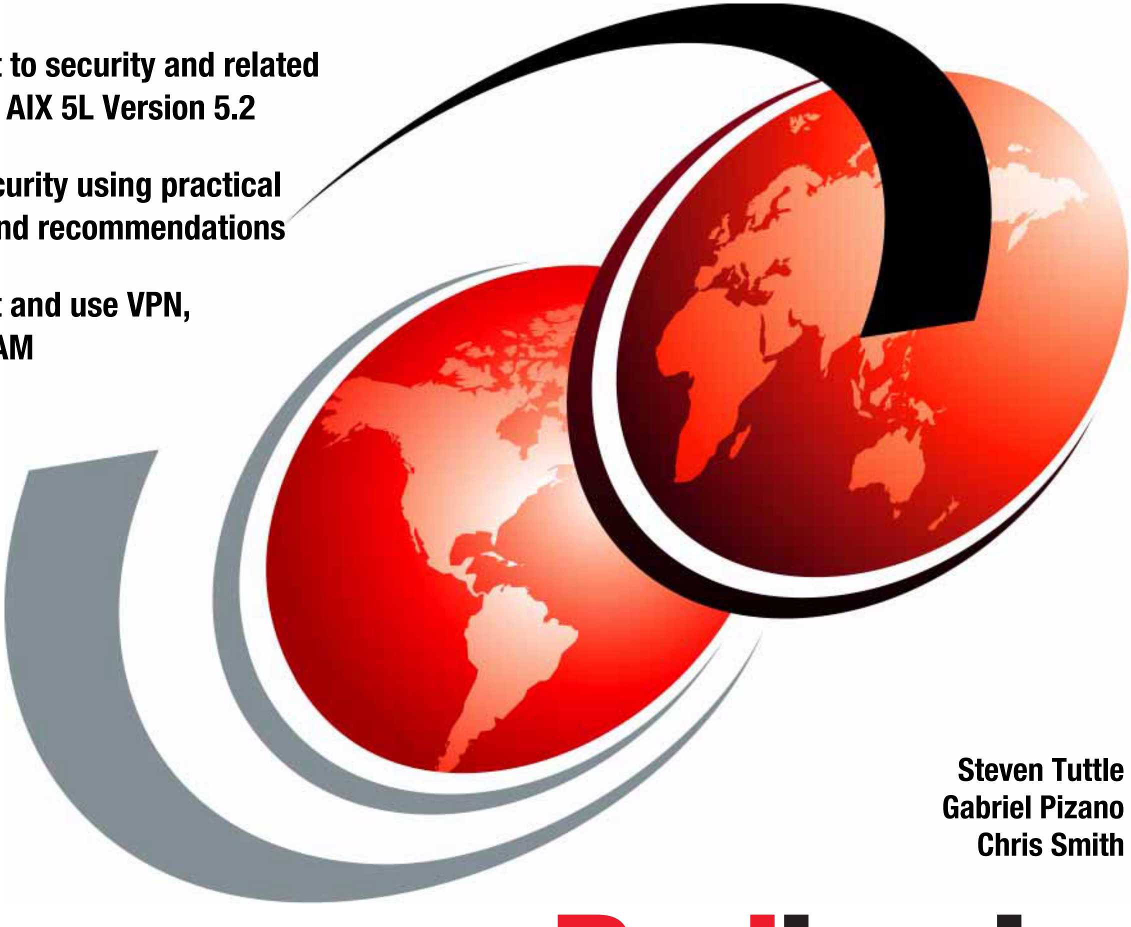
AIX 5L Version 5.2 Security Supplement

Gain insight to security and related features for AIX 5L Version 5.2

Improve security using practical examples and recommendations

Learn about and use VPN, NAS, and PAM



Steven Tuttle
Gabriel Pizano
Chris Smith

Redbooks

ibm.com/redbooks

International Technical Support Organization

AIX 5L Version 5.2 Security Supplement

November 2003

SG24-6066-00

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (November 2003)

This edition applies to AIX 5L Version 5, Release 2, Modification 0.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described 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:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include 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.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

eserver®
eserver®
ibm.com®
pSeries®
z/OS®
zSeries®
AIX 5L™
AIX®
IBM®
OS/390®
Redbooks™
Redbooks (logo) ™
RACF®
RS/6000®
SecureWay®
Tivoli Enterprise™
Tivoli®
WebSphere®

The following terms are trademarks of other companies:

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM® Redbook serves as a supplement to the IBM AIX® 5L™ Version 5.2 product documentation, particularly *AIX 5L Version 5.2 Security Guide*, SC23-4860. This redbook provides additional detailed information about virtual private networks (VPN), Kerberos security and the use of secure remote commands (RCMDS), Pluggable Authentication Modules (PAM), and examples on how to restrict users. You can use these features individually or integrate them together to improve AIX system security.

Use this redbook as an additional source for security information. Together with existing sources, you may use this redbook to enhance your knowledge of security and the features included with AIX 5L Version 5.2. You learn about the practical use of these security features, why they are necessary, and how you can use them in your environment to improve security. Plus you gain practical guidance through the examples that are provided and the recommendations for best practice.

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 (ITSO), Austin Center.

Steven Tuttle is a Project Leader for the ITSO, Austin center. He has 13 years of experience in the IT industry. He has worked at IBM for 10 years, with five years in direct involvement with IBM security products. He holds a degree in computer science from Clarkson University in Potsdam, New York, with concentrations in mathematics and psychology. His areas of expertise include the Tivoli® Enterprise™ products, Tivoli Security Products, and AIX. Before joining the ITSO, he worked for IBM Tivoli Services in the Security Practice as an enterprise security solution designer using IBM Tivoli software products. He is an IBM Certified Advanced Technical Expert for RS/6000® AIX.

Gabriel Pizano is an advisory IT specialist/architect from IBM Uruguay. He has a degree in computer science from the University of Buenos Aires, Argentina, and a degree in computer engineering from the Universidad de la Republica (University of Montevideo, Uruguay). He has worked in Integrated Technology Services (ITS) at IBM Uruguay since 1995. Before joining IBM, he has worked as a UNIX® System Administrator. He gives support to base components of the OS/390® operating system, such as Systems Network Architecture (SNA), TCP/IP, UNIX System Services, Resource Access Control Facility (RACF®), and others. He also supports Linux on the IBM @server zSeries® server, WebSphere® Application Server for z/OS® and other platforms, IBM Tivoli Storage Manager (all platforms), and implementing and architecting Storage Area Network (SAN) solutions. In the security area, his expertise is related to RACF and its components such as Linux and UNIX security environment. He has been a mainframe networking specialist for six years in SNA and TCP/IP. He now focuses on security implementations with networks, operating systems, and e-business applications.

Chris Smith is an Advisory Software Services Specialist with the ISCAIX Support Team, providing AIX support to the Asia-Pacific region from Petone, New Zealand. He has 17 years of experience in the IT field. He has worked at IBM for eight years. His areas of expertise include AIX, RS/6000, and IBM @server pSeries® hardware. He has written extensively on Technical Tips and Procedural information for his teams. He is an IBM Certified Advanced Technical Expert - RS/6000 AIX. He holds a National Certificate in Business Studies and Advanced Certificate in Business Computing from the Waiariki Institute of Technology.

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

Tony Bhe
Linda Robinson
Scott Vetter
International Technical Support Organization, Austin Center

Ufuk Celikkan
IBM AIX Security, Austin, TX

Bill Dodd
IBM Kerberos Development, Austin, TX

Greg Flaig
IBM TCP/IP Level 3 Support, Austin, TX

Ut Le
IBM Kerberos Team Lead, Austin, TX

Dennis P. Lee
IBM UNIX Software Service, Austin, TX

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an Internet note to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. OSJB Building 003 Internal Zip 2834
  11400 Burnet Road
  Austin, Texas 78758-3493

1

AIX security flashes

This chapter contains information about how to stay on top of the latest security flashes for IBM AIX 5L Version 5.2. We recommend that you review and integrate one or more of the options specified in this chapter into your site requirements and policies.

This information is provided to supplement the information and descriptions in *AIX 5L Version 5.2 Security Guide,* SC23-4860.

1.1 Recommended reading

We recommend that you read the *AIX Maintenance Strategy* tip on the Web. It explains the AIX Maintenance Strategy method to help you track and maintain updates to the system. You can find this tip on the Web at:

`https://techsupport.services.ibm.com/server/aix.srchBroker`

1.2 Security flash information by e-mail

We recommend that you subscribe to the e-mail notification services provided by IBM Support and Computer Emergency Response Team (CERT) to learn about fixes.

IBM provides a notification service which includes notification of security and high impact issues by e-mail. You can find more information about, and subscribe to, this service on the Internet at:

`https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs`

You can obtain specific details about the fixes by reading the alert e-mails, the individual fix readme files, or vulnerability details from the Computer Emergency Response Team (CERT) on the Internet. You can find CERT on the Web at:

`http://www.cert.org`

These services provide similar information so you may not want to subscribe to both. If you subscribe to both and receive too much information that doesn’t pertain to you, then you can always reduce the amount of information you receive from them. Or simply only subscribe to the service that offers the most useful information.

1.3 Obtaining fixes

After you gather the fix information, you must obtain and apply the fixes. There are various methods that exist for this task. Other methods that require less attention may have greater risk exposure, which may also be acceptable. The choice is yours.

You can choose from the following fix options:

- Download specific fixes individually or in selected groups.
- Obtain the “Critical Fixes” package. It is produced approximately monthly as required. It includes High Impact (HIPER), Security, and other specific important fixes. You can search for this fix by using the argument “CRITICAL FIXES” as the APAR abstract.
- Download the recommended maintenance package. This package is produced about twice a year as a cumulative package. It provides the latest updates for all AIX filesets, and includes the HIPER and security fixes.

You can access and download these fixes for all supported AIX versions from the Web at:

`https://techsupport.services.ibm.com/server/fixes?view=pSeries`

2

Virtual private networks

Virtual private networks (VPNs) are implemented in IBM AIX 5L Version 5.2 using IP Security (IPSec). IPSec is an open standard security technology developed by the Internet Engineering Task Force (IETF). It provides protection based on cryptography for all data at the Internet Protocol (IP) layer. This protection is transparent for applications. IPSec is the standard security framework chosen by the IETF for IP Version 4 and 6 environments.

2.1 Architecture

IP security is designed to provide cryptographic security for IPv4 and IPv6. It includes access control, connectionless integrity, data origin authentication, and protection against replays and encryption. These services are provided for IP and upper layer protocols at the IP layer. They are implemented through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP). They are also implemented through the use of cryptographic key management protocols and procedures.

IPSec design permits the selection of different sets of algorithms. You may select different sets of algorithms as required. A standard set of default algorithms is specified to obtain interoperability.

For additional information about IP Security Architecture, see Request for Comments (RFC) 2401, *Security Architecture for the Internet Protocol*, from the IETF. You can find this RFC on the Internet at:

`http://www.ietf.org/rfc/rfc2401.txt`

2.2 Security

IPSec authentication algorithms verify the identity of the sender and data integrity. They do this by using a cryptographic hash function to process a data packet (with the fixed IP header fields included), using a secret key to obtain a unique digest. On the receiver side, the data is processed using the same function and key. When data is altered or the validation of the sender key fails, the datagram is discarded.

Encryption uses a cryptographic algorithm to change and randomize the data using a combination of algorithm and key to produce a ciphertext. Encryption makes data unreadable while it is in transit. After received, the data is decrypted using the same combination of algorithm and key (with symmetric encryption algorithms). Encryption must occur with authentication to verify the data integrity of the encrypted data.

IPSec services are implemented using the ESP and AH protocols. ESP provides encryption of the original IP packet, builds an ESP header, and places the encrypted data in the ESP payload.

The Authentication Header can be used alone for authentication and integrity-checking, if confidentiality is not necessary. With AH, a hash algorithm is applied to the static fields of the IP header and the data to compute a keyed digest. The receiver uses its key to compute and compare the digest to make sure the packet is not altered and the sender's identity is validated.

2.2.1 Transport mode

In transport mode, the protocols provide protection for upper layer protocols. A security header is added after the original IP header of the packet, which is before the payload. If confidentiality is needed, a trailer and an authentication are added after the payload. Figure 2-1 shows the transport mode IP packet.

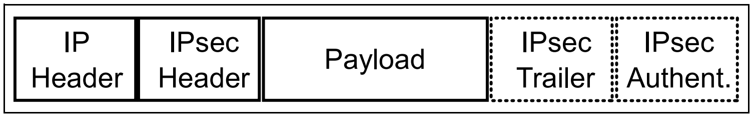


Figure 2-1 IP packet in transport mode

Transport mode is typically used for peer-to-peer communication security where data is sent encrypted. This mode is used when the cryptographic endpoints are also the communication endpoints of the secured IP packets.

2.2.2 Tunnel mode

In tunnel mode, the protocols are applied to tunneled IP packets. The IP packet is encapsulated in a new one. A security header is added between a new IP header and the old one. If confidentiality is needed, a trailer and an authentication are added after the payload. Figure 2-2 shows the tunnel mode IP packet.

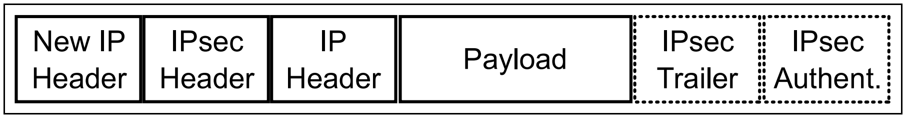


Figure 2-2 IP packet in tunnel mode

Tunnel mode is used for site-to-site communication security where the entire packet is encrypted. It is implemented in gateway scenarios.

2.2.3 Security parameter index

The security parameter index (SPI) value is used to identify different connections with the same destination address and security protocol. The SPI is carried in the header of the security protocol.

In manual tunneling, you must specify this value manually. For more information about specifying the security parameter index for a manual tunnel, see 2.4.6, “Manual tunnels using the System Management Interface Tool” on page 57.

2.2.4 Security associations

The building block, on which secure communications are built, in IBM AIX 5L Version 5.2 is the concept of security associations (SA). It associates a specific set of security parameters to a type of traffic. With data protected by IP Security, a separate security association exists for each direction and for each header type, AH or ESP. The information contained in the security association includes the IP addresses of both ends, SPI, the algorithms selected for authentication or encryption, the authentication and encryption keys, and the key lifetimes.

Two types of security associations exist, transport mode and tunnel mode. You can learn more about each of these modes in 2.2.1, “Transport mode” on page 7, and 2.2.2, “Tunnel mode” on page 7.

2.2.5 Filter rules

IBM AIX 5L Version 5.2 filtering is a basic function in which incoming and outgoing packets are accepted or denied based on a variety of characteristics. This allows you to configure a host to control the traffic between itself 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. Filter rules associate particular types of traffic with a tunnel, but the data being filtered does not necessarily need to travel in a tunnel. This aspect of filter rules provides basic firewall functionality to restrict traffic to or from a machine in a network that does not have the protection of a true firewall.

Static filters

You can add, delete, update, or move static filters. You use them for general filtering or associated to manual tunnels.

A user can manually manage these rules.

Autogenerated filters

These filters include a specific set of rules used for Internet Key Exchange (IKE) generated tunnels. You add them when the phase 2 tunnels are activated. You remove them when the phase 2 tunnel is deactivated.

Predefined filters

You cannot alter or delete predefined filter rules since they are related to all traffic. They are added by AIX IPSec.

Figure 2-3 shows the filter module. From the network, the packet goes to the IP stack. Then it is sent to the filter module. If it is an IPSec packet, it is sent to tunnel definitions. Otherwise it is returned to the IP stack.

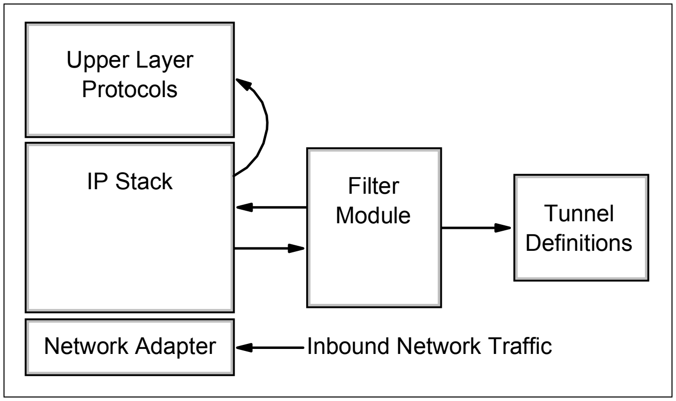


Figure 2-3 Filter module flow

2.2.6 Encapsulating Security Payloads

The ESP header is designed to provide a mix of security services in IPv4 and IPv6. You may apply ESP alone or in combination with the IP AH. You can provide security services between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host.

You can insert the ESP header after the IP header and before the upper layer protocol header (transport mode), as shown in Figure 2-4.

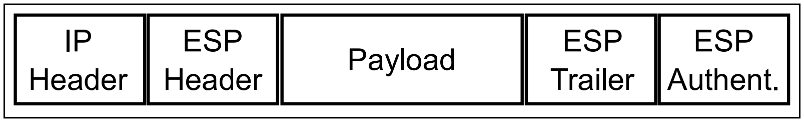


Figure 2-4 ESP protocol in transport mode

Or you can insert the ESP header before an encapsulated IP header (tunnel mode), as shown in Figure 2-5.

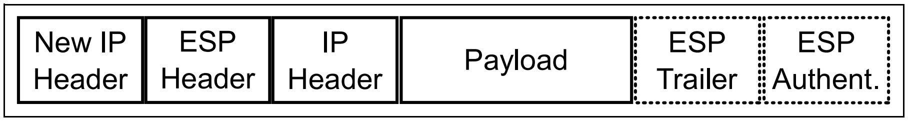


Figure 2-5 ESP protocol in tunnel mode

ESP provides confidentiality, data origin authentication, connectionless integrity, and anti-replay service. Traffic flow confidentiality requires tunnel mode. We recommend that you implement it with a security gateway, where traffic aggregation can hide true source-destination patterns.

For more information about ESP, see the RFC 2406, *IP Encapsulating Security Payloads*, from the IETF. You can find this RFC on the Web at:

http://www.ietf.org/rfc/rfc2406.txt

Important: Although both confidentiality and authentication are optional, you *must* select at least one of them.

Network address translation problem with ESP in transport mode

When an IPSec packet arrives to a network address translation (NAT) device, change the Transmission Control Protocol (TCP) checksum. Because it is inside the payload of the packet, this operation cannot succeed due to the previous encryption. Despite whether the ESP verification is successful at the end, the packet is discarded because of a TCP checksum error.

To use NAT with ESP in transport mode, you must configure two tunnels. This way the NAT device sees a traditional IP packet. All the IPSec headers and trailers are suppressed before the arrival of the information to the NAT device.

To see a well-behaved model of NAT with IPSec, see RFC 2709, *Security Model with Tunnel-mode for IPSec for NAT Domains*, from the IETF. You can find this RFC on the Web at:

http://www.ietf.org/rfc/rfc2709.txt

2.2.7 Authentication Header

The IP Authentication Header provides connectionless integrity and data origin authentication for IP datagrams. It also provides protection against replays. AH provides authentication for some IP header fields and for upper-level protocol data. IP headers may change in transit, and the value of their fields may also change when the packet arrives at the receiver. This may not be predictable by the sender. The values of such fields cannot be protected by AH. Figure 2-6 shows the IP packet for the AH protocol in transport mode.

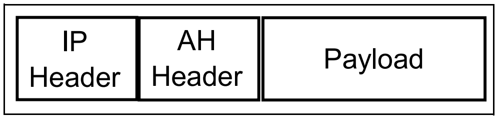


Figure 2-6 AH protocol in transport mode

Figure 2-7 shows the IP packet for the AH protocol in tunnel mode.

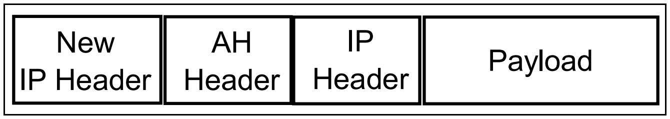


Figure 2-7 AH protocol in tunnel mode

You may apply AH alone or in combination with the IP ESP. For example, you can combine ESP in transport mode with AH in tunnel mode, as shown in Figure 2-8. You can provide security services between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host.

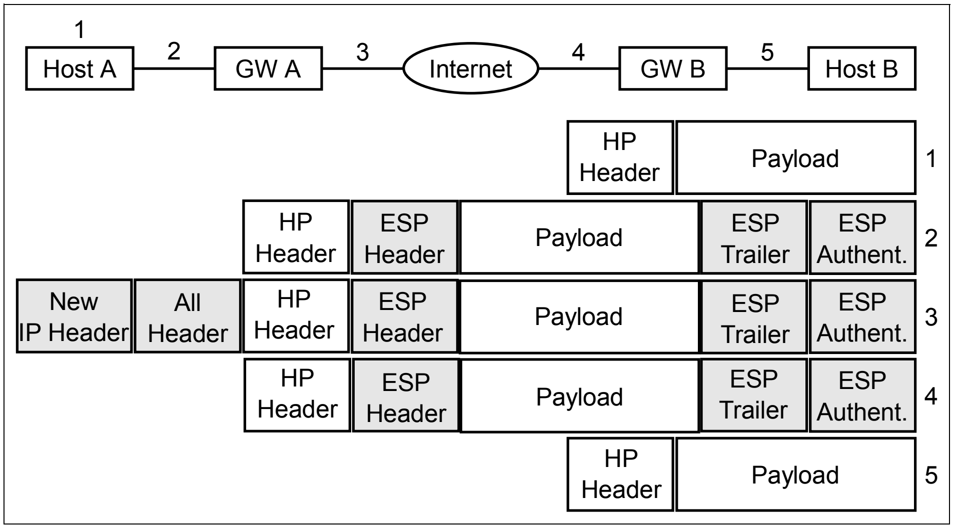


Figure 2-8 Combination of ESP in transport mode and AH in tunnel mode

You may use ESP to provide the same security services and a confidentiality (encryption) service. A difference between the authentication provided by ESP and AH is that ESP does not protect any IP header fields.

For more information about Authentication Headers, see RFC 2402, *IP Authentication Header*, from the IETF. You can find this RFC on the Web at:

http://www.ietf.org/rfc/rfc2402.txt

NAT problem with AH

The source IP address, the IP checksum, and TCP checksum are altered by NAT. At the end when the IPSec packet is verified, the AH authentication that is calculated doesn't match the AH authorization packet field.

Note: IBM AIX developers are addressing this problem with NAT and the AH protocol. They expect to provide a fix in a future release or patch of IBM AIX.

The work-around to using NAT with AH is to configure two tunnels. This way the NAT device sees a traditional IP packet. All the IPSec headers and trailers are suppressed before the arrival of the information to the NAT device.

To see a well-behaved model of NAT with IPSec, see RFC 2709, *Security Model with Tunnel-mode for IPSec for NAT Domains*, from the IETF. You can find this RFC on the Web at:

http://www.ietf.org/rfc/rfc2709.txt

2.2.8 Key management

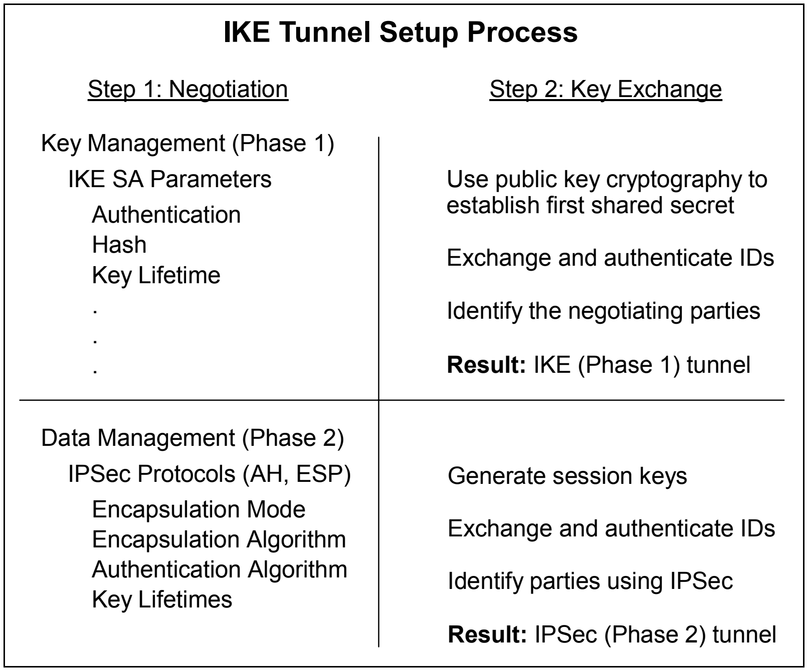
To set up a secure communication between two hosts, you must negotiate security associations and manage them during the use of the tunnel. The following types of tunnels are supported, each using a different key management technique:

- **Internet Key Exchange tunnels**: IKE tunnels have dynamically changing keys. This key management technique is based on an IETF standard.
- **Manual tunnels**: Manual tunnels have static, persistent keys. This key management technique is also based on an IETF standard.

IKE tunnel support

IKE tunnels are based on the standards developed by the IETF. With this protocol, security parameters are negotiated and refreshed. Keys are exchanged securely. IBM AIX 5L Version 5.2 supports the preshared key and X.509v3 digital certificate signatures types of authentication.

The negotiation uses a two-phase approach. The first phase authenticates the communicating parties and specifies the algorithms to be used for securely communicating in the second phase. During the second phase, you negotiate the IP Security parameters to be used during data transfer. You also create and exchange security associations and keys. Figure 2-9 shows this two-phase approach to setting up the IKE tunnel.



IKE Tunnel Setup Process

Step 1: Negotiation	Step 2: Key Exchange
Key Management (Phase 1) IKE SA Parameters Authentication Hash Key Lifetime . . .	Use public key cryptography to establish first shared secret Exchange and authenticate IDs Identify the negotiating parties **Result:** IKE (Phase 1) tunnel
Data Management (Phase 2) IPSec Protocols (AH, ESP) Encapsulation Mode Encapsulation Algorithm Authentication Algorithm Key Lifetimes	Generate session keys Exchange and authenticate IDs Identify parties using IPSec **Result:** IPSec (Phase 2) tunnel

Figure 2-9 Two-phase process to set up an IKE tunnel

For more information about IKE, see RFC 2409, *The Internet Key Exchange (IKE)*, from the IETF. You can find it on the Web at:

http://www.ietf.org/rfc/rfc2409.txt

As RFC 2409 stands, you have two modes for the phase one interchange: main mode and aggressive mode. The differences between the two modes are:

- **Main mode** uses six messages for exchange. The identities of the parties are protected by encryption.
- **Aggressive mode** uses three messages for exchange. The identities of the parties are *not* protected by encryption.

We recommend that you use *main mode* for the phase 1 interchange when possible. If you have performance issues or the IP address of one or both parties is not known, then consider using aggressive mode. For more information about dynamically assigned addresses, see "Using IKE with dynamically assigned addresses" on page 15.

Table 2-1shows the authentication algorithms that you can use with the AH and ESP security protocols for IKE tunnel support.

Table 2-1 Authentication algorithms for IKE tunnels

Algorithm	AH IP Version 4 and 6	ESP IP Version 4 and 6
HMAC MD5	X	X
HMAC SHA1	X	X
DES CBC 8		X
Triple DES CBC		X
ESP Null		X

Perfect forward secrecy

With perfect forward secrecy (PFS), each refreshed key is derived without any dependence on predecessor keys.

Diffie-Hellman

The Diffie-Hellman (DH) algorithm is used to establish a shared secret number to protect an insecure channel. The communicating parties exchange public information from which they derive a key. After they establish a shared number, you can use this number to derive keys with symmetric key algorithms. This number does not authenticate the parties.

The Diffie-Hellman groups defined for IKE are:

- 768-bit, called group 1, supported by IBM AIX
- 1024-bit, called group 2, supported by IBM AIX
- 1536-bit, called group 5 new in IBM AIX 5L Version 5.2
- 2048-bit, 3072-bit, 4096-bit, 6144-bit, and 8192-bit

For more information about Diffie-Hellman groups, see RFC 3562, *More Modular Exponential (MODP) Diffie- Hellman Groups for Internet Key Exchange (IKE)*, from the IETF. You can find this RFC on the Web at:

http://www.ietf.org/rfc/rfc3562.txt?number=3562

Symmetric keys generated with DH group 5 are more secure but require more processing time.

Tunnel type comparison and recommendation

Whether you use manual tunnels or IKE tunnels depends on the tunnel support of the remote end and the type of key management desired. We recommend that you use IKE tunnels because they offer standard secure key negotiation and key management. Optionally, you can configure digital certificates.

> **Attention:** Avoid the use of manual tunnels if you IKE tunnels are available. Manual tunnels are not as secure as IKE tunnels (due to manual key administration).

Using IKE with dynamically assigned addresses

Remote systems may initiate IKE sessions with a server and their identity cannot be tied to a particular IP address. Or remote clients may dial in to a server, and use either a fully qualified domain name or e-mail address to identify the remote ID. In either case, you must use *aggressive mode*, because the IP address is not known before the identity interchange.

When dynamic IP boxes are part of a tunnel configuration, the tunnel starts from a dynamic IP. The static IP boxes only can act as responders.

Manual tunnel support

Manual tunnels provide backward compatibility. They interoperate with machines that do not support IKE key management protocols. The disadvantage of manual tunnels is that the key values are static. The encryption and authentication keys are the same for the life of the tunnel, and you must manually update them. Table 2-2 shows the authentication algorithms that you can use for manual tunnels.

Table 2-2 Authentication algorithms for manual tunnels

Algorithm	**AH IP Version 4**	**AH IP Version 6**	**ESP IP Version 4**	**ESP IP Version 6**
HMAC MD5	X	X	X	X
HMAC SH1	X	X	X	X
Triple DES CBC			X	X
DES CBC 8			X	X
DES CBC 4			X	X

Hash functions

These algorithms typically provide a digital fingerprint of file contents. The fingerprint is used to avoid any intrusion (intruder or virus). The most common algorithms for encrypting passwords are Message Digest 5 (MD5) and Secure Hash Algorithm (SHA)-1. These algorithms are sometimes called *message digest algorithms*. The plain text is transformed mathematically, so the contents and length of the data are not recoverable without the algorithm. A cryptographic key is usually involved.

Hardware acceleration

If you have hardware acceleration, hardware is used instead of software algorithms:

- Encryption and decryption using Data Encryption Standard (DES) or Triple DES algorithms
- Authentication using the MD5 or SHA-1 algorithms
- Storage of the security-association information

To offload IP security functions from IBM AIX 5L Version 5.2, you need to install:

- bos.net.ipsec.rte 5.1.0.25 or later
- devices.pci.1410ff01.rte

The 10/100 Mbps Ethernet PCI Adapter II (Feature code 4962) supports:

- DES, 3DES, or NULL encryption through ESP
- Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA-1 authentication through ESP or AH, but not both

  If ESP and AH are both used, ESP must be performed first. This is always true for IKE tunnels, but the user can select the order for manual tunnels.
- Transport and tunnel mode
- Offload of IPV4 packets

This functionality was delivered in IBM AIX 5L 5.1.0.25 and later.

> **Note:** The 10/100 Mbps Ethernet PCI Adapter II cannot handle packets with IP options.

For more information, see *IP Security Hardware Assist Feature of the 10/100 Mbps Ethernet PCI Adapter II (FC 4962)*. You can find this document at:

`ftp://ftp.software.ibm.com/software/mktsupport/techdocs/ipsec.pdf`

Note: You must enable the IPSec offload function to use this feature. See 2.3.2, “Enabling IPSec offload” on page 23.

2.2.9 Security features

The security features provided by VPNs fall into two different categories: IP features and IKE features.

IP features

The Internet Protocol supports the following features:

- Hardware acceleration with the 10/100 Mbps Ethernet PCI Adapter II
- AH support using RFC 2402 and ESP support using RFC 2406
- Certificate Revocation List (CRL) support with retrieval using Hypertext Transfer Protocol (HTTP) or Lightweight Directory Access Protocol (LDAP) servers
- Automatic key refreshment with tunnels using the IETF IKE protocol
- X.509 Digital Certificate and preshared key support in IKE protocol during key negotiation
- Configuration of manual tunnels to provide interoperability with other systems that do not support the automatic IKE key refreshment method, and for the use of IP Version 6 tunnels
- Tunnel mode and transport mode of encapsulation for host or gateway tunnels
- Authentication algorithms of HMAC, MD5, and HMAC SHA
- Encryption algorithms that include 56-bit DES Cipher Block Chaining (CBC) with 64-bit initial vector (IV), Triple DES, and DES CBC 4 (32-bit IV)
- Dual IP stack support (IP Version 4 and IP Version 6)
- Encapsulating and filtering of IP Version 4 and IP Version 6 traffic

  Because the IP stacks are separate, the IP Security function for each stack can be configured independently.
- Creating IKE tunnels using Linux configuration files (IBM AIX 5L Version 5.1 and later)
- Filtering of secure and nonsecure traffic by a variety of IP characteristics such as source and destination IP addresses, interface, protocol, port numbers, and more
- Automatic filter-rule creation and deletion with most tunnel types

- Using host names for the destination address when defining tunnels and filter rules

  The host names are converted to IP addresses automatically as long as the Domain Name Service is available.
- Logging of IP Security events to syslog
- Using system traces and statistics for problem determination
- User-defined default action that allows the user to specify whether to allow traffic that does not match defined tunnels

IKE features

Internet Key Exchange supports the following features:

- Authentication with preshared keys and X.509 digital signatures
- Use of main mode (identity protect mode) and aggressive mode
- Support for Diffie Hellman groups 1, 2, and 5
- ESP encryption support for DES, Triple DES, Null encryption and ESP authentication support with HMAC MD5 and HMAC SHA
- AH support for HMAC MD5 and HMAC SHA1
- IP Version 4 and Version 6 support

2.3 Installing IPSec

This section explains how to install IPSec. It also provides an easy Installation Verification Procedure (IVP).

The operating system level is IBM AIX 5L Version 5.2, maintenance level 5200-01.

Install the IPSec filesets as explained in the following section. Then apply the following program temporary fixes (PTFs):

- U486472 bos.net.ipsec.keymgt.5.2.0.11
- U486435 bos.net.ipsec.rte.5.2.0.11

You can download the IBM AIX 5L Version 5.2 PTFs from the IBM Web site at:

`https://techsupport.services.ibm.com/server/aix.fixsearch52`

2.3.1 Installing the IP Security feature

The IP Security feature in AIX is separately installable and loadable. The filesets that you must install are:

- bos.net.ipsec.rte
- bos.msg.LANG.net.ipsec

  LANG is the desired language, such as en_US for United States English.

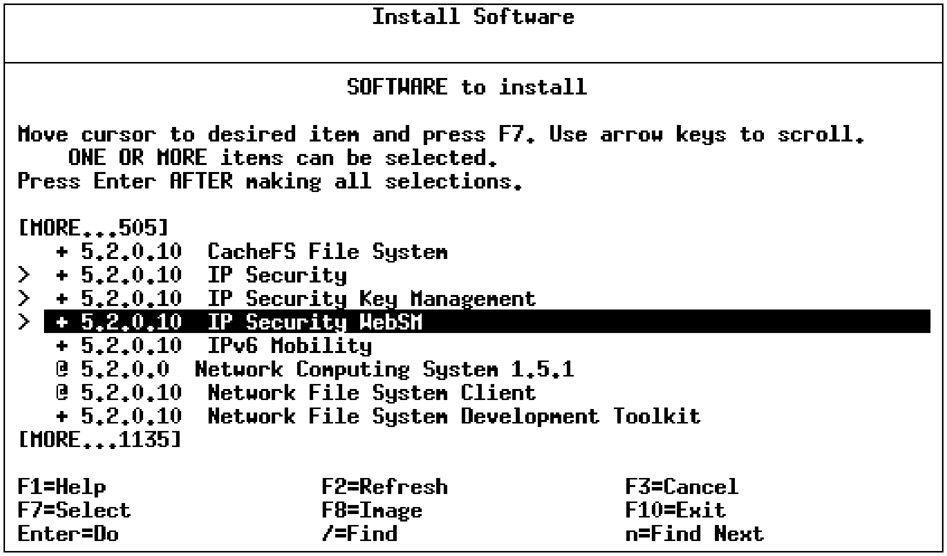
- bos.net.ipsec.keymgt
- bos.net.ipsec.websm
- bos.crypto-priv

To install the ipsec filesets, complete these steps:

1. From a command line, type:

   ```
   smitty installp
   ```

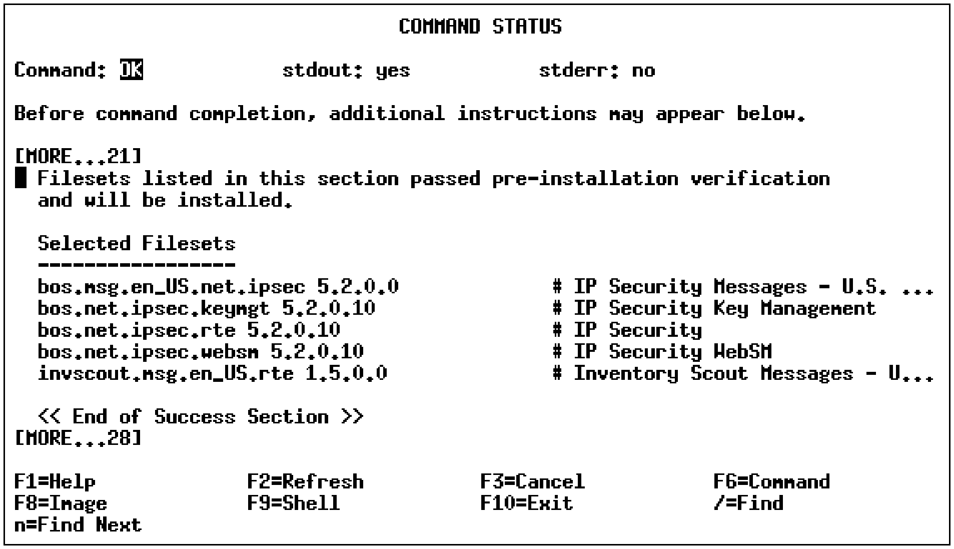
2. Choose **Install Software**.
3. Select a device. For example, select **/dev/cd0** for the compact disc device.
4. Select the packages shown in Figure 2-10 for installation. Then press Enter to install the selected filesets.



```
                             Install Software

                           SOFTWARE to install

Move cursor to desired item and press F7. Use arrow keys to scroll.
    ONE OR MORE items can be selected.
Press Enter AFTER making all selections.

[MORE...505]
   + 5.2.0.10  CacheFS File System
>  + 5.2.0.10  IP Security
>  + 5.2.0.10  IP Security Key Management
>  + 5.2.0.10  IP Security WebSM
   + 5.2.0.10  IPv6 Mobility
   @ 5.2.0.0  Network Computing System 1.5.1
   @ 5.2.0.10  Network File System Client
   + 5.2.0.10  Network File System Development Toolkit
[MORE...1135]

F1=Help                 F2=Refresh              F3=Cancel
F7=Select               F8=Image                F10=Exit
Enter=Do                /=Find                  n=Find Next
```

Figure 2-10 IPSec packages selection

5. Review the output of the installation to ensure that the filesets were applied successfully, as shown in Figure 2-11.



```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...21]
█ Filesets listed in this section passed pre-installation verification
  and will be installed.

  Selected Filesets
  -----------------
  bos.msg.en_US.net.ipsec 5.2.0.0             # IP Security Messages - U.S. ...
  bos.net.ipsec.keymgt 5.2.0.10               # IP Security Key Management
  bos.net.ipsec.rte 5.2.0.10                  # IP Security
  bos.net.ipsec.websm 5.2.0.10                # IP Security WebSM
  invscout.msg.en_US.rte 1.5.0.0              # Inventory Scout Messages - U...

  << End of Success Section >>
[MORE...28]

F1=Help             F2=Refresh          F3=Cancel           F6=Command
F8=Image            F9=Shell            F10=Exit            /=Find
n=Find Next
```

Figure 2-11 IPSec filesets installed

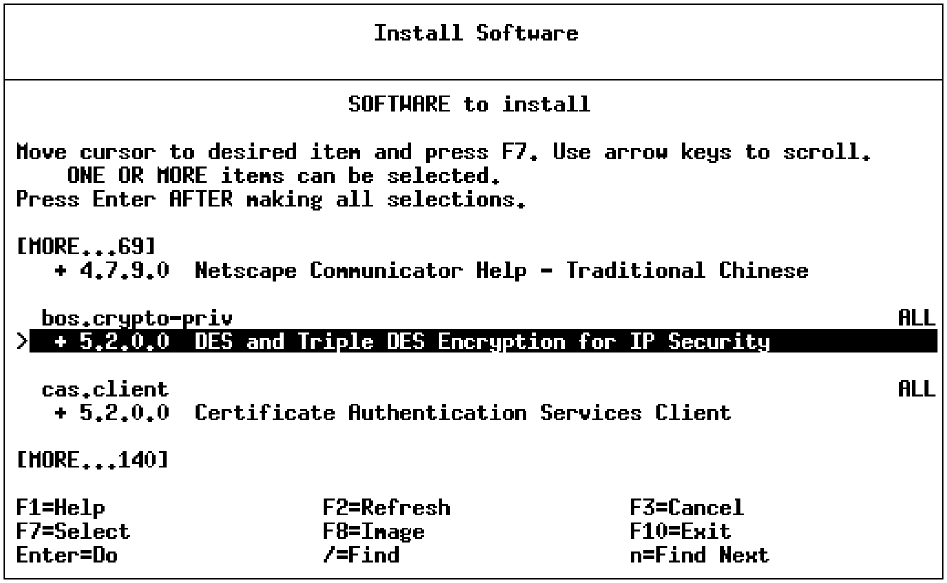
The bos.crypto-priv fileset is located on the Expansion Pack CD. For IKE digital signature support, you must also install the gskit.rte fileset (AIX Version 4) or gskkm.rte (AIX 5.1) located on the Expansion Pack CD.

To install these ipsec filesets, complete these steps:

1. From a command line, type:

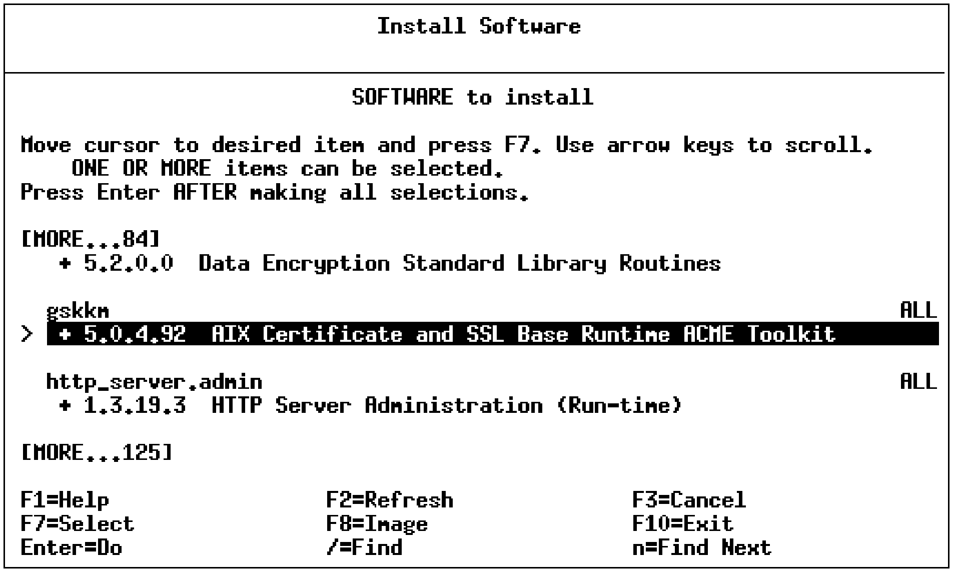
   ```
   smitty installp
   ```

2. Select **Install Software**.
3. Select the device. For example, select **/dev/cd0** for the compact disc device.
4. Select the packages shown in Figure 2-12 and Figure 2-13 for installation. Press Enter to install the selected filesets.



```
                            Install Software

                          SOFTWARE to install

Move cursor to desired item and press F7. Use arrow keys to scroll.
    ONE OR MORE items can be selected.
Press Enter AFTER making all selections.

[MORE...69]
   + 4.7.9.0  Netscape Communicator Help - Traditional Chinese

  bos.crypto-priv                                                 ALL
>  + 5.2.0.0  DES and Triple DES Encryption for IP Security

  cas.client                                                      ALL
   + 5.2.0.0  Certificate Authentication Services Client

[MORE...140]

F1=Help                 F2=Refresh              F3=Cancel
F7=Select               F8=Image                F10=Exit
Enter=Do                /=Find                  n=Find Next
```

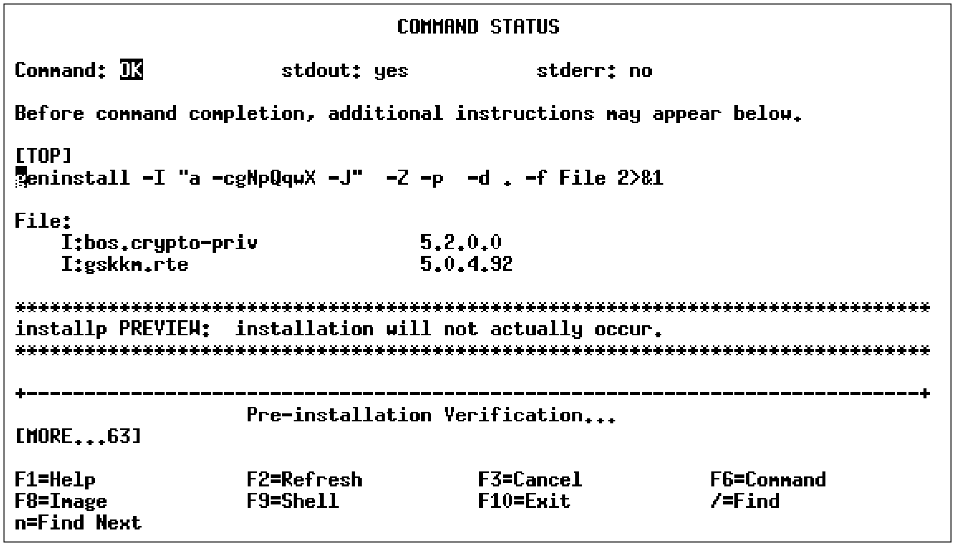
Figure 2-12 Crypto package selection



```
                            Install Software

                          SOFTWARE to install

Move cursor to desired item and press F7. Use arrow keys to scroll.
    ONE OR MORE items can be selected.
Press Enter AFTER making all selections.

[MORE...84]
   + 5.2.0.0  Data Encryption Standard Library Routines

  gskkm                                                           ALL
>  + 5.0.4.92  AIX Certificate and SSL Base Runtime ACME Toolkit

  http_server.admin                                               ALL
   + 1.3.19.3  HTTP Server Administration (Run-time)

[MORE...125]

F1=Help                 F2=Refresh              F3=Cancel
F7=Select               F8=Image                F10=Exit
Enter=Do                /=Find                  n=Find Next
```

Figure 2-13 IKE package selection

5. Review the output of the installation to ensure that the filesets were applied successfully, as shown in Figure 2-14.



```
                              COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[TOP]
geninstall -I "a -cgNpQqwX -J"  -Z -p  -d . -f File 2>&1

File:
    I:bos.crypto-priv             5.2.0.0
    I:gskkm.rte                   5.0.4.92

*******************************************************************************
installp PREVIEW:  installation will not actually occur.
*******************************************************************************

+-----------------------------------------------------------------------------+
                    Pre-installation Verification...
[MORE...63]

F1=Help             F2=Refresh          F3=Cancel           F6=Command
F8=Image            F9=Shell            F10=Exit            /=Find
n=Find Next
```

Figure 2-14 IKE filesets installed

For IP Security support in Web-based System Manager, you must install the Java131.ext.xml4j fileset at level 1.3.1.1 or later. In our case, it was already installed.

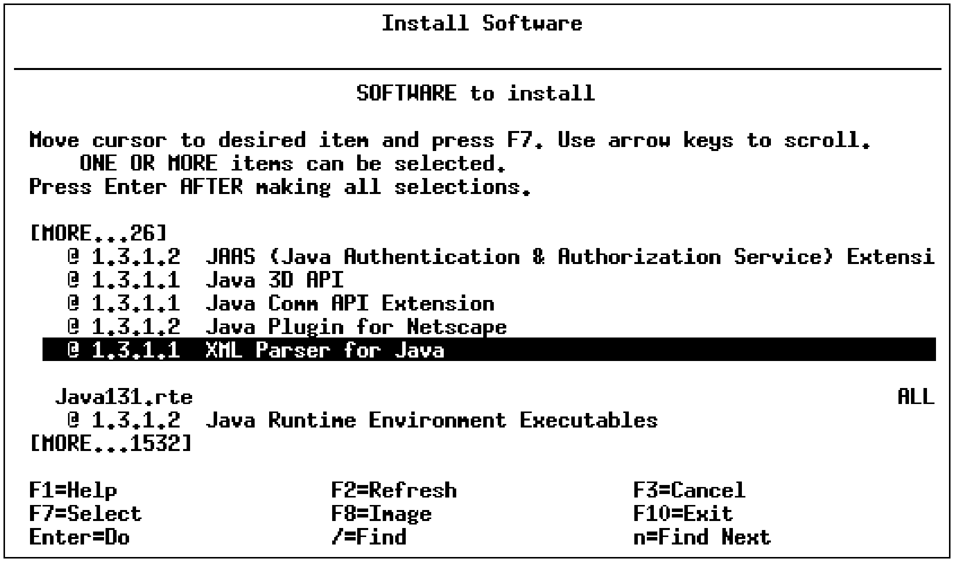
If you need to install this fileset, complete these steps:

1. From a command line, type:

   ```
   smitty installp
   ```

2. Select **Install Software**.
3. Select the device. For example, select **/dev/cd0** for the compact disc device.

4. Select the package shown in Figure 2-15 to install it.



```
                              Install Software

                             SOFTWARE to install

 Move cursor to desired item and press F7. Use arrow keys to scroll.
     ONE OR MORE items can be selected.
 Press Enter AFTER making all selections.

 [MORE...26]
    @ 1.3.1.2  JAAS (Java Authentication & Authorization Service) Extensi
    @ 1.3.1.1  Java 3D API
    @ 1.3.1.1  Java Comm API Extension
    @ 1.3.1.2  Java Plugin for Netscape
    @ 1.3.1.1  XML Parser for Java

   Java131.rte                                                       ALL
    @ 1.3.1.2  Java Runtime Environment Executables
 [MORE...1532]

 F1=Help                  F2=Refresh               F3=Cancel
 F7=Select                F8=Image                 F10=Exit
 Enter=Do                 /=Find                   n=Find Next
```

Figure 2-15   XML Parser for Java™ package selection

> **Note:** The @ character in the SOFTWARE to install window means that this fileset is already installed. If it is not already installed, press F7 to select it and follow the same procedure as for the other packages.

2.3.2 Enabling IPSec offload

To enable IPSec offload, you must first remove the network interface and then enable the IPSec offload feature.

Enabling IPSec offload using the System Management Interface Tool

To detach the network interface, use the System Management Interface Tool (SMIT) to complete these steps:

1. From a command line, type:

   ```
   smitty inet
   ```

2. Select the **Remove a Network Interface** option.
3. Select the network interface that corresponds to the 10/100 Mbps Ethernet PCI Adapter II.
4. Press Enter to remove the network interface.

To enable the IPSec offload feature, use SMIT to complete these steps:

1. From a command line, type:

   ```
   smitty eadap
   ```

2. Select the **Change / Show Characteristics of an Ethernet Adapter** option.
3. Select the **10/100 Mbps Ethernet PCI Adapter II**.
4. Change the IPSec Offload field to `Yes`.

Enabling IPSec offload from a command line

Complete the following steps:

1. Bring the network interface down and detach the network interface from the command line. Type the following command:

   ```
   # ifconfig enX inet down
   # ifconfig enX detach
   ```

   Here X corresponds to your Ethernet adapter device. In our case, it was the first Ethernet adapter device numbered 0.

2. Enable the IPSec offload attribute. From the command line, type:

   ```
   # chdev -l entX -a ipsec_offload=yes
   ```

3. Verify that the IPSec offload attribute is enabled. On the command line, type:

   ```
   # lsattr -El entX
   ```

4. Attach the network interface. From the command line, type:

   ```
   # ifconfig entX attach
   # ifconfig entX inet up
   ```

   Here X corresponds to your Ethernet adapter device. In our case, it was the first Ethernet adapter device numbered 0.

5. Use the **`enstat`** command to ensure that your tunnel configuration is taking advantage of the IPSec offload attribute. The **`enstat`** command shows all the statistics of the transmit and receive IPSec packets when the IPSec offload attribute is enabled. The output is similar to Example 2-1.

Example 2-1 Output of the enstat command

```
# entstat -d entX
10/100 Mbps Ethernet PCI Adapter II (1410ff01) Specific Statistics:
--------------------------------------------
Transmit IPsec packets: 3
Transmit IPsec packets dropped: 0
Receive IPsec packets: 2
Receive IPsec packets dropped: 0
```

2.3.3 Starting IP Security

> **Attention:** Loading IP Security enables the filtering function. Before you load it, you *must* ensure the correct filter rules are created. Otherwise, all outside communication may be blocked.

Use SMIT or the Web-based System Manager to automatically load the IP Security modules when IP Security is started. The Web-based System Manager ensures that the kernel extensions and IKE daemons load in the correct order.

To load the IP Security V4 Modules through SMIT, follow these steps:

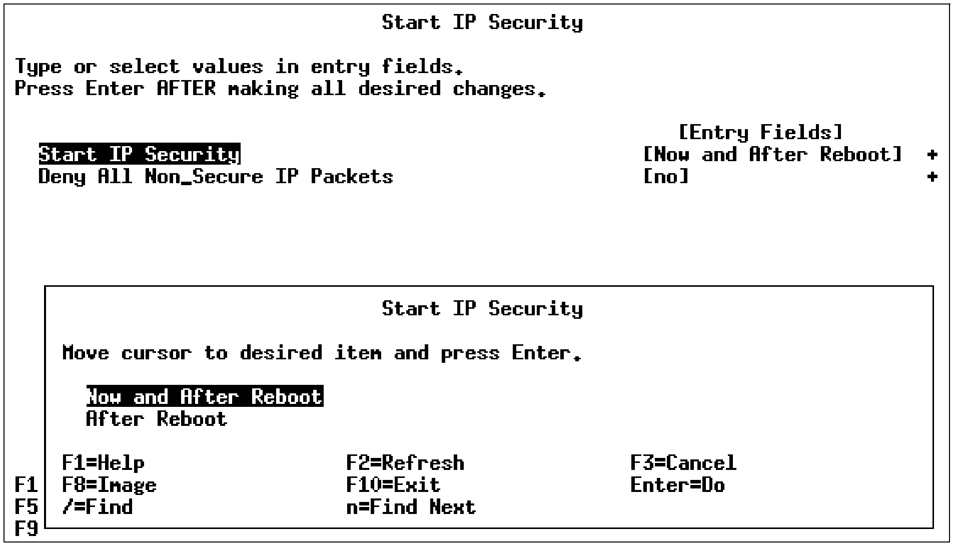
1. From a command line, type:

   ```
   smitty ipsec4
   ```

2. Select **Start/Stop IP Security**.
3. Select **Start IP Security**.
4. On the Start IP Security display (Figure 2-16), choose the moment to apply the change. Then choose what to do with non-secure packets. The recommended value for first-time configurations is **No**.

   If you choose **Yes** to deny non-secure packets and you have not created correct filter rules, you experience problems, for example, when pinging other machines. See 2.8, “Common problems and solutions” on page 94.

   By default, the value for IPSec is *Permit all*.



```
                                Start IP Security

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
  Start IP Security                                 [Now and After Reboot]  +
  Deny All Non_Secure IP Packets                    [no]                    +




                                Start IP Security

    Move cursor to desired item and press Enter.

      Now and After Reboot
      After Reboot

    F1=Help                 F2=Refresh              F3=Cancel
F1  F8=Image                F10=Exit                Enter=Do
F5  /=Find                  n=Find Next
F9
```

Figure 2-16 Starting IP Security V4

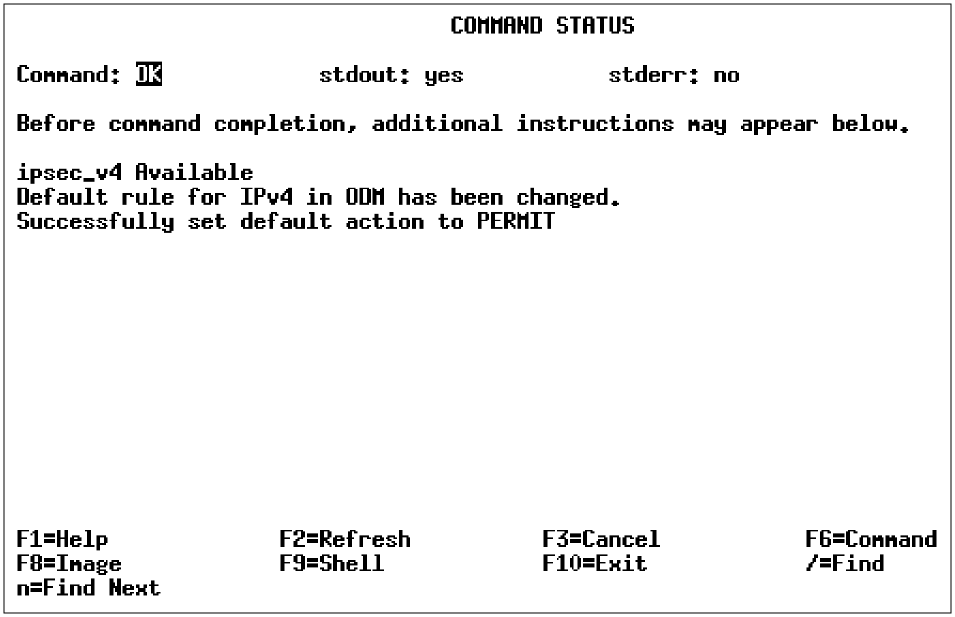
Note: IPSec Version 6 Modules are loaded in the same way, but you use **smitty ipsec6** from the command line. For some reason, the IKE daemons need both IP V4 and V6 loaded in order to start. This is being analyzed by developers and a fix should be available in a future release or patch. See 2.4.1, “Starting IPSec” on page 33.

Example 2-2 shows the output from the **lsdev** command.

Example 2-2 Output of the lsdev command

```
lsdev -C -c ipsec
ipsec_v4 Available IP Version 4 Security Extension
ipsec_v6 Available IP Version 6 Security Extension
```

If the loading completes successfully, you see output like the example in Figure 2-17. The **lsdev** command shows the IP Security devices as *Available*.



```
                                COMMAND STATUS

Command: OK             stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

ipsec_v4 Available
Default rule for IPv4 in ODM has been changed.
Successfully set default action to PERMIT
```

Figure 2-17 IP Security V4 successfully started

5. Activate the IKE daemons by using the **/etc/rc.ike** executable as shown in Example 2-3.

Example 2-3 Starting the IKE daemons with /etc/rc.ike

```
# /etc/rc.ike
0513-059 The cpsd Subsystem has been started. Subsystem PID is 14412.
0513-059 The tmd Subsystem has been started. Subsystem PID is 14416.
0513-059 The isakmpd Subsystem has been started. Subsystem PID is 9634.
```

After you load the IP Security kernel extension, you can use the tunnels and filters.

2.3.4 Installation Verification Procedure

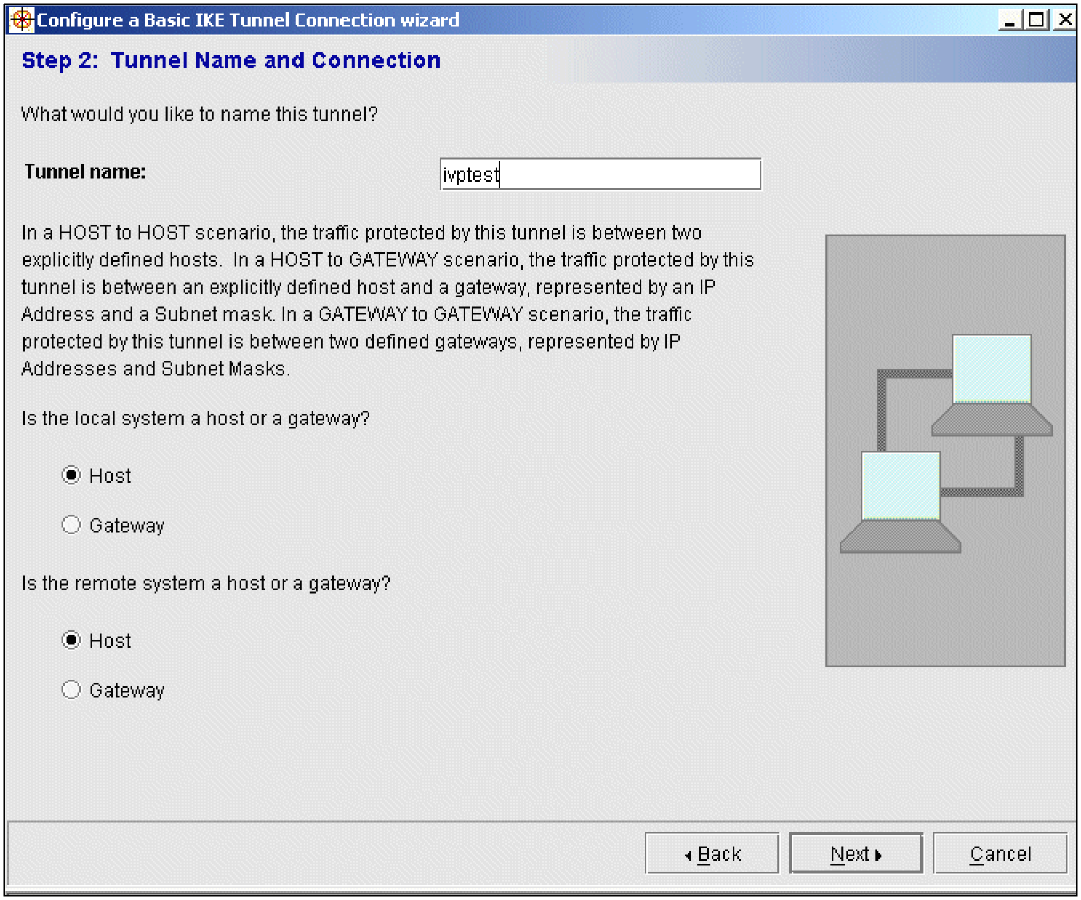
We use the Web-based System Manager (wsm) to create an IKE tunnel and the wizard to verify our environment:

1. From a command line type the following command and press Enter:

   ```
   wsm
   ```

2. Expand ***your machine*-> Network-> Virtual Private Networks**.
3. Select **Internet Key Exchange Tunnels**.
4. From the menu bar, select **Tunnels-> New**.
5. Select **Basic Tunnel Connection**.

6. On the Step 2: Tunnel Name and Connection panel (Figure 2-18), in the Tunnel name field, enter the name of this tunnel and then click **Next**.



Configure a Basic IKE Tunnel Connection wizard

Step 2: Tunnel Name and Connection

What would you like to name this tunnel?

Tunnel name: ivptest

In a HOST to HOST scenario, the traffic protected by this tunnel is between two explicitly defined hosts. In a HOST to GATEWAY scenario, the traffic protected by this tunnel is between an explicitly defined host and a gateway, represented by an IP Address and a Subnet mask. In a GATEWAY to GATEWAY scenario, the traffic protected by this tunnel is between two defined gateways, represented by IP Addresses and Subnet Masks.

Is the local system a host or a gateway?

● Host

○ Gateway

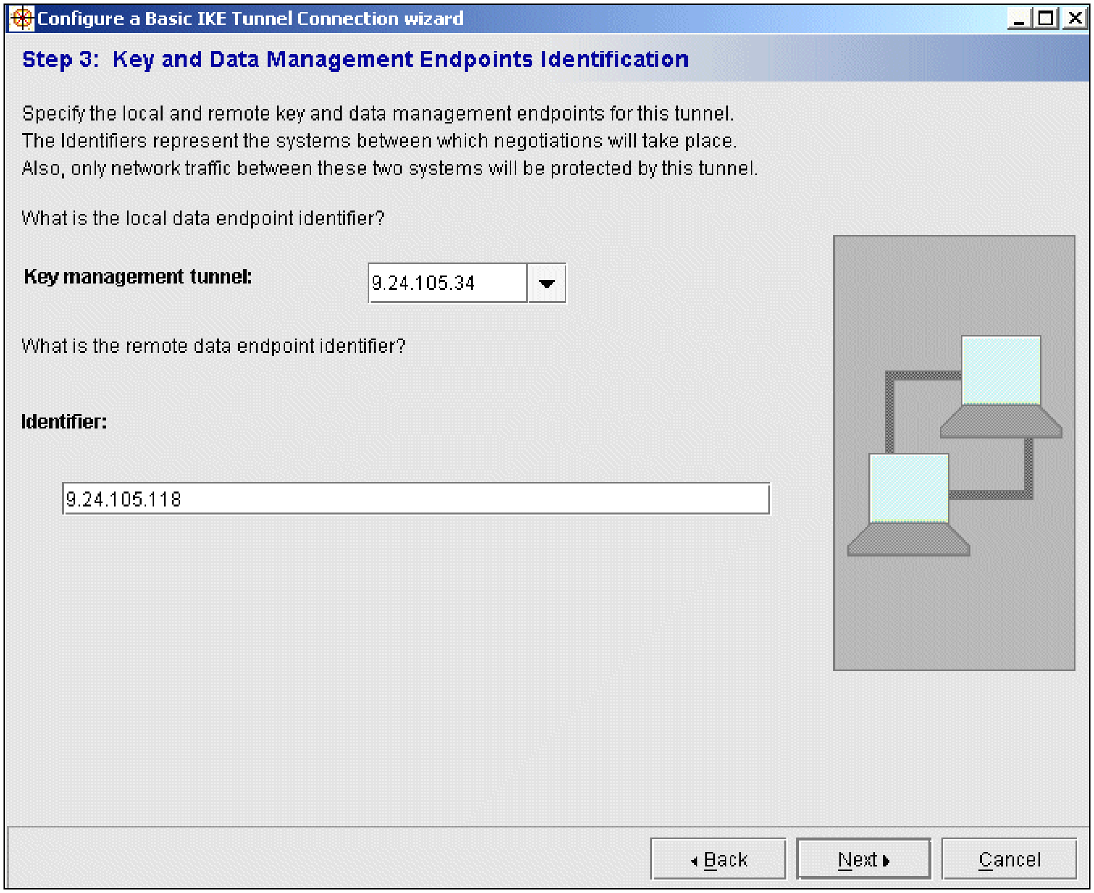
Is the remote system a host or a gateway?

● Host

○ Gateway

Figure 2-18 Specifying the tunnel name

7. On the Step 3: Key and Data Management Endpoints Identification panel (Figure 2-19), from the Key management tunnel list, select the correct key management tunnel IP address. Specify the identifier, which is the IP address of the other machine, and click **Next**.



Configure a Basic IKE Tunnel Connection wizard

Step 3: Key and Data Management Endpoints Identification

Specify the local and remote key and data management endpoints for this tunnel.
The Identifiers represent the systems between which negotiations will take place.
Also, only network traffic between these two systems will be protected by this tunnel.

What is the local data endpoint identifier?

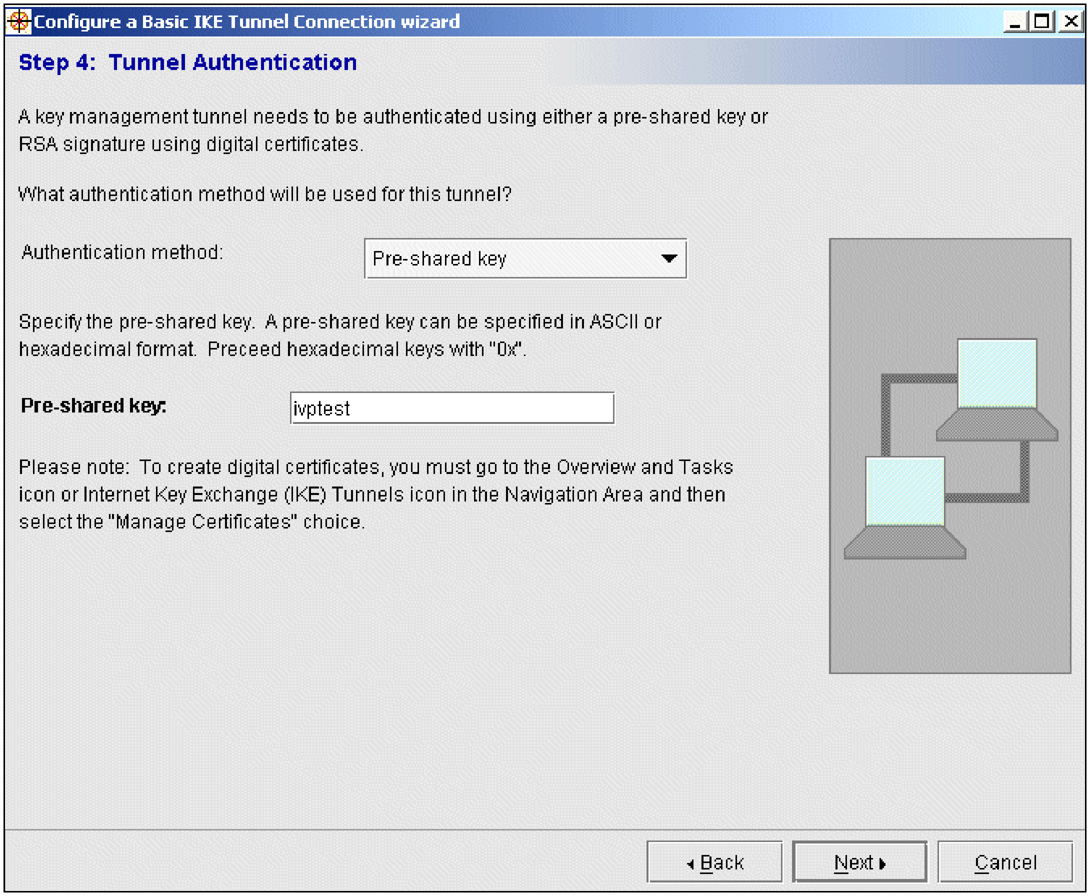
Key management tunnel: 9.24.105.34

What is the remote data endpoint identifier?

Identifier: 9.24.105.118

Figure 2-19 Specifying the key management tunnel and identifier

8. On the Step 4: Tunnel Authentication panel (Figure 2-20), for Authentication method, select **Preshared key**. Then specify the Pre-shared key. This key must be the same on both sides. Click **Next**.



Configure a Basic IKE Tunnel Connection wizard

Step 4: Tunnel Authentication

A key management tunnel needs to be authenticated using either a pre-shared key or RSA signature using digital certificates.

What authentication method will be used for this tunnel?

Authentication method: Pre-shared key

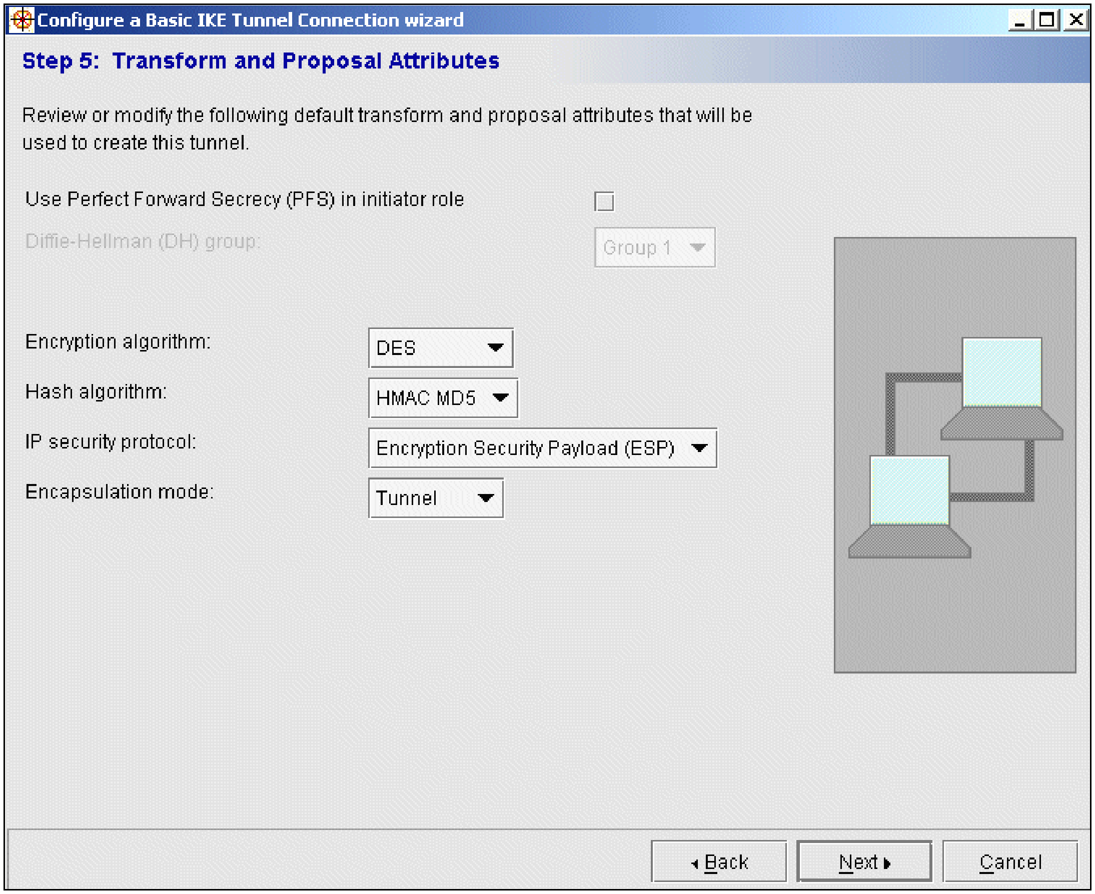
Specify the pre-shared key. A pre-shared key can be specified in ASCII or hexadecimal format. Preceed hexadecimal keys with "0x".

Pre-shared key: ivptest

Please note: To create digital certificates, you must go to the Overview and Tasks icon or Internet Key Exchange (IKE) Tunnels icon in the Navigation Area and then select the "Manage Certificates" choice.

Figure 2-20 Specifying the Pre-shared key value

9. On the Step 5: Transform and Proposal Attributes panel (Figure 2-21), do not change the defaults for encryption algorithm, hash algorithm, security protocol, or encapsulation mode. Click **Next**.



Configure a Basic IKE Tunnel Connection wizard

Step 5: Transform and Proposal Attributes

Review or modify the following default transform and proposal attributes that will be used to create this tunnel.

Use Perfect Forward Secrecy (PFS) in initiator role □

Diffie-Hellman (DH) group: Group 1

Encryption algorithm: DES

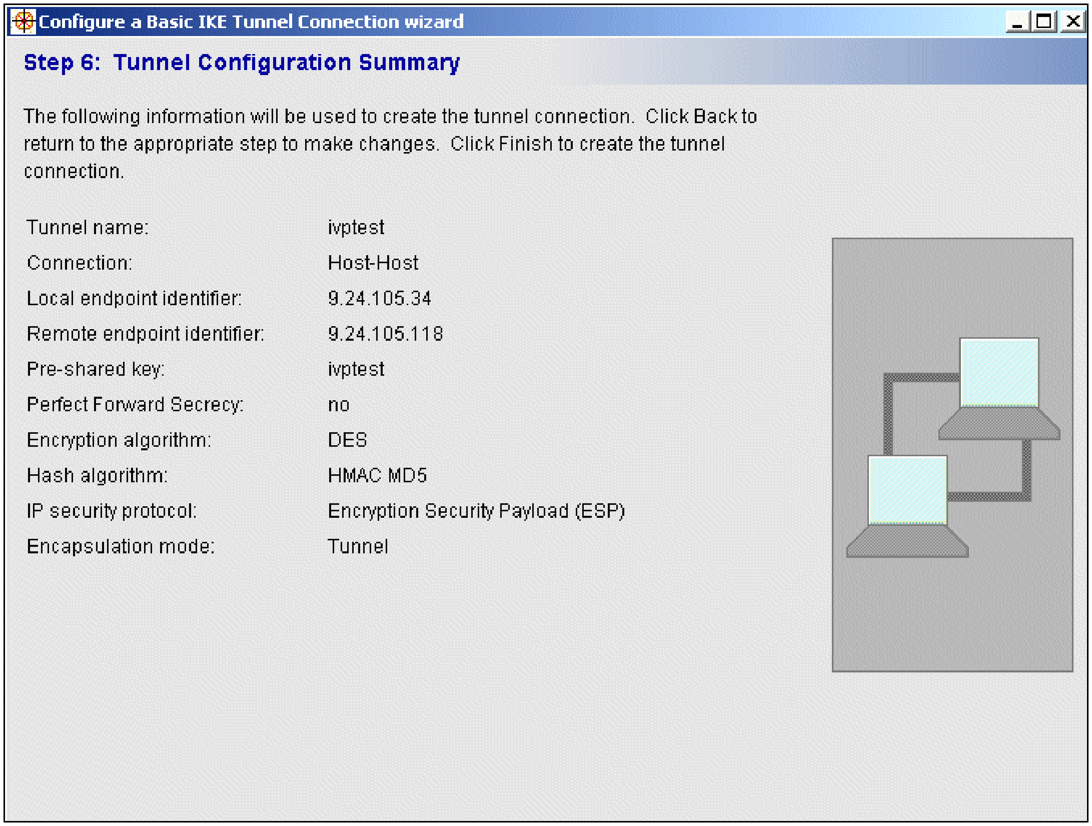
Hash algorithm: HMAC MD5

IP security protocol: Encryption Security Payload (ESP)

Encapsulation mode: Tunnel

Figure 2-21 Transform and proposal attributes

10. On the Step 6: Tunnel Configuration Summary panel (Figure 2-22), review the information and click **Finish**.



Configure a Basic IKE Tunnel Connection wizard

Step 6: Tunnel Configuration Summary

The following information will be used to create the tunnel connection. Click Back to return to the appropriate step to make changes. Click Finish to create the tunnel connection.

Tunnel name:	ivptest
Connection:	Host-Host
Local endpoint identifier:	9.24.105.34
Remote endpoint identifier:	9.24.105.118
Pre-shared key:	ivptest
Perfect Forward Secrecy:	no
Encryption algorithm:	DES
Hash algorithm:	HMAC MD5
IP security protocol:	Encryption Security Payload (ESP)
Encapsulation mode:	Tunnel

Figure 2-22 Summary of the configuration

11. You need another host to make this test. Follow the steps from 2.3.1, “Installing the IP Security feature” on page 19, to 2.3.4, “Installation Verification Procedure” on page 27. The only change to these steps is to switch IP addresses to define the tunnel on the other host. See Figure 2-19 on page 29.

12. After you finish both tunnel definitions, activate them. Right-click each tunnel and select **Activate**. If you activate one and then select the IKE Tunnel Monitor option, you see the tunnel in the status *Negotiating*. It changes to *Active* after handshaking with the other side is done. It is not necessary to activate the other side of the tunnel by hand.

You have finished the Installation Verification Procedure.

2.4 Using administration interfaces

This section explains how to use the various administration interfaces to administer VPNs.

2.4.1 Starting IPSec

You can start IPSec using the methods that are explained in the following sections.

Starting IPSec from SMIT

Follow these steps:

1. To start the IPSec environment, follow the steps in 2.3.3, “Starting IP Security” on page 25.

   > **Note:** To start IPSec V6, use `smitty ipsec6` instead of `smitty ipsec4`.

2. In the start/stop security option, select the values for the following fields:
   - **Start IP Security**: The possible choices are Now, Now and after reboot, or After reboot.
   - **Deny all non_secure IP packets**:
     - Selecting *No* results in the acceptance of network traffic that does not apply to user-defined filter rules or tunnels.
     - Selecting *Yes* results in the rejection of any IP network traffic that does not go through an active security tunnel or does not match any user defined filter rules.
3. Start the IKE daemons using the **`/etc/rc.ike`** command:

```
# /etc/rc.ike
0513-059 The cpsd Subsystem has been started. Subsystem PID is 14412.
0513-059 The tmd Subsystem has been started. Subsystem PID is 14416.
0513-059 The isakmpd Subsystem has been started. Subsystem PID is 9634.
```

> **Important:** If you are configuring this host remotely, remember to add filter rules for this host *before* IP Security is enabled. The filter rules specified also indicate how traffic is handled when filtering is deactivated.

Starting IPSec from a command line

The following sections explain how to start IPSec from the command line and to permit or deny non-secure packets.

Activating IPSec and permitting non-secure packets

Follow these steps:

1. Enter the following command to make the ipsec device available:

```
# mkdev -c ipsec -t 4
ipsec_v4 Available
```

2. Activate filtering now (-u option) and permit non-secure packets (-z option):

```
# mkfilt -v 4 -u -z p
Default rule for IPv4 in ODM has been change
Successfully set default action to PERMIT
```

Activating IPSec and denying non-secure packets

To activate IPSec now and deny non-secure packets, follow these steps:

1. Enter the following commands:

```
# mkdev -c ipsec -t 4
ipsec_v4 Available

# mkfilt -v 4 -u -z d
Default rule for IPv4 in ODM has been changed.
Successfully set default action to DENY
```

   If you want to activate IPSec after a reboot only, you must omit the -u option.

   Note: To activate IPSec for IPSec v6, set the version option (-v option) to 6.

2. Start the IKE daemons using the **/etc/rc.ike** command:

```
# /etc/rc.ike
0513-059 The cpsd Subsystem has been started. Subsystem PID is 14412.
0513-059 The tmd Subsystem has been started. Subsystem PID is 14416.
0513-059 The isakmpd Subsystem has been started. Subsystem PID is 9634.
```

Attention: If you don’t use the -u option but instead use the -z d option, the denying of non-secure packets is in effect immediately.

Starting IPSec from the Web-based System Manager interface

From the Web-based System Manager interface, follow these steps:

1. Select the machine.
2. Expand **Network-> Virtual Private Networks**.
3. Select **Overview and Tasks**.
4. Select **Start IP Security**.

A window opens. See “Starting IPSec from SMIT” on page 33 for an explanation of the options in this window.

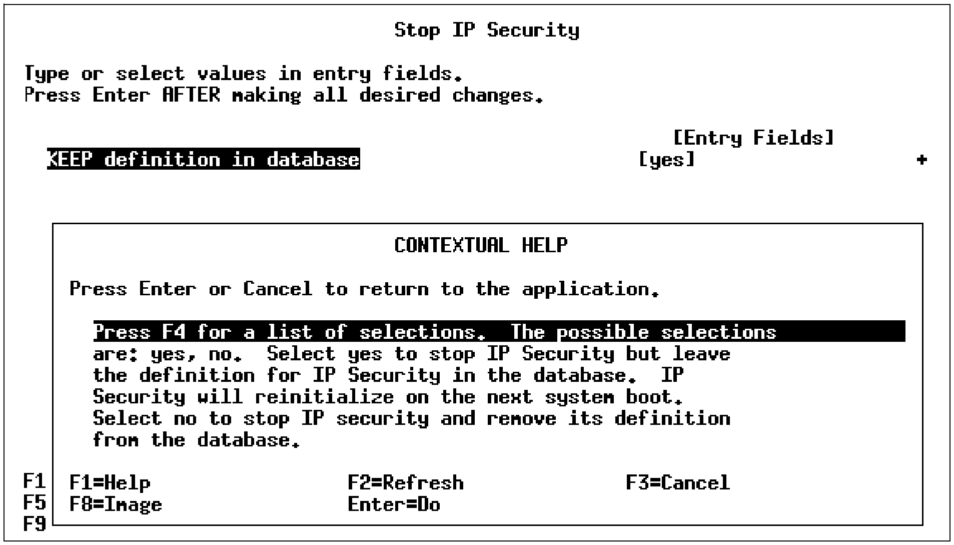
Note: You can use the Web-based System Manager to start IPSec V4 and V6.

2.4.2 Stopping IPSec

You can use the following methods to stop IPSec.

Stopping IPSec with SMIT

Stop IPSec from SMIT. On the Stop IP Security display (Figure 2-23), set the KEEP definition in database parameter to `yes`. Then press Enter to stop IPSec.



```
                              Stop IP Security

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                       [Entry Fields]
  KEEP definition in database                        [yes]              +


   ┌──────────────────────────────────────────────────────────────────────┐
   │                          CONTEXTUAL HELP                             │
   │                                                                      │
   │ Press Enter or Cancel to return to the application.                  │
   │                                                                      │
   │   Press F4 for a list of selections.  The possible selections        │
   │   are: yes, no.  Select yes to stop IP Security but leave            │
   │   the definition for IP Security in the database.  IP                │
   │   Security will reinitialize on the next system boot.                │
   │   Select no to stop IP security and remove its definition            │
   │   from the database.                                                 │
   │                                                                      │
F1 │ F1=Help                  F2=Refresh               F3=Cancel          │
F5 │ F8=Image                 Enter=Do                                    │
F9 └──────────────────────────────────────────────────────────────────────┘
```

Figure 2-23 Stopping IPSec from the System Management Interface Tool

Stopping IPSec from a command line

To stop IPSec from a command line, enter either of the following commands:

```
# /usr/sbin/rmdev -l ipsec_v4
ipsec_v4 Defined

# /usr/sbin/rmdev -l ipsec_v4 -d
ipsec_v4 deleted
```

To avoid starting IPSec, at the next reboot, add the `-d` option to delete the ipsec_v4 definition from the database.

Note: For IPSec V6, replace ipsec_v4 with `ipsec_v6`.

Stopping IPSec from the Web-based System Manager

From the Web-based System Manager, complete the following steps:

1. Expand ***your machine*-> Network-> Virtual Private Networks**.
2. Select **Overview and Tasks**.
3. Select **Stop IP Security**.

A window opens. See 2.4.2, "Stopping IPSec" on page 35, which explains the options in this window.

> **Note**: You can use the Web-based System Manager to stop IPSec V4 and V6.

2.4.3 IKE tunnels using SMIT

You can access the IKE tunnels configuration display by following these steps:

1. Type the following command:

   ```
   smitty ipsec4
   ```

2. Select **Basic IP Security Configuration**.
3. Select **Use Internet Key Exchange Refresh Method**.

You can select from the following options:

- **List IKE Entries**: Displays what is stored in the IKE database in Extensible Markup Language (XML) format.
- **Add an IKE Tunnel**: Allows users to edit an IKE template file for the specific tunnel setup.
- **Change/Remove IKE Entries**: Allows users to alter or remove tunnel definitions.
- **Import Linux IKE Entries**: Converts Linux tunnels definitions to IKE database.
- **Activate IKE Tunnels**: Activates the specified IKE tunnels.
- **Deactivate IKE Tunnels**: Deactivates the specified IKE tunnels.
- **Export IKE Tunnels**: Extracts the IKE tunnel definitions into an XML file.
- **Import AIX IKE Tunnels**: Imports IKE tunnel definitions from a peer. This function switches the identifiers, except in the case where the remote ID is a group definition.

> **Note:** To work with IKE tunnels (add, modify, delete), we recommend that you use Web-based System Manager to avoid editing the XML files.

2.4.4 IKE tunnels using Web-based System Manager

You can use the Web-based System Manager to configure both phase 1 and phase 2 tunnels.

Phase 1 tunnels

To reach the IKE tunnels definition window from the Web-based System Manager, use these steps:

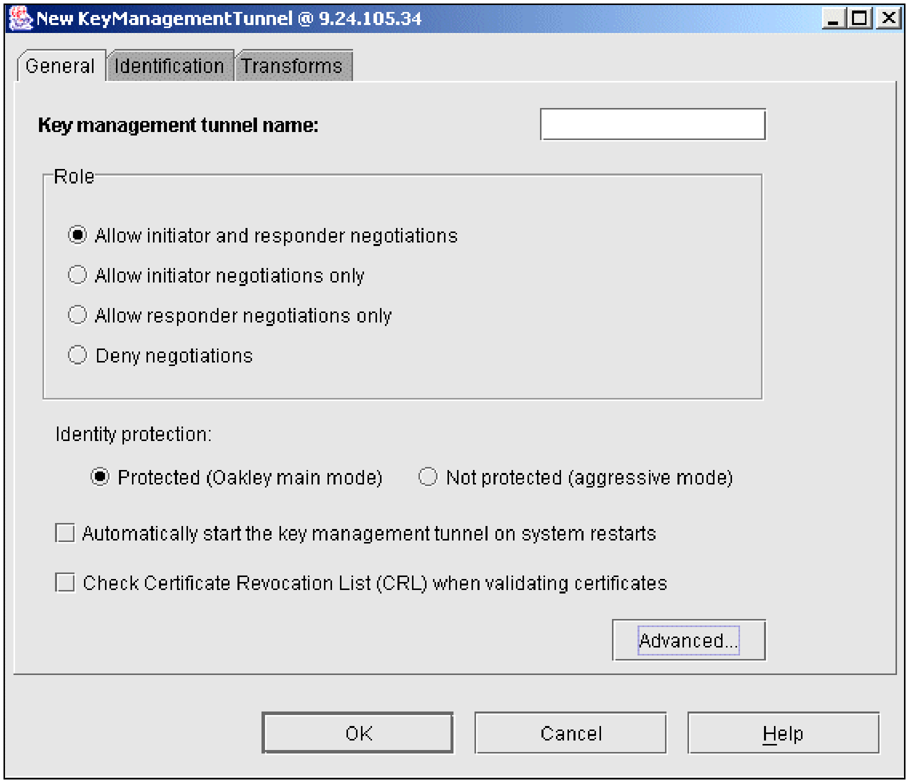
1. Expand ***your machine*****-> Network-> Virtual Private Networks**.
2. Select **Internet Key Exchange Tunnels**.
3. From the menu bar, select **Tunnels-> New-> Key Management Tunnel**.
4. Figure 2-24 shows the New Key Management Tunnel window where you can configure a phase1 tunnel. On the General page, select the following options:
   a. Use the following options to define the role that this machine will have in the IKE Tunnel negotiation:
      - **Allow Initiator and responder negotiations**: This machine can act as the one who initiates the handshaking (Initiator) or the one that is asked for a handshaking (responder).
      - **Allow initiator negotiations only**: This machine can only be the initiator of the handshaking.
      - **Allow responder negotiations only**: This machine can only be the responder of the handshaking.
      - **Deny negotiations**: Negotiations are not allowed.

   b. You can configure protection mode using the following options:
      - Protected (main mode)
      - Not protected (aggressive mode)

      See “IKE tunnel support” on page 12 for more information.

   c. You can define the starting behavior of the IKE Tunnel to automatically start the key management tunnel on system restarts.

d. You can define the use of a Certificate Revocation List (CRL) to check Certificate Revocation List when validating certificates. With this option, a Certificate Revocation List is inspected to see if a certificate was revoked by a CA administrator previous to its expiration date. If you choose this option when you are using digital certificates, then you must configure the window on where to retrieve the CRLs.



Key management tunnel name:

Role

● Allow initiator and responder negotiations
○ Allow initiator negotiations only
○ Allow responder negotiations only
○ Deny negotiations

Identity protection:

● Protected (Oakley main mode) ○ Not protected (aggressive mode)

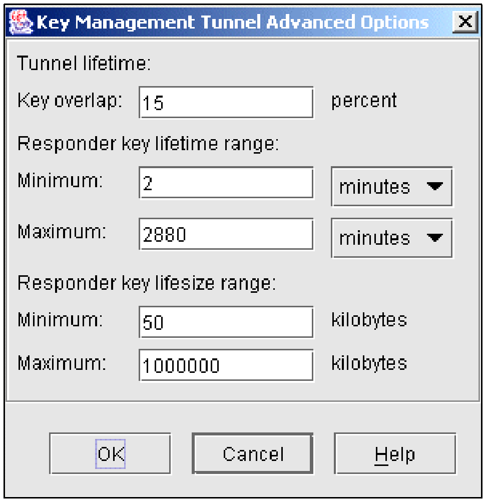
□ Automatically start the key management tunnel on system restarts

□ Check Certificate Revocation List (CRL) when validating certificates

Figure 2-24 IKE Tunnel General page

5. Now that you have decided how to negotiate, and protect your phase 1 tunnel, click the **Advanced** button.
6. Figure 2-25 shows the Key Management Tunnel Advanced Options window. Set the following options:
   a. Tunnel lifetime key overlap: Specify the key refresh overlap that is allowed.
   b. Responder key lifetime minimum and maximum: Specify the range in minutes, hours, or days. Figure 2-25 shows the recommended initial values.
   c. Responder key lifesize range minimum and maximum: Specify the range in KB. Figure 2-25 shows the recommended initial values.

   > **Note:** These keys take some time to change so two days is an acceptable value.



Key Management Tunnel Advanced Options

Tunnel lifetime:

Key overlap: 15 percent

Responder key lifetime range:

Minimum: 2 minutes

Maximum: 2880 minutes

Responder key lifesize range:

Minimum: 50 kilobytes

Maximum: 1000000 kilobytes

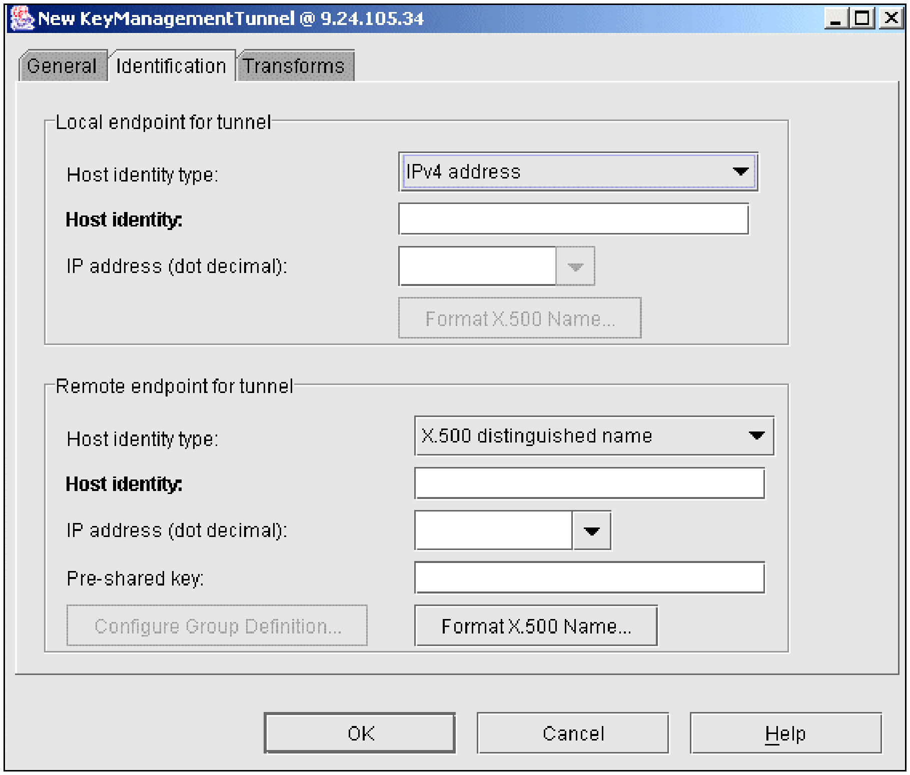
Figure 2-25 IKE tunnel advanced options

   d. Click **OK** to return to the New Key Management Tunnel window (Figure 2-24).
7. Click the **Identification** tab (see Figure 2-24). Identify the local and remote parties, as shown in Figure 2-26.
   – **Host identity type**: You can specify the following options:
      - *IPV4 address*: Specify the IP address in V4 format.
      - *IPV6 address*: Specify the IP address in V6 format.

- *Fully qualified domain name*: For example, `itso.ral.ibm.com`
- *user@fully qualified domain name*: For example, `ashley@itso.ral.ibm.com`
- *X.500 distinguished name*: For example, `/C=US/O=ITSO/CN=MALKA/L=DURHAM/ST=NORTH CAROLINA/ZIP=27713`. See Figure 2-27 on page 41. This is the format that is used with certificates (RSA security option). For VPNs, use as the common name (CN) the full domain name for the hosts.
- *Key identifier*: If a host has more than one key, then in the Host Identity field, enter the key ID for this connection.
- *Group ID definition*: Select to configure group ID definitions. See Figure 2-28 on page 42.

– **IP address**: Specify the host IP address in dot decimal.

– **Pre-shared key**: Specify the common key between both sides.


New KeyManagementTunnel @ 9.24.105.34
General
Identification
Transforms
Local endpoint for tunnel
Host identity:
IP address (dot decimal):
Format X.500 Name...
Remote endpoint for tunnel
Host identity:
IP address (dot decimal):
Pre-shared key:
Configure Group Definition...
Format X.500 Name...
OK
Cancel
Help

Local endpoint for tunnel

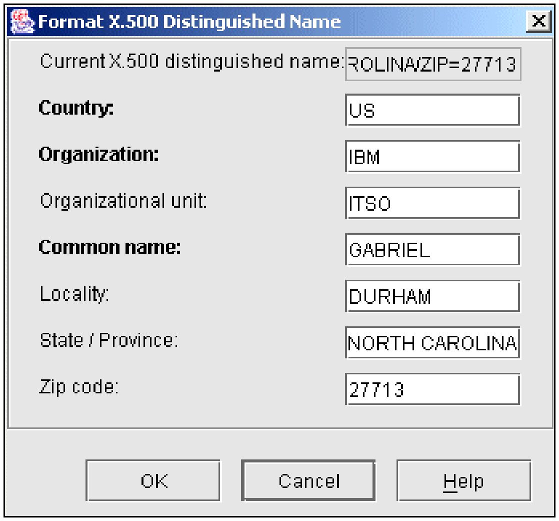
Host identity type: IPv4 address

Remote endpoint for tunnel

Host identity type: X.500 distinguished name

Figure 2-26 IKE tunnel identification options

– **Format X.500 Name**: You click this option to access the Format X.500 Distinguished Name window (Figure 2-27). You use this option when you are using certificates. You click OK to return to the New Key Management Tunnel window (Figure 2-26).



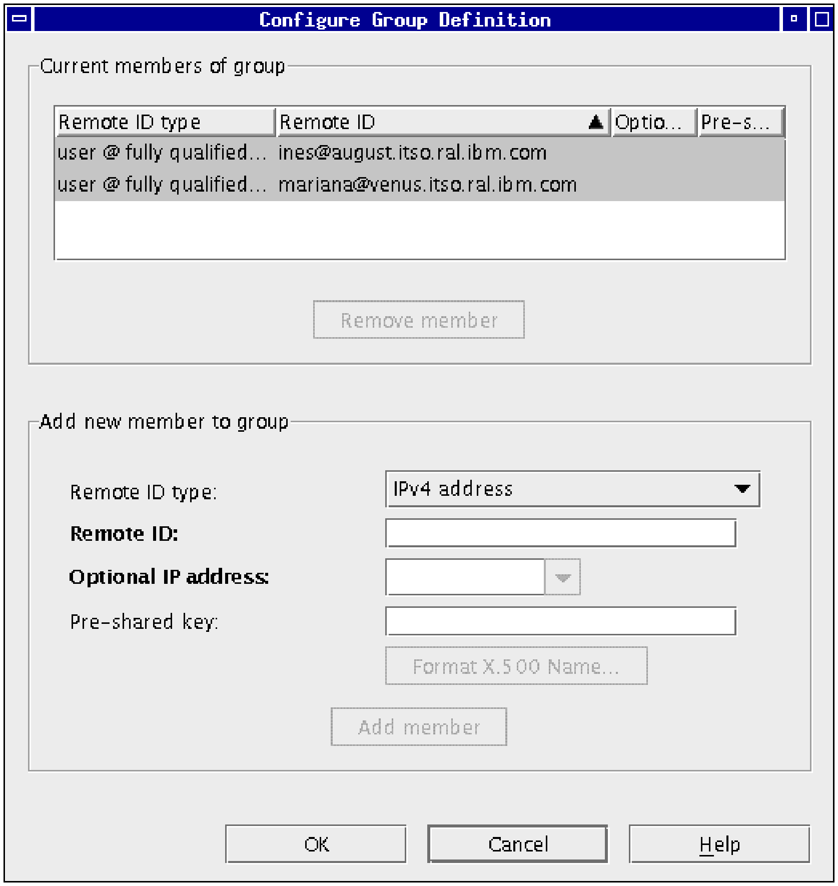
Format X.500 Distinguished Name

Current X.500 distinguished name:	ROLINA/ZIP=27713
Country:	US
Organization:	IBM
Organizational unit:	ITSO
Common name:	GABRIEL
Locality:	DURHAM
State / Province:	NORTH CAROLINA
Zip code:	27713

Figure 2-27 IKE X.500 format

- **Configure Group Definition**: You can click this button on the window shown in Figure 2-26 to configure many tunnels from your machine to others machines. You can manage configurations with common characteristics. Figure 2-28 shows an example of the Configure Group Definition window. You click OK to return to the New Key Management Tunnel window (Figure 2-26 on page 40).

> **Note:** There is limit on the number of members that can be in one group. It depends on the types of members in the group and how much space the characters require. For example, `mariana@venus.itso.ral.ibm.com` may require more bytes than an IP address.



Remote ID type	Remote ID ▲	Optio...	Pre-s...
user @ fully qualified...	ines@august.itso.ral.ibm.com		
user @ fully qualified...	mariana@venus.itso.ral.ibm.com		

Remote ID type: IPv4 address

Figure 2-28 IKE group definitions

8. On the Key Management Tunnel Properties window, configure the IKE transforms. Click the **Transforms** tab (Figure 2-29). On the Transforms page, set the following options:

   – **Authentication Method**: Can be RSA signatures or preshared keys. To use RSA signatures, you must use the X.500 format to identify the certificate. RSA is a trustable algorithm. For more information about breaking RSA keys, see *Number Field Sieve algorithm* on the Web at:

     http://www.nfsnet.org

   – **Encryption Algorithm**: Can be DES or T-DES.

     > **Attention:** DES is not considered secure by the cryptographic community. In fact, 56-bit keys are vulnerable to exhaustive search algorithms. If you must use DES, we recommend that you change DES keys frequently (lifetime less than 30 minutes).

   – **Hash algorithm**: Can be HMAC-MD5 or HMAC-SHA. Both are trustable algorithms. HMAC-MD5 has better performance. For more information, see the following Web site:

     http://www.research.ibm.com/security/draft-ietf-ipsec-hmac-md5-00.txt

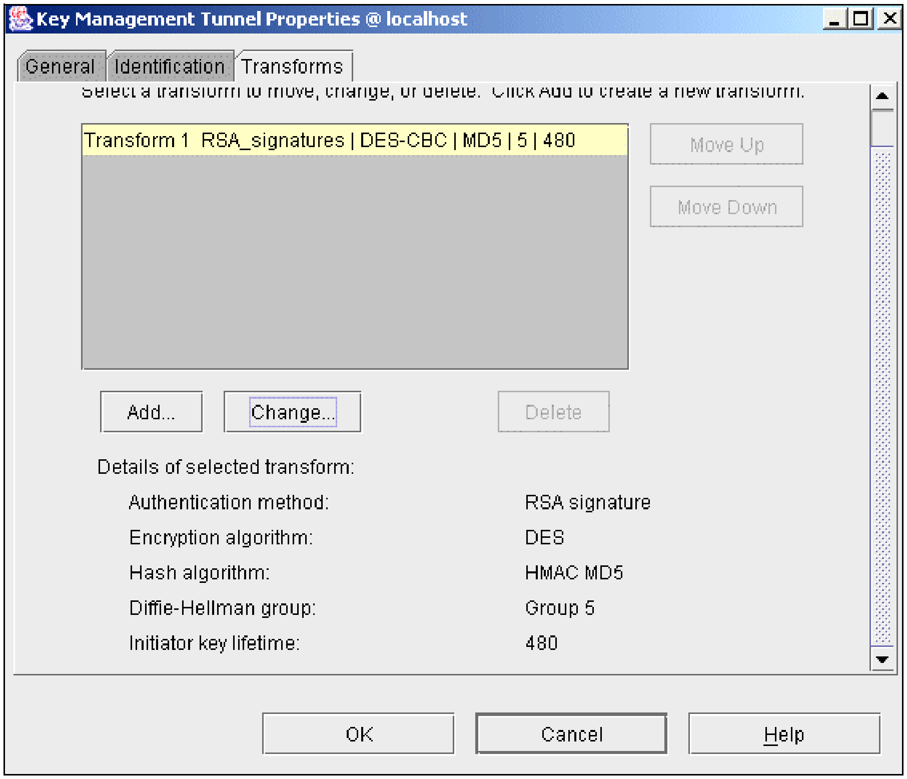
   – **Diffie-Hellman group**: Can be 1, 2, or 5 (group 5 is new for AIX 5.2).

     > **Attention:** DH is vulnerable to a man-in-the-middle attack. If you need to implement DH, we recommend that you use RSA to authenticate the participants.

     For more information about theDH algorithm and vulnerability, see:

     http://www.rsasecurity.com/rsalabs/faq/3-6-1.html

   – **Initiator key lifetime**: Can be in hours, minutes, or days. The recommended initial value is 480 minutes.



Select a transform to move, change, or delete. Click Add to create a new transform.

Transform 1 RSA_signatures | DES-CBC | MD5 | 5 | 480

Details of selected transform:

Authentication method:	RSA signature
Encryption algorithm:	DES
Hash algorithm:	HMAC MD5
Diffie-Hellman group:	Group 5
Initiator key lifetime:	480

Figure 2-29 IKE Transforms page

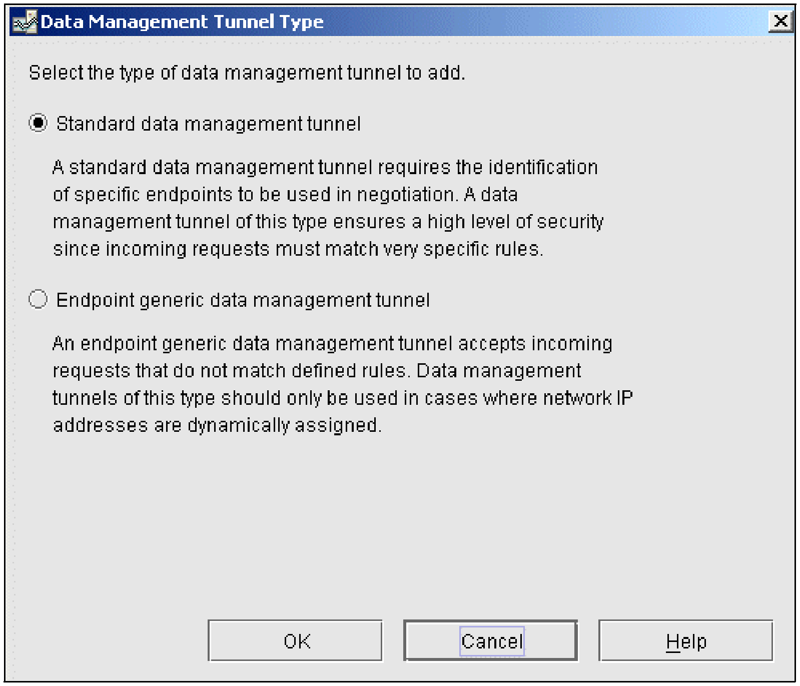
9. After you configure each page, click **OK** to save the definitions for the phase 1 tunnel.

Phase 2 tunnels

You can access the IKE Tunnels phase 2 definition display from the Web-based System Manager using the following steps:

1. Expand ***your machine*-> Network-> Virtual Private Networks**.
2. Select **Internet Key Exchange Tunnels**.
3. From the menu bar, select **Tunnels-> New-> Key Management Tunnel**.
4. Select the phase 1 tunnel for adding a phase 2 tunnel (or data management tunnel). Right-click the tunnel and select **Add a Management Tunnel**.

5. Select the data management tunnel type, as shown in Figure 2-30. We select the **Standard data management tunnel** option. Click **OK**.



Select the type of data management tunnel to add.

● Standard data management tunnel

A standard data management tunnel requires the identification of specific endpoints to be used in negotiation. A data management tunnel of this type ensures a high level of security since incoming requests must match very specific rules.

○ Endpoint generic data management tunnel

An endpoint generic data management tunnel accepts incoming requests that do not match defined rules. Data management tunnels of this type should only be used in cases where network IP addresses are dynamically assigned.

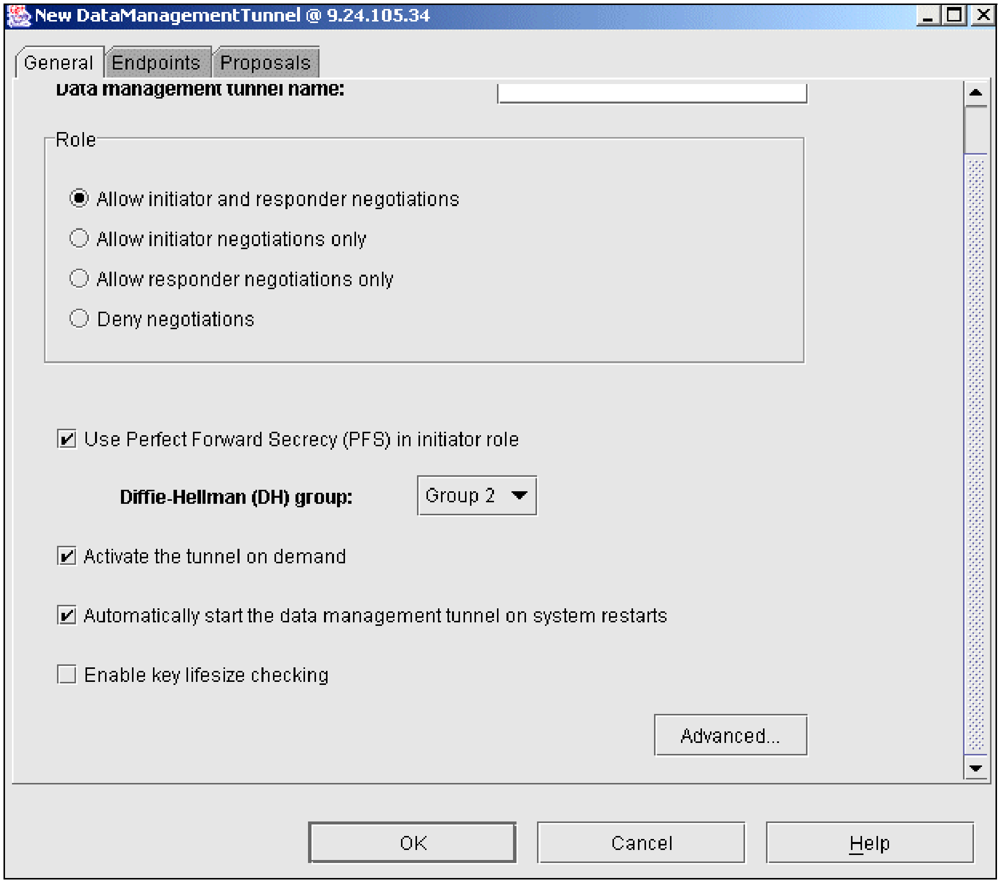
Figure 2-30 Selecting the data management tunnel type

6. The New Data Management Tunnel window (Figure 2-31) opens. We only focus on the new fields. For the rest of the fields, see “Phase 1 tunnels” on page 37. The following fields are for the endpoint management tunnel option:

   – **Use PFS in initiator role**: Each refreshed key is derived without any dependence on predecessor keys.

   – **DH group**: You can choose between groups 1, 2 or 5. They are 768, 1024, and 1536 bits respectively.

   Click the **Advanced** button.



New DataManagementTunnel @ 9.24.105.34

Data management tunnel name:

Role

● Allow initiator and responder negotiations
○ Allow initiator negotiations only
○ Allow responder negotiations only
○ Deny negotiations

☑ Use Perfect Forward Secrecy (PFS) in initiator role

Diffie-Hellman (DH) group: Group 2

☑ Activate the tunnel on demand

☑ Automatically start the data management tunnel on system restarts

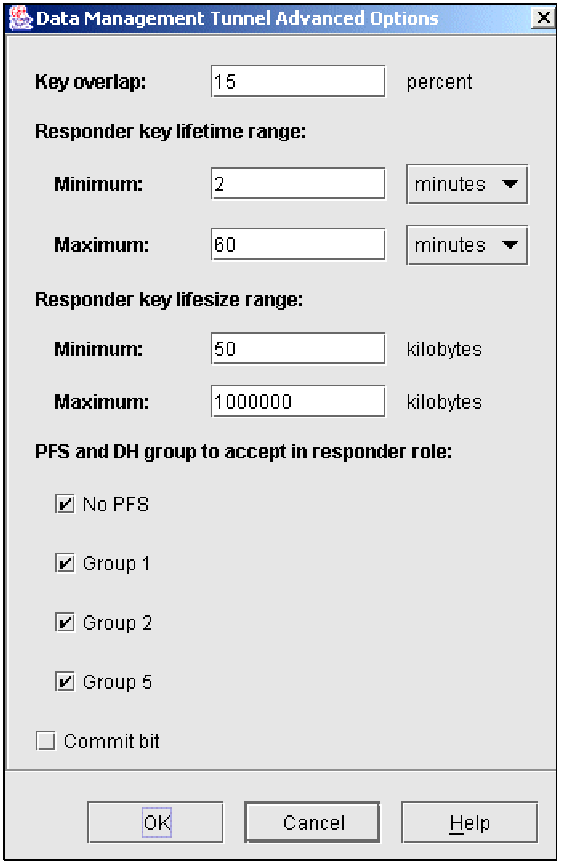
☐ Enable key lifesize checking

Figure 2-31 IKE data management General definition page

7. In the Data Management Tunnel Advanced Options window (Figure 2-32) that opens, set the key attributes and how secure they will be. You can choose which options to apply to a key in a responder role. You can set these to *no* to have PFS, or if you have PFS, specify which DH group will be used.

   The purpose of the *Commit bit* option is to synchronize key exchange. The key related information is received only after the SA establishment. See RFC 2408 on the Web at:

   `http://www.ietf.org/rfc/rfc2408.txt`



Key overlap: 15 percent

Responder key lifetime range:

Minimum: 2 minutes

Maximum: 60 minutes

Responder key lifesize range:

Minimum: 50 kilobytes

Maximum: 1000000 kilobytes

PFS and DH group to accept in responder role:

☑ No PFS

☑ Group 1

☑ Group 2

☑ Group 5

☐ Commit bit

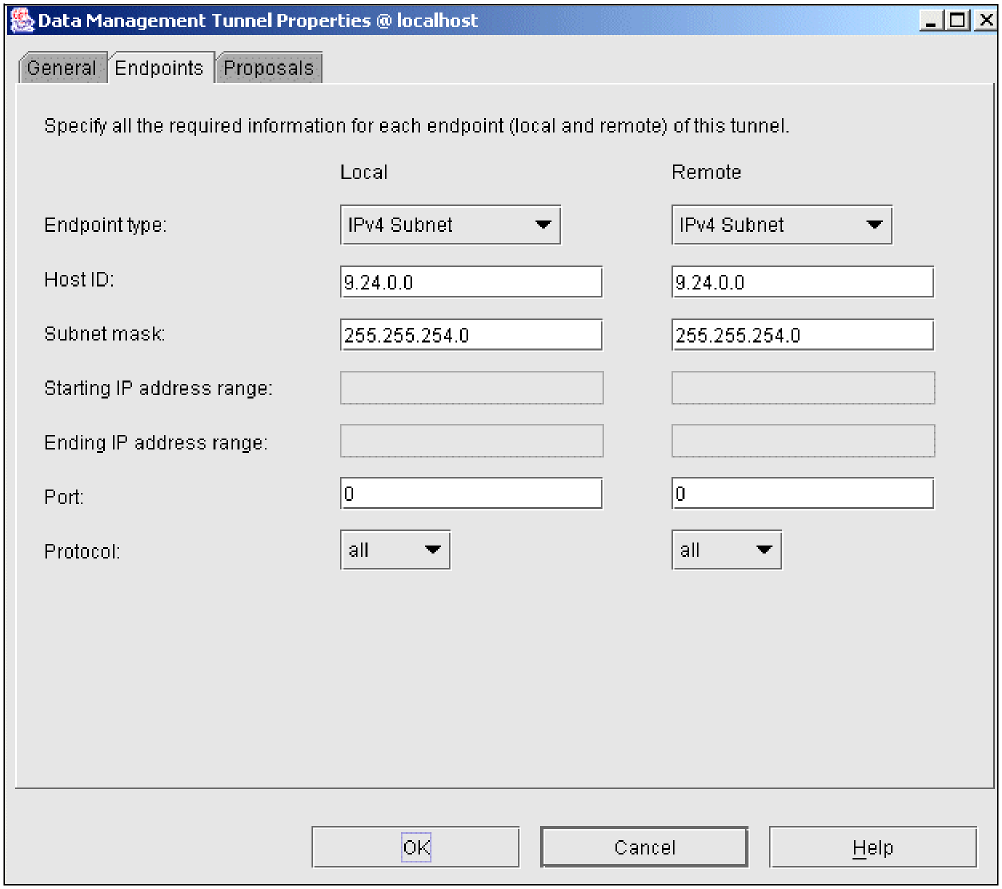
Figure 2-32 Data management tunnel advanced options

   Click **OK** to return to the New Data Management Tunnel window (Figure 2-31).

8. Click the **Endpoints** tab. This takes you to the Endpoints page (Figure 2-33) of the Data Management Tunnel Properties window. On this page, you

configure the host, subnet, or range that indicates whether the data traffic traveling in the tunnel is for a particular host, subnet, or address range.

- **Host ID or Subnet ID plus Subnet Mask**: Contains the host or subnet identity of the local and remote systems passing traffic over this tunnel. Determines the IDs sent in the phase 2 negotiation and the filter rules that will be built, if the negotiation is successful.
- **Starting/Ending IP Address Range**: Range of addresses that uses the tunnel.
- **Port**: Describes a specific port number used by data.
- **Protocol**: Describes data being transported with a specific protocol. Determines the protocol sent in the phase 2 negotiation and the filter rules that will be built if the negotiation is successful. The protocol for the local endpoint must match the protocol for the remote endpoint.

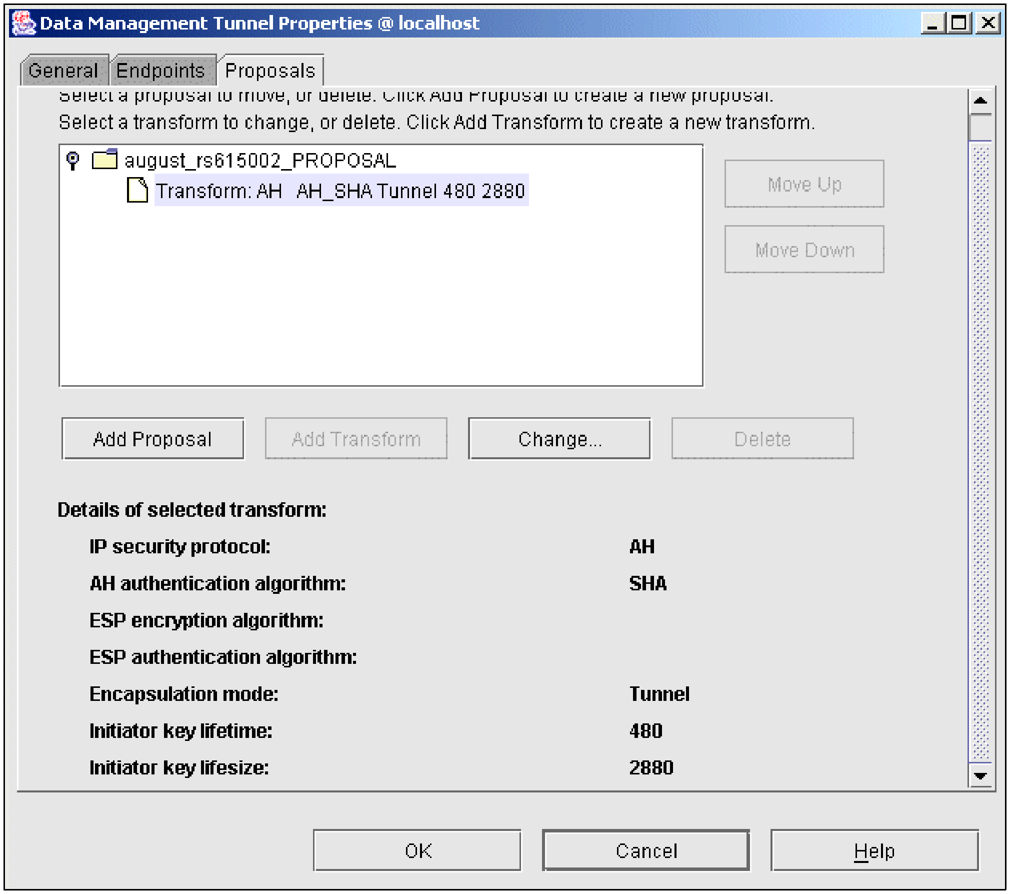


Specify all the required information for each endpoint (local and remote) of this tunnel.

	Local	Remote
Endpoint type:	IPv4 Subnet	IPv4 Subnet
Host ID:	9.24.0.0	9.24.0.0
Subnet mask:	255.255.254.0	255.255.254.0
Starting IP address range:		
Ending IP address range:		
Port:	0	0
Protocol:	all	all

Figure 2-33 Endpoint panel definitions

9. Click the **Proposals** tab. This takes you to the Proposals page (Figure 2-34) of the Data Management tunnel properties window. See the recommended initial values for initiator key lifetime and initiator key lifesize.



Select a proposal to move, or delete. Click Add Proposal to create a new proposal.
Select a transform to change, or delete. Click Add Transform to create a new transform.

august_rs615002_PROPOSAL
Transform: AH AH_SHA Tunnel 480 2880

Details of selected transform:

IP security protocol:	AH
AH authentication algorithm:	SHA
ESP encryption algorithm:	
ESP authentication algorithm:	
Encapsulation mode:	Tunnel
Initiator key lifetime:	480
Initiator key lifesize:	2880

Figure 2-34 DM tunnel proposals

10. Click **OK** to save the configurations for each page.

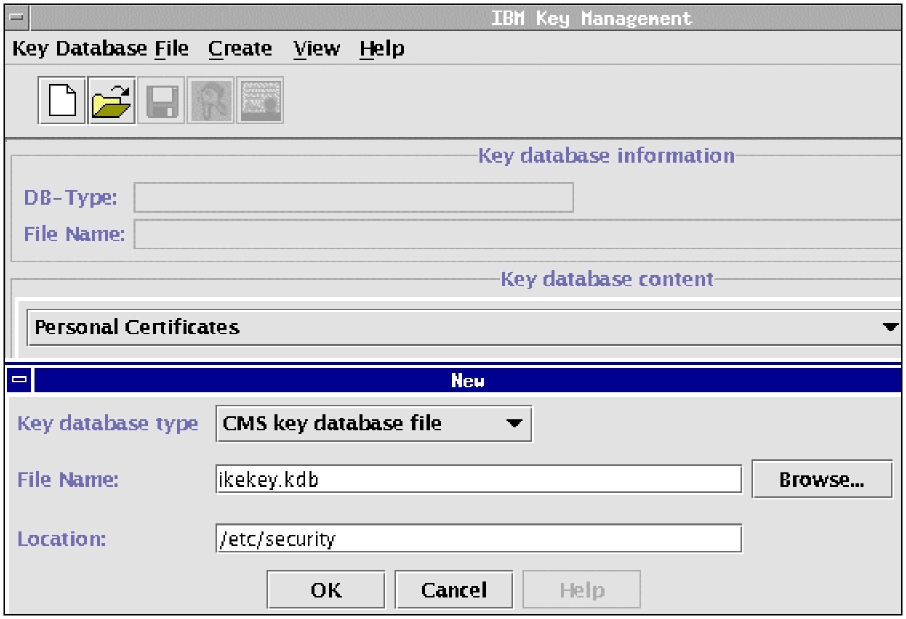
2.4.5 Using certificates

To generate key pairs and to request and receive client and CA certificates, use the **`certmgr`** application. You can launch this application from the command line.

First, create a new database for storing keys:

1. Select **Key Database File-> New**.
2. On the IBM Key Management window as shown in Figure 2-35, select **CMS key database file** as the database type. Name the database `ikekey.kdb` and place it in the **/etc/security** directory. Click **OK**.

> **Attention:** You must enter the name and location of the new key database exactly as shown in Figure 2-35. Otherwise, it cannot be used with IKE. The reason is that these names are hardcoded into the **`cpsd`** daemon that parses and loads the certificates.



Personal Certificates

Key database type: CMS key database file

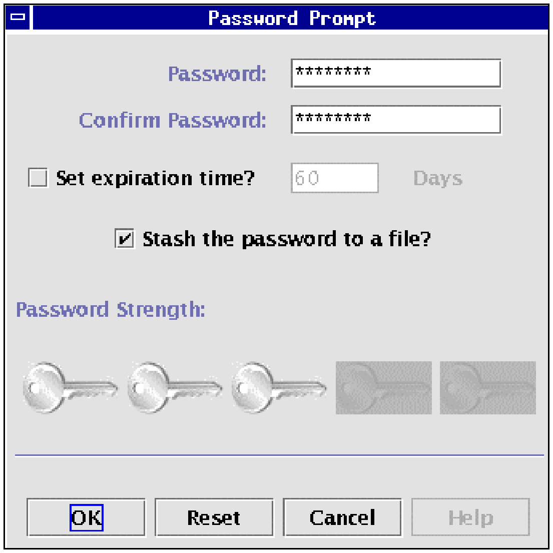
File Name: ikekey.kdb

Location: /etc/security

Figure 2-35 New IKE certificate database

3. On the Password Prompt window (Figure 2-36), specify a password from the key database file. Select **Stash the password file?** and click **OK**.

> **Note:** The keys in Figure 2-36 indicate the strength of the password that you selected.



Password Prompt

Password: *********

Confirm Password: *********

□ Set expiration time? 60 Days

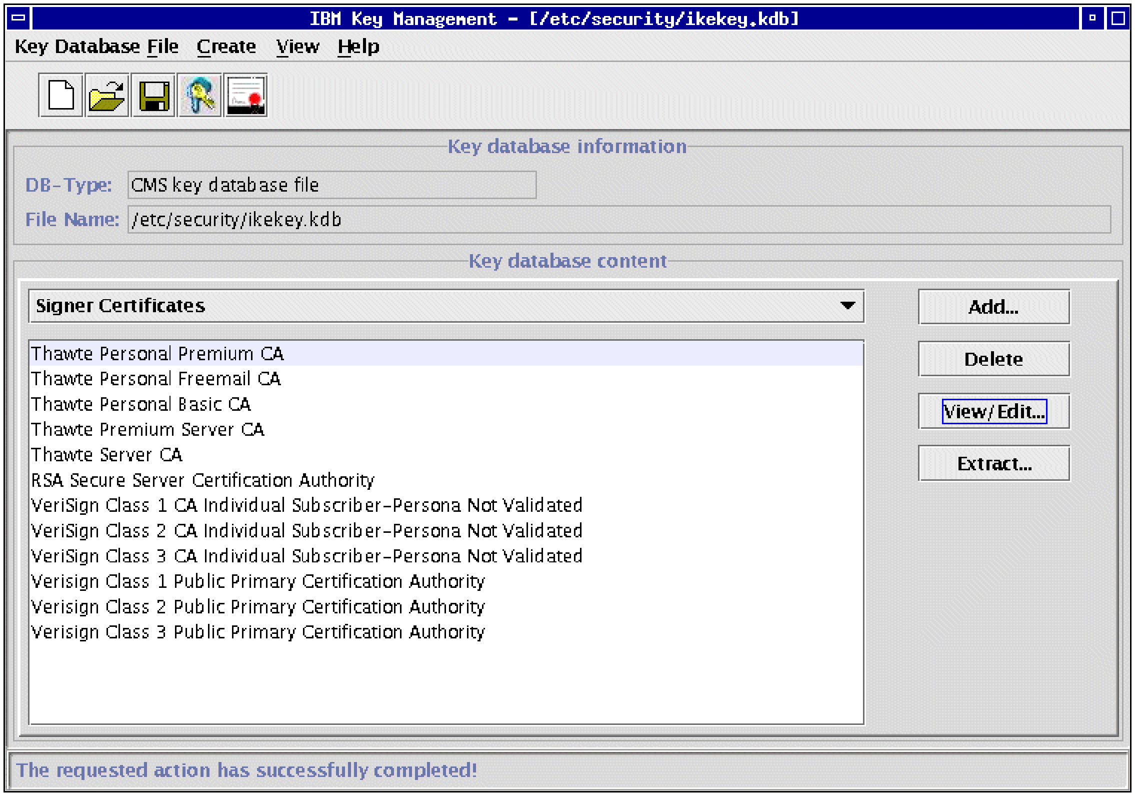
☑ Stash the password to a file?

Password Strength:

Figure 2-36 IKE key database password

4. After the new key database is created, you see a list of pre-loaded CA certificates in the pane. See Figure 2-37. From the menu bar, select **Create-> New certificate request**.

Important: If the signer certificate is not loaded by default, you must add it to the kdb database before you generate your certificate request.



DB-Type: CMS key database file

File Name: /etc/security/ikekey.kdb

Signer Certificates

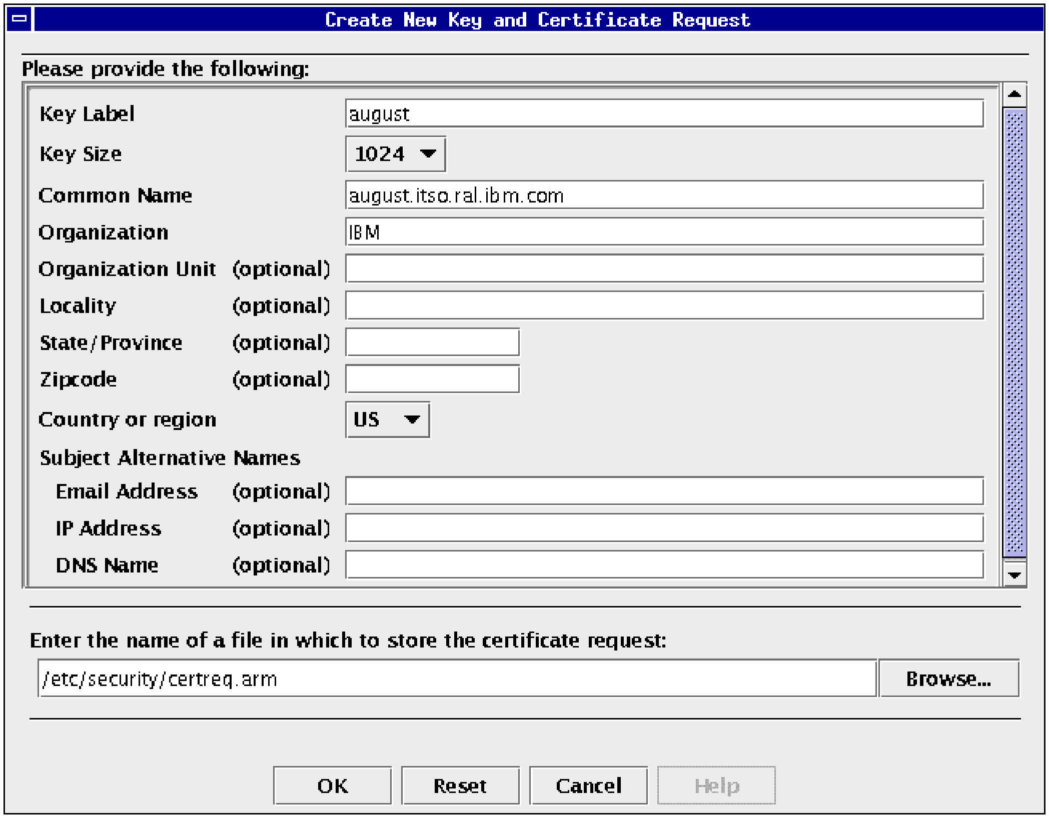
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
RSA Secure Server Certification Authority
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
VeriSign Class 2 CA Individual Subscriber-Persona Not Validated
VeriSign Class 3 CA Individual Subscriber-Persona Not Validated
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority

The requested action has successfully completed!

Figure 2-37 IKE kdb database successfully created

5. On the Create New Key and Certificate Request window (Figure 2-38), complete the required fields. Click **OK**.

> **Important:** The fields Common Name, Organization, Organization Unit, Locality, State, Zipcode, and Country or region must match the values you write when the phase 1 tunnel is defined. See Figure 2-27 on page 41.



Create New Key and Certificate Request

Please provide the following:

Key Label		august
Key Size		1024 ▼
Common Name		august.itso.ral.ibm.com
Organization		IBM
Organization Unit	(optional)	
Locality	(optional)	
State/Province	(optional)	
Zipcode	(optional)	
Country or region		US ▼
Subject Alternative Names		
Email Address	(optional)	
IP Address	(optional)	
DNS Name	(optional)	

Enter the name of a file in which to store the certificate request:

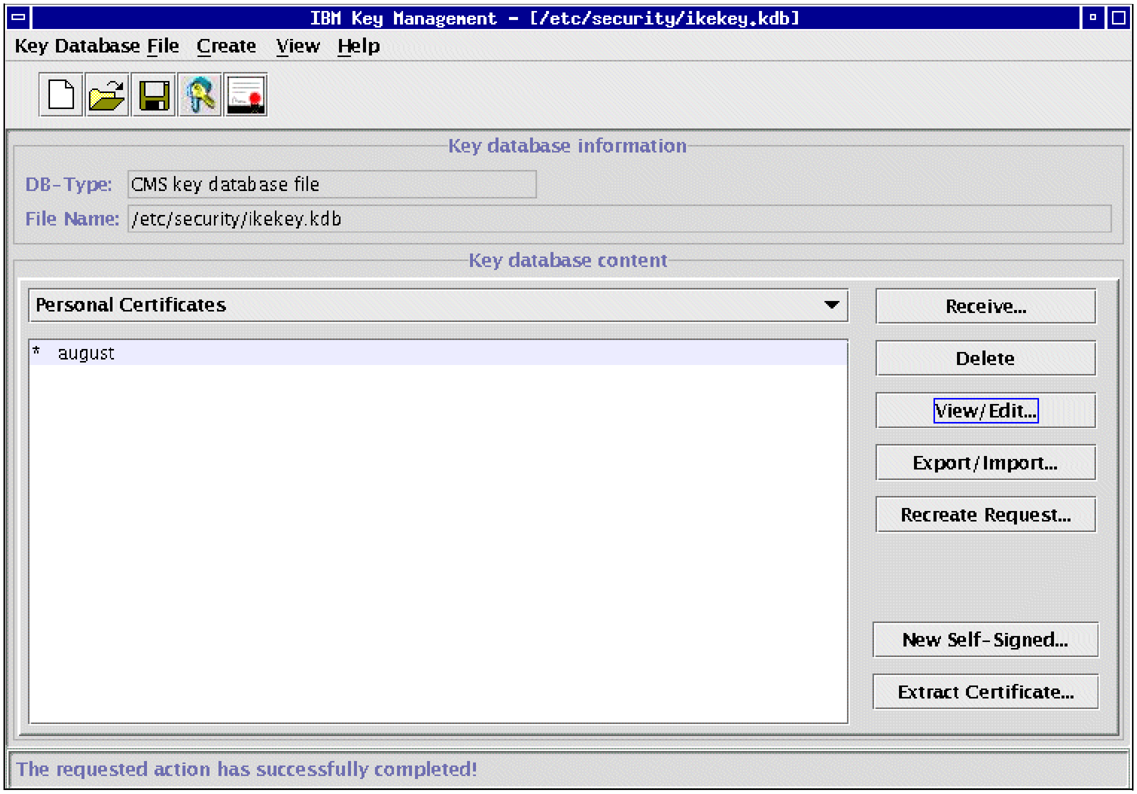
/etc/security/certreq.arm

Figure 2-38 Create New Key and Certificate Request window

6. The system creates a private and public key pair, the certificate request file, and the default name certreq.arm. The certificate manager displays a list of pending certificate requests in the key database content pane.
7. Send the certificate to a CA by means of the infrastructure that you are using, such as file transfer, e-mail, copy/paste into a Web browser, or mail a diskette.
8. Retrieve a CA certificate and a device certificate for your system. First load the CA certificate, and then the device certificate, into the key database.

9. From the list in the key database content pane, select **Signer Certificates**, and then click **Add**.
10. Select the file that holds the CA certificate you just received and choose the proper format (binary DER or base64 ASCII). Click **OK**.
11. Enter a name for this CA in the Label field and click **OK**. The new CA certificate is added to the list.
12. From the list in the key database content pane, select **Personal Certificates**, and then click **Receive**.
13. Select the file that holds the device certificate you just received. Choose the proper format (binary DER or base64 ASCII). In the label field, enter a name for the device. Click **OK**.

The new certificate is added to the list as shown in Figure 2-39. This completes this part of the configuration. You may now exit the certificate manager.


IBM Key Management - [/etc/security/ikekey.kdb]

Key database information

DB-Type: CMS key database file

File Name: /etc/security/ikekey.kdb

Key database content

Personal Certificates

* august

The requested action has successfully completed!

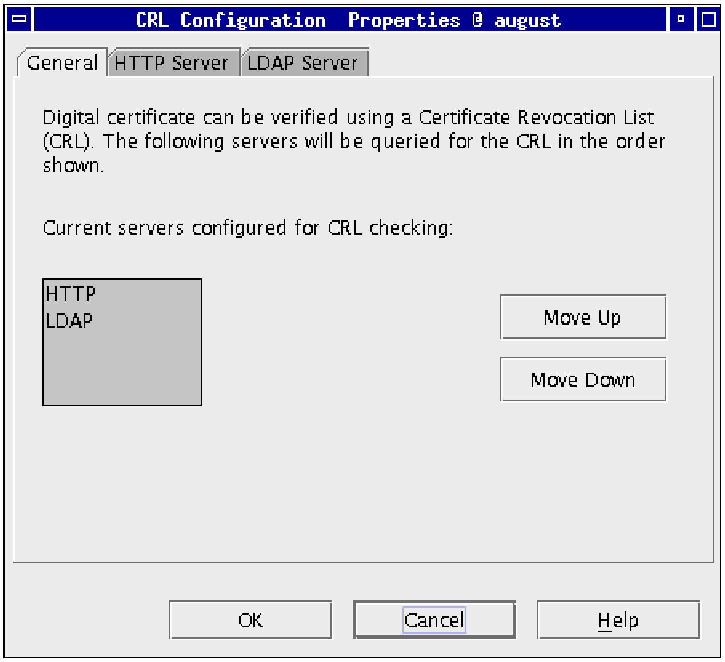
Figure 2-39 Certificate signed

Next, you must define the tunnels. See 2.4.4, “IKE tunnels using Web-based System Manager” on page 37.

Certificate Revocation List

When you want to revoke a certificate prior to its expiration date, a CA administrator adds it in this list.

On the CRL Configuration window (Figure 2-40), you select which type of CRL server to use (HTTP or LDAP server). Using the Move Up and Move Down buttons, you can choose the search order.



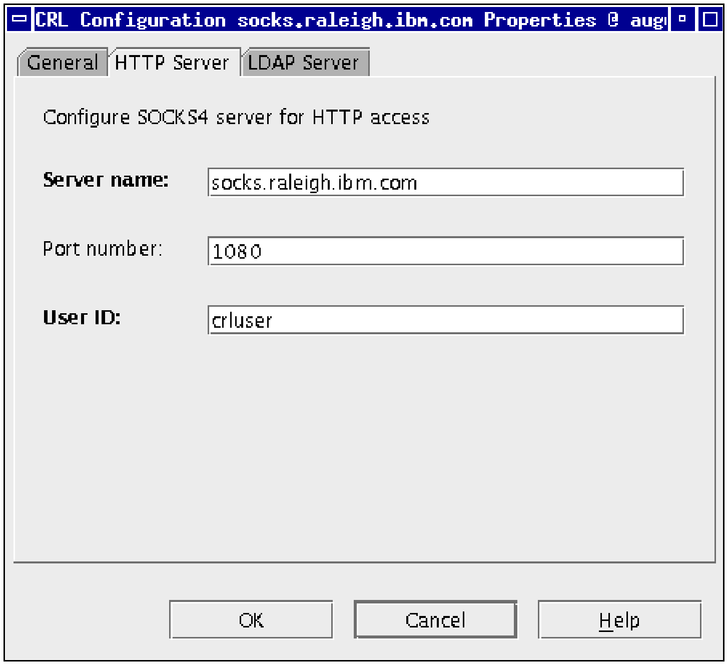
Digital certificate can be verified using a Certificate Revocation List (CRL). The following servers will be queried for the CRL in the order shown.

Current servers configured for CRL checking:

HTTP
LDAP

Figure 2-40 CRL search order window

Note: To use the CRL feature of IP Security, you must configure your system to use a SOCKS server (Version 4 for HTTP servers), an LDAP server, or both. If you know which SOCKS or LDAP server you are using to obtain CRLs, you can make the necessary configuration selections by using the Web-based System Manager. You configure the HTTP Server CRL from the HTTP Server tab as shown in Figure 2-41. You configure the LDAP Server CRL from the LDAP Server tab as shown in Figure 2-42 on page 57.



Configure SOCKS4 server for HTTP access

Server name: socks.raleigh.ibm.com

Port number: 1080

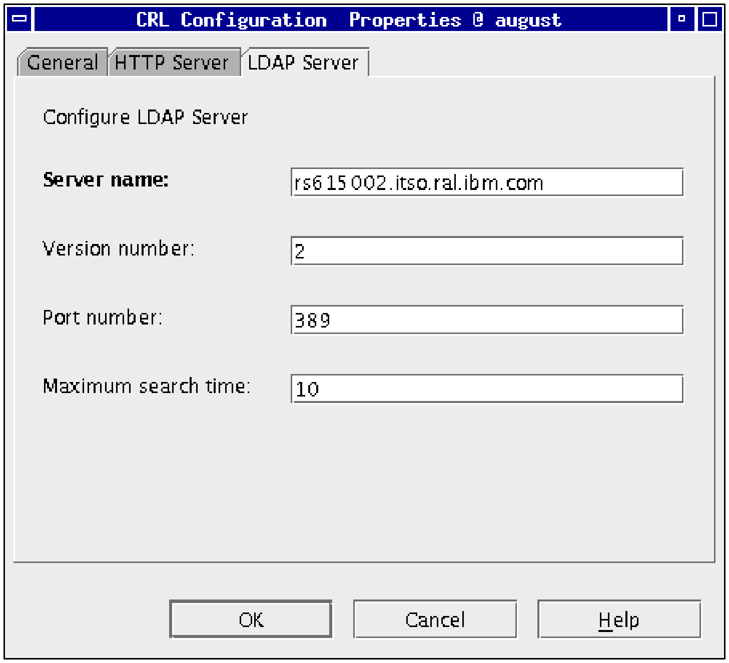
User ID: crluser

Figure 2-41 HTTP Server SOCKS configuration

The /etc/isakmpd.conf file should look similar to Example 2-4.

Example 2-4 /etc/isakmpd.conf file contents

```
# tail -12 /etc/isakmpd.conf
###########################################################################
#none
SOCKS4_SERVER=socks.raleigh.ibm.com
SOCKS4_PORTNUM=1080
SOCKS4_USERID=crluser
LDAP_SERVER=rs615002.itso.ral.ibm.com
LDAP_VERSION=2
LDAP_SERVERPORT=389
LDAP_SEARCHTIME=10
CRL_FETCH_ORDER=HTTP,LDAP
#none
information
```



Configure LDAP Server

Server name: rs615002.itso.ral.ibm.com

Version number: 2

Port number: 389

Maximum search time: 10

Figure 2-42 LDAP Server configuration

2.4.6 Manual tunnels using the System Management Interface Tool

> **Note:** Because the most important operating systems on the market have developed IKE functionality, we strongly advise that you do *not* to use manual tunneling excepting those installations where old tunneling implementations still exist. The following configuration should only be used for compatibility purposes.

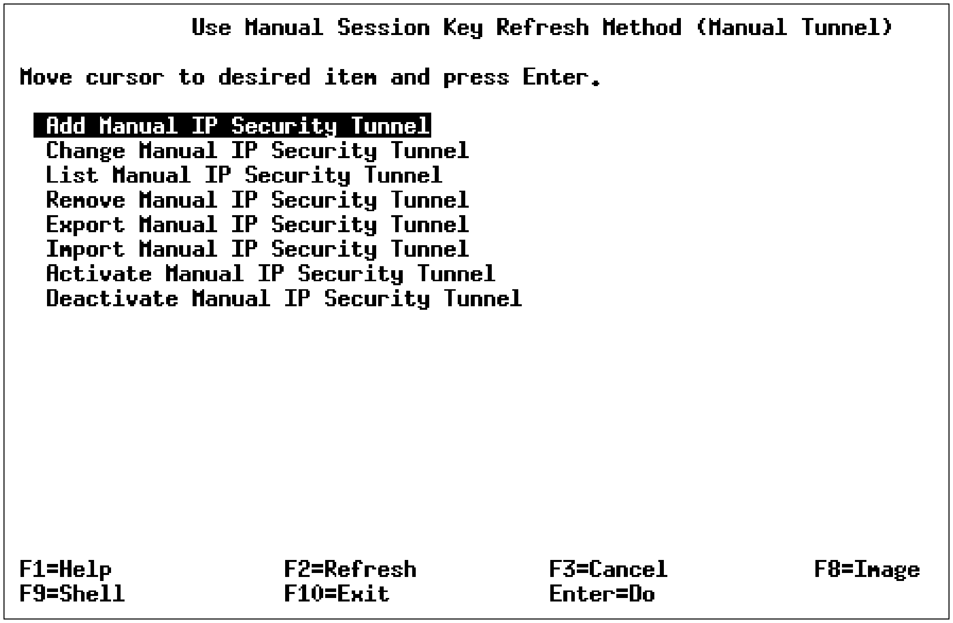
You can access the manual tunnel configuration display by using these steps:

1. Enter the following command:

   ```
   smitty ipsec4
   ```

2. Select **Basic IP Security Configuration**.
3. Select **Use Manual Session Key Refresh Method**.

Use the options on the Use Manual Session Key Refresh Method display (Figure 2-43) as shown from the System Management Interface Tool window.



```
             Use Manual Session Key Refresh Method (Manual Tunnel)

Move cursor to desired item and press Enter.

  Add Manual IP Security Tunnel
  Change Manual IP Security Tunnel
  List Manual IP Security Tunnel
  Remove Manual IP Security Tunnel
  Export Manual IP Security Tunnel
  Import Manual IP Security Tunnel
  Activate Manual IP Security Tunnel
  Deactivate Manual IP Security Tunnel









F1=Help             F2=Refresh          F3=Cancel           F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Figure 2-43 Manual tunneling options

You can have two environments with manual tunneling in AIX:

- **Host-host environment**: This environment sets up a tunnel between two hosts. The parameters defining the tunnel must be exchanged and matching between the two hosts.
- **Host-firewall-host environment**: This environment sets up a tunnel between two hosts that have a firewall between them. You must specify firewall information. You may specify a destination mask to send packets to a group of hosts behind the firewall.

The default rules for User Datagram Protocol (UDP), Authentication Headers, and ESP headers should already handle the host to firewall communication. You must configure the firewall appropriately to complete the setup.

For both environments, you have three possibilities for authentication and encryption in AIX V5.2:

- **Authentication Only with AH**: For users who want to authenticate network data.

- **Authentication with AH and Encryption with ESP**: Authentication is provided by a separate AH header. Encryption s provided with an ESP header.
- **Encryption and Authentication with ESP**: Encryption and authentication are provided by using the ESP header format.

Important: We recommend that you use the System Management Interface Tool windows for manual tunneling configurations. You have more configuration options.

We explain only the host-firewall-host windows, because the fields for the host-host window are included in host-firewall-host windows.

Host-firewall-host tunnels

You can identify host-firewall-host tunnels with the authentication and encryption options that are explained in the following sections.

Encryption and authentication with ESP

Figure 2-44 shows the configuration options for encryption and authentication with ESP. This section explains fields on this display.

The source and destination addresses are the two endpoints of communication. If you want to communicate this host with a group of hosts behind the firewall, optionally you can specify the subnet mask of those hosts. You must specify the firewall IP address.

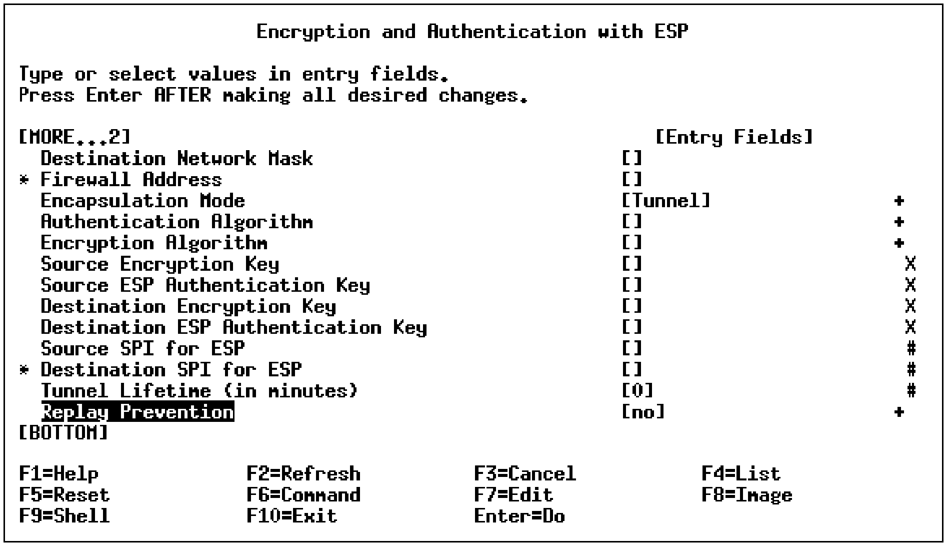
For Authentication Algorithm, you can use HMAC_MD5 or HMAC_SHA. For Encryption Algorithm, you can use 3DES_CBC or DES_CBC_8.

You can write the source and destination key fields by yourself, or the system can automatically generate them for you.

The value for Source SPI is generated automatically. You must enter a value for the Destination SPI field.

The Tunnel Lifetime value indicates the time of operability before tunneling expiration. You enter this value in minutes.

A sequence counter in the AH header prevents old packets from being replayed as a form of attack. This option is only available with HMAC-MD5 or HMAC-SHA.



```
                      Encryption and Authentication with ESP

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...2]                                              [Entry Fields]
  Destination Network Mask                           []
* Firewall Address                                   []
  Encapsulation Mode                                 [Tunnel]                 +
  Authentication Algorithm                           []                       +
  Encryption Algorithm                               []                       +
  Source Encryption Key                              []                        X
  Source ESP Authentication Key                      []                        X
  Destination Encryption Key                         []                        X
  Destination ESP Authentication Key                 []                        X
  Source SPI for ESP                                 []                        #
* Destination SPI for ESP                            []                        #
  Tunnel Lifetime (in minutes)                       [0]                       #
  Replay Prevention                                  [no]                     +
[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Figure 2-44 Host to host with ESP for both operations

Authentication only with AH

The authentication algorithms are HMAC_MD5, HMAC_SHA, or KEYED_MD5. For the other fields see, “Encryption and authentication with ESP” on page 59.

Authentication with AH and encryption with ESP

It allows the ability to combine authentication and encryption. For other values see “Encryption and authentication with ESP” on page 59.

2.4.7 Filtering through the System Management Interface Tool

> **Note:** You can also use the Web-based System Manager interface. Filtering is located in the VPN networks option in this interface.

To reach the Filter management display, follow these steps:

1. On a command line, enter the following command and press Enter:

   ```
   smit ips4_advanced
   ```

2. Select **Configure IP Security Filter Rules**.
3. Select **Add an IP Security Filter Rule**.
4. On the Add an IP Security Filter Rule display (Figure 2-45), complete the following information:

a. Determine the traffic criteria. This panel has the actions (permit or deny) and the IP addresses and subnet masks for source and destination that are used in the comparison.

b. Decide whether this rule applies to source routing packets, the kind of routing (forwarded or local), the packet direction (incoming or outgoing), and the fragmentation control required.

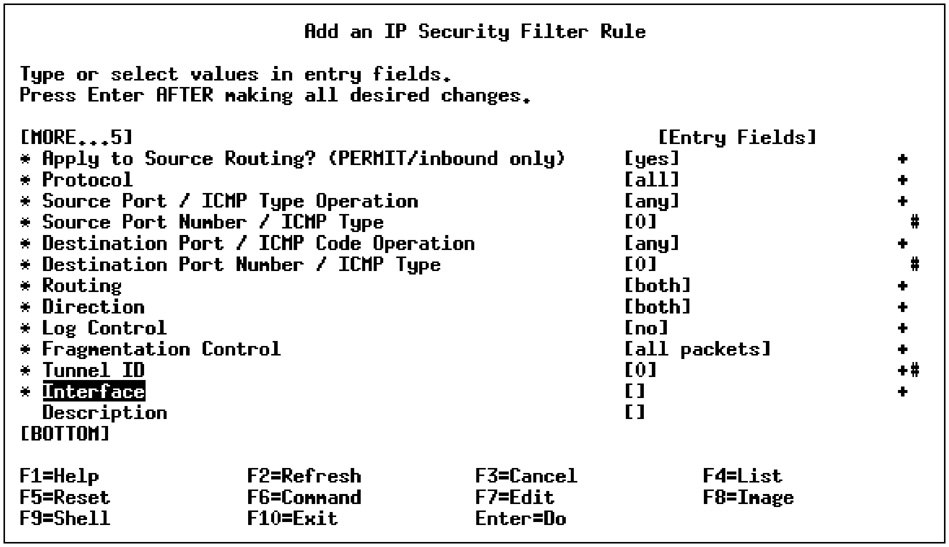
c. For fragmentation control, select from the following options:

- **All packets**: This is the default option.
- **Fragment headers and unfragmented packets only**: Fragments are excluded.
- **Fragments and fragment headers only**: For fragment headers, port information must match. For fragments, port information is ignored.
- **Unfragmented packets only**: Fragment headers and fragments are excluded.

d. Specify the tunnel ID if the rule is associated with the tunnel. For incoming packets, the rule applies only if you entered it through the tunnel ID. For outgoing packets, the rule applies if the packet is sent through the tunnel.

e. Decide whether you want to send a message to the log each time a packet matches this rule.

f. Choose the matching criteria for a protocol, the source and destination ports or ICMP operations, and the source and destination IP addresses.



```
                         Add an IP Security Filter Rule

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...5]                                             [Entry Fields]
* Apply to Source Routing? (PERMIT/inbound only)     [yes]                  +
* Protocol                                           [all]                  +
* Source Port / ICMP Type Operation                  [any]                  +
* Source Port Number / ICMP Type                     [0]                     #
* Destination Port / ICMP Code Operation             [any]                  +
* Destination Port Number / ICMP Type                [0]                     #
* Routing                                            [both]                 +
* Direction                                          [both]                 +
* Log Control                                        [no]                   +
* Fragmentation Control                              [all packets]          +
* Tunnel ID                                          [0]                    +#
* Interface                                          []                     +
  Description                                        []
[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Figure 2-45   Filtering options

5. After you add, alter, or remove a rule, update the rules in memory using the **smitty ips4_upd_filter** option.

2.5 Functionality

This section applies the theory and AIX configuration panels described in the previous sections to work with six scenarios.

These scenarios use the **ike** command. This command functionality is available in the Web-based System Manager. Any error messages or output shown also apply to the Web-based System Manager. In normal operations, the Web-based System Manager is more friendly. In an emergency or when you have bandwidth restrictions, the command line may be a better choice.

> **Important:** These scenarios are for education purposes. We highly recommend that you employ authentication for network security. If you don't have nested tunnels and you are using ESP, always select *authentication*.

2.5.1 Scenario I

In this scenario, a company requires the authentication of the IPSec packets. They want to avoid IP packets from being altered between two company sites connected through the Internet. Figure 2-46 shows this scenario.

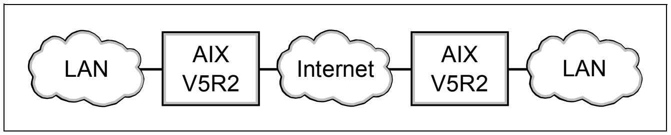


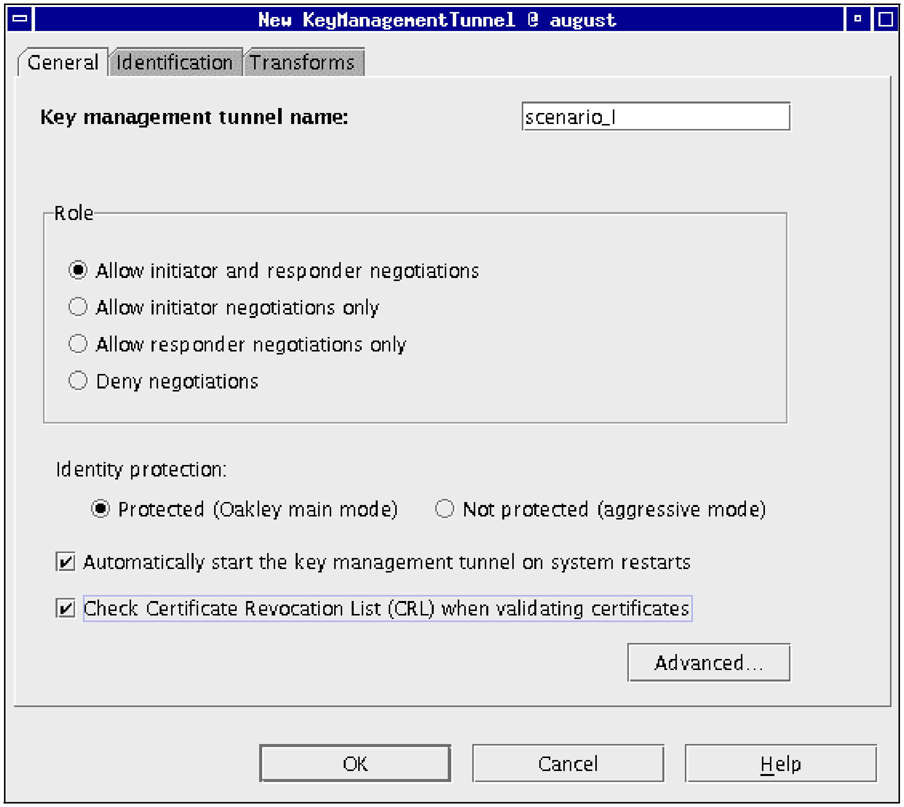
Figure 2-46 Internet link between both buildings

To implement this solution, you need private IP packets to go from one side to the other. You also need authentication of the IP packet. Use tunnel mode and AH as the IPSec protocol.

First think about the phase 1 tunnel. Because this is a gateway-to-gateway connection, you want the link to work again immediately if something happens to the link. For this reason, choose to allow initiator and responder negotiations at both sides. Configure both sides to automatically start the key management tunnel upon system restarts.

The General page of the New Key Management Tunnel window (Figure 2-47) shows the main mode and CRL options selected for this scenario. Because the machines in this scenario are important for the flow of information in the organization, assign both of them static IP addresses. In this scenario, we use the Oakley main mode and RSA signatures.

If you use certificates for the phase 1 tunnel (PFS is chosen later) and your CA administrator has a procedure to invalidate certificates before the date of expiration, we strongly recommend that you select the **Check Certificate Revocation List (CRL) when validating certificates** option. See “Certificate Revocation List” on page 55. If you are not using a CRL, do not select this option.



Key management tunnel name: scenario_l

Role

● Allow initiator and responder negotiations
○ Allow initiator negotiations only
○ Allow responder negotiations only
○ Deny negotiations

Identity protection:

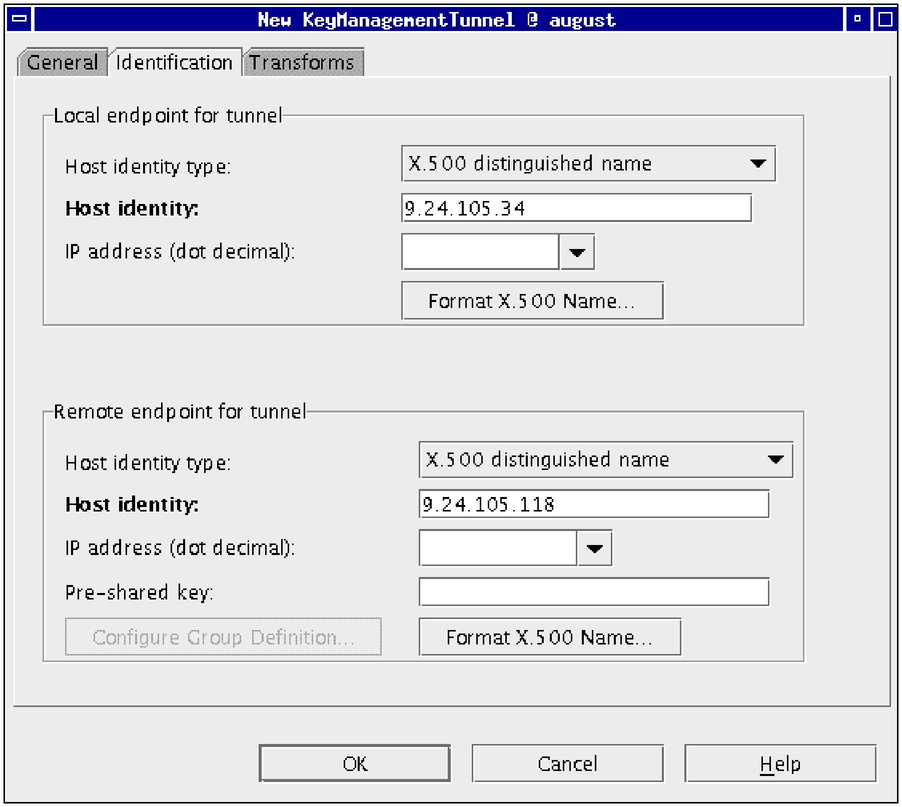
● Protected (Oakley main mode) ○ Not protected (aggressive mode)

☑ Automatically start the key management tunnel on system restarts

☑ Check Certificate Revocation List (CRL) when validating certificates

Figure 2-47 Main mode and CRL options selected

On the Identification page (Figure 2-48), select the Format X.500 formation and IP addresses.



New KeyManagementTunnel @ august

Local endpoint for tunnel

Host identity type: X.500 distinguished name

Host identity: 9.24.105.34

IP address (dot decimal):

Remote endpoint for tunnel

Host identity type: X.500 distinguished name

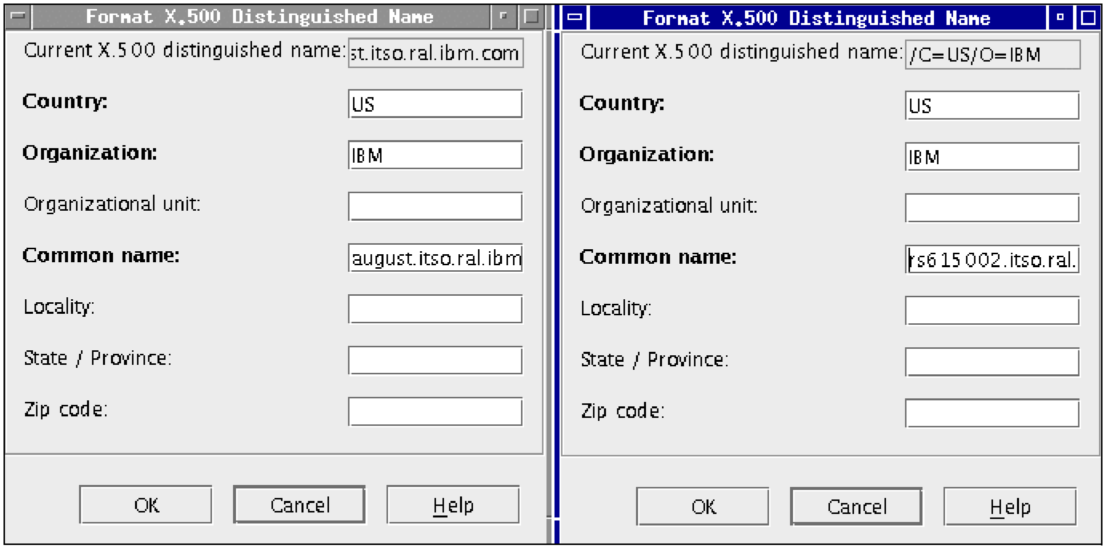
Host identity: 9.24.105.118

IP address (dot decimal):

Pre-shared key:

Figure 2-48 Selecting the X.500 format and writing the static IP addresses

When you click Format X.500 Name (Figure 2-48) button, remember that the values that you specified must match the actual certificate values. See Figure 2-49.



Format X.500 Distinguished Name

Current X.500 distinguished name: st.itso.ral.ibm.com

Country: US

Organization: IBM

Organizational unit:

Common name: august.itso.ral.ibm

Locality:

State / Province:

Zip code:

Format X.500 Distinguished Name

Current X.500 distinguished name: /C=US/O=IBM

Country: US

Organization: IBM

Organizational unit:

Common name: rs615002.itso.ral.

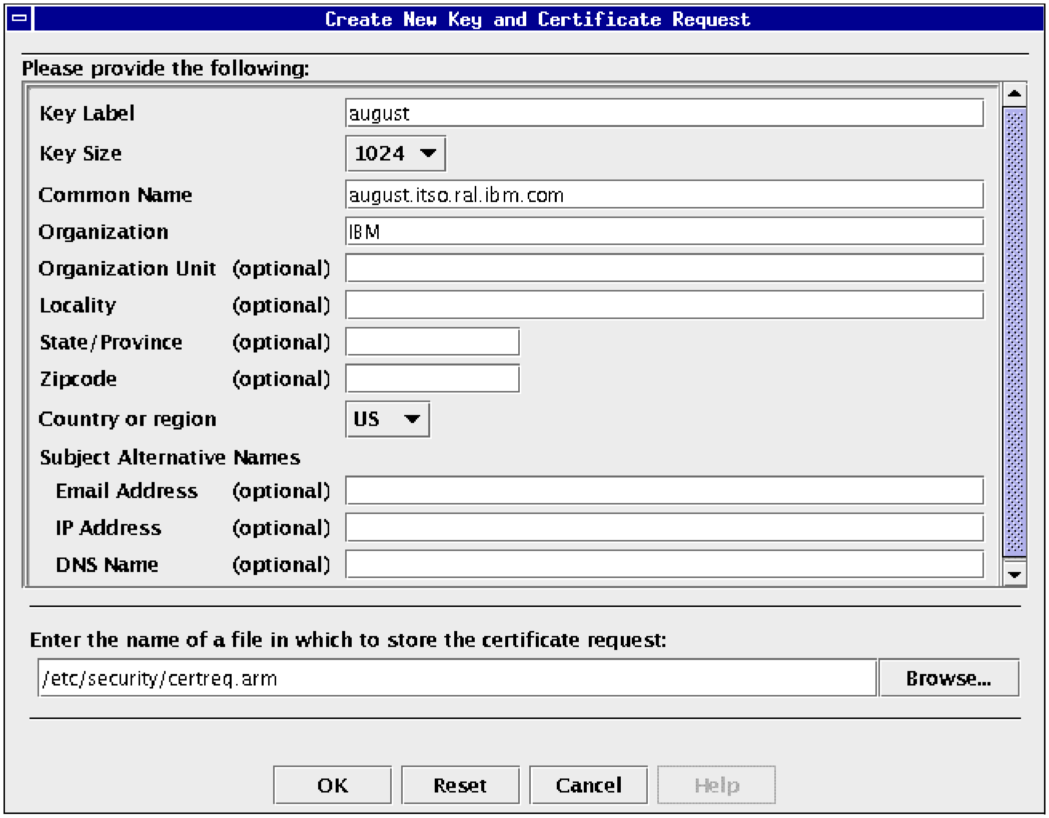
Locality:

State / Province:

Zip code:

Figure 2-49 X.500 format for both endpoints

Figure 2-50 shows a certificate example for the information in Figure 2-49.



Create New Key and Certificate Request

Please provide the following:

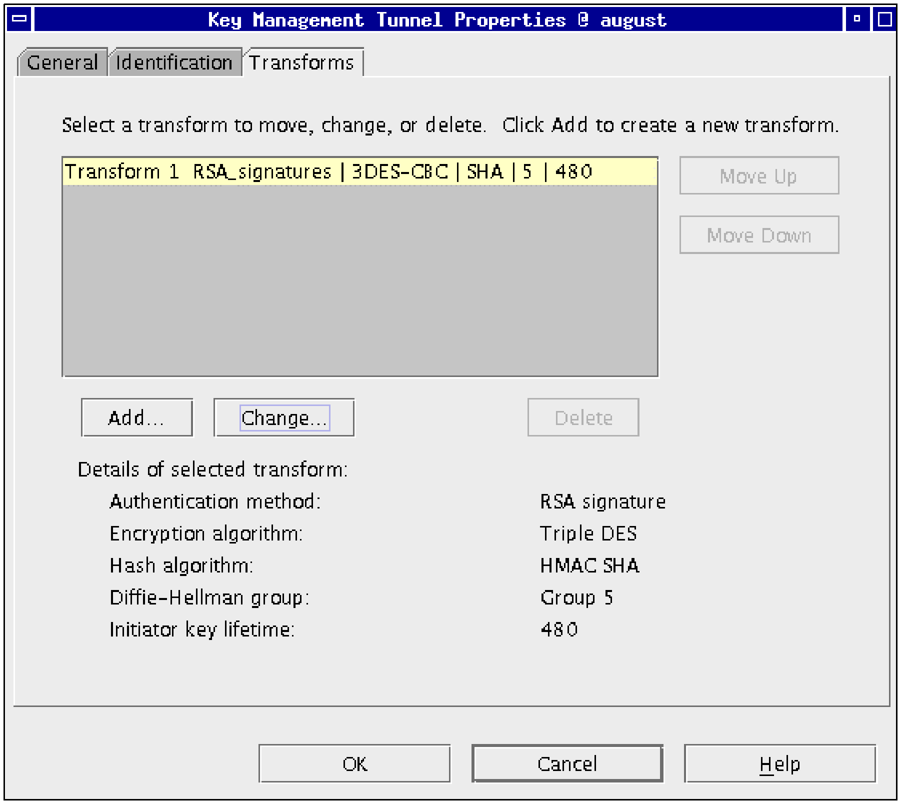
Key Label: august
Key Size: 1024
Common Name: august.itso.ral.ibm.com
Organization: IBM
Organization Unit (optional):
Locality (optional):
State/Province (optional):
Zipcode (optional):
Country or region: US
Subject Alternative Names
Email Address (optional):
IP Address (optional):
DNS Name (optional):

Enter the name of a file in which to store the certificate request:
/etc/security/certreq.arm

Figure 2-50 Certificate details for comparing with the Format X.500

The IKE tunnel advanced options depend on the environment where IPSec is deployed. We recommend that you use the default values and then adjust them as necessary, or make an in-depth evaluation of the environment. See Figure 2-25 on page 39.

When you choose the options for key management, consider your environment. For example, the difference of MD5 or SHA is the bit-encryption size. MD5 is 128 bit and SHA is 160 bit. The same applies for DH groups. The difference is the group bit. Group 5 is the strongest of the DH groups supported. You set these options on the Key Management Tunnel Properties Transforms page (Figure 2-51).



Select a transform to move, change, or delete. Click Add to create a new transform.

Transform 1 RSA_signatures | 3DES-CBC | SHA | 5 | 480

Details of selected transform:

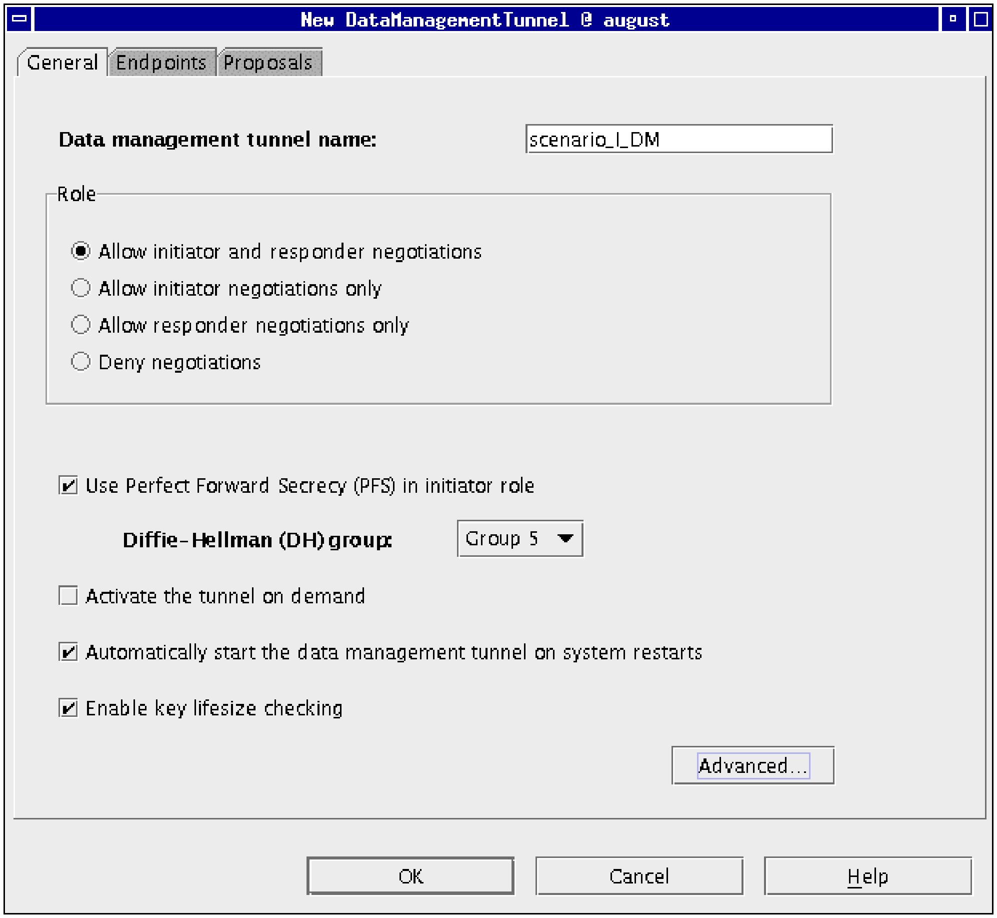
Authentication method:	RSA signature
Encryption algorithm:	Triple DES
Hash algorithm:	HMAC SHA
Diffie-Hellman group:	Group 5
Initiator key lifetime:	480

Figure 2-51 Selecting values on the Transforms page

Then think about the phase 2 tunnel. Because you know the IP addresses, select the **Standard data management tunnel** option as shown in Figure 2-30 on page 45.

On the New Data Management Tunnel window (Figure 2-52), select the **Use Perfect Forward Secrecy (PFS) in initiator role** option. You select this option because this is an important tunneling and you don't want the keys based one on the other.

The selection of the DH group depends on the environment of the customer. In this scenario, we select **Group 5**. Also select the **Automatically start the data management tunnel on system restarts** option.



Data management tunnel name: scenario_I_DM

Role

● Allow initiator and responder negotiations
○ Allow initiator negotiations only
○ Allow responder negotiations only
○ Deny negotiations

☑ Use Perfect Forward Secrecy (PFS) in initiator role

Diffie-Hellman (DH) group: Group 5

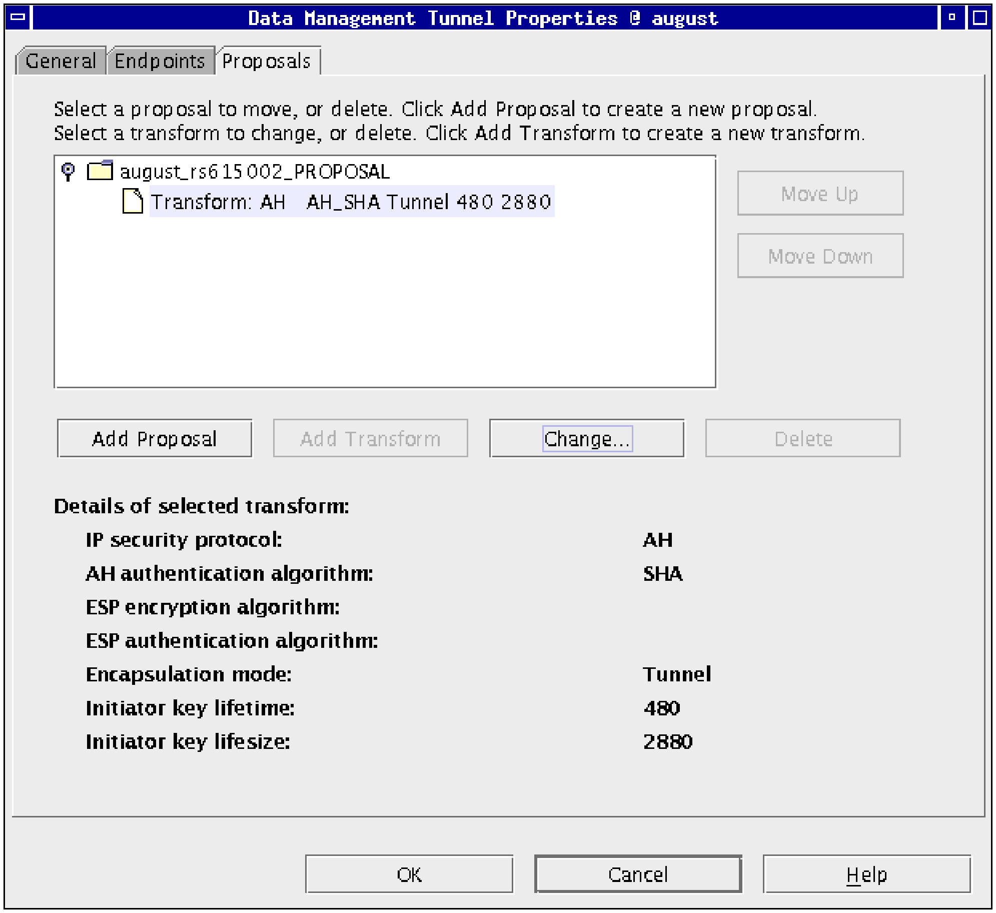
☐ Activate the tunnel on demand

☑ Automatically start the data management tunnel on system restarts

☑ Enable key lifesize checking

Figure 2-52 Selecting values for the standard data management tunnel

On the Proposals page (Figure 2-53), you specify AH for the IP Security protocol for the phase 2 tunnel and tunneling for the encapsulation mode.



Select a proposal to move, or delete. Click Add Proposal to create a new proposal.
Select a transform to change, or delete. Click Add Transform to create a new transform.

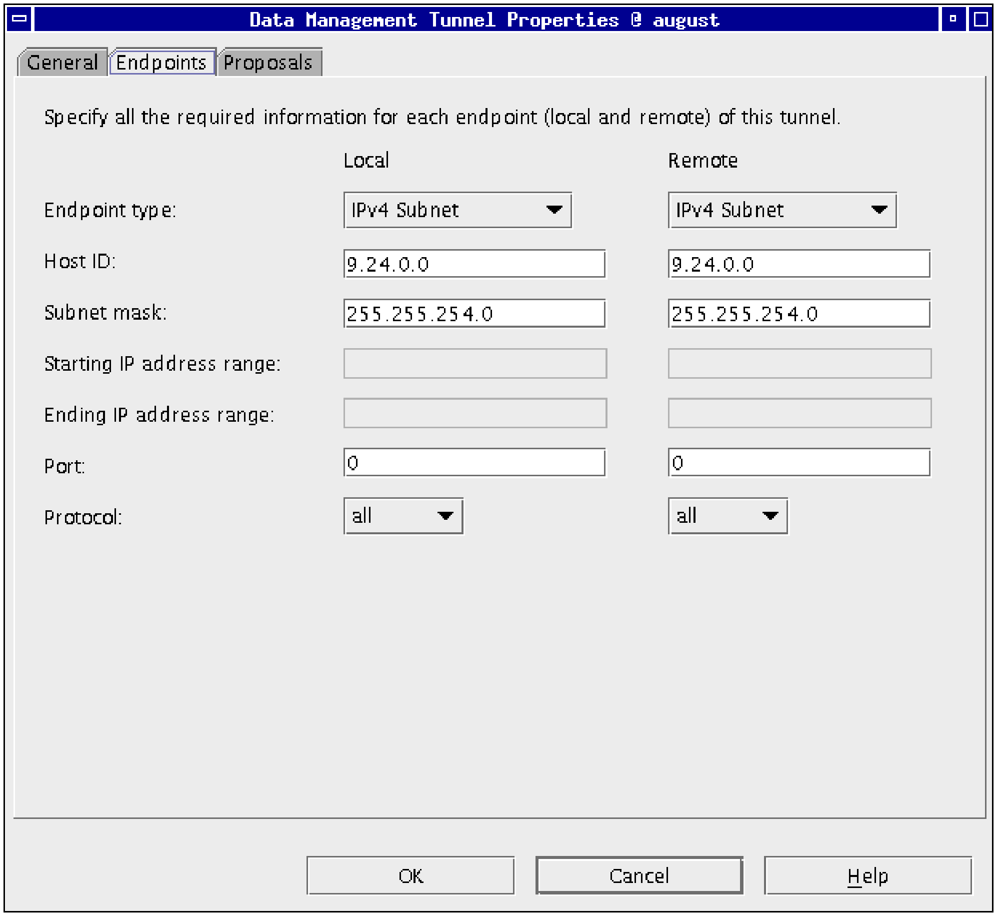
august_rs615002_PROPOSAL
Transform: AH AH_SHA Tunnel 480 2880

Details of selected transform:

IP security protocol:	AH
AH authentication algorithm:	SHA
ESP encryption algorithm:	
ESP authentication algorithm:	
Encapsulation mode:	Tunnel
Initiator key lifetime:	480
Initiator key lifesize:	2880

Figure 2-53 Proposal for standard data management tunnel

You configure this tunnel from the Web-based System Manager through a Web browser. Therefore, you need a permit rule that allows this machine access to the endpoints of the tunnel. You also need the access of all non-secure machines from a specific subnet to this tunnel. In this case, the machine to configure tunneling is in the same subnet as the non-secure machines. To allow this, add a permit rule. Specify the subnet and the subnet mask for any port and any protocol, as shown in Figure 2-54.



Specify all the required information for each endpoint (local and remote) of this tunnel.

	Local	Remote
Endpoint type:	IPv4 Subnet	IPv4 Subnet
Host ID:	9.24.0.0	9.24.0.0
Subnet mask:	255.255.254.0	255.255.254.0
Starting IP address range:		
Ending IP address range:		
Port:	0	0
Protocol:	all	all

Figure 2-54 Filter rule

These are the steps to configure one side. To configure the other side, repeat these steps, switching the identifiers. Or you can export the configuration to an XML file and import it from the other side. See 2.4.3, “IKE tunnels using SMIT” on page 36.

Now you can activate the tunnel. Figure 2-55 shows the tunnel.

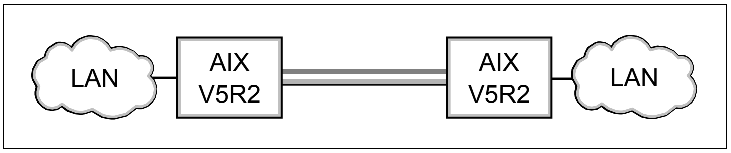


Figure 2-55 Tunnel encapsulation between two AIX systems

You can see the tunnel definitions using the **`ike cmd=list db`** command, as shown in Example 2-5. It shows the static information that is related to the tunnels.

Example 2-5 Output from the ike cmd=list db command

```
# ike cmd=list db
Phase 1 Tunnel ID:        1
Remote ID:                9.24.105.118
Remote IP Address:        0
Phase 2 Tunnel ID:        1
Associated P1 Tunnel:     1
Local ID:                 9.24.0.0
Local ID Netmask:         255.255.254.0
Local ID Protocol ID:     any
Local ID Port Number:     all
Remote ID:                9.24.0.0
Remote ID Netmask:        255.255.254.0
Remote ID Protocol ID:    any
Remote ID Port Number:    all
```

If you want to see only information about dynamic (active) tunnels, enter:

```
ike cmd=list
```

If you want more information in both cases, add the word `verbose`.

After you activate the tunnels using the **`ike cmd=activate`** command (activates all phase 1 and phase 2 tunnels), you can display the status using the **`ike cmd=list`** command as shown in Example 2-6. If both are active, all is OK.

Example 2-6   Output from the ike cmd=list command

```
# ike cmd=list
Phase  Tun Id  Status      Local Id                        Remote Id
1      1       Active      /c=US/o=IBM/cn=august.itso.ral.ibm.com
/c=US/o=IBM/cn=rs615002.itso.ral.ibm.com
2      1       Active      9.24.0.0/255.255.254.0 9.24.0.0/255.255.254.0

Phase  Tun Id  Status      Local Id                        Remote Id
1      1       Active      9.24.105.34                     9.24.105.118
2      1       Active      9.24.0.0/255.255.254.0 9.24.0.0/255.255.254.0
```

If phase 1 is negotiating and phase 2 is initial as shown in Example 2-7, then the handshake is taking place. Or it is delayed by some networking problem between both, or there is a configuration problem with the other side.

Example 2-7   Output where phase 1 is negotiating and phase 2 is initial

```
Phase  Tun Id  Status      Local Id                        Remote Id
1      1       Negotiating /c=US/o=IBM/cn=august.itso.ral.ibm.com
/c=US/o=IBM/cn=rs615002.itso.ral.ibm.com
2      1       Initial 9.24.0.0/255.255.254.0         9.24.0.0/255.255.254.0
```

If the state is that SA has expired, then the tunnel lifetime is exhausted or the other side was deactivated. This is shown in Example 2-8.

Example 2-8   Output with a status of SA expired

```
Phase  Tun Id  Status      Local Id                        Remote Id
1      1       SA expired /c=US/o=IBM/cn=august.itso.ral.ibm.com
/c=US/o=IBM/cn=rs615002.itso.ral.ibm.com
```

You can verify that after activating the phase 2 tunnel the filter rules were added using the **lsfilt -d** command. This command shows the filter rules added by the activation of IKE phase 2 tunnels. See Example 2-9.

Example 2-9   Output of the lsfilt -d command

```
Dynamic rule 3:
Rule action         : permit
Source Address      : 9.24.0.0
Source Mask         : 255.255.254.0
Destination Address : 9.24.0.0
Destination Mask    : 255.255.254.0
Source Routing      : no
Protocol            : all
Source Port         : any 0
Destination Port    : any 0
Scope               : both
Direction           : outbound
Fragment control    : all packets
Tunnel ID number    : 1

Dynamic rule 4:
Rule action         : permit
Source Address      : 9.24.0.0
Source Mask         : 255.255.254.0
Destination Address : 9.24.0.0
Destination Mask    : 255.255.254.0
Source Routing      : no
Protocol            : all
Source Port         : any 0
Destination Port    : any 0
Scope               : both
Direction           : inbound
Fragment control    : all packets
Tunnel ID number    : 1
```

Finally, you can verify that IPSec conversation is taking place by entering the **ipsecstat** command, as shown in Example 2-10.

Example 2-10 Output of the ipsecstat command

```
# ipsecstat
IPSec Devices:
   ipsec_v4 Available
   ipsec_v6 Not Found

Authentication Algorithm:
   HMAC_MD5 -- Hashed MAC MD5 Authentication Module
   HMAC_SHA -- Hashed MAC SHA Hash Authentication Mo
   KEYED_MD5 -- Keyed MD5 Hash Authentication Module

Encryption Algorithm:
   NULL -- Null Encryption Algorithm module
   3DES_CBC -- Triple DES CBC Encryption Module
   DES_CBC_4 -- DES CBC 4 Encryption Module
   DES_CBC_8 -- DES CBC 8 Encryption Module

IPSec Statistics -
```

```
Total incoming packets:          1936557
   Incoming AH packets:              719
   Incoming ESP packets:               0
   Srcrte packets allowed:             0
Total outgoing packets:          1770492
   Outgoing AH packets:             1019
   Outgoing ESP packets:               0
Total incoming packets dropped:     4000
  Filter denies on input:           4000
  AH did not compute:                  0
  ESP did not compute:                 0
  AH replay violation:                 0
  ESP replay violation:                0
Total outgoing packets dropped:        0
  Filter denies on output:             0
Tunnel cache entries added:          112
Tunnel cache entries expired:          0
Tunnel cache entries deleted:        109
```

You can use the **tcpdump** command to identify AH headers, if you want a to see IPSec traffic in detail.

2.5.2 Scenario II

This scenario (Figure 2-56) entails two intranet hosts that are important for the company. The information that they interchange in the near future is highly confidential, so you need to encrypt the data. Because of the recent acquisition of Intrusion Detection Systems, the company inspects IP packets looking for attackers. You don't need to encapsulate IP packets, so you use transport mode and ESP for encryption.

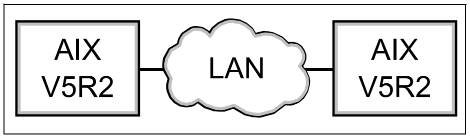


Figure 2-56 Encryption between two intranet hosts

Because this is an important connection, you want the link to work again immediately if something happens it. For this reason, choose to allow initiator and responder negotiations at both sides. Configure both sides to automatically start the key management tunnel upon system restarts.

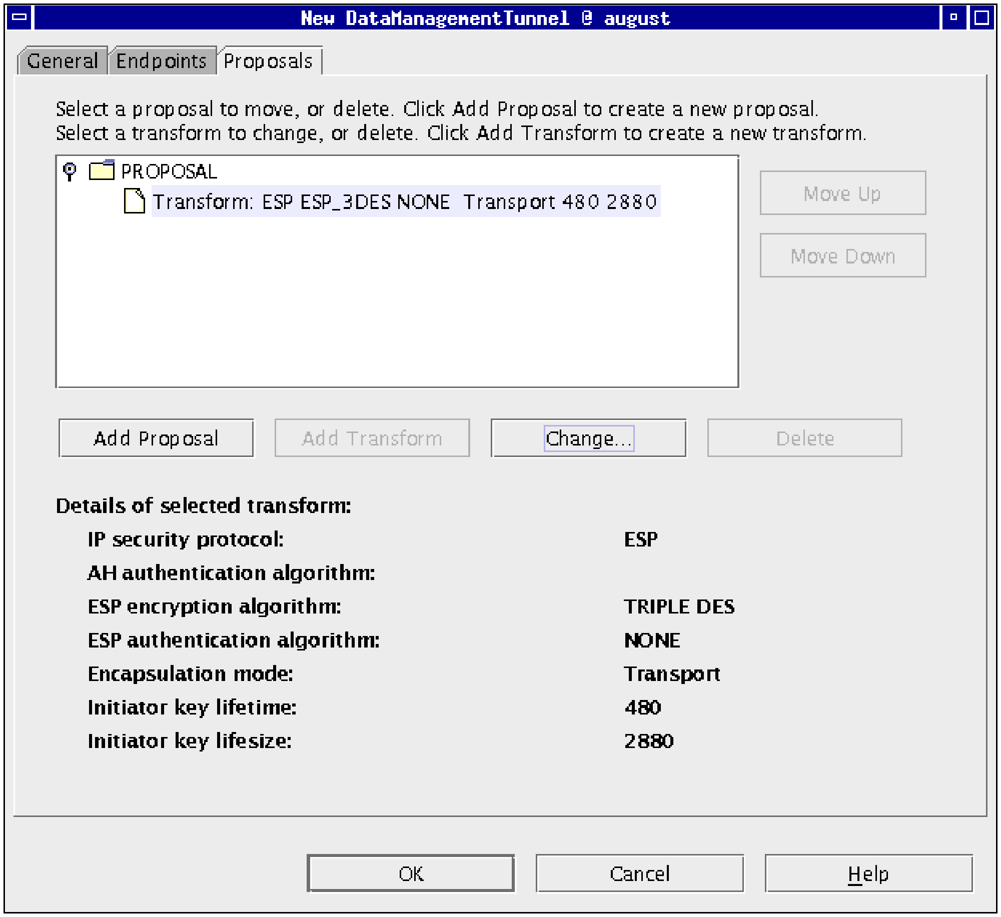
These machines are important for the flow of information in the organization. Give both of them static IP addresses. You can use the Oakley main mode and RSA signatures.

If you use certificates for the phase 1 tunnel and your CA administrator has a procedure to invalidate certificates before the date of expiration, we recommend that you select this option.

Define the phase 1 tunnel as explained in 2.5.1, “Scenario I” on page 62. The IKE tunnel advanced options depend on the environment where IPSec is deployed. We recommend that you use the default values and then adjust them as necessary, or make an in-depth evaluation of the environment.

The identification for both sides is their IP addresses and each site certificate.

Define the phase 2 tunnel as explained in 2.5.1, “Scenario I” on page 62, with the exception of the options on the Proposals page (Figure 2-57) of the New Data Management Tunnel window. Set the ESP authentication algorithm field to **NONE** and the ESP encryption algorithm field to **TRIPLE DES**.



Select a proposal to move, or delete. Click Add Proposal to create a new proposal.
Select a transform to change, or delete. Click Add Transform to create a new transform.

PROPOSAL
Transform: ESP ESP_3DES NONE Transport 480 2880

Details of selected transform:

IP security protocol:	ESP
AH authentication algorithm:	
ESP encryption algorithm:	TRIPLE DES
ESP authentication algorithm:	NONE
Encapsulation mode:	Transport
Initiator key lifetime:	480
Initiator key lifesize:	2880

Figure 2-57 ESP transport encapsulation mode

You can see the tunnel definitions using the **`ike cmd=list db`** command. It displays the static information related to tunnels. If you want only information about dynamic (active) tunnels, you enter the **`ike cmd=list`** command. If you want more information, add the word `verbose` to the command.

You activate the tunnels using the **`ike cmd=activate`** command (activates all phase 1 and phase 2 tunnels). Then, you can display the status using the **`ike cmd=list`** command. If both tunnels are active, all is OK.

If phase1 is negotiating and phase 2 is initial, then the handshake is taking place, it is delayed by some networking problem between both, or there is a configuration problem with the other side.

If the state of SA expired, then the tunnel lifetime is exhausted or the other side was deactivated.

After you activate the phase 2 tunnel, you can verify that the filter rules were added using the **lsfilt -d** command. This command shows the filter rules added by the activation of IKE phase 2 tunnels.

Finally you can verify that IPSec conversation is taking place by entering the **ipsecstat** command, as shown in Example 2-11.

Example 2-11 Output of the ipsecstat command

```
# ipsecstat
IPSec Devices:
   ipsec_v4 Available
   ipsec_v6 Available

Authentication Algorithm:
   HMAC_MD5 -- Hashed MAC MD5 Authentication Module
   HMAC_SHA -- Hashed MAC SHA Hash Authentication Module
   KEYED_MD5 -- Keyed MD5 Hash Authentication Module

Encryption Algorithm:
   NULL -- Null Encryption Algorithm module
   3DES_CBC -- Triple DES CBC Encryption Module
   DES_CBC_4 -- DES CBC 4 Encryption Module
   DES_CBC_8 -- DES CBC 8 Encryption Module

IPSec Statistics -
Total incoming packets:               178636
   Incoming AH packets:                    0
   Incoming ESP packets:                   2
   Srcrte packets allowed:                 0
Total outgoing packets:                78206
   Outgoing AH packets:                    0
   Outgoing ESP packets:                   2
Total incoming packets dropped:           75
  Filter denies on input:                 75
  AH did not compute:                      0
  ESP did not compute:                     0
  AH replay violation:                     0
  ESP replay violation:                    0
Total outgoing packets dropped:          155
  Filter denies on output:               155
```

```
Tunnel cache entries added:              17
Tunnel cache entries expired:             0
Tunnel cache entries deleted:             9
#
```

You can use the **tcpdump** command to identify ESP headers, if you want to see IPSec traffic in detail.

Figure 2-58 shows the result of implementing this scenario.

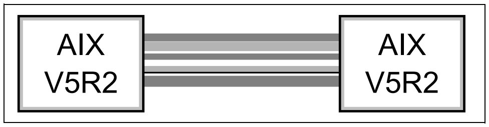


Figure 2-58 Transport encapsulation between two AIX hosts

2.5.3 Scenario III

The company needs authentication between both intranets separated by an Internet connection. It also needs encryption between hosts beside this gateway-to-gateway connection. Figure 2-59 shows the problem space for this scenario.

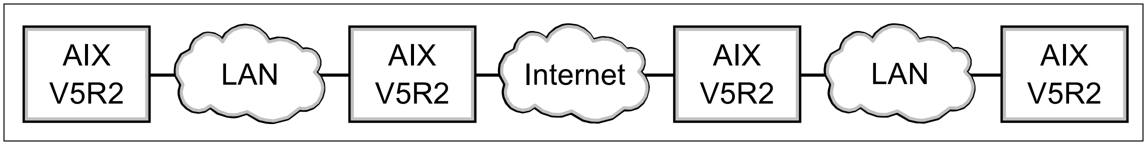


Figure 2-59 Encryption and encapsulation at the same time

This company must use authentication between the gateways and encryption between the hosts. Set up a tunnel encapsulation between gateways and a transport encapsulation between hosts. The host information is encrypted when packets travel from one gateway to the other. You will have two nested tunnels.

You must combine both definitions from the previous scenarios. See 2.5.1, “Scenario I” on page 62, for the gateway-to-gateway environment. Then see 2.5.2, “Scenario II” on page 74, for the host-to-host connection that you set up through the gateway-to-gateway connection.

Figure 2-60 shows the result of implementing this scenario.

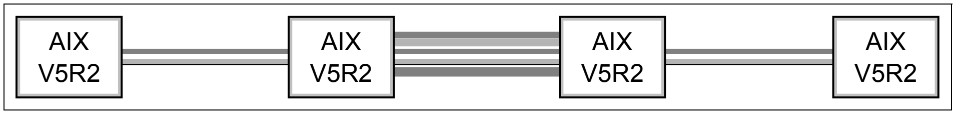


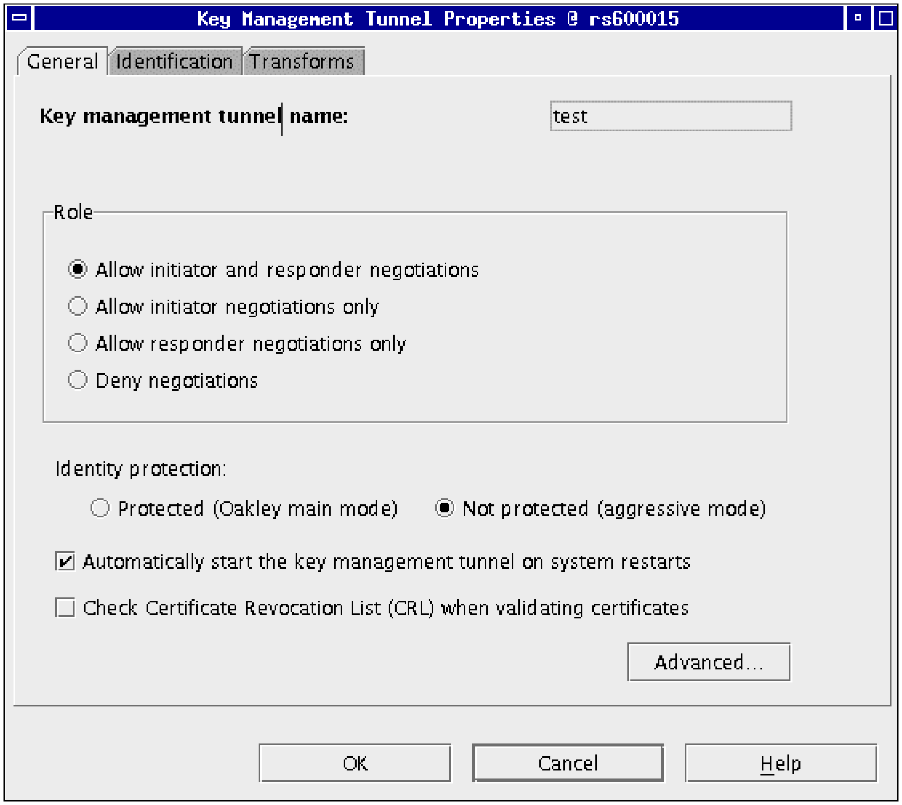
Figure 2-60 Encryption encapsulated in an AH IPSec package (nested tunnels)

2.5.4 Scenario IV

In this scenario, the customer has two machines, one with a dynamic IP address and the other with a static IP address. They want to connect them through an IPSec tunnel.

You will use preshared keys. Therefore, it is important that you select aggressive mode (see Figure 2-61 and "IKE tunnel support" on page 12) because one of the machines has a dynamic IP address, so you cannot know the IP address. Also, you must configure the dynamic IP address box as an fully qualified domain name (FQDN) in the tunnel panels for both machines. Figure 2-61 shows how to configure the aggressive mode.

Note: If you are using preshared keys, you must use aggressive mode. If you use RSA signatures, you can use main and aggressive modes with dynamic IP addresses.



Key Management Tunnel Properties @ rs600015

Key management tunnel name: test

Role

● Allow initiator and responder negotiations

○ Allow initiator negotiations only

○ Allow responder negotiations only

○ Deny negotiations

Identity protection:

○ Protected (Oakley main mode) ● Not protected (aggressive mode)

☑ Automatically start the key management tunnel on system restarts

□ Check Certificate Revocation List (CRL) when validating certificates

Figure 2-61 Selecting aggressive mode for the DHCP AIX client box

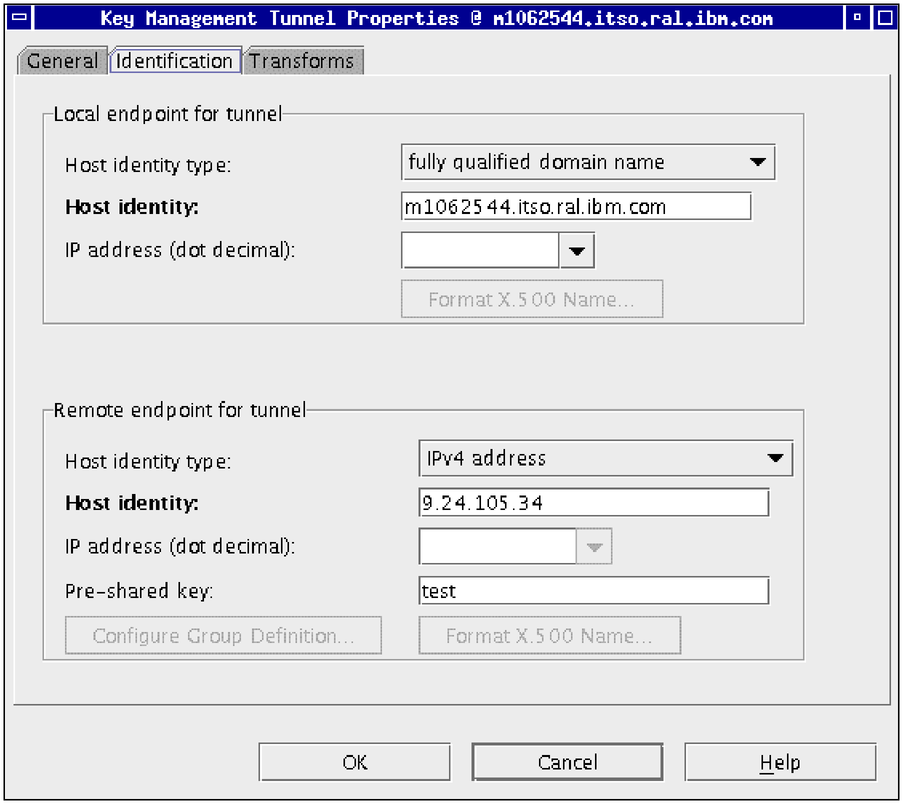
When you activate the tunnel, you can do it *only* from the AIX box that has the dynamic IP address. If you try to activate the tunnel from the AIX box with the static IP address, it fails. When you use a dynamic IP address in one of the two machines, you can only activate the tunnel from the Dynamic Host Configuration Protocol (DHCP) AIX client box (or any other DHCP client box). If you try to do it from the static IP address machine, you receive an error message.

For more information, see RFC 3456 on the Web at:

http://www.ietf.org/rfc/rfc3456.txt

Restriction: DHCP clients on both sides are not supported.

Figure 2-62 shows how to configure the host name for the DHCP AIX client. This is only one side. You must configure the other side with aggressive mode and FQDN for a successful configuration, and switch the identifiers. See 2.4.3, "IKE tunnels using SMIT" on page 36, for tunnel export and import options.



Key Management Tunnel Properties @ m1062544.itso.ral.ibm.com

Local endpoint for tunnel

Host identity type: fully qualified domain name

Host identity: m1062544.itso.ral.ibm.com

IP address (dot decimal):

Remote endpoint for tunnel

Host identity type: IPv4 address

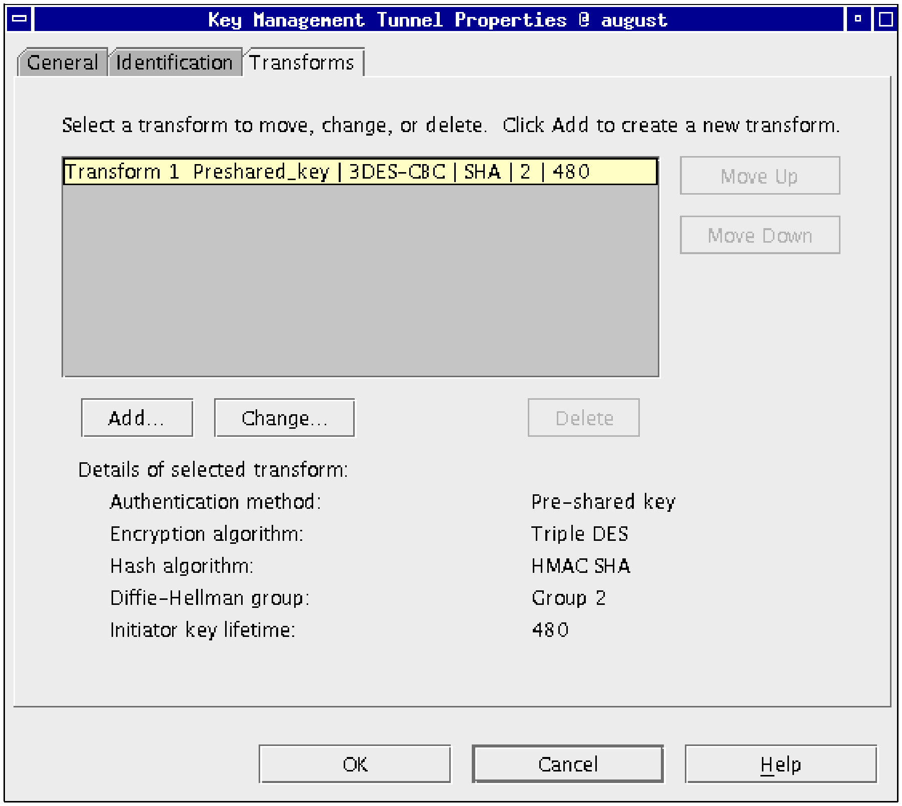
Host identity: 9.24.105.34

IP address (dot decimal):

Pre-shared key: test

Figure 2-62 Full domain name for the DHCP AIX client box

Figure 2-63 shows the Transforms page. For Authentication method, remember to select Pre-shared key. The keys in both AIX boxes must be the same.



Select a transform to move, change, or delete. Click Add to create a new transform.

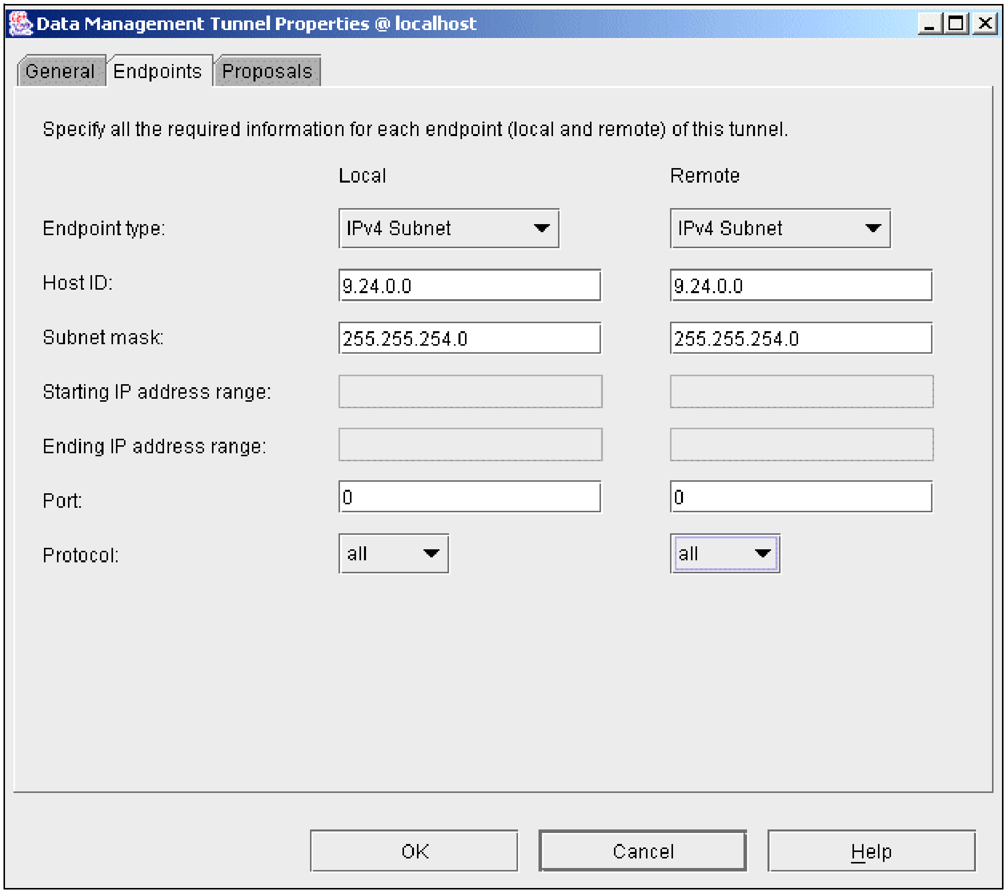
Transform 1 Preshared_key | 3DES-CBC | SHA | 2 | 480

Details of selected transform:

Authentication method:	Pre-shared key
Encryption algorithm:	Triple DES
Hash algorithm:	HMAC SHA
Diffie-Hellman group:	Group 2
Initiator key lifetime:	480

Figure 2-63 Transform page with preshared keys

Now you need a data management tunnel. Use a standard data management tunnel for this scenario. See Figure 2-52 on page 68. You use a subnet configuration to avoid using the IP address of the DHCP client. This works because you know the subnet mask and the subnet address. You must define this kind of data management tunnel for both sides as shown in Figure 2-64.



Specify all the required information for each endpoint (local and remote) of this tunnel.

	Local	Remote
Endpoint type:	IPv4 Subnet	IPv4 Subnet
Host ID:	9.24.0.0	9.24.0.0
Subnet mask:	255.255.254.0	255.255.254.0
Starting IP address range:		
Ending IP address range:		
Port:	0	0
Protocol:	all	all

Figure 2-64 Defining endpoints for the DHCP AIX client box

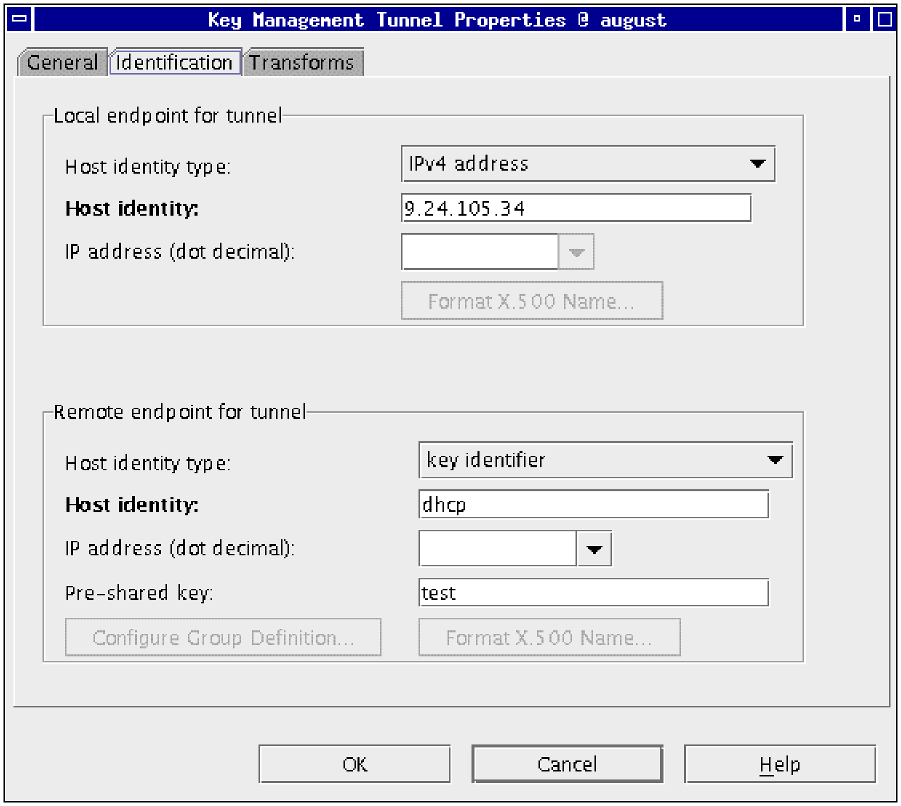
Important: You can activate a connection only from the DHCP clients.

2.5.5 Scenario V

The customer needs to connect many DHCP client boxes to one AIX system with a static IP address. They want to insert an IPSec tunnel between those machines and the AIX box. You can base the phase 1 tunnel configuration parameters on any scenario that you want, excepting the pages related with this configuration.

For this scenario, you need a generic data management tunnel to connect all DHCP client boxes. You make the connection with two AIX DHCP client boxes, for example.

In the machine with the static IP address, you must configure a phase 1 tunnel and a phase 2 generic management tunnel, as shown in Figure 2-65. In the phase 1 tunnel, you choose the aggressive mode (see Figure 2-61 on page 80) and the key ID as the identifier.


Key Management Tunnel Properties @ august

Local endpoint for tunnel

Host identity type: IPv4 address

Host identity: 9.24.105.34

IP address (dot decimal):

Remote endpoint for tunnel

Host identity type: key identifier

Host identity: dhcp

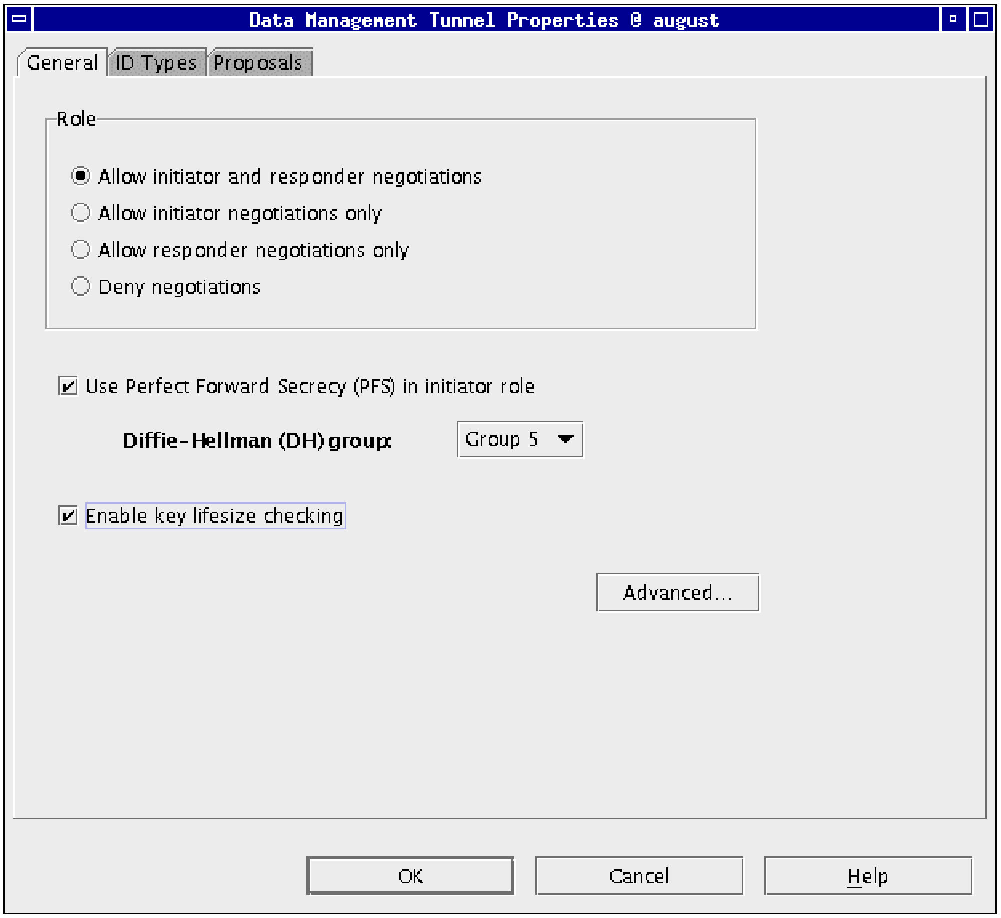
IP address (dot decimal):

Pre-shared key: test

Figure 2-65 Identification for AIX with a static IP address

You use preshared keys as shown in Figure 2-63 on page 82.

Then, in the phase 2 generic data tunnel, you configure a DH Group 5 as shown in Figure 2-66.


Data Management Tunnel Properties @ august

Role

● Allow initiator and responder negotiations
○ Allow initiator negotiations only
○ Allow responder negotiations only
○ Deny negotiations

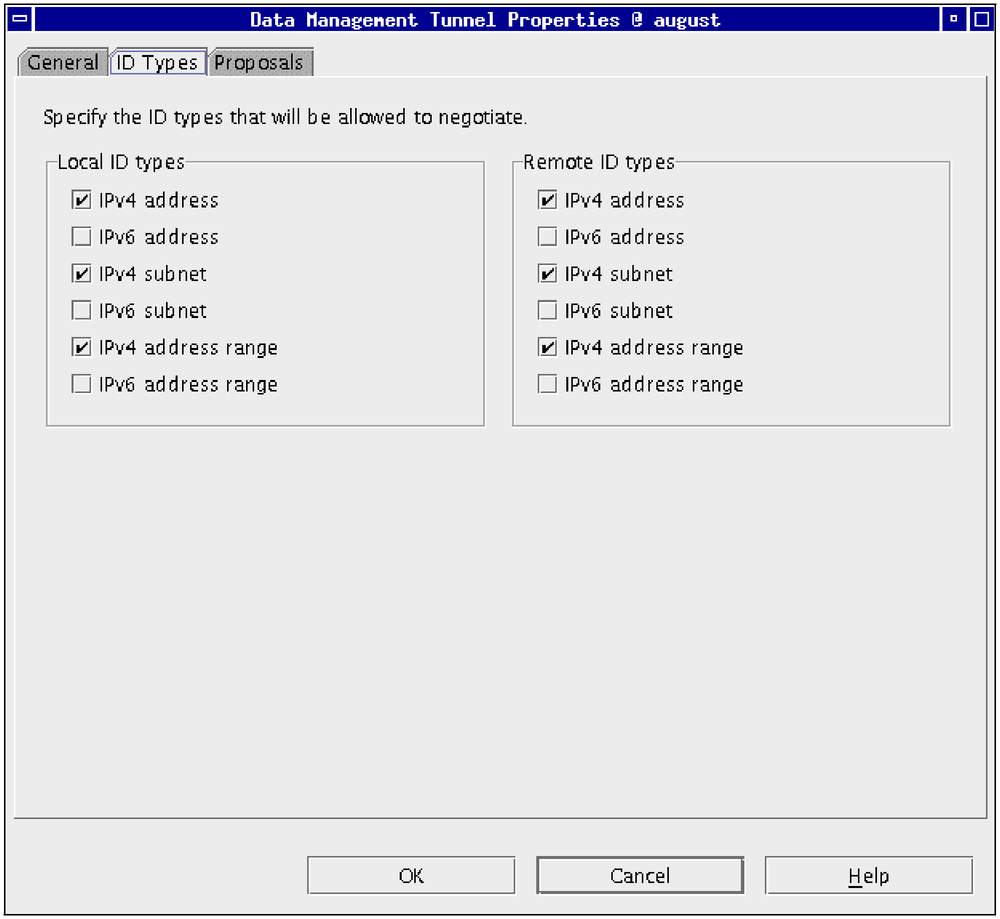
☑ Use Perfect Forward Secrecy (PFS) in initiator role

Diffie-Hellman (DH) group: Group 5

☑ Enable key lifesize checking

Figure 2-66 Selecting DH Group 5 for the generic tunnel

Select all the IP V4 types as shown in Figure 2-67. This generic tunnel is used to satisfy any incoming IPSec connection that matches the key ID identifier.



Specify the ID types that will be allowed to negotiate.

Local ID types

- ☑ IPv4 address
- □ IPv6 address
- ☑ IPv4 subnet
- □ IPv6 subnet
- ☑ IPv4 address range
- □ IPv6 address range

Remote ID types

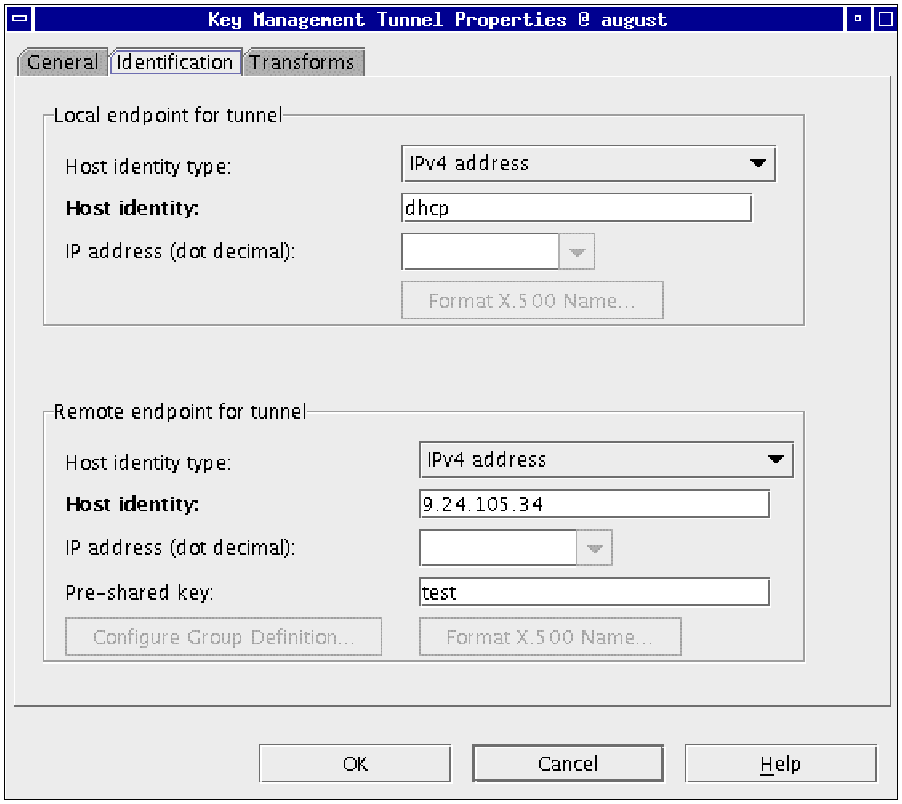
- ☑ IPv4 address
- □ IPv6 address
- ☑ IPv4 subnet
- □ IPv6 subnet
- ☑ IPv4 address range
- □ IPv6 address range

Figure 2-67 ID types for generic tunnel

As an example, configure one DHCP AIX client box. All client boxes are configured in the same way. For the General page configuration, see Figure 2-61 on page 80. For the Transforms page configuration, see Figure 2-63 on page 82.

You have to write the same key ID to use the generic data tunnel as you defined previously. See Figure 2-65 on page 84.

Figure 2-68 shows the Identification page for a DHCP client.



Key Management Tunnel Properties @ august

Local endpoint for tunnel

Host identity type: IPv4 address

Host identity: dhcp

IP address (dot decimal):

Remote endpoint for tunnel

Host identity type: IPv4 address

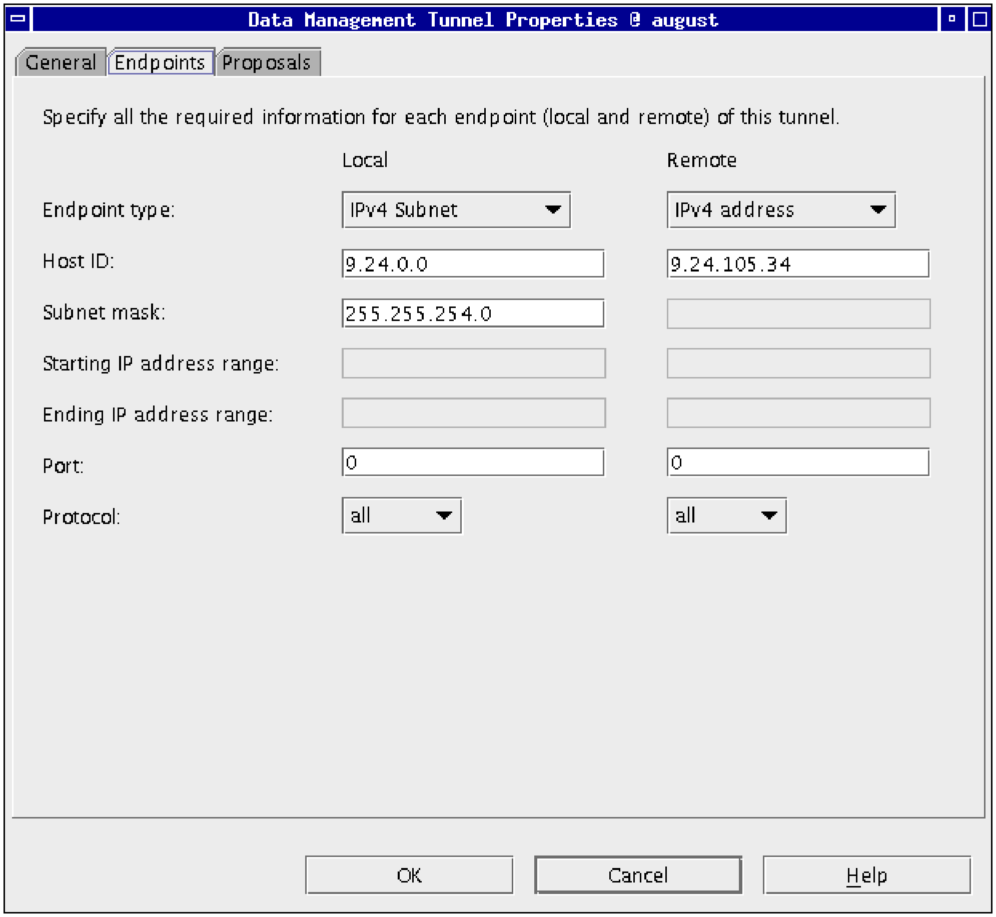
Host identity: 9.24.105.34

IP address (dot decimal):

Pre-shared key: test

Figure 2-68 Identification page for each DHCP client box

After this, define a standard data management tunnel with the options shown on the Endpoints page in Figure 2-69.



Specify all the required information for each endpoint (local and remote) of this tunnel.

	Local	Remote
Endpoint type:	IPv4 Subnet	IPv4 address
Host ID:	9.24.0.0	9.24.105.34
Subnet mask:	255.255.254.0	
Starting IP address range:		
Ending IP address range:		
Port:	0	0
Protocol:	all	all

Figure 2-69 Endpoints page for AIX DHCP clients

The subnet definition lets this box have any IP address, which is assigned by the DHCP server that belongs to a specific subnet. As an example, we show the tunnel output for these boxes.

Using the **`ike cmd=list numlist=2`** command from the AIX with the static IP address, you see:

```
# ike cmd=list numlist=2
Phase  Tun Id  Status      Local Id                         Remote Id
1      2       Active      9.24.105.34                      dhcp
```

Using the **ike cmd=list** command from the AIX DHCP clients, you see:

```
# ike cmd=list
Phase  Tun Id  Status      Local Id                        Remote Id
1      1       Active      dhcp                            9.24.105.34
2      1       Active      9.24.0.0/255.255.254.0          9.24.105.34
```

Important: You can activate a connection only from the DHCP clients.

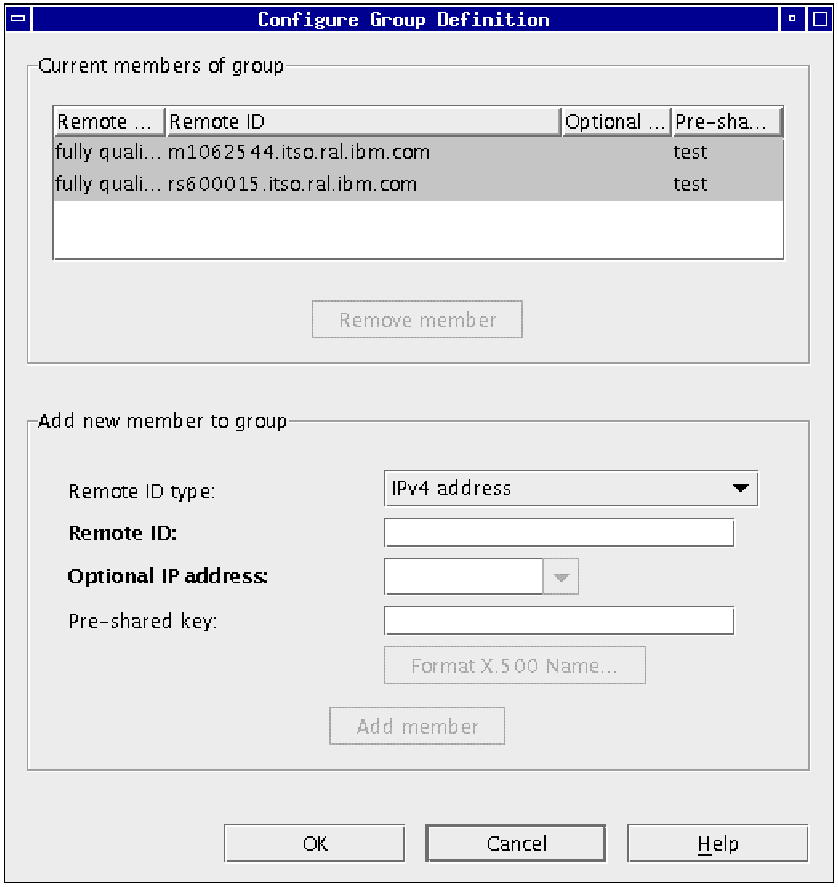
2.5.6 Scenario VI

Note: This scenario required a pre-release fix from IBM AIX development. This is a fix to the reported APAR IY47723. The final PTF release date was not yet announced at the time this redbook was published. This fix will be available as a patch and included in the next version of IBM AIX.

A customer has DHCP clients that want to connect to a host with static IP address. In this scenario, you use aggressive mode, preshared keys, and FQDN as the identifiers.

You must first configure the static IP address AIX box. You set up the phase 1 tunnel General page as shown in Figure 2-61 on page 80.

On the Identifier page, define a group definition for this configuration. Select **Group ID definition** for the remote location. Then add the fully qualified domain name. For the local identifier, select the **IPV4 address** format, as shown in Figure 2-70.



Current members of group

Remote ...	Remote ID	Optional ...	Pre-sha...
fully quali...	m106254 4.itso.ral.ibm.com		test
fully quali...	rs600015.itso.ral.ibm.com		test

Add new member to group

Remote ID type: IPv4 address

Remote ID:

Optional IP address:

Pre-shared key:

Figure 2-70 Group ID definition

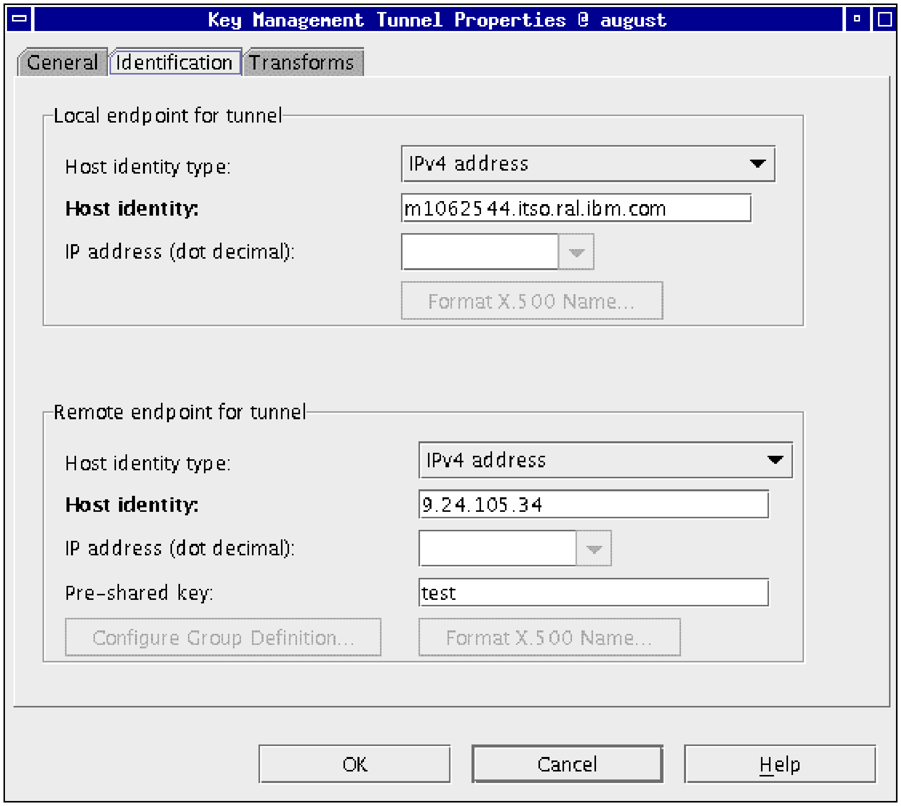
For the Transforms page settings, see Figure 2-63 on page 82.

Next, you need a generic data management tunnel. Set this up as shown in Figure 2-66 on page 85 and Figure 2-67 on page 86.

To configure a client DHCP box, set the mode to aggressive mode. See Figure 2-61 on page 80.

Then configure the endpoints as shown in Figure 2-71. For the Transforms page for the DHCP clients, see Figure 2-63 on page 82.

Important: You can activate a connection only from the DHCP clients.



Local endpoint for tunnel

Host identity type: IPv4 address

Host identity: m106254 4.itso.ral.ibm.com

IP address (dot decimal):

Remote endpoint for tunnel

Host identity type: IPv4 address

Host identity: 9.24.105.34

IP address (dot decimal):

Pre-shared key: test

Figure 2-71 Identification page for the clients

2.6 Differences and limitations

IP Security can offload encryption and security management task to adapters such as the IBM 10/100 Ethernet PCI Adapter II. This allows more network traffic to move through with less Central Processing Unit (CPU). See “Hardware acceleration” on page 16.

Internet Key Exchange is enhanced in this release to support a generic data management tunnel. When defined, this tunnel allows any address to match the generic tunnel definition. You can use it as long as security validation is successful in the key management negotiation phase. In addition, IKE supports Diffie-Hellman Group 5, which generates symmetric keys that are more secure than those generated by other DH groups.

The New System Management Interface Tool pages are available to support basic IKE functions and configurations. You can view, add, alter, delete, activate, deactivate, export, and import IKE tunnels. And you can back up, restore, and initialize the IKE database. And you can view the Document Type Definition using the View IKE DTD XML option.

There are two new ways to configure an IKE tunnel, through Web-based System Manager and the new **ikedb** command and its XML interface. Also IKE now uses the random number generator, the /dev/urandom AIX pseudo device, for random number generation.

Enhancements for Web-based System Manager include:

- IKE wizard access (common default values used in definitions)
- iKeman launch (digital certificates)
- Start and stop security
- Generic data management tunnels

Phase 2 tunnels now have a default policy that you can define using XML. See the /usr/samples/ipsec/default_p2_policy.xml file. Static filter description fields were also enhanced. For more information, see *AIX 5L Differences Guide Version 5.2 Edition*, SG24-5765*.*

There are two limitations that are related to NAT. First, it doesn't work with the AH protocol. Nor does it work with ESP with transport mode encapsulation because NAT has to inspect IP packets. And second, there is a similar problem with firewalls because they must also inspect IP packets. To solve both problems, using NAT and firewalls, you can use several tunnels. This way, NAT devices and firewalls do not inspect or alter IPSec packets.

2.7 Event and alert management

To log IPSec information, follow these steps:

1. Configure syslogd. You add the local4.debug rule to your /etc/syslog.conf file, create an empty file for syslog to write to, and restart the syslogd daemon, as shown in Example 2-12.

Example 2-12 Commands to log IPSec information with syslog

```
# cat “local4.debug /var/adm/ipsec.log” >> /etc/syslog.conf
# touch /var/adm/ipsec.log
# refresh -s syslogd
```

2. Turn on packet logging by entering the following command:

   ```
   smitty ps4_filter_log
   ```

3. Select **Start Filter Logging**.
4. Edit the /etc/isakmp.conf file and change *none* by isakmp_events to an initial value to understand the environment you configured through the reading of the logs. You see the filtering and tunneling information.
5. To activate logging, enter the following command:

   ```
   ike cmd=log
   ```

6. Test that the logging was activated. Enter the following command:

   ```
   ike cmd=list
   ```

   Then see the /var/adm/ipsec.log file.

After you activate a phase 1 tunnel, the contents of the /var/adm/ipsec.log file should look like Example 2-13.

Example 2-13 Contents of /var/adm/ipsec.log showing activation of phase 1 tunnel

```
14:19:13  0: TM is processing a Connection_request_msg
14:19:13  1: Creating new P1 tunnel object (tid)
14:19:13  1: TM is processing a P1_sa_created_msg (tid)
14:19:13  1:   Received good P1 SA, updating P1 tunnel (tid)
14:19:13  0: Checking to see if any P2 tunnels need to start
14:19:13  0: TM is processing a List_tunnels_msg
14:19:13  0: Cannot find tunnel context info associated with this tunnel id.
14:19:13  0: Cannot find this P2 tunnel from Tunnel Cache.
```

When both tunnels are activated for phase1 and phase 2, the contents of the /var/adm/ipsec.log file should look like Example 2-14.

Example 2-14 Contents of /var/adm/ipsec.log showing activation of both tunnels

```
16:03:55 0: TM is processing a Connection_request_msg
16:03:55 1: Creating new P1 tunnel object (tid)
16:03:55 1: Created blank P2 tunnel (tid)
16:03:55 1: TM is processing a P1_sa_created_msg (tid)
16:03:55 1:   Received good P1 SA, updating P1 tunnel (tid)
16:03:55 0: Checking to see if any P2 tunnels need to start
16:03:55 1: Starting negotiations for P2 (P2 tid)
16:03:55 0: TM is processing a P2_sa_created_msg
16:03:55 1: received p2_sa_created for an existing tunnel as initiator (tid)
16:03:55 1: Filter::AddFilterRules: Created filter rules for tunnel
```

```
16:04:09 0: TM is processing a List_tunnels_msg
16:28:19 0: TM is processing a P2_sa_removed_msg
16:28:20 0: TM is processing a P1_sa_removed_msg
```

After you activate the phase 2 tunnel, the rules associated with the tunnel should look like Example 2-15.

Example 2-15 Rules associated with the activated tunnel

```
*** Dynamic table ***
0:permit:0.0.0.0:0.0.0.0:0.0.0.0:0.0.0.0:no:udp:eq:500:eq:500:local:both:all
packets:0
1:permit:0.0.0.0:0.0.0.0:0.0.0.0:0.0.0.0:no:ah:any:0:any:0:both:inbound:all
packets:0
2:permit:0.0.0.0:0.0.0.0:0.0.0.0:0.0.0.0:no:esp:any:0:any:0:both:inbound:all
packets:0
3:permit:9.24.0.0:255.255.254.0:9.24.0.0:255.255.254.0:no:all:any:0:any:0:both:
outbound:all packets:IKE1
4:permit:9.24.0.0:255.255.254.0:9.24.0.0:255.255.254.0:no:all:any:0:any:0:both:
inbound:all packets:IKE1
```

See the IBM AIX 5L Version 5.2 product document *AIX 5L Version 5.2 Security Guide*, SC23-4860*.*

2.8 Common problems and solutions

This section discusses common problems you may have in your IPSec installation.

2.8.1 Activation failure of the tunnel

The cause of this problem is that IPSec is not loaded. The solution is to load it. See 2.3.3, “Starting IP Security” on page 25.

2.8.2 Pinging from a non-secure machine to a secured machine hangs

Your ping response looks like Example 2-16.

Example 2-16 Output of a failing ping command with 100% packet loss

```
PING rs615002.itso.ral.ibm.com: (9.24.105.118): 56 data bytes
----9.24.105.118 PING Statistics----
100 packets transmitted, 0 packets received, 100% packet loss
```

There may be two causes and solutions for this problem:

- **Cause 1**: IPSec V4 was configured to deny all non-secure packets.

  Solution 1: Do not deny all non-secure IP packets. See Figure 2-16 on page 25.

- **Cause 2**: The filter rules are not configured correctly.

  Solution 2: Reconfigure your filter rules. See 2.4.7, “Filtering through the System Management Interface Tool” on page 60.

2.8.3 Cannot ping from a secured machine to a non-secure machine

Your ping response looks like Example 2-17.

Example 2-17 Output of a failing ping command with a -1 return code

```
PING rs600015.itso.ral.ibm.com: (9.24.105.85): 56 data bytes
ping: wrote 9.24.105.85 64 chars, ret=-1
ping: wrote 9.24.105.85 64 chars, ret=-1
ping: wrote 9.24.105.85 64 chars, ret=-1
ping: wrote 9.24.105.85 64 chars, ret=-1
ping: wrote 9.24.105.85 64 chars, ret=-1

----9.24.105.85 PING Statistics----
5 packets transmitted, 0 packets received, 100% packet loss
n.
0821-069 ping: sendto: The file access permissions do not allow the specified
action.
```

There may be two causes and solutions for this problem:

- **Cause 1**: The IPSec V4 was configured to deny all non-secure packets. See Figure 2-16 on page 25.

  Solution 1: Do not deny all non-secure IP packets.

- **Cause 2**: The filter rules are not configured correctly.

  Solution 2: Reconfigure your filter rules. See 2.4.7, “Filtering through the System Management Interface Tool” on page 60.

2.8.4 Network address translation doesn’t work in IPSec environments

There may be two causes and solutions for this problem:

- **Cause1**: If you are in tunnel mode with AH, then you are using only one tunnel between the two ends.

  Solution 1: Evaluate the possibility of changing AH by ESP. See 2.2.6, “Encapsulating Security Payloads” on page 9, and 2.2.7, “Authentication Header” on page 10.

- **Cause 2**: If you are in transport mode, NAT does not work.

  Solution 2: NAT devices should not receive IPSec packets. See 2.2.6, “Encapsulating Security Payloads” on page 9, and 2.2.7, “Authentication Header” on page 10.

2.8.5 Firewall doesn’t work in IPSec environments

The cause for this problem is that the firewall needs to inspect IP packets. Firewalls should not inspect IPSec packets. The solution is to use more than one tunnel. See 2.6, “Differences and limitations” on page 91.

2.8.6 Cannot connect two machines where tunnels used to be active

There may be two causes and solutions for this problem:

- **Cause 1**: A static filter rule is avoiding the connection.

  Solution 1: Change or delete the rule.

- **Cause 2**: An autogenerated filter rule is avoiding the connection. You can see it when you enter the **`lsfilt -d`** command.

  Solution 2: Use the `-f` option (force option) for **`rmfilt`** command when the tunnel is down.

2.8.7 Both tunnels activated but there is no active/negotiating in the IKE tunnel monitor

The cause for this problem is that both tunnels were configured as *Allow responder negotiations only* or as *Deny negotiation*. The solution is to correct the configuration on one or both tunnels.

2.8.8 Can no longer connect from a non-secure machine to a secure machine with the tunnel active

To determine the cause for this problem, see if you have a phase 2 tunnel active. With phase 2 tunnel active, filtering rules are also active.

In this case, if you can, deactivate phase 2 tunnel by entering the following command or using Web-based System Manager:

```
ike cmd=remove phase=2,namelist=<DM tunnel name>
```

Then ping again. If this doesn't solve the problem, you have problems with the static filtering rules, in which case you must inspect them. Or you an autogenerated rule is blocking. See 2.8.6, "Cannot connect two machines where tunnels used to be active" on page 96.

If you cannot deactivate phase 2 tunnels, inspect all filtering rules using the **lsfilt -a** command.

2.8.9 IP security started but IKE command does not work

The cause for this problem is that some daemons are not active. You can see the IKE daemon status using the **lssrc -g ike** command as shown in Example 2-18.

Example 2-18 Output of the lssrc -g ike command

```
# lssrc -g ike
Subsystem         Group            PID          Status
 tmd              ike              2596         inoperative
 isakmpd          ike              16758        inoperative
 cpsd             ike                           inoperative
```

To correct this problem, start IP V4, IP V6, and run **/etc/rc.ike**. See 2.3.3, "Starting IP Security" on page 25. You should receive the state of the tunnels or a message indicating that there is no tunnel through the **ike cmd=list** command. You can start IP Security through Web-based System Manager, which is easier.

2.8.10 isakmpd is not running

In this case, you review the ipsec.log, as shown in Example 2-19, and search for any errors.

Example 2-19 Output of the ipsec.log file

```
not active....aborting.
Jul 29 11:36:23 rs600015 isakmpd:
/usr/sbin/isakmpd:/usr/sbin/isakmpd:isakmpd:initcrypto dlopen of des failed
Jul 29 11:36:23 rs600015 isakmpd: isakmpdError number = 2
Jul 29 11:36:23 rs600015 isakmpd: isakmpdError from dlerror =No such file or
directory
Jul 29 11:36:23 rs600015 isakmpd: error: reading from logpipe failed with
return code -1: Bad file number
```

To correct this error, you must update or install the *bos-crypto.priv* fileset. See 2.3.1, “Installing the IP Security feature” on page 19.

2.8.11 The IKE subsystem group is inoperative

This problem occurs when IP V4, IP V6, or both are not loaded. You correct this problem by loading both versions. Then start the IKE subsystem group using **`/etc/rc.ike`** or through the Web-based System Manager. See 2.8.9, “IP security started but IKE command does not work” on page 97.

2.8.12 Tunnels are in a dormant state after running ike cmd=activate

This problem occurs when the link has not been used yet. Simply use ping or another command to activate the link.

2.8.13 Editing tunnel information with Web-based System Manager panels differs from ike cmd=list db verbose

Web-based System Manager has some known problems. To correct this problem, close Web-based System Manager and open it again to bypass the problems.

2.8.14 Cannot activate a tunnel because the remote ID is invalid

You see the “`Remote ID is not a valid address`” message when you enter the **`ike cmd=active phase=1 namelist=test`** command, as shown in Example 2-20.

Example 2-20 Output of the ike cmd=active phase=1 namelist=test command

```
# ike cmd=activate phase=1 namelist=test
Remote id is not a valid address.
```

The remote identifier is not a static IP address. To solve this problem, activate the tunnel from the other side.

2.8.15 General procedure to obtain the cause of problems

To learn the cause of problems, follow these steps:

1. Deactivate all tunnels by entering the following command:

   ```
   #ike cmd=remove all
   ```

2. Stop IPSec V4 and V6, as well as each IKE daemon:

   ```
   #stopsrc -s tmd
   #stopsrc -s isakmpd
   ```

3. Initialize the IKE database by entering the following command:

   ```
   smitty ips4_advanced
   ```

4. Start IPSec V4 and V6, and the IKE daemons by entering the following command:

   ```
   /etc/rc.ike
   ```

5. Configure your tunnel again.
6. If you have a tunnel that is working between two machines, export them, and change the IP addresses in the XML file. After you initialize the IKE database, import the file into each machine (remember to change the IP address). Then activate tunneling as you do for the other pair of machines.

If you still have problems, read the ipsec.log file and try to find some data to detect the cause.

For more information about problem determination, see the IBM AIX 5L Version 5.2 product document *AIX 5L Version 5.2 Security Guide*, SC23-4860*.*

3

Exploiting Network Authentication Service

This chapter discusses IBM Network Authentication Service Version 1.3 for AIX. You use it for integrated login and system access with secure remote commands (RCMDs) on AIX 5.2.

3.1 Architecture

IBM includes the IBM Network Authentication Service Version 1.3 for AIX with AIX 5L Version 5.2 in the *AIX 5L for POWER V 5.2 Expansion Pack* CD, LCD4-1142. It allows for a secure single signon (SSO) implementation allowing users to sign on to one system to receive Kerberos credentials. Then they can access other systems or applications without needing to enter their password again.

The Network Authentication Service product is a Kerberos implementation. It is based on the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1510 standards protocol for the Kerberos Version 5 Network Authentication Service.

3.1.1 Recommended reading

There are some good references in other recent IBM Redbooks. In particular, you should refer to:

- *AIX 5L Differences Guide Version 5.2 Edition*, SG24-5765
- *AIX and Linux Interoperabilty*, SG24-6622

The Kerberos product was originally implemented and available for various open systems from Massachusetts Institute of Technology (MIT). You can learn more on the following Web site. This site includes documentation and tutorials to provide a better understanding of the protocol and source code availability for interested developers.

http://web.mit.edu/kerberos/

You should also consult IETF RFC 1510, which is available on the Web at:

http://www.ietf.org/rfc/rfc1510

Product documentation for Network Authentication Service is included in the krb5.doc.$LANG.html and krb5.doc.$LANG.pdf filesets. The filesets are located on the *AIX 5L for POWER V 5.2 Expansion Pack CD*, LCD4-1142. These filesets install the product documentation below the /usr/lpp/krb5/doc/ directory. Here you can find *IBM Network Authentication Service Version 1.3: Administrator's and User's Guide* and *IBM Network Authentication Service Version 1.3: Application Development Reference* both in PDF and HTML formats.

In the AIX documentation, there are two main references. AIX 5L introduced a *security guide*, which is a great starting point for all aspects of Security. It includes a section on Kerberos. Also the *commands reference* covers many of the commands used. You can use the search tool to find and review these documents on the AIX 5L POWER 5.2 documentation CD or locate them on the Web at:

http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/aix52.htm

3.1.2 Ease-of-use example

Having a user and administrator with one password to access many systems in the same environment is not only logical, but convenient. In Example 3-1, user *eddie* logs into in to the *nassrv* system. The user automatically obtains the available Kerberos credentials. Then, the user uses the secure RCMD, **rsh**, to run the **date** command, and uses the **rlogin** command to login to the *nascli* system, without re-entering a password.

The commands that are invoked use Network Authentication Service, with the Kerberos Version 5 protocol. This securely authenticates with the other system as required, transparently to the user.

Example 3-1 Using Kerberos

```
AIX Version 5
(C) Copyrights by IBM and by others 1982, 2002.
login: eddie
eddie's Password:
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 5.2!                                                *
*                                                                             *
*                                                                             *
*  Please see the README file in /usr/lpp/bos for information pertinent to    *
*  this release of the AIX Operating System.                                  *
*                                                                             *
*                                                                             *
*******************************************************************************

nassrv$ rsh nascli date
Thu Jul 24 09:42:46 EDT 2003

nassrv$ rlogin nascli
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 5.2!                                                *
*                                                                             *
*                                                                             *
*  Please see the README file in /usr/lpp/bos for information pertinent to   *
*  this release of the AIX Operating System.                                  *
*                                                                             *
*                                                                             *
*******************************************************************************
Last login: Wed Jul 23 14:41:09 EDT 2003 on /dev/pts/1 from nassrv.sgc.com

nascli$ exit

nassrv#
```

3.2 Security

The Kerberos Version 5 protocol used by IBM Network Authentication Service Version 1.3 for AIX provides a secure system to authenticate *principals* (users and services) to each other. Strong encryption and cunning processes were developed, implemented, and time tested to allow this.

The tutorial *Designing an Authentication System: A Dialogue in Four Scenes* by Bill Bryant provides an entertaining description of the process. You can find this tutorial on the Web at:

http://web.mit.edu/kerberos/www/dialogue.html

Kerberos is one of the most secure authentication systems. Like other authentication models, when user information is stored in a single place, using single signon authentication introduces the same weaknesses. The Kerberos master database and application servers’ key tables are sensitive information, which should only be readable as required.

All servers hosting Network Authentication Service data should have limited access and be physically secure. When using Network Authentication Service files for storage, this means any Key Distribution Center (KDC) server. If using Lightweight Directory Access Protocol (LDAP) for storage, this means the LDAP server or servers.

The key table files must be present on all hosts that offer “Kerberized” services. These files must also be protected from unauthorized access.

3.3 Installation example

This section demonstrates a valid implementation that allows automatic initialization at user login to obtain the credentials to use the Kerberos Version 5 protocol. It also demonstrates a system configuration that allows the use of the secure RCMDs included with IBM AIX 5L Version 5.2. While additional features and uses may exist for consideration in implementation, this simple scenario helps you to quickly understand the potential of the product.

The purpose of this scenario is to demonstrate the ability of IBM AIX 5L Version 5.2 to exploit the IBM Network Authentication Service Version 1.3 for AIX functionality rather than to demonstrate Network Authentication Service itself.

3.3.1 Planning

Planning is an important part of a smooth product introduction. For detailed planning information, see Chapter 2 in the *Administrator's and Users Guide*. You can find this guide on the *IBM AIX 5L Expansion Pack CD*, LCD4-1142.

For the purposes of this scenario, you need to plan a realm. In this example, the realm NASREALM.SGC.COM, within the sgc.com domain, consists of a server system *nassrv* and client system *nascli*. You do not need any slave servers although we recommend that you use them in a production environment.

In this scenario, you use the files database rather than LDAP, for simplicity, and without a Distributed Computing Environment (DCE) or service discovery. You use Kerberos for AIX user management and allow full use of the AIX secure RCMDs.

See the IBM Network Authentication Service documentation available on the expansion pack CD for details about these optional Network Authentication Service facilities.

3.3.2 Installation

Use the System Management Interface Tool (SMIT) or the command line utility, **installp**, to install the krb5.server.rte fileset from the AIX 5L for POWER V5.2 Expansion Pack. The client fileset is a prerequisite for the server fileset and is automatically installed. Example 3-2 shows the package filesets.

Example 3-2 Network Authentication Service filesets

```
nassrv# lslpp -l krb5*
Fileset                      Level  State      Description
----------------------------------------------------------------------------
th: /usr/lib/objrepos
krb5.client.rte            1.3.0.0  COMMITTED  Network Authentication Service
                                               Client
```

```
krb5.client.samples        1.3.0.0  COMMITTED  Network Authentication Service
                                               Samples
krb5.doc.en_US.html        1.3.0.0  COMMITTED  Network Auth Service HTML
                                               Documentation - U.S. English
krb5.doc.en_US.pdf         1.3.0.0  COMMITTED  Network Auth Service PDF
                                               Documentation - U.S. English
krb5.msg.en_US.client.rte  1.3.0.0  COMMITTED  Network Auth Service Client
                                               Msgs - U.S. English
krb5.server.rte            1.3.0.0  COMMITTED  Network Authentication Service
                                               Server
krb5.toolkit.adt           1.3.0.0  COMMITTED  Network Authentication Service
                                               App. Dev. Toolkit
```

Various versions of the doc and msg filesets are available for other languages.

As a minimum, you need to install the krb5.server.rte fileset with its requisites on a server and krb5.client.rte on a client system.

For new system installations, you can install the Network Authentication Service Kerberos client software as an installation option. From the main installation menu Welcome to Base Operating System Installation and Maintenance, select **Change/Show Installation Settings and Install-> More Options-> Install More Software-> Kerberos_5**.

3.3.3 Configuring the server

You can set up the server using the **config.krb5** utility. This utility is the native method as part of the Network Authentication Service product. Or in IBM AIX 5L, you can use the **mkkrb5srv** command, which calls the **config.krb5** utility and performs some additional steps. For this scenario, the simplest method is to use the **mkkrb5srv** command.

Use the **mkkrb5srv** command with the following basic options to configure the Kerberos server:

- **-r**: This indicates the realm name or logical group name for systems that will user the service.
- **-s**: This is for the host name with fully qualified domain name (FQDN) of the server system on which you are installing.
- **-d**: This indicates is the domain name.

You need to substitute your own realm, server, and domain information. As in Example 3-3, you must enter a database master password and the password for the admin/admin@NASREALM.SGC.COM principal. Make a note of these passwords for later use.

Example 3-3 Output of the mkkrb5srv command

```
nassrv# mkkrb5srv -r NASREALM.SGC.COM -s nassrv.sgc.com -d sgc.com
Fileset                      Level  State      Description
  ----------------------------------------------------------------------------
Path: /usr/lib/objrepos
  krb5.server.rte            1.3.0.0  COMMITTED  Network Authentication Service
                                                 Server

Path: /etc/objrepos
  krb5.server.rte            1.3.0.0  COMMITTED  Network Authentication Service
                                                 Server
The -s option is not supported.
The administration server will be the local host.
Initializing configuration...
Creating /etc/krb5/krb5.conf...
Creating /var/krb5/krb5kdc/kdc.conf...
Creating database files...
Initializing database '/var/krb5/krb5kdc/principal' for realm
'NASREALM.SGC.COM'
master key name 'K/M@NASREALM.SGC.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter database Master Password:
Re-enter database Master Password to verify:
WARNING: no policy specified for admin/admin@NASREALM.SGC.COM;
  defaulting to no policy. Note that policy may be overridden by
  ACL restrictions.
Enter password for principal "admin/admin@NASREALM.SGC.COM":
Re-enter password for principal "admin/admin@NASREALM.SGC.COM":
Principal "admin/admin@NASREALM.SGC.COM" created.
Creating keytable...
Creating /var/krb5/krb5kdc/kadm5.acl...
Starting krb5kdc...
krb5kdc was started successfully.
Starting kadmind...
kadmind was started successfully.
The command completed successfully.
Restarting kadmind and krb5kdc
```

As you can see from the script output, various tasks were completed. Let’s look at some of the tasks.

The krb5.conf file is created as shown in Example 3-4. It was created with default general information entries for the realm, including various logs that you can use to review problems.

Example 3-4 Example krb5.conf file

```
nassrv# pr /etc/krb5/krb5.conf
[libdefaults]
        default_realm = NASREALM.SGC.COM
        default_keytab_name = FILE:/etc/krb5/krb5.keytab
        default_tkt_enctypes = des3-cbc-sha1 des-cbc-md5 des-cbc-crc
        default_tgs_enctypes = des3-cbc-sha1 des-cbc-md5 des-cbc-crc

[realms]
        NASREALM.SGC.COM = {
                kdc = nassrv.sgc.com:88
                admin_server = nassrv.sgc.com:749
                default_domain = sgc.com
        }

[domain_realm]
        .sgc.com = NASREALM.SGC.COM
        nassrv.sgc.com = NASREALM.SGC.COM

[logging]
        kdc = FILE:/var/krb5/log/krb5kdc.log
        admin_server = FILE:/var/krb5/log/kadmin.log
        default = FILE:/var/krb5/log/krb5lib.log
```

In Example 3-5, the kdc.conf file lists information used by the servers to start the realm.

Example 3-5 Example kdc.conf file

```
nassrv# pr /var/krb5/krb5kdc/kdc.conf
[kdcdefaults]
        kdc_ports = 88

[realms]
   NASREALM.SGC.COM =  {
      database_name = /var/krb5/krb5kdc/principal
      admin_keytab = /var/krb5/krb5kdc/kadm5.keytab
      acl_file = /var/krb5/krb5kdc/kadm5.acl
      dict_file = /var/krb5/krb5kdc/kadm5.dict
      key_stash_file = /var/krb5/krb5kdc/.k5.NASREALM.SGC.COM
      kadmind_port = 749
      kdc_ports = 88
      max_life = 10h 0m 0s
      max_renewable_life = 7d 0h 0m 0s
      master_key_type = des-cbc-crc
```

```
        supported_enctypes = des3-cbc-sha1:normal des-cbc-md5:normal
        des-cbc-crc:normal
        kdc_supported_enctypes = des3-cbc-sha1:normal des-cbc-md5:normal
        des-cbc-crc:normal
    }
```

The kadm5.acl file provides access control information for the administration server. Basically, it lists principals and their access levels. As shown in Example 3-6, the access levels use a ***** wildcard to indicate all privileges and **i** for inquiry.

Example 3-6 Example kadm5.acl file

```
nassrv# pr /var/krb5/krb5kdc/kadm5.acl
admin/admin@NASREALM.SGC.COM        *
root/*@NASREALM.SGC.COM        *
host/*@NASREALM.SGC.COM        i
```

You can also see the Kerberos server processes running, as shown in Example 3-7. These processes are **krb5kdc**, on the Key Distribution Center, and **kadmind**, on the administration server.

Example 3-7 Kerberos processes

```
nassrv# ps -ef | grep krb5
    root 15514     1   0 09:34:25      -  0:00 /usr/krb5/sbin/krb5kdc
    root 16100     1   0 09:34:25      -  0:00 /usr/krb5/sbin/kadmind
```

3.3.4 Configuring the client

For this scenario, you also configure the server as a client. The implications of adding users and giving them access to the Kerberos server is normally not done for security reasons. In any centralized user management scenario, it is important to secure the systems that are holding sensitive information. This includes the master and slave KDC.

Configure the Network Authentication Service client on the server system using the following options:

- **-r**: Use this option to indicate the realm name or logical group name for the systems that will user the service.
- **-c**: Use this option for the KDC server since testing the server and client can be the same.

- **-s**: Use this option for the Kerberos server since testing the server and client can be the same.
- **-d**: Use this option to indicate the domain name.
- **-A**: This this option to add root as an administrator.
- **-i**: This option indicates to set up for integrated login.
- **-K**: Use Kerberos at the default authentication method.
- **-T**: Use this option to acquire a server admin ticket granting ticket.

You must substitute your own realm, server, and domain information. As in Example 3-8, you are prompted to enter the admin/admin@NASREALM.SGC.COM principal's password. In a secure setup, we recommend that you do not configure the client on the Kerberos server.

Example 3-8 Output of the mkkrb5clnt command

```
nassrv# mkkrb5clnt -r NASREALM.SGC.COM -c nassrv.sgc.com -s nassrv.sgc.com -d
sgc.com -A -i files -K -T
/etc/krb5/krb5.conf file already exists
Password for admin/admin@NASREALM.SGC.COM:
Configuring fully integrated login
Authenticating as principal admin/admin with existing credentials.
WARNING: no policy specified for host/nassrv@NASREALM.SGC.COM;
  defaulting to no policy. Note that policy may be overridden by
  ACL restrictions.
Principal "host/nassrv.sgc.com@NASREALM.SGC.COM" created.

Administration credentials NOT DESTROYED.
Authenticating as principal admin/admin with existing credentials.

Administration credentials NOT DESTROYED.
Authenticating as principal admin/admin with existing credentials.
Principal "kadmin/admin@NASREALM.SGC.COM" modified.

Administration credentials NOT DESTROYED.
Configuring Kerberos as the default authentication scheme
Making root a Kerberos administrator
Authenticating as principal admin/admin with existing credentials.
WARNING: no policy specified for root/nassrv@NASREALM.SGC.COM;
  defaulting to no policy. Note that policy may be overridden by
  ACL restrictions.
Enter password for principal "root/nassrv.sgc.com@NASREALM.SGC.COM":
Re-enter password for principal "root/nassrv.sgc.com@NASREALM.SGC.COM":
Principal "root/nassrv.sgc.com@NASREALM.SGC.COM" created.

Administration credentials NOT DESTROYED.
Cleaning administrator credentials and exiting.
```

3.3.5 Creating the keytab file

Keytab files hold a list of available keys. While the previous processes created some specific files, you need to build one at /etc/krb5/krb5.keytab. To simplify maintenance of the keytab file, we recommend that you link the /var/krb5/security/keytab/hostname.keytab file to /etc/krb5/krb5.keytab, as shown here:

```
nassrv# ln -s /var/krb5/security/keytab/nassrv.sgc.com /etc/krb5/krb5.keytab
```

In a production situation, you may have multiple keytab files for users or services. In this case, you can use the KRB5_KTNAME environment variable to override the default_keytab_name in the krb5.conf file. The file is created in the /var/krb5/security/keytab directory using the server and domain information when you run the **mkkrb5clnt** command.

3.3.6 Kerberos administration

The client setup adds the host and root principals for the client system. You can review the full list of principals on the master server using the **kadmin.local** utility as shown in Example 3-9. For this example, you must add the File Transfer Protocol (FTP) principal for each host system, so use the **add_principal** command.

Example 3-9 list_principals in kadmin.local

```
nassrv# /usr/krb5/sbin/kadmin.local

kadmin.local:  list_principals
K/M@NASREALM.SGC.COM
admin/admin@NASREALM.SGC.COM
host/nassrv.sgc.com@NASREALM.SGC.COM
kadmin/admin@NASREALM.SGC.COM
kadmin/changepw@NASREALM.SGC.COM
kadmin/history@NASREALM.SGC.COM
krbtgt/NASREALM.SGC.COM@NASREALM.SGC.COM
root/nassrv.sgc.com@NASREALM.SGC.COM

kadmin.local:  add_principal -randkey ftp/nassrv.sgc.com
WARNING: no policy specified for ftp/nassrv.sgc.com@NASREALM.SGC.COM;
  defaulting to no policy. Note that policy may be overridden by
  ACL restrictions.
Principal "ftp/nassrv.sgc.com@NASREALM.SGC.COM" created.

kadmin.local:  ktadd ftp/nassrv.sgc.com
```

```
Entry for principal ftp/nassrv with kvno 3, encryption type Triple DES cbc mode
with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal ftp/nassrv with kvno 3, encryption type DES cbc mode with
RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.

kadmin.local:  quit
```

3.3.7 Changing authentication methods to allow Kerberos

For the secure RCMDS to accept the Kerberos Version 5 protocol as an authentication method, the root user must allow `-k5` as a valid method. As shown in Example 3-10, the standard method is kept for root access and as a backup.

First you list the current authentication method, then list the options for **`chauthent`**, change the authentication methods to `-k5 -std`, and then list the options again. Note if you try to use an invalid option, such as `-k4` on a non-SP system or `-k5` before you install krb.client.rte, you obtain more information about the various methods.

Example 3-10 Authentication methods

```
nassrv# lsauthent
Standard Aix

nassrv# chauthent ?
Usage: chauthent [-k5] [-k4] [-std]

nassrv# chauthent -k5 -std

nassrv# lsauthent
Kerberos 5
Standard Aix

nassrv# chauthent -k4
Kerberos 4 permitted on SP system only.
Kerberos 5_DCE requires DCE version 3.2 or greater.
Kerberos 4, Kerberos 5_DCE and Kerberos 5 require krb5.client.rte version 1.3.
```

3.3.8 Obtaining Kerberos authentication for administration

To use the **`kinit`** program as root, you must enter the admin/admin@REALM principal's password. First check to see whether you have any tickets using **`klist`**. Next use **`kinit`** to get an initial ticket. As shown in Example 3-11, `krbtgt` is a special Kerberos Ticket Granting Ticket that allows you to obtain additional tickets.

Example 3-11 admin credentials

```
nassrv# /usr/krb5/bin/klist
Unable to get cache name (ticket cache: /var/krb5/security/creds/krb5cc_0).
       Status 0x96c73ac3 - No credentials cache found.

nassrv# /usr/krb5/bin/kinit admin/admin
Password for admin/admin@NASREALM.SGC.COM:

nassrv# /usr/krb5/bin/klist
Ticket cache:  FILE:/var/krb5/security/creds/krb5cc_0
Default principal:  admin/admin@NASREALM.SGC.COM

Valid starting     Expires            Service principal
08/07/03 13:46:40  08/07/03 23:46:38  krbtgt/NASREALM.SGC.COM@NASREALM.SGC.COM
```

3.3.9 Creating a test user

As a root with Kerberos administration, create an AIX user using the **-R KRB5files** option to create the user in AIX. Then add the user as a Kerberos Principal and set the users initial password. See Example 3-12.

Example 3-12 The mkuser command

```
nassrv# mkuser -R KRB5files eddie

nassrv# passwd -R KRB5files eddie
Changing password for "eddie"
eddie's New password:
Enter the new password again:
```

3.3.10 Testing the user and services

If all is working correctly, you can log in using a password stored by Kerberos, and gain the credentials to use **rlogin**, **rsh**, **rcp**, **telnet**, and **ftp** on the same system without re-entering a password.

In Example 3-13, user *eddie* logs in to a Network Authentication Service client. In this case, *nassrv* is both the client and server. With the integrated login, *eddie* obtains a `krbtgt` Ticket Granting Ticket, as you can see, using the **`klist`** command. When the user uses Network Authentication Service to access a “Kerberized” service, such as **`rsh`**, an additional host ticket is given.

Example 3-13 Using Kerberos

```
nassrv# login eddie
eddie's Password:

nassrv$ /usr/krb5/bin/klist
Ticket cache:  FILE:/var/krb5/security/creds/krb5cc_eddie@NASREALM.SGC.COM_203
Default principal:  eddie@NASREALM.SGC.COM

Valid starting     Expires            Service principal
08/08/03 09:51:34  08/08/03 17:51:34  krbtgt/NASREALM.SGC.COM@NASREALM.SGC.COM
08/08/03 09:51:34  08/08/03 12:51:34  kadmin/admin@NASREALM.SGC.COM

nassrv$ rsh nassrv date
Fri Jul 18 15:52:32 EDT 2003

nassrv$ /usr/krb5/bin/klist
Ticket cache:  FILE:/var/krb5/security/creds/krb5cc_eddie@NASREALM.SGC.COM_203
Default principal:  eddie@NASREALM.SGC.COM

Valid starting     Expires            Service principal
08/08/03 09:51:34  08/08/03 17:51:34  krbtgt/NASREALM.SGC.COM@NASREALM.SGC.COM
08/08/03 09:51:34  08/08/03 12:51:34  kadmin/admin@NASREALM.SGC.COM
08/08/03 09:53:02  08/08/03 17:51:34  host/nassrv.sgc.com@NASREALM.SGC.COM
```

3.3.11 Configuring another client system

After you set up your server system, you can add additional clients to the realm. As shown in Example 3-14, you follow most of the steps from the previous section. But this time, you ensure that time is synchronized across the realm.

The Kerberos tickets are time sensitive, so you must keep the time and date on each system very close. We recommend that you use **`timed`** or **`ntp`** to achieve this. This is of benefit to all system services.

Install the krb5.client.rte fileset. You must substitute your own realm, server, and domain information. Remember that `-c` is the KDC server, not the client, so this is your Kerberos server.

Example 3-14   Stand-alone client setup

```
nascli# mkkrb5clnt -r NASREALM.SGC.COM -c nassrv.sgc.com -s nassrv.sgc.com -d
sgc.com -A -i files -K -T

nascli# chauthent -k5 -std

nascli# mkuser eddie

nascli# ln -s /var/krb5/security/keytab/nascli.sgc.com.keytab
/etc/krb5/krb5.keytab

nascli# kinit admin/admin

nascli# kadmin

kadmin: add_principal -randkey ftp/nascli.sgc.com

kadmin: ktadd ftp/nascli.sgc.com

kadmin: quit
```

3.3.12 Testing the user and services on the new host

If all is working correctly, you can log in using a password stored by Kerberos, and gain the credentials to use **rlogin**, **rsh**, **rcp**, **telnet**, and **ftp** on the same system without re-entering a password. Now you should be able to login to this new system, using the users Kerberos password, and use the secure remote commands (RCMDs) from another Kerberized system, as shown in Example 3-15.

Example 3-15   Testing the user and services

```
nascli# login eddie
eddie's Password:

nascli$ rsh nassrv date
Fri Jul 18 15:52:32 EDT 2003
```

3.4 Administration

Additional administration consists of maintaining users and groups using the `-R` flag or directly in Network Authentication Service where appropriate. Ensure that service principals are added for the realm and keytab files are created or distributed.

3.4.1 AIX

After a client system is configured to use the Kerberos Version 5 protocol for authentication, additional administration simply requires using the `-R` flag for normal administration tasks. We recommend that you implement some level of Enterprise Identity Mapping (EIM) to aid in this area. This is as simple as ensuring that the user ID (UID) for each user is unique and used across all systems in the organization.

Uninstall

The **`mkkrb5srv`** and **`mkkrb5clnt`** commands both support the `-U` option to uninstall Network Authentication Service.

3.4.2 Network Authentication Service

When systems and users are created using the **`mkkrb5clnt`** and **`mkuser -R`** commands, Network Authentication Service is updated. This means that most of the administration is completed for you. This includes creating some principals and keytab entries. Additional tasks, as shown in 3.3, “Installation example” on page 104, include adding users and the FTP service principal.

3.5 Functions

These functions are outside the scope of Network Authentication Service. However, they are key to the exploitation of Kerberos on AIX 5L Version 5.2.

3.5.1 Integrated login

In some Kerberos environments, users need to issue the **`kinit`** command to obtain their Ticket Granting Ticket. This is also a valid option in AIX. However, integrated login provides a seamless path from the AIX login to service access without user intervention.

As a user logs in, their password is authenticated by Kerberos to allow the AIX login. Also the user receives their Ticket Granting Ticket to use for other Kerberized services.

3.5.2 Secure remote commands

In AIX 5L Version 5.2, the secure RCMDs such as **rsh**, **rlogin**, **rcp**, **telnet**, and **ftp** are updated to allow open Kerberos authentication. In the past, Kerberos was allowed, but tied to the DCE or RS/6000 SP. These commands support the secure encrypted authentication provided by Kerberos. They also provide ease of use while ensuring the user's password is not passed in a readable form.

The commands also support *cross-realm authentication*. If the local realm is different from the remote realm, you can specify the -k realm command option. For details about configuring a cross-realm relationship, see the *Network Authentications Service Administrators and Users Guide*. This guide is available on the *IBM AIX 5L Expansion Pack CD*, LCD4-1142.

3.5.3 User management commands

You can perform Kerberos principal management using the **kadmin** program. For ease of integrating AIX into a Kerberized environment, the user and group management commands supporting the -R flag allow you to perform much of the Kerberos management from AIX.

The AIX user management commands that support the -R flag are **chfn**, **chgroup**, **chgrpmem**, **chsh**, **chuser**, **lsgroup**, **lsuser**, **mkgroup**, **mkuser**, **passwd**, **rmgroup**, and **rmuser**.

3.6 Differences and limitations

LDAP is another common tool used to centralize user information and user management. The key difference is that Kerberos provides your credentials for you. In LDAP, you have only one password, but you still need to enter it to access another system or application.

As we have seen, adding users to Kerberos does not appear to be a lengthy process. But consider adding 10, 100, or 1000 users at the same time.

While many AIX services support the Kerberos protocol, your key applications or other common utilities may not support the protocol. Many applications today support Pluggable Authentication Modules (PAM). You can use the **pam_krb** module to allow these applications to share in the Kerberos environment.

3.7 Event and alert management

As shown in Example 3-4 on page 108, logs are automatically setup through krb5.conf writing to various files. If you use syslog, you may also consider forwarding this information to syslog to allow further integration with your current logging and monitoring processes.

3.8 Common problems and solutions

The following checklist offers solutions to most problems. Gather support information to assist in faster problem resolution time if additional support is required.

3.8.1 Checklist

Many symptoms may relate to the same problem in setting up Network Authentication Service. Most problems come down to a few solutions.

Environment

Check your KRB5CCNAME and KRB5_KTNAME environment variables. The command string, **`env | grep KRB`**, shows the Kerberos variables.

Authentication

Check the valid authentication methods using the **`lsauthent`** command.

Configuration

Review your Network Authentication Service configuration. Primarily check the krb5.conf file.

Processes

Check whether the server processes are running. The command string, **`ps -ef | grep krb5`**, should show the **`krb5kdc`** and **`kadmind`** processes running. You should also check LDAP, if used. Check for any new core files, if processes are missing or have been restarted.

Filesystems

Check for full filesystems, in particular the logs normally located in the /var filesystem, which can grow very quickly. The database can become corrupted if the filesystem uses all available space while writing to the database. You should ensure that you have enough available space, or move the logs to another filesystem with more available space.

System time

Check the system time and time zone details. The symptoms will vary, so ensure that time between systems is in sync. We recommend that you deploy **`ntp`** or **`timed`** to implement time synchronization between all servers in a Kerberos realm.

Hostname resolution

Ensure that the fully qualified domain name is resolvable. You can do this using name resolution, such as DNS or in the local /etc/hosts file. The file, /etc/hosts, lists the systems as `ip.address hostname.FQDN hostname`, for example:

```
10.0.0.1   nassrv.sgc.com  nassrv
```

You can check the setup using the **`host`** ***`hostname`*** command, for example:

```
nassrv# host nassrv
nassrv.sgc.com is 10.0.0.1
```

Principals

The secure RCMDs use two principals, ftp for FTP and host for the others. The principals must exist for each service and server combination that you want to provide. Use **`kadmin`** or **`kadmin.local list_principals`**.

Keytab files

The keytab files, normally /etc/krb5/krb5.keytab, /etc/krb5.keytab, and /var/krb5/security/keytab/<hostname>.keytab, must be in the location where a service can look for them. Each keytab file exists for its own reason, but you may consider linking them together to ensure the right key is available for any service at each location. Review the available keys in the keytab file using the **`klist -k -e`** command.

Tickets

Review the users' tickets using the **`klist`** command (check using additional flags `-e`, `-a`, and `-f`). Primarily you need a current Ticket Granting Ticket. If you think there is a problem with your tickets, try destroying the tickets using the **`kdestroy`** command. Then get a new Ticket Granting Ticket using the **`kinit`** command.

3.8.2 Logs

Initial logging is sent to files in /var. You can refine them using syslog. The logs are useful for problem determination. Review them along with the other system logs syslog errpt and LDAP logs if used.

3.8.3 Typical problems

This section lists the typical problems that users experience when working with Network Authentication Service. The recommended solutions follow each problem.

Client not found in the Kerberos database

- Check the KDC log to see whether the principal name exists.
- If using LDAP, it may be that the LDAP server is down or has been restarted. Verify that the LDAP server is up and restart KDC.

Server not found in the Kerberos database

- See the previous notes for “Client not found in the Kerberos database”.
- Often a FQDN issue.

Cannot find KDC for requested realm

- Check krb5.conf.
- If you are using KDC discovery via LDAP, be sure unauthenticated users can read and search the domain components. To check this, use the **ksetup** command without specifying **bind dn** or password:

```
ksetup -h ldap-server.austin.ibm.com
ksetup> listkdc REALM.AUSTIN.IBM.COM
```

Cannot contact any KDC for requested realm

- Check krb5.conf to see if the correct servers are listed.
- Check whether the correct servers are listed in ksetup.
- The servers may be overloaded. Retry the request.

Preauthentication failed

- Check whether the password was mistyped.
- Check the clock skew.

Clock skew is too great

- Check and reset the clocks on the client and server machines.
- Use a time sync protocol such as the Network Time Protocol (NTP).

Ticket expired

- Obtain a fresh Ticket Granting Ticket using the **kinit** command.

KDC can’t fulfill the requested option

- Try to get a ticket option, such as a forwardable ticket, for a principal that doesn’t allow that option.

KDC has no support for the encryption type

- Check enctypes in krb5.conf on client, enctypes of client and server keys in the database (kadmin getprinc), and enctypes of tickets and session keys (klist -e).

No such file or directory

- An application server cannot find the keytab file.
- Application servers look for a keytab file here, from highest to lowest priority:
  - KRB5_ KTNAME environment variable
  - default_ keytab_ name in krb5.conf
  - /etc/ krb5/ krb5. keytab

Decrypt integrity check failed

- The key (password) used to decrypt ticket or message was incorrect.
- This is usually due to a local keytab file being out of sync with the database.
- Rerun the **`ktadd`** command on an application server machine.

Incorrect net address

- The IP address, from which a request came, does not match the address or addresses in the ticket.

Illegal cross-realm ticket

- Using the transitive cross-realm ticket and the application server doesn’t think the trust path is valid.
- Be sure the [capaths] stanza on all machines agree and are correct.

4

Pluggable Authentication Module

This chapter discusses the Pluggable Authentication Module (PAM) for AIX. PAM is used for authentication to various authentication services such as AIX and Lightweight Directory Access Protocol (LDAP).

4.1 Architecture

The PAM framework provides system administrators with the ability to incorporate multiple authentication mechanisms into an existing system. They do this using pluggable modules without changing application commands. They can plug applications that are enabled to use PAM into new technologies, without modifying the applications.

System administrators can use PAM to integrate an AIX login with other security mechanisms such as Distributed Computing Environment (DCE), LDAP, or Kerberos. They can also plug-in mechanisms for account, session, and password management using this framework.

PAM has emerged as the industry standard integrated login framework. The flexibility of PAM allows administrators to:

- Select any authentication service on the system for an application
- Use multiple authentication mechanisms for a given service
- Add new authentication service modules without modifying existing applications
- Use a previously entered password for authentication with multiple modules

4.1.1 PAM library

The PAM library, /usr/lib/pamlib.a, provides the PAM application programming interface (API) that serves as a common interface to all PAM applications. It also controls module loading. Modules are loaded by the PAM library, based on the stacking behavior defined in the /etc/pam.conf file.

4.1.2 PAM modules

PAM modules allow multiple authentication mechanisms to be used collectively or independently on a system. A given PAM module must implement at least one of four module types. More than one module type can be associated with each module. However, each module needs to manage at least one module type. The following sections describe each module type.

Authentication modules

These module authenticates users and sets, refreshes, or destroys credentials. They also identify users based on their authentication and credentials.

Account management modules

These modules determine the validity of the user account and subsequent access after identification from the authentication module. Checks performed by these modules typically include account expiration and password restrictions.

Session management modules

These modules initiate and terminate user sessions. Additionally, support for session auditing may be provided.

Password management modules

These modules perform password modification and related attribute management.

4.1.3 PAM configuration file

The /etc/pam.conf configuration file consists of service entries for each PAM module type and served to route services through a defined module path. Entries in the file are composed of the following white-space-delimited fields:

```
service_name module_type control_flag module_path module_options
```

Note the following explanation:

- **service_name**: Specifies the name of the service. The keyword OTHER is used to define the default module to use for applications not specified in an entry.
- **module_type**: Specifies the module type for the service. Valid module types are auth, account, session, and password.
- **control_flag**: Specifies the stacking behavior of the module. Supported control flags are required, sufficient, or optional.
- **module_path**: Specifies the path name to a library object that implements the service functionality. Entries for module_path should start from the root directory. If the entry does not begin with a forward slash (/), then /usr/lib/security is prepended to the file name.
- **module_options**: Specifies a list of options that can be passed to the service modules. Values for this field depend on the options supported by the module defined in the module_path field.

All of these fields are required for each entry except for the module_options field, which is optional. Malformed entries with invalid values for the module_type or control_flag fields are ignored by the PAM library. Entries beginning with a number sign (#) at the beginning of the line are also ignored because this denotes a comment.

Stacking is implemented in the configuration file by creating multiple entries with the same module_type field. The modules are invoked in the order in which they are listed in the file, with the final result determined by the control_flag field specified for each entry. Valid values for the control_flag field and the corresponding behavior in the stack are:

- **required**: All required modules in a stack must pass for a successful result. If one or more of the required modules fail, all of the required modules in the stack are attempted, but the error from the first failed module is returned.
- **sufficient**: If a module flagged as sufficient succeeds and no previous required or sufficient modules have failed, all remaining modules in the stack are ignored and success is returned.
- **optional**: If none of the modules in the stack are required and no sufficient modules have succeeded, then at least one optional module for the service must succeed. If another module in the stack is successful, a failure in an optional module is ignored.

Example 4-1 shows the /etc/pam.conf file for a system that has additional PAM modules installed.

Example 4-1 /etc/pam.conf file

```
#
# PAM configuration file /etc/pam.conf
#

# Authentication Management
login auth required /usr/lib/security/pam_aix
login auth required /usr/lib/security/pam_verify
login auth optional /usr/lib/security/pam_test use_first_pass
su auth sufficient /usr/lib/security/pam_aix
su auth required /usr/lib/security/pam_verify
OTHER auth required /usr/lib/security/pam_aix
# Account Management
OTHER account required /usr/lib/security/pam_aix
# Session Management
OTHER session required /usr/lib/security/pam_aix
# Password Management
OTHER password required /usr/lib/security/pam_aix
```

This example configuration file contains three entries for the login service. Having specified both pam_aix and pam_verify as required, the user must enter two passwords to be authenticated. Both passwords must succeed for the user to be authenticated. The third entry for the pam_test module is optional. Its success or failure does not affect whether the user can log in. The option use_first_pass to the pam_test module allows a previously entered password to be used instead of prompting for a new one.

The **su** command behaves so that if pam_aix succeeds, authentication succeeds. If pam_aix fails, then pam_verify must pass for successful authentication.

Using the keyword OTHER as a service name enables a default to be set for any other services that are not explicitly declared in the configuration file. Setting up a default ensures that all cases for a given module type are covered by at least one module.

4.1.4 Recommended reading

The following references are good starting points to gain knowledge about PAM. PAM is a complicated subject. Reading its associated manuals is a necessity.

AIX 5L Version 5.2 product documentation

For AIX documentation, consult the following references:

- *AIX 5L Version 5.2: Security Guide*, SC23-4860

  This is a great starting point for all aspects of AIX security. The security guide includes a section on PAM which covers in depth the architecture and configuration of PAM.

- *AIX 5L Version 5.2: System Management Concepts: Operating System and Devices*, SC23-4311

  This document provides a good overview of PAM including terminology, and a high-level overview of administration and configuration.

IBM Redbooks

The following IBM Redbooks contain various amounts of information about PAM:

- *AIX 5L Differences Guide Version 5.2 Edition*, SG24-5765
- *AIX and Linux Interoperability*, SG24-6622

4.2 Security

With PAM, you enable the use of third-party authentication mechanisms. The level of security depends on the pluggable module and on the behavior defined for the services. This allows the use of more secure authentication mechanisms.

Administrators can select one or more authentication methods without modifying existing applications. This insulates the application developers from security implementation.

With the numerous authentication mechanisms available and the advances in authentication technologies, it is difficult, expensive, and time consuming to have application developers implement these. By using PAM, the applications can be deployed using these authentication mechanisms without changing the application code.

PAM is flexible and can be enhanced to take advantage of new authentication technologies. This can increase overall security at a lower cost to application development. PAM enables the administrator the ability to configure authentication mechanisms on a per-application basis.

PAM also allows the ability to configure multiple authentication mechanisms (stacking authentication mechanisms) for each application. Through this concept of stacking authentication mechanisms, a service can be configured to authentication through multiple authentication methods. Stacking multiple authentication methods can either be configured to require the password to be entered for each authentication mechanism. Or if supported by the authentication module, the authentication module can be configured to use a previously submitted password rather than prompting the use for additional input.

4.2.1 Security issues

The following sections discuss some potential security risks of using PAM.

Single signon and single source signon

Single signon is the ability to have users authenticate once and have access to any resources that are provisioned to them. This includes operating systems and applications.

Single source signon is the ability to have the user's passwords synchronized, or made the same, for each of the resources that they are provisioned. This allows the user to access these resources by using the same username and password.

The difference between single source signon and single signon is that the user has to authenticate with each provisioned resource with single source signon using the same username and password. The security issue with single signon or single source signon is that, if the users password is compromised for any one resource, the password is compromised for all the user's resources. This is a trade off with the user's ease of use and security.

Password mapping

Password mapping is the ability to have a user encrypt their secondary passwords (mapped password) with the user's primary password. It is used in a stacked authentication module PAM environment where the user has different passwords for the different resources that they are provisioned.

The secondary passwords are available to the user by knowing the primary password. If the primary password of a user is compromised, then the secondary passwords are also compromised in this solution.

Security of the system configuration files

The security policy of how users are to authenticate are defined in the pam.conf file. This file should be protected from unauthorized access.

Stacking various PAM modules

With the ability to have multiple authentication modules stacked, it is imperative that the system administrator fully understands the implications of stacking the authentication modules. They must also know the order in which they are stacked and the interactions of the modules.

4.3 Installing and configuring PAM

This section takes you through the installation and configuration of two different PAM modules. The high-level steps are:

1. Determine the authentication requirements and determine which PAM modules fulfill these.
2. Identify which services may need special attention.
3. Decide on the sequence in which the modules should be run (if there is more than one module).
4. Select a control flag for each module.
5. Choose options if necessary for each module.
6. Copy the new module to /usr/lib/security.
7. Set the permissions so that the module file is owned by `root` and permissions are `555`.
8. Edit the PAM configuration file, /etc/pam.conf, to add this module to the appropriate services.
9. Test the changes.

The first section, 4.3.1, “Installing PAM for AIX (pam_aix)” on page 130, explains how to install a PAM module, pam_aix, that comes with IBM AIX 5L Version 5.2. It provides an simple example to help you gain experience and knowledge about how to install and configure PAM modules.

The next section, 4.3.2, “Installing PAM for LDAP (pam_ldap)” on page 131, explains how to install a PAM module, pam_ldap, that does not come with IBM AIX 5L Version 5.2. It covers the porting of the LINUX pam_ldap module. You can download this module to IBM AIX 5L Version 5.2 from the Web at:

http://www.padl.com/OSS/pam_ldap.html

This section provides a more involved example of how to extend PAM to different third-party authentication mechanisms such as LDAP.

4.3.1 Installing PAM for AIX (pam_aix)

IBM AIX 5L Version 5.2 ships with the pam_aix PAM module. This module allows PAM-enabled applications to use the AIX security services for authentication. To install this module, follow these steps:

1. Decide the sequence in which the PAM modules should be run (if there is more than one module).
2. Select a control flag for the pam_aix module.
3. Choose the options for the pam_aix module.
4. Make sure the pam_aix module is in the /usr/lib/security directory. Since the pam_aix module comes with IBM AIX 5L Version 5.2, this module should already exist in this directory.
5. Make sure that the pam_aix permissions are set so the module file is owned by the user `root` and the group `security`, and the base file permissions are `444`, as shown here:

   ```
   # chown root:security /usr/lib/security/pam_aix
   # chmod 444 /usr/lib/security/pam_aix
   ```

6. Edit the PAM configuration file, /etc/pam.conf, to add the pam_aix module to the appropriate services. Make sure the file /etc/pam.conf is owned by the user `root` and the group `security`, and the base file permissions are `644`, as shown here:

   ```
   # chown root:security /etc/pam.conf
   # chmod 644 /etc/pam.conf
   ```

7. Test the changes by using the PAM-enabled application.

PAM-enabled applications are now capable of using the pam_aix module.

Important: Verify that the affected applications work as expected before you log out of the system.

4.3.2 Installing PAM for LDAP (pam_ldap)

As mentioned earlier, PAM is a flexible architecture. It allows the ability to hook into may different authentication mechanisms without changing the PAM-enabled applications. This section explains how to extend PAM by porting the PAM module pam_ldap to allow PAM-enabled applications to authenticate to an LDAP server.

The pam_ldap open source code was obtained from PADL Software Pty. Ltd., which is located on the Web at:

`http://www.padl.com`

The LDAP PAM is a PADL open source project to integrate LDAP authentication into operating systems supporting the PAM API, such as Darwin, FreeBSD, HP-UX, Linux, Solaris, and AIX. The pam_ldap module supports the LDAP authentication (rfc2307) schema, and it is a standard on Linux.

Port pam_ldap overview

To port the pam_ldap open source code, follow these steps:

1. Download the module source code.
2. Compile the source code.
3. Install the module.
4. Configure the module.
5. Test the module.

Porting the pam_ldap open source code to AIX requires that you install some of the development filesets on your AIX machine. The following development filesets are installed:

- AIX development toolkit (bos.adt.* from the Base operating system)
- Development tools and utilities from the Linux toolbox CD (autoconf, automake, binutils, bison, db, fileutils, flex, gcc, libtool, m4, make, patch, sh-utils, and wget)

Not all of the listed packages are necessary to compile open source software, but it is helpful to install them.

Downloading the pam_ldap open source code

First, download and unpacked the source code tape archive (tar) file. We used the **`wget`** command to download the tar file, and the **`gzip`** and **`tar`** commands to extract the contents. Example 4-2 shows the output of these commands.

Example 4-2 Downloading and extracting the pam_ldap open source code

```
$ wget -q ftp://ftp.padl.com/pub/pam_ldap.tgz
$ gzip -dc pam_ldap.tgz | tar xf -
$ ls -l
total 240
drwxr-xr-x 3 joe staff 4096 Oct 25 16:01 pam_ldap-164
-rw-r--r-- 1 joe staff 115648 Oct 25 15:53 pam_ldap.tgz
$ cd pam_ldap-164
```

Note that the version number may change. The version we downloaded was the Version 164. You can list the directory to see which version you downloaded.

Configuring the pam_ldap open source code for compilation

To configure the source code for compilation, you use the **configure** script. There are many options that you can use for the **configure** script. The **configure** script uses the options that it receives and updates the file name, Makefile. The Makefile is then used during the compilation process. Example 4-3 shows the options that we used and the output of the configuration script.

Example 4-3 Example output of the configure script

```
#  CPPFLAGS="-I/opt/freeware/include -I/usr/ldap/include -D_LINUX_SOURCE_COMPAT
-DPAM_EXTERN=” ./configure --with-ldap-lib=openldap
--with-ldap-conf-file-/etc/pam_ldap.conf --enable-ssl
checking build system type... powerpc-ibm-aix5.2.0.0
checking host system type... powerpc-ibm-aix5.2.0.0
checking target system type... powerpc-ibm-aix5.2.0.0
checking for a BSD-compatible install... ./install-sh -c
checking whether build environment is sane... yes
checking for gawk... no
checking for mawk... no
checking for nawk... nawk
checking whether make sets ${MAKE}... yes
checking for gcc... gcc
checking for C compiler default output... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc
checking how to run the C preprocessor... gcc -E
checking for a BSD-compatible install... ./install-sh -c
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.h... yes
checking security/pam_appl.h usability... yes
checking security/pam_appl.h presence... yes
checking for security/pam_appl.h... yes
checking security/pam_misc.h usability... no
checking security/pam_misc.h presence... no
checking for security/pam_misc.h... no
checking security/pam_modules.h usability... yes
checking security/pam_modules.h presence... yes
checking for security/pam_modules.h... yes
checking pam/pam_appl.h usability... no
checking pam/pam_appl.h presence... no
checking for pam/pam_appl.h... no
checking pam/pam_misc.h usability... no
checking pam/pam_misc.h presence... no
checking for pam/pam_misc.h... no
checking pam/pam_modules.h usability... no
checking pam/pam_modules.h presence... no
checking for pam/pam_modules.h... no
checking des.h usability... no
checking des.h presence... no
checking for des.h... no
checking crypt.h usability... yes
checking crypt.h presence... yes
checking for crypt.h... yes
checking lber.h usability... yes
checking lber.h presence... yes
checking for lber.h... yes
checking ldap.h usability... yes
checking ldap.h presence... yes
checking for ldap.h... yes
checking ldap_ssl.h usability... no
checking ldap_ssl.h presence... no
checking for ldap_ssl.h... no
checking for main in -ldl... yes
checking for main in -lpam... yes
checking for main in -lresolv... no
checking for main in -lcrypt... yes
checking for main in -lnsl... yes
checking for gethostbyname... yes
checking for main in -llber... no
checking for main in -lldap... yes
checking for ldap_init... yes
checking for ldap_get_lderrno... yes
checking for ldap_set_lderrno... yes
checking for ldap_parse_result... yes
checking for ldap_memfree... yes
checking for ldap_controls_free... yes
checking for ldap_set_option... yes
checking for ldap_get_option... yes
checking for ldapssl_init... no
checking for ldap_start_tls_s... no
checking for ldap_pvt_tls_set_option... no
checking for ldap_initialize... no
checking for gethostbyname_r... yes
checking whether gethostbyname_r takes 6 arguments... 6
checking for ldap_set_rebind_proc... yes
checking whether ldap_set_rebind_proc takes 3 arguments... 2
configure: creating ./config.status
config.status: creating Makefile
config.status: creating config.h
config.status: executing default-1 commands
```

Editing the Makefile file

The default Makefile is fairly large. There are a few lines in it to set the group ownership of the pam_ldap.so file to a group named *root*. There is no default group named *root* on AIX, so you change the option **-g root** to **-g system** in the install-exec-local section of the Makefile file. The section in the file named Makefile should look similar to Example 4-4 after you edit it.

Example 4-4 Changes made to the Makefile file

```
install-exec-local: pam_ldap.so
   @$(NORMAL_INSTALL)
   $(mkinstalldirs) $(DESTDIR)$(libdir)/security
#  $(INSTALL_PROGRAM) -o root -g system pam_ldap.so 
$(DESTDIR)$(libdir)/security/pam_ldap.so
#  $(INSTALL_PROGRAM) -o root -g system pam_ldap.so 
$(DESTDIR)$(libdir)/security/libpam_ldap.1
   $(INSTALL_PROGRAM) -o root -g system pam_ldap.so 
$(DESTDIR)$(libdir)/security/pam_ldap.so.1
   (cd $(DESTDIR)$(libdir)/security; rm -f pam_ldap.so; ln -s pam_ldap.so.1 
pam_ldap.so)
```

Creating the exports.aix file

The exports.aix file tells what the published PAM service module interfaces are for the pam_ldap module, as shown in Example 4-5. You create this file in the same directory where the open source code is located.

Example 4-5 The exports.aix file

```
pam_sm_authenticate
pam_sm_acct_mgmt
pam_sm_setcred
pam_sm_open_session
pam_sm_close_session
pam_sm_chauthtok
```

Compiling and linking the pam_ldap module

The **gmake** command compiles the pam_ldap module. This command uses the file name Makefile to know which options to use during the compile and link steps. Example 4-6 shows the **gmake** command and the **gmake** command output to compile the pam_ldap module.

Example 4-6 Output of the pam_ldap compilation

```
# gmake pam_ldap.so
source='pam_ldap.c' object='pam_ldap.o' libtool=no \
depfile='.deps/pam_ldap.Po' tmpdepfile='.deps/pam_ldap.TPo' \
depmode=gcc /bin/sh ./depcomp \
gcc -DHAVE_CONFIG_H -I. -I. -I.   -I/opt/freeware/include -I/usr/ldap/include
-D_LINUX_SOURCE_COMPAT -DPAM_EXTERN= -DLDAP_REFERRALS -D_THREAD_SAFE  -g -O2
-Wall -fPIC -c `test -f pam_ldap.c || echo './'`pam_ldap.c
source='md5.c' object='md5.o' libtool=no \
depfile='.deps/md5.Po' tmpdepfile='.deps/md5.TPo' \
depmode=gcc /bin/sh ./depcomp \
gcc -DHAVE_CONFIG_H -I. -I. -I.   -I/opt/freeware/include -I/usr/ldap/include
-D_LINUX_SOURCE_COMPAT -DPAM_EXTERN= -DLDAP_REFERRALS -D_THREAD_SAFE  -g -O2
-Wall -fPIC -c `test -f md5.c || echo './'`md5.c
ld  -o pam_ldap.so   -bM:SRE -bnoentry -bE:./exports.aix -L/opt/freeware/lib
pam_ldap.o md5.o  -lldap -lnsl -lcrypt -lpam -ldl -lc
```

Installing the pam_ldap module

The **gmake** command can also install the pam_ldap module into the correct directory. Example 4-7 shows the **gmake** command and the **gmake** command output to install the pam_ldap module.

Example 4-7 Output example of installing the pam_ldap module

```
# gmake install
gmake[1]: Entering directory `/usr/local/pam_ldap/pam_ldap-164'
/bin/sh ./mkinstalldirs /lib/security
./install-sh -c -o root -g system pam_ldap.so /lib/security/pam_ldap.so.1
(cd /lib/security; rm -f pam_ldap.so; ln -s pam_ldap.so.1 pam_ldap.so)
gmake[1]: Leaving directory `/usr/local/pam_ldap/pam_ldap-164'
```

Creating the pam_ldap.conf file for applications to use pam_ldap

The pam_ldap.conf file is used by the pam_ldap module to gather information about the LDAP server that it is going to use. This file is also used for the nss_ldap module for which PADL also provides open source code.

Because of this, there are several NSS variables in the configuration file. These variables are not important for the pam_ldap module. The main variables that are needed for pam_ldap are highlighted in bold in Example 4-8. Other variables may be needed depending on your configuration.

For this example, we use the openldap LDAP server installed on a Linux server, which the pam_ldap module on Linux also used. Example 4-8 shows the default pam_ldap.conf configuration file.

Example 4-8 Default pam_ldap.conf file that ships with pam_ldap

```
# @(#)$Id: ldap.conf,v 1.27 2003/01/17 21:37:12 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# PADL Software
# http://www.padl.com
#

# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host 127.0.0.1

# The distinguished name of the search base.
base dc=padl,dc=com

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
#ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=padl,dc=com

# The credentials to bind with.
# Optional: default is no credential.
#bindpw secret

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
#rootbinddn cn=manager,dc=padl,dc=com

# The port.
# Optional: default is 389.
#port 389

# The search scope.
#scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30

# Bind timelimit
#bind_timelimit 30

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid
```

```
# Search the root DSE for the password policy (works
# with Netscape Directory Server)
#pam_lookup_policy yes

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
#pam_check_host_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=padl,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.

# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password nds
```

```
# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad

# Use the OpenLDAP password change
# extended operation to update the password.
#pam_password exop

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change your
password.

# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd ou=People,
# to append the default base DN but this
# may incur a small performance impact.
#nss_base_passwd ou=People,dc=padl,dc=com?one
#nss_base_shadow ou=People,dc=padl,dc=com?one
#nss_base_group ou=Group,dc=padl,dc=com?one
#nss_base_hosts ou=Hosts,dc=padl,dc=com?one
#nss_base_services ou=Services,dc=padl,dc=com?one
#nss_base_networks ou=Networks,dc=padl,dc=com?one
#nss_base_protocols ou=Protocols,dc=padl,dc=com?one
#nss_base_rpc ou=Rpc,dc=padl,dc=com?one
#nss_base_ethers ou=Ethers,dc=padl,dc=com?one
#nss_base_netmasks ou=Networks,dc=padl,dc=com?ne
#nss_base_bootparams ou=Ethers,dc=padl,dc=com?one
#nss_base_aliases ou=Aliases,dc=padl,dc=com?one
#nss_base_netgroup ou=Netgroup,dc=padl,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute rfc2307attribute mapped_attribute
#nss_map_objectclass rfc2307objectclass mapped_objectclass

# configure --enable-nds is no longer supported.
# For NDS now do:
#nss_map_attribute uniqueMember member

# configure --enable-mssfu-schema is no longer supported.
# For MSSFU now do:
```

```
#nss_map_objectclass posixAccount User
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# For authPassword support, now do:
#nss_map_attribute userPassword authPassword
#pam_password nds

# For IBM SecureWay support, do:
#nss_map_objectclass posixAccount aixAccount
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs/cert7.db

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
#ssl on

# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is "no"
#tls_checkpeer yes

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
#tls_cacertfile /etc/ssl/ca.cert
#tls_cacertdir /etc/ssl/certs
```

```
# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key
```

Editing the pam.conf file to use the new pam_ldap module

You must update the /etc/pam.conf file so that PAM-enabled applications take advantage of the new pam_ldap module. Example 4-9 shows the /etc/pam.conf file that defines how a PAM-enabled application named *pamapp1* will use the pam_ldap module for authentication.

Example 4-9 Example /etc/pam.conf file to use the pam_ldap module

```
#
# PAM configuration file /etc/pam.conf
#

# Authentication Management
pamapp1 auth required /usr/lib/security/pam_ldap
OTHER auth required /usr/lib/security/pam_aix
# Account Management
OTHER account required /usr/lib/security/pam_aix
# Session Management
OTHER session required /usr/lib/security/pam_aix
# Password Management
OTHER password required /usr/lib/security/pam_aix
```

4.4 Common problems and solutions

The main method to understand problems and resolve them is to enable PAM debugging through the use of the syslog daemon.

4.4.1 Enabling PAM debug

The PAM library can provide debugging information during execution. After you enable the system to collect debug output, you can use the information gathered to track PAM API invocations. You can also use it to determine failure points in the current PAM setup. To enable PAM debug output, follow these steps:

1. Create an empty file named /etc/pam_debug. The PAM library checks for the existence of /etc/pam_debug file. If found, it enables syslog output.

   ```
   # touch /etc/pam_debug
   ```

2. Edit the /etc/syslog.conf file to contain the appropriate entries for the desired levels of messages. To capture debug information for authentication calls, use **auth.debug** and send the output to a file. The following example line is in the syslog.conf file that sends the authentication debug information to a file:

   ```
   auth.debug        /tmp/syslog_auth.log
   ```

3. Restart the syslogd daemon so that the configuration changes made in /etc/syslogd.conf are recognized:

   ```
   # stopsrc -s syslogd
   # startsrc -s syslogd
   ```

4. When an authentication action occurs, including PAM authentications, debug messages are collected in the output file defined in the /etc/syslog.conf configuration file, in this case /tmp/syslog_auth.log. Example 4-10 shows sample debug messages.

Example 4-10 PAM syslog debug messages

```
Aug 14 14:22:02 venus PAM: pam_start(squid squid@)
Aug 14 14:22:02 venus PAM: pam_set_item(1)
Aug 14 14:22:02 venus PAM: pam_set_item(2)
Aug 14 14:22:02 venus PAM: pam_set_item(5)
Aug 14 14:22:02 venus PAM: pam_set_item(2)
Aug 14 14:22:02 venus PAM: pam_set_item(5)
Aug 14 14:22:02 venus PAM: pam_authenticate()
Aug 14 14:22:02 venus PAM: load_modules: /usr/lib/security/pam_ldap.so
Aug 14 14:22:02 venus PAM: load_function: successful load of
pam_sm_authenticate
Aug 14 14:22:02 venus PAM: pam_set_item(6)
Aug 14 14:22:02 venus PAM: pam_acct_mgmt()
Aug 14 14:22:02 venus PAM: load_modules: /usr/lib/security/pam_ldap.so
Aug 14 14:22:02 venus PAM: load_function: successful load of pam_sm_acct_mgmt
```

5

Restricting users

This chapter provides information about:

- Restricted shells
- User limits for system resources
- User login controls
- Creating a secure login template
- Preventing denial-of-service attacks

You can also find practical examples for setting restrictions in these cases.

5.1 Restricted shells

An AIX restricted shell is useful for creating a specific user logon environment. In this environment, minimal base functions are supported and you, as the administrator, control the additional programs that are available to the user. The cost of configuring restricted shells is increased administration in making sure that users have the necessary access to do what they need to do.

You should be aware that restricted shells can be compromised by users running applications that allow them to "shell out" of the program using a different shell (for example, **vi** and many other editors do this). With **vi**, you can set your shell to a non-restrictive shell and then shell out.

While **bsh** and **ksh** offer the `-r` flag to denote a restricted version, we demonstrate the feature using **Rsh**, a restricted Bourne shell. This gives you the option to use **shell=** in the **mkuser** or **chuser** commands. Alternately you can edit the /etc/passwd file to specify the user's shell:

```
alex:!:202:1::/home/alex:/usr/bin/ksh -r
```

5.1.1 Recommended reading

We recommend that you consult these technical tips that are available from the following Web site:

- *Define Restricted Logins*
- *Overview of Shell Startup Files*

https://techsupport.services.ibm.com/server/aix.srchBroker

Refer to *AIX 5L Version 5.2: System Management Concepts: Operating System and Devices,* SC23-4311 to learn about the **Rsh**, **bsh**, and **ksh** commands and references to restricted shell. You can use the search tool to find and review these commands and references on the AIX 5L POWER 5.2 Documentation CD or access them on the Web at:

http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/aix52.htm

5.1.2 Configuring the system and creating a restricted shell user

To configure the system and create a restricted shell user, follow these steps:

1. Make a reduced bin directory to contain links to programs for the user or users:

   ```
   # mkdir /usr/rbin
   ```

2. Link the necessary commands and programs in the reduced bin directory. For example, give access to the **ls** and **vi** commands:

```
# ln -s /usr/bin/ls /usr/rbin/ls
# ln -s /usr/bin/vi /usr/rbin/vi
```

3. Add **Rsh** as a valid shell in /etc/security/login.cfg:

```
# vi /etc/security/login.cfg
```

4. Add **/usr/bin/Rsh** to the list of shells in the `usw` stanza:

```
usw:
shells =
/bin/sh,/bin/bsh,/bin/csh,/bin/ksh,/bin/tsh,/bin/ksh93,/usr/bin/sh,/usr/bin
/bsh,/usr/bin/csh,/usr/bin/ksh,/usr/bin/tsh,/usr/bin/ksh93,/usr/sbin/uucp/u
ucico,/usr/sbin/sliplogin,/usr/sbin/snapp,/usr/bin/Rsh
```

5. Add the restricted shell user:

```
# mkuser shell=”/usr/bin/Rsh” alex
```

6. Assign an initial password:

```
# passwd alex
```

7. Change the ownership of the users profile to root:

```
# chown root:system /home/alex/.profile
```

8. Change the permissions of the users profile to 755:

```
# chmod 755 /home/alex/.profile
```

9. Edit the users profile setting the PATH and Shell variables:

```
# vi /home/alex/.profile
```

   a. Set PATH for the new bin directory:

   ```
   PATH=/usr/rbin
   ```

   b. Set SHELL to rksh:

   ```
   export SHELL=/usr/bin/Rsh
   ```

5.2 User limits for a system resource

A computer system can be incapacitated by any number of methods, some intentionally and some by accident. For example, a poorly written (or well written, if the intention is bad) process can consume large amounts of Central Processing Unit (CPU) time. This can cause high paging activity, slowing the system down. This problem reduces the available resources for all other system users creating a denial-of-service situation. By accident or intent, system administrators can limit or prevent the situation by setting system resource limits, as system defaults or against a specific user account.

As an example, a hacker's exploit may involve crashing one of your applications. Each time the application crashes, there is the potential for a core file to be created. If there is an unlimited or large core file size, this quickly results in filling up a filesystem until there is no more available free space. In turn, this can result in further problems with the system. To combat this, you can set the default core size to 0. Unfortunately, the core file may be useful for problem determination. In such a case, you need to capture a full size core file for analysis.

5.2.1 Architecture

When a user logs in to the system, they are assigned the default user limit or ulimit values from the /etc/security/limits file. Or they may have specified a different value explicitly in their user stanza.

Within a user session, the user can increase or decrease the soft limit values up to the hard limit value. They can also reduce their hard limit values, but cannot increase them. These values are reset upon login to the limits specified in /etc/security/limits.

Setting limits in the default stanza sets them system wide and applies them to all users and processes.

You can find additional information in the AIX documentation about the **`ulimit`** command, `setrlimit()` and `getrlimit()` subroutines, and limits file reference. You can use the search tool to find and review these from the AIX 5L POWER 5.2 Documentation CD. Or you can find them on the Web at:

`http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/aix52.htm`

5.2.2 Security

The limits file is in the secure /etc/security/ directory. You cannot increase hard limits without root authority.

5.2.3 Resources

You can define user limits by editing the /etc/security/limits file, or by using the **`ulimits`** command. You can limit the following system resources from user access.

-t time(seconds): CPU time

```
cpu = -1
hard_cpu = -1
```

This this the maximum amount of CPU time, in seconds, to be used by each process.

-f file(blocks): File size

```
fsize = 2097151
hard_fsize = 2097151
```

This is the largest size, specified in 512-byte blocks, of any single file that can be created.

-d data(kbytes): Data segment

```
data = 262144
hard_data = -1
```

This is the maximum size, specified as 512-byte blocks in the /etc/security/limits file or specified in kilobytes in the **ulimit** command, of the data region for a process.

-s stack(kbytes): Stack segment

```
stack = 65536
hard_stack = -1
```

This is the maximum size, specified as 512-byte blocks in the /etc/security/limits file or specified in kilobytes in the **ulimit** command, of the stack region for a process.

-m memory(kbytes): Resident set size

```
rss = 65536
hard_rss = -1
```

This is the maximum size, specified as 512-byte blocks in the /etc/security/limits file or specified as kilobytes in the **ulimit** command, to which the resident set size of a process may grow.

-c core(blocks): Core file size

```
core = 2097157
hard_core = -1
```

This is the largest size, specified as 512-byte blocks, of a core file that can be created.

-n nofiles(descriptors): Number of open files

```
nofiles = 2000
hard_nofiles = -1
```

This is the maximum number of file descriptors allowed by a process.

5.2.4 Administration

You can view and change limits in the /etc/security/limits file or by using the **ulimit** command. You can view the soft limits using the **ulimit** command as shown in Example 5-1.

Example 5-1 Using the ulimit command to see the soft limits

```
# ulimit -a
time(seconds)        unlimited
file(blocks)         2097151
data(kbytes)         131072
stack(kbytes)        32768
memory(kbytes)       32768
coredump(blocks)     2097151
nofiles(descriptors) 2000
```

You can view the hard limits using the **ulimit** command as shown in Example 5-2.

Example 5-2 Using the ulimit command to see the hard limits

```
# ulimit -Ha
time(seconds)        unlimited
file(blocks)         2097151
data(kbytes)         unlimited
stack(kbytes)        4194304
memory(kbytes)       unlimited
coredump(blocks)     unlimited
nofiles(descriptors) unlimited
```

The values used as default settings are stored in the /etc/security/limits file.

To change the limit using the **chuser** command, enter:

```
chuser <limit>=<value> <username>
# chuser nofiles=3000 alex
```

To change your current soft limit use, enter:

```
ulimit <-flags> <value>
$ ulimit -Sn 1000
```

To change your current hard limit use, enter:

```
ulimit <-flags> <value>
$ ulimit -Hn 1000
```

To change system default limits, enter:

```
chsec -f file -s stanza -a "attr=value" ...
# chsec -f /etc/security/limits -s default -a “fsize=100000”
```

5.3 User login controls

Integrating various options together is required to create a secure login template. Various files used when creating users and when they login define most aspects of the users environment. Knowing and customizing what is in these files, you can control the users’ security environment.

In most cases, you use values in the default stanzas to ensure the changes affect all users. However, you should check the relevant files and verify any settings for specific users.

At login, a series of files are run that set up the users environment. Careful control of these files ensures that users have sufficient access to complete the system tasks without unnecessary access to the system.

5.3.1 Setting up login controls

To make it more difficult to attack a system with password guessing, set up system default login controls in the /etc/security/login.cfg file as shown in Table 5-1.

Table 5-1 Attributes and recommended values for the login.cfg file

Attribute	Applies to PtYs (network)	Applies to TTYs	Suggested value	Comments
sak_enabled	Y	Y	False	The Secure Attention Key is rarely needed.
logintimes	N	Y		Specify allowed login times here.
logindisable	N	Y	4	Disable login on this terminal after four consecutive failed attempts.

Attribute	Applies to PtYs (network)	Applies to TTYs	Suggested value	Comments
logininterval	N	Y	60	Terminal is disabled when the specified invalid attempts are made within 60 seconds.
loginreenable	N	Y	30	Re-enable the terminal after it is automatically disabled after 30 minutes.
logindelay	Y	Y	5	The time in seconds between login prompts. This is multiplied with the number of failed login attempts; for example, 5, 10, 15, 20 seconds when 5 is the initial value.

These port restrictions work mostly on attached serial terminals, not on pseudo-terminals used by network logins. You can specify explicit terminals in this file as shown in Example 5-3.

Example 5-3 Specifying explicit terminals

```
/dev/tty0:
   logintimes = 0600-2200
   logindisable = 5
   logininterval = 80
   loginreenable = 20
```

5.3.2 Changing the welcome message on the login display

To prevent displaying certain information on login screens, edit the herald parameter in the /etc/security/login.cfg file. The default herald contains the welcome message that displays with your login prompt. To change this parameter, you can either use the **chsec** command or edit the file directly.

The following example uses the **chsec** command to change the default herald parameter:

```
# chsec -f /etc/security/login.cfg -a default -herald
“Unauthorized use of this system is prohibited.\n\nlogin: “
```

For more information about the **chsec** command, see *IBM AIX 5L Version 5.2 Commands Reference, Volume 1*, SC23-4115.

To edit the file directly, open the /etc/security/login.cfg file and update the herald parameter as shown in Example 5-4.

Example 5-4 Updating the herald parameter in /etc/security/login.cfg

```
default:
herald = "Unauthorized use of this system is prohibited\n\nlogin: "
   sak_enable = false
   logintimes =
   logindisable = 0
   logininterval = 0
   loginreenable = 0
   logindelay = 0
```

Note: To make the system more secure, set the logindisable and logindelay variables to a number greater than 0.

5.3.3 Changing the login display for the CDE

The CDE login display also shows, by default, the host name and the operating system version. To prevent this information from being displayed, edit the /usr/dt/config/C/Xresources file to remove the welcome messages that include the host name and operating system version.

5.3.4 Securing unattended terminals

All systems are vulnerable if terminals are left logged in and unattended. The most serious problem occurs when a system manager leaves a terminal unattended that was enabled with root authority.

In general, users should log out any time they leave their terminals. Leaving system terminals not secured poses a potential security hazard. To lock your terminal, use the **lock** command. If your interface is AIXWindows, use the **xlock** command.

5.3.5 Enforcing automatic logoff

Another valid security concern results from users leaving their accounts unattended for a lengthy period of time. This situation allows an intruder to take control of the user’s terminal, potentially compromising the security of the system.

To prevent this type of potential security hazard, you can enable automatic logoff on the system. To do this, edit the /etc/security/.profile file to include an automatic logoff value for *all* users, as in the following example:

```
TMOUT=600 ; TIMEOUT=600 ; export readonly TMOUT TIMEOUT
```

The number 600, in this example, is in seconds, which is equal to 10 minutes. However, this method only works from the shell.

While the previous action allows you to enforce an automatic logoff policy for all users, system users can bypass some restrictions by editing their individual .profile files. To completely implement an automatic logoff policy, take authoritative action by providing users with the appropriate .profile files. This prevents write-access rights to these files.

5.4 Preventing denial-of-service attacks

Denial-of-service attacks are an attempt to restrict or prevent valid users from using a service. Various standard methods are defined to categorize known attacks.

For more information, see the *Denial-of-service Attacks* document from the CERT Coordination Center on the Web at:

http://www.cert.org/tech_tips/denial_of_service.html

In AIX, there are several changes that you can make to reduce the vulnerability to these types of attacks.

Maintain your system software levels in particular to the latest available security fixes. For details, see Chapter 1, “AIX security flashes” on page 1.

Be sure to secure or remove unnecessary network services. You can do this by changing the /etc/inittab, /etc/rc.tcpip, and /etc/inetd.conf files. For a reference on how to do this, see Table A-1 on page 156.

Configure the network options for your system using the **no** command. This command allows you to adjust the state of various network tuning parameters. For details about each option, see the **no** command in *IBM AIX 5L Version 5.2 Commands Reference, Volume 4*, SC23-4118. For specific recommendations, see Table A-1 on page 156.

Enable system resource limits for disk, memory, and processor resources. This provides some barrier for runaway use of these resources. See 5.2, “User limits for a system resource” on page 145, for more information.

Know your system’s normal performance behavior and running processes. Check and record benchmarks for your system at various times. Be sure to record performance statistics and process output listing. This gives you accurate comparisons. If you suspect that performance is down, you can verify it and review the process listing and investigate differences.

Check your sites’ physical security. Be sure to tag and list all network appliances.

Consider implementing a security layer such as AIX’s Trusted Computing Base (TCB) or another third-party tool. A security layer, such as TCB, can verify your critical system and that configuration files are not tampered with.

Maintain user login and password controls to be in accordance with your company’s policies. By setting restrictive passwords and using login controls, you can slow automated attacks.

A

AIX Security Planning and Implementation Worksheet

The worksheet shown in Table A-1 presents the installation options and a set of values for these options that available when you install and configure IBM AIX 5L Version 5.2. The columns on the right (Default value, Low security, Medium security, and High security) represent the default installation values.

For example, if you want to install IBM AIX 5L Version 5.2 in a high security installation, follow the values in the High security column. Keep in mind that you must address specific security. The following worksheet is provided only as an example.

Table A-1 AIX Security Planning and Implementation Worksheet

Description	Action	Default value	Low security	Medium security	High security
Planning					
Planning your AIX installation allows you to gather data about your system and desired configuration, agree to responsibilities, and develop an installation schedule. To use this worksheet, mark the value for each option selected as each item is discussed, add additional items and comments as required.					
System setup					
Your AIX system may already be setup and require customer setup or assistance from a specialized IBM Representative. If applicable, install and connect the IBM-supported customer setup machines, display unit, IBM tape drive, terminal, and printer.					
AIX install					
Install the base operating system and optional components, as appropriate. You should understand each option and decide if it is required on the system in question. Generally the more you install, the greater the security risk is simply because there are more points to consider. However, if you need a particular option, you must install it. If in doubt, leave it out. You can always add it later.					
Method of installation	New and complete overwrite, Preservation install migration install		Migr	Pres	New
Desktop	CDE, KDE, GNOME, None	CDE	Any	CDE	None
Enable Trusted Computing Base	No, Yes	No	No	Yes	Yes
Enable CAPP and EAL4+ Technology (English only, 64-bit kernel enablement, JFS2 file systems)	No, Yes	No	No	Yes	Yes
Enable 64-bit kernel	Yes, No			Yes	Yes
Create JFS2 file systems (requires a 64-bit kernel enabled)	Yes, No			Yes	Yes
Graphics software	Yes, No	Yes	Yes	Yes	No
Documentation services software	No, Yes	No	Yes	No	No
Enable system backups to install any system (installs all devices and kernels)	Yes, No	Yes	Yes	No	No
Netscape (Expansion Pack)	No, Yes	No	Yes	No	No

Description	Action	Default value	Low security	Medium security	High security
HTTP_Server (Expansion Pack)	No, Yes	No	Yes	No	No
Kerberos_5 (Expansion Pack)	No, Yes	No	Yes	No	No
Server (Volume 2)	No, Yes	No	Yes	No	No
Alternate Disk Install (Volume 2)	No, Yes	No	Yes	No	No
Initial configuration					
These options are available through the Configuration Assistant graphical user interface (GUI) or Installation Assistant (text session) which automatically load on the first boot of an new installation. You can also start the tool using `install_assist` or `smit assist`.					
Set the password for administration Set the root password (text).	passwd root	N	N	Y	Y
Set or verify the system date, time. Set date and time (text).	This places a TZ entry in the /etc/environment file	CDT	N	Y	Y
Configure Network Communications (TCP/IP). If you are installing the system in a prone situation, consider leaving this until the system is secured.	Manual or automatically via DHCP Hostname: Internet address: Network mask: Name server Internet address: Name server domain: Default gateway address:	N	Y	Y	N
Configure the Online Documentation Library Service.		N	Y	Y	N
Configure the Web server to run Web-based System Manager in a browser (text).		N	Y	Y	N
Manage the software. Install software applications (text).		N	Y	Y	Y
Additional software					
Install additional IBM programs as agreed in the planning session. Some common filesets can include:					
Base operating system data	bos.data	N	Y	N	N
DOS utilities	bos.dosutil	N	Y	N	N

Description	Action	Default value	Low security	Medium security	High security
Asynchronous Terminal Emulator	bos.net.ate (modem pager)	N	Y	N	N
Performance diagnostic tool	bos.perf.diag_tool	N	Y	Y	N
Performance PMR data	bos.perf.tools	N	Y	Y	Y
C Compiler (requires additional software)		N	Y	Y	N
AIX updates: Install the latest available AIX Recommended Maintenance Level	# smitty update_all	Y	Y	Y	Y
Configure your console					
Configure your console type to allow full use of supported features.					

ASCII Terminal	# smit chtty
	TERM=ibm3151
		N			

Graphical display	# smit g_display Select the Display Type	N			
Configure optional root user changes					
Configure changes for the root user to provide additional security, audit, and reliability.					
Make a dedicated home directory for the root user ID and change the root user ID home directory to use new directory, allowing a cleaner / directory. Change directory permissions to allow for root access only.	# mkdir /root # chuser home=/root root # chmod 700 /root	N			
Create the smit files in the tmp directory, change the file permissions to prevent unauthorized access, and link the smit files to roots home directory. This option prevents these filling the / filesystem.	# touch /tmp/smit.log # touch /tmp/smit.script # touch /tmp/smit.transaction # chmod 600 /tmp/smit.* # ln -s /tmp/smit.log /root/smit.log # ln -s /tmp/smit.script /root/smit.script # ln -s /tmp/smit.transaction /root/smit.transaction	N			

Description	Action	Default value	Low security	Medium security	High security
Create and configure the root users profile with preferred options. If you migrated the system, move the current /.profile to /root/.profile to maintain previous customization. Some common customizations to consider are the prompt and editor. **Note**: Special characters are used in the PS1 string. Either side of the commands **uname** and **whoami** are back-quotation marks (`), usually below the ESC key on most keyboards. There are spaces either side of the hash sign “ # ”. Change file permissions to allow for execution, and prevent non-root access.	# vi /root/.profile set -o vi export PS1=`whoami`@`uname -n`':$PWD # ' # chmod 700 /root/.profile				
Increase the maximum file size to one that can be written by root UID.	fsize = 2097151 (default) # chuser fsize=-1 root		-1		
Increase the maximum core file size to one that can be written by a root UID.	core = 2097151 (default) # chuser core=-1 root		-1	0	0
Prevent root login: Users need to login with their own ID and then **su** to root. Ensure that you created an administrative user before you disallow root login.	login = true (default) # chuser login=false root	true	true	true	false
Prevent remote root login: Users need to log in at the console or with their own ID and then **su** to root.	rlogin = true (default) # chuser rlogin=false root	true	true	false	false

Description	**Action**	**Default value**	**Low security**	**Medium security**	**High security**
The number of unsuccessful login attempts allowed before locking a users account. While this is the default, set it explicitly for root so you can change the default for other users.	loginretries = 0 # chuser loginretries=0 root	0	0	0	0
Maximum time (weeks) after the maxage a user can change their expired password. While this is the default, set it explicitly for root so you can change the default for other users.	maxexpired = -1 # chuser maxexpired=-1 root	-1	-1	-1	-1
Configure the /etc/security/login.cfg system default entries					
Configure login controls, as required. These settings apply to terminal ports (ttys), with sak_enabled, logindelay, herald, and logintimeout applying to all sessions (tty and pty). Restricting these options helps to prevent unwelcome and automated hacking attacks. It restricts information that is displayed in the default herald (operating system and version), slowing or delaying system access after invalid login attempts.					
Enable a secure attention key (SAK) on login ports.	sak_enabled = false	False	False	False	True
The times a port is allowed for login.	logintimes =				
Number of failed login attempt allowed before disabling the port.	logindisable = 0	0	0	0	10
Time (seconds) in which failed login attempts must be entered.	logininterval = 0	0	0	0	200
Time (minutes) before a locked port is re-enabled.	loginreenable = 0	0	0	0	20
Time in seconds to delay port access after an unsuccessful login attempt.	logindelay = 0	0	0	4	10
Override the default login herald to reflect business access policy or remove clues about the operating system. The system is running to potential hackers (22 "\n").	herald = “\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\nAccess Restricted\r\nlogon: ”				

Description	Action	Default value	Low security	Medium security	High security
Time (seconds) allowing the user to enter the password.	logintimeout	60	120	60	60
Configure /etc/security/user					
You can use various security features by updating the user file. By tightening the password, they are more difficult to guess or crack. They should not be too difficult to remember so users don’t write them down.					
Enforce use of the correct system authentication method, local (files) LDAP Kerberos etc.	registry =				files
Trusted path status.	tpath = nosak				
File creation mask to prevent file sharing amongst users.	umask = 022	022	022	027	077
Time (days) warning a user before a password change is required.	pwdwarntime = 0	0	5	5	5
Number of unsuccessful login attempts allowed before locking a users account.	loginretries = 0	0	0	0	3
Time (weeks) before a password can be reused.	histexpire = 0	0	0	13	26
Number of previous passwords that cannot be reused.	histsize = 0	0	0	20	20
Minimum age (weeks) before a password can be changed.	minage = 0	0	0	0	1
Maximum age (weeks) before a password must be changed.	maxage = 0	0	26	12	4
Maximum time (weeks) after maxage a user can change their expired password.	maxexpired = -1	-1	-1	5	2
Minimum number of alphabetic characters required in a password.	minalpha = 0	0	0	2	2

Description	Action	Default value	Low security	Medium security	High security
Minimum number of non-alphabetic characters required in a password.	minother = 0	0	0	1	2
Minimum number of characters required in a password.	minlen = 0	0	0	4	8
Minimum number of characters that must be changed from the previous password.	mindiff = 0	0	0	4	4
Maximum number or repeated characters allowed in a password.	maxrepeats = 8	8	8	2	2
Configure /etc/motd					
When text session access to the system is attained, the message of the day motd file is displayed. This is another opportune time to appeal to unauthorized users the consequences of their actions.					
Change the "Welcome" message of the day file to reflect business use and access policy	Use SGC assets, including this computer system, only for SGC management approved purposes. You should be aware that it may be a criminal offense to secure unauthorized access to any program or data in the system or to make unauthorized modifications to its contents. If you are not authorized by SGC management to access this system, log out now.				
Configure /etc/security/.profile					
In the default environment, users using the korn shell `ksh` have this file copied to their home directory as their default profile. Choosing to place these entries here allows flexibility and enforcement if you are using restricted shells. Normally the user can change this file at will. If you want to control the user's environment, consider using a restricted shell.					
Enable shell command retrieval (ESC k).	export readonly EDITOR=/usr/bin/vi				600
Enable a larger command history for auditing.	export readonly HISTSIZE=1000				

Description	Action	Default value	Low security	Medium security	High security
Set the shell inactivity time-out values to 1 hour.	export readonly TMOUT=3600 export readonly TIMEOUT=3600			3600	600
Prompt string. **Note**: Special characters used in the PS1 string. Either side of the commands **uname** and **whoami** are back-quotation marks (`) usually below the ESC key on most keyboards. There are spaces either side of the hash sign " $ ".	export readonly PS1=`whoami`@`uname -n`':$PWD \$ '				
Check and lock down the available user accounts					
By default, many user accounts exist on the system for specific system processes to operate. These commands check existing users, groups, passwords, and file settings. With the -y flag, they disable additional access methods to these accounts. If you are not sure, run them without automatic correction and review the suggested changes.					
Check and validate all users definitions on the system.	# usrck -y ALL		N	Y	Y
Check and validate all group definitions on the system.	# grpck -y ALL		N	Y	Y
Check and validate all password definitions on the system.	# pwdck -y ALL		N	Y	Y
Audits the security state of the system.	# tcbck -y ALL		N	N	Y
Filesystems					
Ensuring filesystems are large enough to accommodate expected files may prevent your system from crashing when large files are created or additional software is installed. Check increase and create standard file systems. Then monitor the available space to prevent filling.					
Review the currently configured paging space and increase if necessary.	# /usr/sbin/bootinfo -r # lsps -a # chps -s16 hd6				

Description	Action	Default value	Low security	Medium security	High security
Review the estimated dump space requirement, check the dump device size and increase if necessary, or consider using a separate dump logical volume. X is the number of additional LPs or Y is the total number of LPs for the dump device.	# sysdumpdev -e # lsps -a (if using hd6 default) # chps -sX hd6 or # mklv -y dumplv rootvg Y # sysdumpdev -P -p /dev/dumplv				
Review the dump device settings	# sysdumpdev -l				
Allow a special key sequence to force a system dump.	# sysdumpdev -K				
Increase the / filesystem to 64 MB.	# chfs -asize=131072 /				
Increase the /usr filesystem to 512 MB.	# chfs -asize=1048576 /usr				
Increase the /var filesystem to 256 MB.	# chfs -asize=524288 /var				
Increase the /tmp filesystem to 128 MB.	# chfs -asize=262144 /tmp				
Increase the /home filesystem to 128 MB.	# chfs -asize=262144 /home				
Increase the /opt filesystem to 128 MB.	# chfs -asize=262144 /opt				
Create a a CD filesystem to allow later access to other non installp formatted CDs. This allows us to `mount /cdrom`, providing easier access to the data on the CD.	# smitty crcdrfs DEVICE name - cd0 MOUNT POINT - [/cdrom] Mount AUTOMATICALLY at system restart? - no	N	Y	Y	N
Mirror the rootvg hard disk.	smitty mirrorvg	N	Y	Y	Y

Description	Action	Default value	Low security	Medium security	High security
System environment					
Give additional consideration to changing these common settings. This allows for greater reliability, availability, and serviceability (RAS).					
Check and increase error log buffers and log file size to provide a larger audit trail.	# /usr/lib/errdemon -l # /usr/lib/errdemon -s4194304 -B32768		Y	Y	Y
Enable auto restart after system crash.	chdev -lsys0 -aautorestart=true	True	True	True	True
Enable full size core dump.	chdev -lsys0 -afullcore=false	False	True	True	True
Enable iostat disk statistics.	chdev -lsys0 -aiostat=false	False	True	True	False
Increase maximum number or processes per user.	chdev -lsys0 -amaxuproc=400	128			
Set up system message logging.	# touch /var/adm/messages # chmod 640 /var/adm/messages # vi /etc/syslog.conf Append the line: *.warn /var/adm/messages Exit, then: # refresh -s syslogd				
Set up system auditing.	/etc/security/audit/config binmode=on streammode=off bytethreshold=1000 default=login				
Review and disable unnecessary inittab entries					
As installed, AIX provides a rich set of available services. While they do not offer specific security problems, if you are not using them, in a secure system, disable them. This makes it easier to track what services are running when you are auditing the system.					
NFS start script `rmnfs` removes the entry in the inittab file and stops NFS daemons that are currently executing. The -B flag is the default.	# rmnfs -B				
Print job manager for the printer backend.	# rmitab piobe				

Description	Action	Default value	Low security	Medium security	High security
Schedules jobs enqueued by the enq command.	# rmitab qdaemon				
Allows users to send messages to and receive messages from a remote system.	# rmitab writesrv				
Constructs and writes kernel messages.	# rmitab uprintfd				
Starts the documentation search engine	# rmitab itess				
Graphical start daemon	# rmitab dt				
Lite NetQuestion Web server software	# rmitab httpdlite				
Review and disable unnecessary rc.tcpip entries					
As with inittab, many TCP/IP services are started in the /etc/rc.tcpip startup script. Again for any services that you do not require, disable them on most systems, unless they are specifically required.					
Sendmail	/usr/lib/sendmail	Y		N	N
Simple Network Management Protocol	/usr/sbin/snmpd	Y		N	N
hostmibd dpi2 sub-agent daemon	/usr/sbin/hostmibd	Y		N	N
hostmibd dpi2 sub-agent daemon	/usr/sbin/snmpmibd	Y		N	N
AIX Enterprise Management Information Base (MIB) extension subagent	/usr/sbin/aixmibd	Y		N	N
Review and disable unnecessary inetd.conf entries					
Tighten security by removing most TCP/IP services started from /etc/inetd.conf. The inetd super server starts further TCP/IP processes. They can be disabled individually or you can stop inetd from the rc.tcpip file. Of course, you may need some services to allow normal operation of the system, and many of these services can provide secure implementations.					
ftp	/usr/sbin/ftpd	Y	Y	Y	N
telnet	/usr/sbin/telnetd	Y	Y	Y	N

Description	Action	Default value	Low security	Medium security	High security
shell	/usr/sbin/rshd	Y	Y	N	N
kshell	/usr/sbin/krshd	Y	Y	Y	N
login	/usr/sbin/rlogind	Y	Y	N	N
klogin	/usr/sbin/krlogind	Y	Y	Y	N
exec	/usr/sbin/rexecd	Y	Y	N	N
ntalk	/usr/sbin/talkd	Y	Y	N	N
daytime	tcp internal	Y	Y	N	N
time	tcp internal	Y	Y	N	N
daytime	udp internal	Y	Y	N	N
time	udp internal	Y	Y	N	N
cmsd (comment unless using X Window)	/usr/dt/bin/rpc.cmsd	Y	Y	N	N
ttdbserver (comment unless using X Window	/usr/dt/bin/rpc.ttdbserver	Y	Y	N	N
wsmserver	/usr/websm/bin/wsmserver	Y	Y	N	N
Network options					
AIX provides the /usr/sbin/no command to configure network options. Setting an attribute to 0 disables the option while setting it to 1 enables it. This section of the table contains suggestions for setting the network attributes. Proper configuration depends on individual network requirements. The network options are restored to defaults when the system is rebooted. To enforce these options upon every reboot, ensure that you use the -p flag with the appropriate no commands to configure the change permanently. Prior to automating the setting of network options, test the system with desired settings to verify that the network behaves as expected.					
Allows response to ICMP echo packets to the broadcast address. Disabling this prevents Smurf Attacks.	bcastping	0			0

Description	Action	Default value	Low security	Medium security	High security
After the system is enabled, it periodically cleans partial connections (SYN recv, SYN/ACK sent). A SYN attack tries to flood your system with requests to open connections, so you cannot respond to legitimate requests. Legitimate partial connections need to reconnect.	clean_partial_conns	0			1
Specifies whether to allow a directed broadcast to a gateway. Disabling this helps prevent directed packets from reaching a remote network.	directed_broadcast	0			0
Specifies if the system responds to an ICMP address mask request. Disabling this prevents access through source routing attacks.	icmpaddressmask	0			0
Specifies if the kernel should forward packets. Disabling this prevents redirected packets from reaching remote network.	ipforwarding	0			0
Specifies whether to process redirects that are received.	ipignoreredirects	0			1
Specifies whether the kernel should send redirect signals. Disabling this prevents redirected packets from reaching remote network.	ipsendredirects	1			0
Specifies whether the system forwards source-routed packets. Disabling this prevents access through source routing attacks.	ipsrcrouteforward				0
Specifies whether the system accepts source-routed packets. Disabling this prevents access through source routing attacks.	ipsrcrouterecv	0			0

Description	Action	Default value	Low security	Medium security	High security
Specifies whether applications can send source-routed packets. Disabling this prevents access through source routing attacks.	ipsrcroutesend				0
Specifies whether the system forwards source-routed IPv6 packets. Disabling this prevents access through source routing attacks.	ip6srcrouteforward	1			0
Tells the Internet Protocol that strictly source-routed packets may be addressed to hosts outside the local network. Disabling this prevents access through source routing attacks.	nonlocsroute	0			0
Enables or disables path MTU discovery for TCP applications. Disabling this prevents access through source routing attacks.	tcp_pmtu_discover	1			0
Enables or disables path MTU discovery for User Datagram Protocol (UDP) applications. Disabling this prevents access through source.	udp_pmtu_discover	1			0
Other networking suggestions					
Give additional consideration to changing these common settings allowing for greater RAS.					
Configure /etc/sendmail.cf to allow mail out DMsmtp [MX.IP.addr]	vi /etc/sendmail.cf DMsmtp [MX.IP.addr]				
Configure /usr/lib/share/Mail.rc to forward mail to mail server - alias root user@domain.com	vi /usr/share/lib/Mail.rc alias root user@domain.com				
Review /etc/hosts add hosts as required in the preferred format: 10.0.0.1 hostname.fqdn hostname					

Description	Action	Default value	Low security	Medium security	High security
Control DNS lookup order	vi /etc/netsvc.conf Add a line hosts=local,bind				
Time synchronization should be enabled on all systems to ensure accurate timekeeping.	Use ntp or timed in line with your environment.				
Operational verification					
Verify that AIX system and utilities are operational on your new RS/6000 system. Initiate a full system backup.					
Review installed hardware, adapters, and disks against your order.	lscfg or prtconf				
Test hardware components	diag -a then diag				
Take a system snapshot	snap -a then snap -c				
Test the Dump Facility Crash running system	ctrl-alt-numpad1 or reset button then reboot				
Review the dump file.	#kdb /var/adm/ras/vmcore.0 /unix (0)> status (0)> stat (0)> quit				
Perform a mksysb backup of your RS/6000 system image.	smitty mksysb				
Documentation					
Content from the following Web sites is very valuable. Review and bookmark these Web sites as needed.					
Recommended Web sites	http://techsupport.services.ibm.com® http://www.redbooks.ibm.com http://www.ibm.com/aix http://www.ibm.com/servers				
Tape information	http://www.rs6000.ibm.com/support/micro/tapewhdr.html				
IBM Learning Services provides a full range of courses for AIX system administration	http://www.ibm.com/education				

Abbreviations and acronyms

AH	Authentication Header
AIX	Advanced Interactive Executive
APAR	Authorized Program Analysis Report
API	application programming interface
ASCII	American National Standard Code for Information Interchange
CA	Certificate Authority
CBC	Cipher Block Chaining
CERT	Computer Emergency Response Team
CRL	Certificate Revocation List
DCE	Distributed Computing Environment
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DTD	Document Type Definition
EIM	Enterprise Identity Mapping
ESP	Encapsulating Security Payloads
FQDN	Fully Qualified Domain Name
HMAC	Hashed Message Authentication Code
HTTP	Hypertext transfer Protocol
IBM	International Business Machines Corporation
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ITSO	International Technical Support Organization
IVP	Installation Verification Procedure
KDC	Key Distribution Center
KRB	Kerberos
LAN	local area network
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
NAT	network address translation
NTP	Network Time Protocol
OS	operating system
PAM	Pluggable Authentication Module
PFS	perfect forward secrecy
PTF	Program Temporary Fix
RAS	reliability, availability, and serviceability
RCMDS	Remote Commands
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman Algorithm
SA	Security Associations
SHA	Secure Hash Algorithm
SNA	Systems Network Architecture
SPI	Security Parameter Index
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TGT	Ticket Granting Ticket

VPN	virtual private network
XML	Extensible Markup Language
WSM	Web-based System Manager

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 175. Note that some of the documents referenced here may be available in softcopy only.

- *TCP/IP Tutorial and Technical Overview*, GG24-3376
- *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management*, SG24-5309
- *AIX 5L Differences Guide Version 5.2 Edition*, SG24-5765
- *AIX 4.3 Elements of Security: Effective and Efficient Implementation*, SG24-5962
- *Auditing and Accounting on AIX*, SG24-6020
- *Implementing VPNs in a z/OS Environment*, SG24-6530
- *AIX and Linux Interoperabilty*, SG24-6622

Other publications

These publications are also relevant as further information sources:

- *IBM AIX 5L Version 5.2 Commands Reference, Volume 1*, SC23-4115
- *IBM AIX 5L Version 5.2 Commands Reference, Volume 4*, SC23-4118
- *AIX 5L Version 5.2: System Management Concepts: Operating System and Devices*, SC23-4311
- *AIX 5L Version 5.2: Security Guide*, SC23-4860
- *IBM AIX 5L Expansion Pack CD*, LCD4-1142

Online resources

The following online resources are also relevant as further information sources:

- CERT, particularly the *Denial of Service Attacks* article

  `http://www.cert.org`

- Diffie- Hellman

  `http://www.rsasecurity.com/rsalabs/faq/3-6-1.html`

- HMAC-MD5

  `http://researchweb.watson.ibm.com/security/draft-ietf-ipsec-hmac-md5-00.txt`

- IBM AIX 5L operating system

  `http://www-1.ibm.com/servers/aix/index.html`

- IBM AIX Product Documentation library

  `http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/aix52.htm`

- IBM AIX Product Fixes

  `https://techsupport.services.ibm.com/server/aix.fixsearch52`

- IBM AIX Technical Tips

  `https://techsupport.services.ibm.com/server/aix.srchBroker`

- Kerberos information from the Massachusetts Institute of Technology (MIT)

  `http://web.mit.edu/kerberos/`

- NFSNET

  `http://www.nfsnet.org`

- RFC

  `http://www.rfc.org/rfc`

  In particular, refer to the following RFCs:

  - RFC 2307: *An Approach for using LDAP for a Network Information Service*
  - RFC 2401: *Security Architecture for the Internet Protocol*
  - RFC 2402: *IP Authentication Header*
  - RFC 2406: *IP Encapsulating Security Payload (ESP)*
  - RFC 2408: *Internet Security Association and Key Management Protocol (ISAKMP)*
  - RFC 2409: *The Internet Key Exchange (IKE)*

- RFC 2709: *Security Model with Tunnel-mode IPSec for NAT Domains*
- RFC 3456: *Dynamic Host Configuration Protocol (DHCPv4): Configuration of IPSec Tunnel Mode*
- RFC 3526: *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*

- *Designing an Authentication System: A Dialogue in Four Scenes* by Bill Bryant

  http://web.mit.edu/kerberos/www/dialogue.html

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

IBM Redbooks

AIX 5L Version 5.2 Security Supplement

(0.2”spine)
0.17”<->0.473”
90<->249 pages

IBM®

AIX 5L Version 5.2 Security Supplement

Redbooks

Gain insight to security and related features for AIX 5L Version 5.2

Improve security using practical examples and recommendations

Learn about and use VPN, NAS, and PAM

This IBM Redbook serves as a supplement to the IBM AIX 5L Version 5.2 product documentation, particularly *AIX 5L Version 5.2 Security Guide*, SC23-4860. This redbook provides additional detailed information about virtual private networks (VPN), Kerberos security and the use of secure remote commands (RCMDS), Pluggable Authentication Modules (PAM), and examples on how to restrict users. You can use these features individually or integrate them together to improve AIX system security.

Use this redbook as an additional source for security information. Together with existing sources, you may use this redbook to enhance your knowledge of security and the features included with AIX 5L Version 5.2. You learn about the practical use of these security features, why they are necessary, and how you can use them in your environment to improve security. Plus you gain practical guidance through the examples that are provided and the recommendations for best practice.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6066-00 ISBN 0738499072