| XML | Extensible Markup Language |
| X11 | X Window System Version 11 |
| X.25 | CCITT Packet Switching Standard |
| X.400 | CCITT and ISO Message-handling Service Standard |
| X.500 | ITU and ISO Directory Service Standard |
| X.509 | ITU and ISO Digital Certificate Standard |
| 3DES | Triple Digital Encryption Standard |

Index

Numerics

3DES 40

A

- AAA request 87
- AAA service 87
- abbreviations 649
- access control 21, 403, 404, 407
 - restrict access via certificates 357
- access control lists (ACLs) 307
- access control policy 8
- accounting 86
- ACE/Server 35
- acronyms 649
- action 308
- Actions Group 117
- add ipsec-proposal command 328
- add ipsec-transform command 329
- add isakmp-action command 332
- add isakmp-proposal command 332
- add policy command 313, 324
- add policy templates 100
- add profile command 325
- add tunnel command 318
- ADD TUNNEL-PROFILE command 584
- add user command 323
- address spoofing 361
- address translation 309
- AH 46, 47, 90
- AH policy 318
- AH_ESP policy 318
- AIX
 - /etc/isakmpd.conf file 472
 - /etc/syslog.conf file 468
- activate manual tunnel 171
- activate tunnel 140
- Activate/Update/Deactivate IP Security Filter Rule 150
- Advanced IP Security Configuration 150
- AH authentication algorithm 148
- Bonus Pack 130, 175
- bos.crypto 130, 155
- bos.crypto_priv 155
- bos.crypto_wt 155
- bos.crypto-priv 130
- bos.crypto-us 130
- bos.msg.en_US.net.ipsec 130
- bos.msg.LANG.net.ipsec 155
- bos.net.ipsec.keymgt 131, 155, 176
- bos.net.ipsec.rte 130, 155
- bos.net.ipsec.websm 131, 176
- CA certificate 178
- certificate manager 176
- certificate request file 178
- certreq.arm file 178
- Configure IP Security Filter Rules 150
- cpd daemon 176, 179
- crypto packages 130
- customize policy 141
- data management policy 138, 147
- data management tunnel 132, 136, 380, 423, 470, 582
- device certificate 178
- Diffie-Hellman group 145
- dynamic filter table 472
- encapsulation mode 149
- encryption algorithm 144
- ESP encryption algorithm 148
- filter rule 137
- filter rules 150
- gateway-to-gateway tunnel 377
- gsk4ikm command 176
- gskit.rte 175
- hash algorithm 144
- hexadecimal notation 135, 581
- IBM_high_AH_transport 140
- IBM_high_AH_tunnel 139
- IBM_high_ESP_transport 139
- IBM_high_ESP_tunnel 139
- IBM_high_prekey 135
- IBM_low_AH_transport 140
- IBM_low_AH_tunnel 139
- IBM_low_ESP_transport 139
- IBM_low_ESP_tunnel 139
- IBM_low_prekey 135
- IBM_med_AH_transport 140
- IBM_med_AH_tunnel 139
- IBM_med_ESP_transport 139
- IBM_med_ESP_tunnel 139
- IBM_med_prekey 135
- IKE database 149
- IKE Tunnel Monitor 140, 381, 424, 470, 582
- ikekey.kdb 176
- initiator 140, 150
- installation components 130
- IP security 131
- IP Security daemon 470
- IP Security network kernel 132
- IP Version 4 155
- IP Version 6 155
- ISAKMP daemon 132, 471
- isakmpd 471
- isakmpd.log file 179
- JAVA_HOME environment variable 176
- key and certificate management tool 175
- key database 176
- key lifetime 145, 149
- key management policy 134
- key management tunnel 132, 145, 180, 380, 423, 470, 581
- List Active IP Security Filter Rules 150
- local4 facility 469
- log file 469
- logging 150
- manual key values 169

- manual SPI values 169
- manual tunnel export file 171
- on-demand tunnel 380
- packet filtering 150
- policy 143, 145
- port number 137
- pre-defined data management policies 139
- predefined key management policies 135
- pre-shared key 423, 581
- proposal 142, 147
- protocol 137, 148
- PTFs 131, 176
- refresh -s command 469
- responder 140, 150, 470
- sample filter rules 150
- self-signed certificates 177
- signature authentication mode 179
- SMIT 131
- Start IP Security 132
- Stop IP Security 132
- syslogd subsystem 469
- system log 468
- tcpdump command 612
- tmd 471
- touch command 469
- transform 144
- tunnel cache 472
- tunnel lifetime 143, 149
- tunnel manager daemon 132, 471
- tunnel status 141
- Web System Management 422, 581
- Web-based System Manager 130, 132
- AIX V4.3.2 99
- AIX V4.3.2 Bonus Pack 99
- alerting 457
- anonymous bind 105
- APF authorization 250, 255
- ARP-subnet-routing 584
- AS/400
 - 3DES 190
 - 5250 emulator session 233
 - 5769-AC2 Cryptographic Access Provider for AS/400 189
 - 5769AC3 Cryptographic Access Provider for AS/400 189
 - 5769-SS1 option 34 OS/400 - Digital Certificate Manager 189
 - 5769-SS1 V4R4 OS/400 189
 - 5769-TC1 TCP/IP Connectivity Utilities for AS/400 189
 - 5769-XE1 Client Access/400 Express for Windows 189
 - action type IPSEC 192
 - activate filter rules 230
 - Active Connections 232, 473, 542
 - authentication method 200
 - Balanced Security and Performance (BS) 195
 - communication trace 473
 - connection group 538
 - connection manager 191
 - connection wizard 424
 - create VPN configurations 199
 - CRTDUPOBJ command 477
 - customize policies 539
 - Data Connections 199
 - Data Policy 199, 201, 222, 237, 397, 425, 539, 540
 - Data Protection Transform 195
 - default values 196
 - DES 190
 - Diffie-Hellman group 200
 - Diffie-Hellman perfect forward security 540
 - Display Emulator 233
 - DSPJRN command 476, 479
 - dynamic IP connections 189, 218
 - Dynamic IP Groups 479
 - Dynamic key connections 420
 - dynamic key connections 189, 192, 218, 541
 - dynamic key group 214
 - Dynamic key groups 478
 - encryption algorithm 200
 - ENDTCPIFC command 208
 - ENDTCPSVR *VPN command 212
 - Filter Interface 541
 - filter Set name 429
 - filter set name 198, 541
 - filters rules 540
 - hash algorithm 200
 - Highest Security, Lowest Performance (HS) 195
 - Identifier type 538
 - IFS directory path 205
 - inbound filter rule 227
 - inbound IPSec filter rule 206
 - InfoCenter Web site 480
 - initiator 230
 - initiator negotiation 200
 - IP filter rules 205, 391
 - IP filtering 197
 - IP filters 421, 428, 540
 - IP Packet Filter journal 476
 - IP packet filter rules 192
 - IP packet filter rules file 215
 - IP packet filter rules filename 208
 - IP packet filtering 192
 - IP packet filtering configuration GUI 192
 - IP packet filters 223
 - IP packet security 205, 474
 - IP packet security status 207
 - IP Security 538
 - IPSec action 541
 - IPSec filter rule 228, 229
 - job logs 473, 482
 - journal logging 479
 - journals 473
 - Key Connection Groups 199
 - key lifetime 539
 - key management 200
 - key manager 191
 - Key Policy 199, 200, 220, 236, 396, 425, 538, 539
 - Key Protection Transform 195
 - L2TP connections 189, 479

- ciphertext 13
- circuit level gateway 91
- Cisco
 - 2612 router 503, 544
 - aaa authentication login command 554
 - aaa authentication ppp command 554
 - aaa authorization network command 554
 - aaa new-model command 554
 - access list 505, 546
 - access-list command 510, 524, 536, 547
 - Apply crypto map to interface 511
 - ASCII format 507
 - basic IPsec configuration 510
 - basic L2TP connection 553
 - basic VPN configuration 504
 - CA certificate 550
 - CA URL path 509
 - CEP protocol 548
 - certificate-based authentication 504
 - clear crypto isakmp command 513
 - clear crypto sa command 513
 - connection ID 512
 - cry ca auth command 509, 549
 - cry ca enroll command 510, 550
 - cry ca iden command 509, 549
 - cry isa pol command 553
 - cry key gen rsa command 509, 549
 - crypto ipsec sa command 505
 - crypto ipsec transform-set command 511, 524, 536, 547
 - crypto isakmp enable command 505
 - crypto isakmp identity command 507, 524, 535, 547
 - crypto isakmp key command 507, 524, 535, 547
 - crypto isakmp policy command 505, 506, 524, 535, 547
 - crypto isakmp sa command 505
 - crypto map 546, 553
 - crypto map command 511, 524, 536, 547
 - crypto show isakmp key command 504
 - default policy 506
 - delete a crypto map 511
 - delete a transform set 511
 - delete IKE policy 506
 - deleting an IPsec SA 513
 - Diffie-Hellman group 506
 - digital certificates 548
 - dynamic crypto map 546
 - enable mode 512
 - encryption keys 509, 548
 - enrollment mode RA option 549
 - global configuration mode 504
 - hostname command 549
 - IKE aggressive mode 545
 - IKE connection 527
 - IKE peer 511
 - IKE policy 506, 510, 511, 534
 - interface command 512, 525, 537, 548
 - interface Virtual-Template command 554
 - IOS 12.0(5) 503
 - ip domain-name command 509, 549
 - ip host command 549
 - ip hostname command 509
 - ip local pool command 554
 - IPsec access list 510, 511
 - IPsec crypto map entry 511
 - IPsec protocol 511
 - IPsec transform set 511, 553
 - IPsec transforms 511
 - ISAKMP ID 552
 - ISAKMP peer 545
 - ISAKMP policy 552
 - key pairs 548
 - L2TP tunnel 553
 - LNS 554
 - no ip domain-lookup command 509
 - passwords 504
 - PFS 511
 - pre-shared key 545
 - pre-shared key authentication 504
 - pre-shared keys 507, 552
 - RA certificate 550
 - remove a crypto map 512
 - request CA certificate 509, 549
 - request router certificate 510, 549
 - router certificate 550
 - RSA encryption 552
 - RSA key pairs 508
 - RSA signatures 552
 - save configuration 537
 - sh cry ca cert command 509, 551
 - sh cry isa sa command 527
 - show access-list command 506, 525
 - show crypto ipsec sa 527
 - show crypto ipsec sa command 512, 542
 - show crypto ipsec transform-set command 525
 - show crypto isakmp policy command 510
 - show crypto isakmp sa command 512, 542
 - show crypto isakmp policy command 534
 - show crypto map command 512, 525
 - show crypto transform-set command 512
 - show running command 504, 525, 537, 548
 - signature keys 509, 548
 - store the certificates in NVRAM 552
 - subnet masks 523
 - vpdn enable command 554
 - vpdn-group command 554
 - VPN features 503
 - Windows 2000 client 553
 - write terminal command 504
- Ciscocrypto dynamic map command 547
- cleartext 13
- Communications Server 86, 92
- compulsory layer 2 tunneling 455, 554
- compulsory tunnel 88
- Conditions Group 117
- configuration changes 97
- Configuration Management 109
- connection hijacking 468
- connection lifetime 333
- content inspection 17, 19

- Cookies 47
- corporate address pool 593
- corporate policy 97
- cost-effective 365
- CRL 357
- cross-certificate 80, 82
- cryptographic algorithm 37, 46
- cryptographic features in OS/390 249
- cryptographic key 29, 37
- cryptographic keys 406
- cryptology-based authentication 9
- CSFSERV 257

D

- data confidentiality 405
- DCE 88
- debug facility 457
- default rule 104
- demilitarized zone 21
- demultiplexing filter 308
- denial-of-service attack 5, 46, 49, 361, 406, 468
- DES 378
- DES_CBC 40
- DES-MAC 40, 41
- DHCP 585
- dial-in 87
- dial-in client 7
- dial-in connections 435
- dial-in segment 5, 6, 7
- Differentiated Services 10, 314
- Diffie-Hellman 47
- Diffie-Hellman exchange 45, 50, 67, 460
- Diffie-Hellman group 281
- Diffie-Hellman public value 54
- Diffie-Hellman shared secret 66
- DiffServ action 97
- digital certificate 73
- digital certificates 548, 553, 598, 608
- digital signature 46, 74
- Directory Enabled Networks (DEN) 97, 382
- directory server 97, 101
- directory-assisted policy management 97
- disable policy 336
- Distinguished Encoding Rules (DER) 344
- distinguished name 105
- DMZ 17, 375
- DNS server 507, 510
- Domain of Interpretation (DOI) 49
- DS domain 11
- DSS 46
- DUN session 616, 623
- dynamic address assignment 453
- dynamic filter rules 435
- Dynamic VPN 239, 271

E

- e-business 4, 7
- enable policy 341
- Encapsulating Security Payload (ESP) 28

- authentication 363, 365, 405, 407, 436
- combinations with AH 42
- encryption 363, 407, 436
- ESP 362, 405, 406, 407, 436
- transport mode 44, 405
- tunnel mode 44, 362, 363
- encapsulation mode 318
- encryption 13, 20, 29, 37, 47, 92, 362, 407, 436
- Encryption Control Protocol (ECP) 35
- encryption key 13
- encryption overhead 11
- encryption package 311
- encryption transforms 40
- end-to-end data path 5
- end-to-end encryption 405, 406
- end-to-end path 10
- Entrust CA 509, 548, 605, 607
- Entrust VPN Connector 509, 548
- Environment Variable
 - NLSPATH 263
 - PATH 263
 - STEPLIB 263
- ESP 46, 47
- ESP policy 318
- ESP proposal 329
- ESP_AH policy 319
- ethical hacking 467
- Event Logging System (ELS)
 - IKE and PKI messages 353
 - LDAP messages 101
- Export/Import Regulations 13
- extattr command 250, 256
- Extensible Authentication Protocol (EAP) 34
- external CA 504
- external segment 5, 6
- Extranet VPN 46

F

- F/X Communications InJoy Firewall 637
- false tunnel 8
- FC 2511 645
- FC 2585 645
- FDDI 31
- firewall 5, 7, 8, 16, 20, 38, 89, 363, 404, 407, 437
- firewall configuration client 263
- fixed host 7
- forwarding engine 308
- fragmentation 39
- frame relay 31
- FreeS/WAN 636
- FTP 48
- fully qualified domain name (FQDN) 448, 510, 552, 615, 634
- fully qualified host name (FQDN) 507
- fwauthinfo 303
- fwconns 262, 305
- fwdaemon command 260
- fwdynconns 305
- fwdyntun 302, 303
- fwfilter 262

- fwrule 261, 303
- FWGRP 246
- FWKERN 246
- fwkeypol 302
- fwkeyprop 302
- fwkeysrv 303
- fwkeytran 302
- fwnwobj 262, 301, 305
- fwservice 261, 304
- fwstack command 259

G

- generate a certificate request 343
- generate a public and private key pair 343
- GRE 9
- GSKKYMANN utility 263
- gskrf301 component 99
- gskru301 component 99

H

- hardware interface 312
- hardware-based encryption 11
- hash function 74
- hashed message authentication codes (HMAC) 39
- hexadecimal format 420
- hierarchical structure 78
- HMAC 361
- HMAC-MD5 52, 319
- HMAC-MD5-96 39, 41
- HMAC-SHA-1-96 39, 41
- Host On-Demand 92
- host-to-host security policies 364
- HTTP 92
- hub-and-spoke connections 455

I

- IBM 2212 544
- IBM 2216 523
- IBM DataGlance 458
- IBM eNetwork Firewall 376
- IBM eNetwork LDAP Directory Server V2.1 99
- IBM eNetwork VPN solutions 10
- IBM Enterprise Specific MIB tree 117
- IBM GSKit packages 100
- IBM routers
 - add ipsec-action command 521
 - add ipsec-proposal command 521
 - add ipsec-transform command 521
 - add isakmp-action command 520
 - add isakmp-proposal command 520
 - add policy command 522
 - add user command 520
 - encryption package 485
 - feature ipsec command 525
 - feature policy command 525
 - gateway-to-gateway tunnel 367
 - IKE policies 525
 - IPSec policy 525

- LIST STATS command 401
- policy feature 520
- policy user 394
- PPP user 584
- problem determination 485
- STATS command 400
- take down an IPSec tunnel 526
- tunnel ID 375, 526
- tunnel profile 373, 395
- IBM routes
 - add profile command 521
 - IPSec traffic 526
 - list tunnel active command 526
- IBM TCP/IP V4.2 for OS/2 637
- IBM Universal Database Version 5 99
- iconv command 257
- ICRF 257
- ICSF 256
- ICSF/MVS 257
- IDEA 40
- IKE 28, 319
 - aggressive mode 45, 51, 378, 451, 507, 544, 553, 557, 632
 - authentication 50
 - authentication method 50
 - authentication via public key encryption 49
 - authentication via revised public key encryption 49
 - authentication with pre-shared keys 49
 - Certificate Payload 48
 - Certificate Request Payload 48
 - certificate-based authentication 340, 544
 - certificates 84, 337
 - compatibility scenarios 124, 126
 - cookies 49
 - data endpoint 230
 - Delete Payload 48
 - Diffie-Hellman group 50
 - Diffie-Hellman public value 54
 - digital signature authentication 49
 - digital signature authentication mode 175
 - digital signature mode 179
 - Domain of Interpretation (DOI) 49
 - Encryption algorithm 50
 - endpoint type 137
 - Exchange Type 462
 - Flags 463
 - Fully qualified domain name 134
 - Hash algorithm 50
 - Hash Payload 48
 - hash value 53
 - Hash_1 65
 - Hash_2 65
 - Hash_3 65
 - HASH_I 54
 - HASH_R 54
 - IBM platform implementations 121
 - ID type 448, 599, 634
 - Identification Payload 48
 - identifier 323
 - identifier type 221

- identity 506, 510
- identity type 134
- informational exchange 68
- Informational mode 45
- initiator 50
- Initiator Cookie 462
- ISAKMP peer 64
- ISAKMP SA 45, 50
- Key Exchange Payload 48
- keying material 51
- Length 463
- list tunnel command 492
- main mode 45, 50, 323, 354, 459, 506, 544, 600, 602
- Major Version 462
- Message ID 463
- Minor Version 462
- New Group Mode 45, 67
- Next Payload 462
- nonce 51
- Nonce Payload 48
- Notification Payload 48
- on-demand tunnel 375
- peer identity 544
- PFS 65
- Phase 1 45, 50, 84, 116, 132, 200, 333, 354, 458, 510, 538, 571, 580, 601, 607
- Phase 2 45, 64, 116, 132, 201, 327, 356, 458, 572, 601
- PKI 337
- policy 322
- pre-shared key 103, 200, 412, 458
- pre-shared key authentication 544
- pre-shared keys 322, 378, 504, 548
- proposal 50
- Proposal Payload 48
- pseudo random function 52, 65
- quick mode 45, 459, 602
- responder 50
- Responder Cookie 462
- revised RSA 47
- RSA encryption mode 548
- RSA signature authentication 608
- RSA signature authentication mode 548
- SA lifetime/lifesize 50
- Security Association Payload 48
- Signature Payload 48
- situation 49
- SKEYID 52
- SKEYID_a 53
- SKEYID_d 53
- SKEYID_e 53
- SPI 66
- status 491
- traffic trace 461
- transform 50
- Transform Payload 48
- Vendor ID Payload 48
- VPN platforms 121
- IKE authentication methods 47
- IKE control channel 116
- IKE module 308
- IKE negotiation 69, 354
- IKE negotiations statistics 491
- IKE peer 331
- IKE Phase 1 47
- IKE Phase 2 47
- IKE proposal 330
- IKE SAs 116
- IKE tunnel 107
- IKESKEYID_a 65
- impostor gateway 8
- input packet filter 308
- installation verification procedures (IVP) 253
- Integrated Cryptographic Feature (ICRF) 257
- Integrated Cryptographic Service Facility (ICSF) 245, 257
- Integrated Key Exchange (IKE) 319
- Integrated Services 11
- Integrity Check Value (ICV) 320
- internal segment 5, 6
- Internet Assigned Numbers Authority (IANA) 89
- Internet Engineering Task Force (IETF) 6, 86
- Internet Key Exchange
 - See IKE
- Internet Key Exchange (IKE) 28, 45, 239
- Internet Key Exchange Protocol (IKE) 46
- Internet Security Association and Key Management Protocol (ISAKMP) 45, 239
- Internet Security Associations and Key Management Protocol (ISAKMP) 46
- Internet VPN management 109
- Internet VPN service provider 110
- interoperability 5
- intrusion detection 19
- IP address 92, 312
- IP forwarding 193
- IP packet 28
- IP protocol 47 9
- IP protocol 50 9, 414, 505
- IP protocol 51 9, 505
- IP routing protocol 363
- IP Security Architecture (IPSec) 37
 - authentication 406
 - authentication protocols 361
 - combinations of AH and ESP 42
 - HMAC 361
 - IPSec module 38
 - iterated tunneling 43
 - nested tunneling 43
 - nesting of IPSec protocols 406
 - processing sequence 44
 - SA bundle 38, 43
 - Security Association (SA) 38, 362
 - Security Association Database (SAD) 38
 - Security Parameter Index (SPI) 38
 - Security Policy Database (SPD) 38
 - transport adjacency 43
 - tunnel policies 318
- IP Security MIB 117
- IP Security related traps 117

- IP spoofing 39
- IPSec 16, 19, 28, 37, 46, 90, 239, 407
 - anchor filter rule 240, 292, 303
 - authentication data 240
 - Authentication Information 289, 303
 - authentication method 281
 - compatibility scenarios 125
 - Connection Activation 297
 - connection lifetime 286
 - Connection Setup 294
 - Data Policy 285, 302
 - Data Proposal 284, 302
 - Diffie-Hellman group 281
 - Dynamic Tunnel Policy 286, 302
 - Dynamic VPN 239
 - Dynamic VPN connection 289, 305
 - Dynamic VPN worksheet 272
 - encryption algorithm 281
 - encryption features 249
 - ESP Transform 283, 302
 - firewall configuration client 263
 - initiation role 286
 - Internet Key Exchange (IKE) 239, 281
 - Internet Security Association and Key Management Protocol (ISAKMP) 239
 - Key Management 281
 - Key Policy 282, 301
 - Key Proposal 282, 301
 - Key Server 240, 286
 - Key Server Group 288
 - Key Transform 281, 301
 - manual keying 609
 - manual tunneling 376
 - negotiation mode 282
 - Network Objects 290
 - policies 240
 - policy 372, 408, 414, 442
 - protect routing information 363
 - remote client 437
 - RSA signature authentication 248
 - Rules 292
 - Services 293, 303
 - shared key 289
 - VPN Connection Setup 291, 298
- IPSec action 318, 327, 331, 339, 373, 395, 410, 445, 521, 629
- IPSec daemon 457
- IPSec dial-up 553
- IPSec feature 318
- IPSec header 328
- IPSec History Group 117
- IPSec Levels Group 117
- IPSec MIB 115
- IPSec module 308
- IPSec monitoring MIB 115
- IPSec Phase-1 Group 117
- IPSec Phase-2 Group 117
- IPSec processing 70
- IPSec proposal 328, 339, 373, 394, 410, 445, 521, 629
- IPSec protection suite 116
- IPSec SA 513
- IPSec status MIB 115
- IPSec technology 18
- IPSec transform 97, 329, 521
- IPSec TRAP Control Group 117
- IPSec tunnel
 - automatic 322
 - configuration 309
 - create 318
 - enabling 312
 - encapsulate L2TP tunnel 626
 - endpoint 312
 - IKE policy 324
 - manual 312
 - tunnel policy 318
- IPSec virtual tunnel 116
- IPv4 37
- IPv6 5, 37
- IPX 32, 88
- IRE
 - Authentication Method 607
 - CA certificate 603, 606
 - CEP 605
 - Certificate Manager 603
 - certificate request file 604
 - certificate request form 604
 - certificates 603
 - client certificate 603, 605
 - context menu 599
 - Enrollment method 604
 - ID type 600, 606
 - Inbound Keys 611
 - install 599
 - key pair 604
 - Log Viewer 602
 - manual IPSec tunnels 608
 - My Identity 453
 - Outbound Keys 611
 - PFS 600
 - pre-shared key 548, 600
 - private IP address 452
 - proposal 601
 - proposals for manual connection 610
 - reload policy 602
 - RSA Signature 607
 - SafeNet VPN client 603
 - Security Policy Editor 453, 599, 606
 - SPI values 612
 - task bar icon 599
 - token-ring 597
 - VPN capabilities 598
- IRE SafeNet VPN client 438, 451, 544
 - See also* IRE
- IRR.DIGTCERT RACF facility class 245, 248
- ISAKMP action 104, 332, 340, 373, 394, 412, 447, 520, 632
- ISAKMP daemon 457
- ISAKMP Header 49
- ISAKMP header format 462
- ISAKMP Identity Protect exchange 460

- ISAKMP message 48
- ISAKMP proposal 340, 373, 394, 412, 447, 520, 632
- ISAKMP SA 47, 49, 512
- ISAKMP/Oakley 45, 319
- ISP 361, 436
- ISP access box 5, 7
- iterated tunneling 43
- IVP 253

K

- Kerberos 19, 88
- key distribution 46
- Key escrow 13
- key exchange protocol 37, 46
- key management 46
- Key modulus size 344
- key pair 73
- Key recovery 13
- key recovery agent 13
- Keyed-MD5 40
- keying material 52
- keysvgrp 303

L

- L2F 18, 32
- L2F encapsulation 32
- L2TP 18, 37, 436
- L2TP Access Concentrator (LAC) 23
- L2TP Compulsory Tunnel 26
- L2TP Network Server (LNS) 24
- L2TP Voluntary Tunnel 27
- Layer 2 Forwarding (L2F) 23, 31, 553, 554
- layer 2 tunneling 88, 123, 454, 553, 583, 584
- Layer 2 Tunneling Protocol (L2TP) 8, 23, 553, 557
- LDAP 382
- LDAP client 97
- LDAP configuration 106
- LDAP Data Interchange Format 100
- LDAP directory 97
- LDAP rule 105
- LDAP schema 98
- LDAP server 97, 99, 116
- LDAP server configuration 104
- LDAP server configuration files 100
- LDAP traffic 104, 107
- LDAP Version 3 98
- ldap.client component 99
- ldap.html.lang component 99
- ldap.server component 99
- lifetime 316
- Lightweight Directory Access Protocol (LDAP) 97, 116, 382
- link-by-link encryption 8
- link-layer encryption 8
- Linux 618, 636
- Linux kernel 636
- list certificates 353
- load CA certificate 352
- load certificate 349

- local authentication 319
- local key 319
- log files 457, 467
- logical topology 110
- Lotus Domino Go V4.6.2 99

M

- Macintosh 618
- Management Information Base (MIB) 115
- manual key distribution 407
- manual tunnel 107, 310, 312, 318
- MAXFILEPROC 243
- MAXPROCSYS 243
- MAXPROCUSER 243
- MAXSOCKETS 243
- MAXTHREAD 243
- MAXTHREADTASKS 243
- message authentication code (MAC) 93
- MIB objects 115
- MIB values 467
- Microsoft Dial-up Networking 598, 613, 619
- Microsoft Internet Explorer 5.0 612
- Microsoft Management Console (MMC) 560
- Microsoft Network Monitor 458
- minimum tolerance percentage level 630
- mknod command 258
- mobile user 85
- modem initialization string 439
- monitor tunnel connection 115
- multicast 308, 364
- multiple CAs 80
- multiprotocol tunnel 436
- MVS Messages
 - EZZ0349I 241
 - EZZ0641I 241
 - ICH408I 253

N

- NAT Limitations 90
- nested tunneling 43
- NetBEUI 31, 32
- NetBIOS 31, 618
- Netscape 92
- netstat -r command 616, 617, 624
- network access server (NAS) 87
- network access servers (NAS) 24
- Network Address Translation (NAT) 19, 474
- network address translation (NAT) 9, 94, 364, 408
- Network Associates Sniffer 458
- network layer 6
- Network News Transfer Protocol (NNTP) 92
- network security 20
- network security policy 21
- network sniffing tools 458
- Network TeleSystems (NTS) 618
 - See also* NTS
- Next Header field 40
- next protocol field 407
- nonce 50

- Nonces 47
- noncryptographic authentication 9
- NTS
 - configuration 620
 - connection details 623
 - EnterNet 636
 - fine-tuning 620
 - IP configuration 624
 - IP routing table 624
 - L2TP tunnel 621
 - NTS VPN virtual adapter 619
 - protocol configuration 621
 - tunnel protocol 622
 - TunnelBuilder 618, 622
 - TunnelMaster 618
 - virtual PPP interface 624
 - VPN capabilities 619
- NULL 40

O

- Oakley 46
- Oakley Main Mode 460
- Oakley Quick Mode 461
- object class 100
- OCEP 249, 255
- OCSF 240, 248
- on-demand dial-up 455
- on-demand inbound SA 70
- on-demand outbound SA 69
- on-demand tunnels 383
- Open Cryptographic Enhanced Plug-Ins (OCEP) 249, 255
- Open Cryptographic Services Facility (OCSF) 240, 248
- Operations Management 109
- OS/2 637
- OS/2 Warp 637
- OS/390
 - Configuration Client 483
 - dynamic connection 484
 - Firewall Log 483
 - network objects 484
 - OBROWSE command 483
 - tunnel ID 484
- OSPF 308, 364
- output packet filter 309

P

- packet filtering 9, 365, 406, 457
- Paktronix Guardian 636
- password authentication 21
- Password Authentication Protocol (PAP) 33
- path MTU discovery 39
- peer topology 83
- Perfect forward security (PFS) 46
- perfect forward security (PFS) 64
- performance 47, 93
- Performance Management 109
- Personal Communications 92
- PFS 328, 356

- physical topology 110
- PIN code 35
- PKI authenticated tunnel 337
- PKI initialization 354
- Pluto 637
- point of presence (POP) 23, 436
- Point-to-Point Protocol (PPP) 6
- Point-to-Point Tunneling Protocol (PPTP) 23, 30, 557
- policy class structure 101
- policy database 104, 308, 312
- policy engine 307
- policy feature 313
- policy file 101
- Policy Group 117
- policy information 97
- policy infrastructure 97
- policy management 381
- Policy schema 101
- policy search agent 101
- policy tree 313, 322
- policy, in tunnel definition 318
- port 93
- PPP 88
- PPP dial-up 544
- PPP over Ethernet (PPPoE) 618
- PPP user 585
- PPTP 18, 37
- predefined data management policies 139
- predefined ISAKMP proposals 334
- Pre-shared keys 46
- primary LDAP server 104
- Privacy Enhanced Mail (PEM) 344
- private IP address 89, 114, 362, 404, 406, 436, 453
- private key 47, 73
- private network 361
- problem determination 457
- Problem Management 109
- program controlled 250, 255
- Protocol SA 47
- proxy negotiation 48
- pseudo random function 52
- public IP address 90, 113, 404
- public IP addresses 362, 436
- public key 47, 73
- public key authentication 47
- public key encryption 46

Q

- QoS 11, 101
- quality of service 10

R

- RA certificate 550
- RACDCERT RACF command 248
- RACF 88
 - ADDGROUP command 246
 - ADDUSER command 246
 - BPX.DAEMON facility class 244, 247
 - BPX.FILEATTR.APF facility class 244, 250

BPX.FILEATTR.PROGCTL facility class 245, 250
 BPX.SERVER facility class 244, 251
 BPX.SMF facility class 244, 246
 BPX.SUPERUSER facility class 244
 CDS.CSSM facility class 245, 251
 CONNECT command 248
 CSFSERV class 245
 CSFSERV resource class 257
 FWKERN.START.REQUEST facility class 245, 246
 ICA.CFGSRV facility class 245, 247, 269
 IRR.DIGTCERT facility class 245, 248, 255
 LISTGRP command 245
 PROGRAM class 247, 251
 program controlled 247
 RACDCERT command 248, 257
 STARTED class 245, 246
 RADIUS 19, 32, 34, 88, 557, 585
 RADIUS client 87
 RADIUS server 87
 RC5 40
 RedCreek IPsec VPN Card 636
 Registration Authority (RAs) 75
 reliability 23
 reload command 337
 Remote Access Server (RAS) 21, 85
 remote authentication 319
 Remote Authentication Dial-In User Service (RADIUS) 86
 remote host 7
 remote IKE peer 323
 remote key 319
 remote user 6
 replay prevention 320
 repository 75
 reset database command 322, 336
 resource-clogging attack 468
 restart command 322, 337
 RFC 1492 86
 RFC 1825 637
 RFC 1828 40
 RFC 1968 35
 RFC 2058 86
 RFC 2138 86, 645
 RFC 2139 645
 RFC 2314 645
 RFC 2315 645
 RFC 2341 31, 32, 645
 RFC 2401 37, 644
 RFC 2402 37, 644
 RFC 2403 39, 41, 644
 RFC 2404 39, 41, 644
 RFC 2405 40, 644
 RFC 2406 644
 RFC 2407 49, 239, 644
 RFC 2408 45, 239, 463, 644
 RFC 2409 239, 644
 RFC 2410 40, 644
 RFC 2411 644
 RFC 2412 37, 45, 644
 RFC 2437 645
 RFC 2451 37, 40, 644
 RFC 2459 645
 RFC 2484 34
 RFC 2510 645
 RFC 2527 645
 RFC 2528 645
 RFC 2559 645
 RFC 2560 645
 RFC 2587 645
 RFC 2637 31, 32, 645
 RFC 2661 23, 32, 553, 644
 RFC1777 645
 RFC2251 645
 RFC2252 645
 RIP 364
 root CA 77
 router interface 312
 routing algorithms 364
 routing collisions 404
 routing decision 308
 routing domains 6
 routing protocol 406
 RSA 46, 92
 RSA key pairs 508
 RSA keys 548
 RSVP 11
 RSVP module 308

S
 SA bundle 38, 405
 SA characteristics 327
 SA lifesize 630
 SA lifetime 333, 378, 630
 save certificate 350
 secondary LDAP server 104
 secret key 73
 Secure Sockets Layer (SSL) 19, 98, 107, 263
 SecureID 35, 88
 security 13, 18, 19, 21, 28, 88, 91
 security association 45, 46, 64, 69, 319, 362, 365, 404, 405, 407
 Security Association Database (SAD) 38
 Security Associations Database (SAD) 69
 security database 86
 Security Dynamics, Inc. 35
 security exposures 10
 security gateway 5, 7, 8, 48, 361
 security holes 21
 Security Parameter Index (SPI) 38, 66
 security policy 17, 20, 21, 100
 Security Policy Database (SPD) 38, 69
 Security Server 240
 security solutions 19
 security strategy 19
 seed file 113
 sequence number 320
 session hijacking 39, 46
 SETROPTS WHEN(PROGRAM) 247
 shared secret 40, 46
 Shiva Password Authentication Protocol (SPAP) 34
 Simple Authentication and Security Layer (SASL) 98

- Simple Network Management Protocol (SNMP) 111
- single root CA 78
- SKEME 45
- SKEYID 52
- slapd.conf file 100
- SLIP 88
- sniffing attack 468
- SNMP 467
- SNMP agent 111
- SNMP community 112
- SNMP manager 111, 467
- SNMP messages 112
- SNMP request/response 111
- SNMP trap 112
- SOCKS 19, 89, 91, 94, 361, 408
- SOCKSified 92
- SOCKSv4 92
- SOCKSv5 92
- SPI 319
- spoofing attack 468
- SSL 263, 407
- SSL Handshake Protocol 92
- SSL Record Protocol 92
- SSL Version 3 support 99
- SSL-aware 94
- static filter rules 435
- Subject name 344
- subject_alternate_name 84, 180, 607
- Subject-Alt-Name 344
- System Group 117
- System SSL 249
- Systems Management disciplines 109

T

- TACACS 34
- TALK 5 525
- TCP header 406
- TCP port 1723 9
- TCPIP.PROFILE
 - DATAGRAMFWD keyword 241
 - FIREWALL keyword 241
 - IPCONFIG statement 241
- Telnet 48, 92
- Terminal Access Controller Access Control System (TACACS) 86
- Test Group 117
- TFTP server 342
- throughput 39
- time set command 316
- Tivoli TME10 NetView 118
- TLS 94
- TN3270 92
- topology information 364
- tracing 457
- traffic analysis 458
- traffic profile 313, 325, 337, 357
- transport adjacency 43
- transport mode 318, 405
- TTL 39
- tunnel

- tunnel mode 404, 405
- tunneling protocol 8
- tunnel endpoint 563, 629
- tunnel lifetime 318
- tunnel mode 90, 318
- tunnel name 318
- tunnel policy 318
- tunnel profile 521
- tunnel server 590

U

- U.S. export regulations 636
- UDP 28
- UDP port 1701 9, 626
- UDP port 500 9, 46, 193, 197, 226, 228, 408, 474, 505
- UNIX System Services
 - APF authorization 250, 255
 - extattr command 250, 256
 - fwauthinfo command 303
 - fwconns command 262, 305
 - fwdaemon command 260
 - fwdatapol command 302
 - fwdataprop command 302
 - fwdynconns command 305
 - fwdyntun command 302, 303
 - fwespran command 302
 - fwfilter command 262
 - fwfrule command 261, 303
 - fwkeysrv command 303
 - fwnwobj command 262, 301, 305
 - fwservice command 261, 304
 - fwstack command 259
 - iconv command 257
 - keysvrgrp command 303
 - mknod command 258
 - program controlled 250, 255
- user group 357

V

- V.34 dial-in interface 439
- validity period 316, 326, 339, 372, 394, 410, 444, 520, 628
- virtual private network
 - considerations 5
 - definition 3
 - end-to-end security 6
 - scenarios 14
 - security policy 22
 - security requirements 3
- virtual private networks
 - design 14
- virtual tunnel 32
- virus protection 17
- voluntary layer 2 tunneling 455
- VPN
 - IBM platform implementations 121
 - Linux 636
 - OS/2 637
- VPN certificate 345, 607

- VPN clients 597
- VPN gateway 30
- VPN management 12
- VPN management function 118
- VPN Policy MIB 117
- VPN technology 17

W

- wildcard 228, 541
- Wind River Systems (WRS) 612
 - See also* WRS
- Windows 2000
 - Authentication Method 562
 - authentication method 565
 - Broadcast 566
 - certificate-based authentication 557
 - certificates 562
 - Connection Wizard 587
 - data management tunnel 568
 - default policies 575
 - default response rule 562, 580
 - Diffie-Hellman Group 573, 580
 - Dynamic Default Response rule 563
 - EAP 557
 - EGP 567
 - Encryption algorithm 573, 580
 - endpoint type 564
 - Filter Action Wizard 568
 - HMP 567
 - host-to-host VPN 579
 - ICMP 568
 - Integrity Algorithm 572, 580
 - IP Security Management 559
 - IP Security Monitor 575
 - IP Security Policy Agent service 560
 - IP Security Policy Wizard 561, 579
 - IPSec 557
 - IPSec filter action 568, 581
 - IPSec filter list 566, 580
 - IPSec policy 573
 - IPSec rule 564
 - ipsecmon command 575
 - Kerberos 566
 - Kerberos V5 562
 - key exchange settings 571
 - key generation values 572
 - key management tunnel 571
 - L2TP 557, 583, 591
 - LDAP 566
 - Local Security Policy console 560
 - master key 572
 - Multicast 566
 - network type 565, 580
 - on-demand tunnels 575
 - Perfect Forward Secrecy 580
 - policy 560
 - PPP connection profile 587
 - PPTP 557, 591
 - pre-defined security method 570
 - pre-defined security methods 572

- pre-shared key 562, 580
- protocol type 567
- RADIUS 557
- RAW 568
- RDP 568
- RSVP 566
- security methods 569, 580
- Security Rule Wizard 570
- TCP 568
- UDP 568
- VPN connection profile 589
- XNS-IDP 568

- WinVPN client 630
- write command 337

WRS

- certificate-based authentication 614
- controlling traffic 616
- IKE Mode 615
- IKE negotiation 617
- IPSec Authentication 614
- IPSec Encryption 614
- iVasion VPNic virtual adapter 613
- L2TP tunnel 617
- L2TP Tunnel Authentication 615
- L2TP tunnel status 618
- pre-shared key 614
- task bar icon 614
- VPN capabilities 613
- WinVPN Client 612, 616

X

- X.500 name 344
- X.509 84
- X.509 Certificate 265
- xDSL 618

IBM Redbook evaluation

A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management
SG24-5309-00

Your feedback is very important to help us maintain the quality of ITSO 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!)

SG24-5309-00

Printed in the U.S.A.

