AIX IP Security

By Kay Chang, Jackie Wilson, and Jason Wu

The Virtual Private Network (VPN) provides end-to-end secure connectivity over the Internet. AIX Version 4.3 has a VPN built-in to its operating system. AIX IP Security is a robust, IETF standards-conforming product implementing a VPN solution with easy-to-use, policy-based management.

The Internet has become a ubiquitous means of connectivity, and most companies now include the World Wide Web Uniform Resource Locator (URL) in their business addresses. Nearly everyone is now aware of the Internet, the enormous volume of information made available by both organizations and individuals, and the ability to retrieve that information.

Gradually, people have begun to view the loosely interconnected Internet as a means of extending the enterprise network. For example, remote business users can connect to their corporate network or to their business partners' network. The greatest challenge, however, has been to provide authenticity and privacy as needed, yet have the ability to use an insecure, open, public data network like the Internet.

The Virtual Private Network (VPN) is a mechanism to create a private "tunnel" over the public Internet that enables remote corporate users, branch offices, and business partners/suppliers to exchange information. The goal of a VPN is to provide end-to-end connectivity using the Internet, yet provide the dependability, security, and reliability that enterprises require in a private network. A VPN can also provide significant savings. A 1997 VPN Research Report by Infonetics Research, Inc. estimates that companies can save from 20% to 47% of their wide area network (WAN) costs by replacing leased lines with VPNs to remote sites.

AIX IP Security functions provide those VPN requirements since AIX® uses open, standard IP security functions including integrity, authenticity, and confidentiality. It interoperates with other IP security providers, and configures and manages its resources with a policy-based mechanism.

In addition to the IP security function, AIX IP Security also filters non-secure packets based on user-defined criteria (filter rule). This is primarily a firewall function where packet control between networks and machines is enforced.

What is AIX IP Security?

IP Security provides cryptography-based protection for all data at the IP layer for both IP Security Versions 4 and 6. It transparently provides secure communications, with no changes required to existing applications. Using robust cryptographic techniques, IP Security protects your data traffic in three ways:

- **Authentication:** Verifies the identity of a host or endpoint. Authentication algorithms provide proof of identity of the sender and data integrity. These algorithms use a cryptographic hash function to process a packet of data (with the immutable IP header fields included) with a secret key to produce a unique digest. On the receiver's side,

Kay Chang

Jackie Wilson

Jason Wu

the data is deciphered using the same function and key. If either the data has been altered or the sender's key is not valid, the datagram is discarded.

- **Integrity checking:** Ensures that no modifications were made to the data while in transit across the network. If any part of the data is modified during communication, the authentication check will fail.

- **Encryption:** "Hides" data and private IP addresses while in transit across the network in order to ensure privacy. Encryption uses a cryptographic algorithm to modify and randomize the data using a certain algorithm and key to produce "cyphertext." This makes the data unreadable while in transit. Once received, the data is recovered using the same algorithm and key using symmetric encryption algorithms. Encryption must occur with authentication to verify the data integrity of the encrypted data.

Tunnels

A *tunnel* is a virtual connection between two data endpoints. Tunnels can be used to set up a secure communication between two machines. Both sides must agree to the security parameters before the tunnel will work. This is known as setting up a security association.

The security association can use either static, manually distributed keys, or automatically refreshed keys. To comply with Internet Engineering Task Force (IETF) standards, all implementations must use manual keying. This ensures a base set of cryptographic capabilities that will allow IP security implementations from different vendors to interoperate.

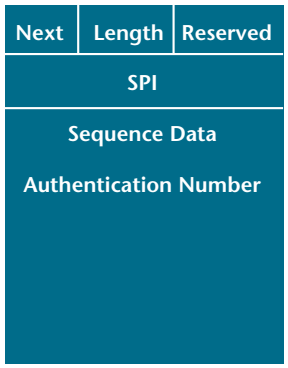
IBM has developed a method known as *IBM tunnels* for automatically refreshing keys. Packets sent and received on an agreed-upon port number negotiate the security association parameters and automatically refresh keys.

The IETF is currently developing a standard for implementing automatic key management known as ISAKMP/Oakley. This protocol, once fully defined and implemented, will replace IBM tunnels. IBM tunnels are currently implemented in AIX Firewall beginning with Version 2.1 and in AIX 4.3. It can be used today for automatically refreshing keys.

Evolving Standards

IP Security protects data by using the Authentication Header (AH) or Encapsulating Security Payload (ESP) header and encrypted payload inserted in the IP packet. The authentication header can be used by itself or in combination with the ESP header. In the first RFC versions of the IP security headers, authentication data was sent using an AH. Encrypted data, or cyphertext, was sent in a separate ESP header. In 1997, the ESP header format was extended to include a field for the authentication digest to enable both encryption and authentication information to be processed in one header. In addition, both AH and ESP formats were extended for replay protection by including a sequence number that prevents old replay packets from being accepted. Figure 1 shows the AH format and Figure 2 shows the ESP format for the new IETF headers.

Authentication Header



AH Format Features

- **NEXT** is the 8-bit "next protocol" field from IP
- **LENGTH** is the length of this header in 32-bit words
- **SPI** is a 32-bit field identifying this security association
- **SEQUENCE NUMBER** is a 32-bit counter used to detect and reject replayed packets
- **RESERVED** is a 16-bit field, currently all zeros
- **AUTHENTICATION DATA** contains the value computed by the authentication algorithm, padded to an integral multiple of 32 bits

Figure 1. Authentication header for new IEFT headers

A new Hashed Message Authentication Code (HMAC) standard for strengthening the security of authentication algorithms was adopted in RFC 2104. IP security support for AIX 4.3 implements the RFC versions of the headers for backward compatibility and the new draft standards. Supported authentication algorithms in AIX 4.3 are HMAC MD5 (Message Digest 5, RFC 1321), HMAC SHA1 (Secure Hash Algorithm) and Keyed MD5 (for backward compatibility). The authentication algorithm determines the header format.

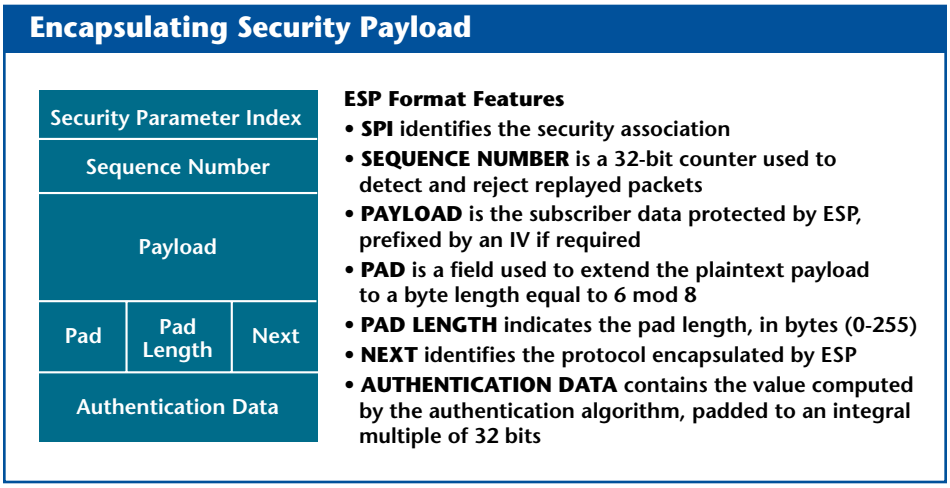


Figure 2. ESP format for new IETF headers

Encryption algorithms include DES_CBC_8 (Data Encryption Standard Cypher Block Chaining), DES_CBC_4, and an exportable version of DES known as Common Data Masking Facility (CDMF). AIX 4.3 IP Security also supports the ability to send authentication data in the ESP header, sometimes referred to as DES_CBC_MD5.

Filtering Capability

Filtering is a function in which incoming and outgoing packets can be accepted or denied based on a variety of characteristics. This allows a user or systems administrator to configure the host to control the traffic between this host and other hosts. Filtering is done on a variety of packet properties, such as source and destination addresses, IP Security Version (4 or 6), subnet masks, protocol, port, routing characteristics, fragmentation, interface, and tunnel definition.

Rules known as filter rules associate certain kinds of traffic with a particular tunnel. In our basic configuration, when a user defines a tunnel, filter rules are automatically generated to direct all traffic from that host through the secure tunnel. If more specific types of traffic are desired, the filter rules can be modified to allow precise control of the traffic using a particular tunnel.

Similarly, when the tunnel is modified or deleted, the filter rules for that tunnel are automatically modified or deleted. This greatly simplifies IP Security configuration and helps reduce human error. Tunnel definitions can be propagated and shared among AIX machines and AIX Firewall using import and export utilities.

Filter rules are necessary to associate a particular type of traffic with a tunnel, but data being filtered does not necessarily need to travel in a tunnel. This allows AIX to provide base firewall function for users who want to restrict the flow of certain types of traffic to or from their machine. This is especially useful for the administration of machines in an intranet or for those that do not have firewall protection.

Dual Stack Support

AIX IP Security Versions 4 and 6 implement two separate stacks. This enables the IP Security function to be configured independently. The IP Security function can be enabled, disabled, or modified on one IP Version without affecting the behavior of the other. (See Figure 3).

Configuring AIX IP Security

Since all IP traffic will get filtered, it is important to set the default filtering behavior before IP Security is started. The default rule will determine whether traffic that does not match any prior filter rule will be permitted or denied. In a client scenario where a user wants to set up a secure tunnel, but otherwise not use filters, the default action

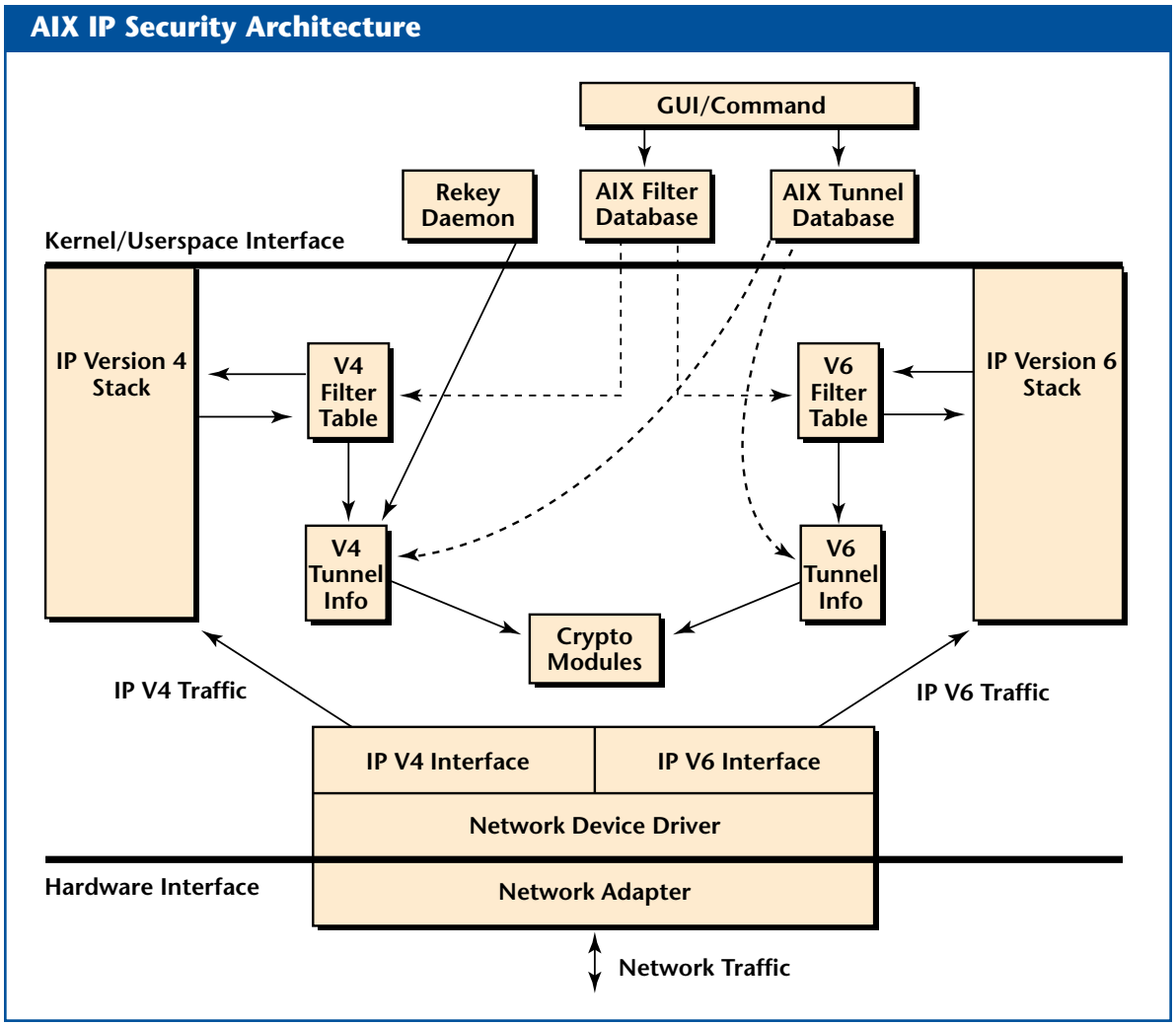


Figure 3. Architecture for AIX IP Security

would be permit. In the case where filter rules were being used to protect incoming and outgoing traffic, such as in a firewall or intermediate gateway, the default action would be deny. The default action is selected using the SMIT Start/Stop IP Security panel shown in Figure 4.

Once the default behavior is set, the user can define tunnels. To define a tunnel, the user must know the IP address of the remote host, whether the remote host is behind a firewall, and how the data in the tunnel should be protected. The tunnel may provide authentication, or both authentication and encryption. If the security characteristics of the remote side are known, then the user simply matches the characteristics of the remote and inserts the appropriate IP address information. If the user is setting up the initial end of the tunnel, then the user can select the characteristics desired.

For an IBM tunnel, the user specifies the IP addresses of the endpoints of the tunnel and firewall (if applicable), the encryption algorithm (if encryption is to be used), the life time of the session key, the key refresh time, and whether that

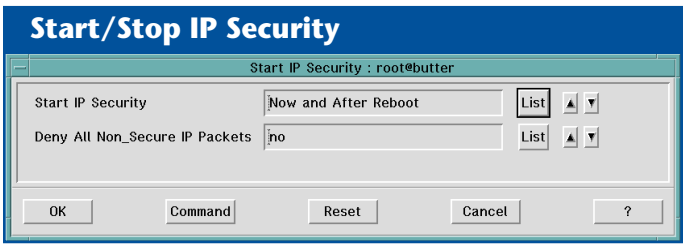


Figure 4. Start/Stop IP Security

host will act as the initiator of the key exchange communication.

For a manual tunnel, the user specifies the IP addresses of the endpoints and firewall (if applicable), selects the AH and ESP algorithms, and the destination Security Parameter Index (SPI) value. Together with the IP address, this uniquely identifies the tunnel. The keys can be manually entered or automatically generated.

Due to export regulations, U.S. and Canadian customers get a higher degree of encryption (for example, DSS), whereas other countries have their own import restrictions.

SMIT Configuration Path

Figures 5 and 6 show examples of setting up two types of manual tunnels. One tunnel is connected to a remote system 9.3.97.112 using SPI value 500. The other tunnel is connected to a remote system 9.53.159.251 behind a firewall using SPI value 501. Both use an AH/ESP combination with HMAC MD5 for authentication and DES_CBC_8 for encryption. The data will be encapsulated in the draft standard versions of the AH and ESP headers. Since this is a manual tunnel, the remote machine can be any vendor's machine running IP Security with the draft standard version of AH and ESP. The keys are manually exchanged.

Both tunnels have automatically generated filter rules, and all traffic between the tunnel endpoints will be sent through the tunnel. Any packets that are not protected by the specified security parameters are discarded, and all packets will be authenticated and encrypted.

Additional filter rules can be specified by using any of the modifiers such as IP Source and destination masks, protocol, port number, routing, interface, and fragmentation control. Operators, such as less than, greater than, equal to, and not equal can be used on the port number fields. This provides great flexibility and control in specifying data to be protected in a tunnel or to be permitted or denied from flowing outbound or inbound. See Figure 7 for an example of the filter rules that were automatically generated.

Once the filter rules are generated, they are stored in a table and loaded into the kernel. When packets are ready to be sent or received from the network, the filter rules are checked in the list from top to bottom to determine whether the packet should be

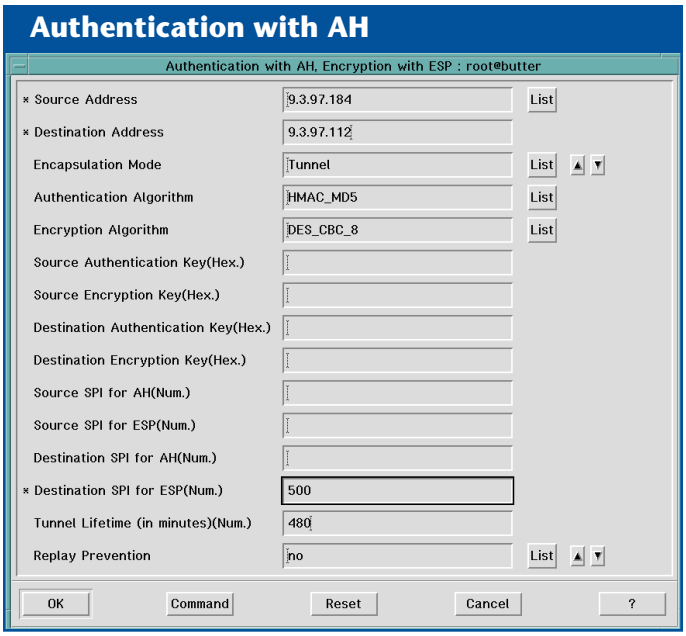


Figure 5. Using AH for authentication

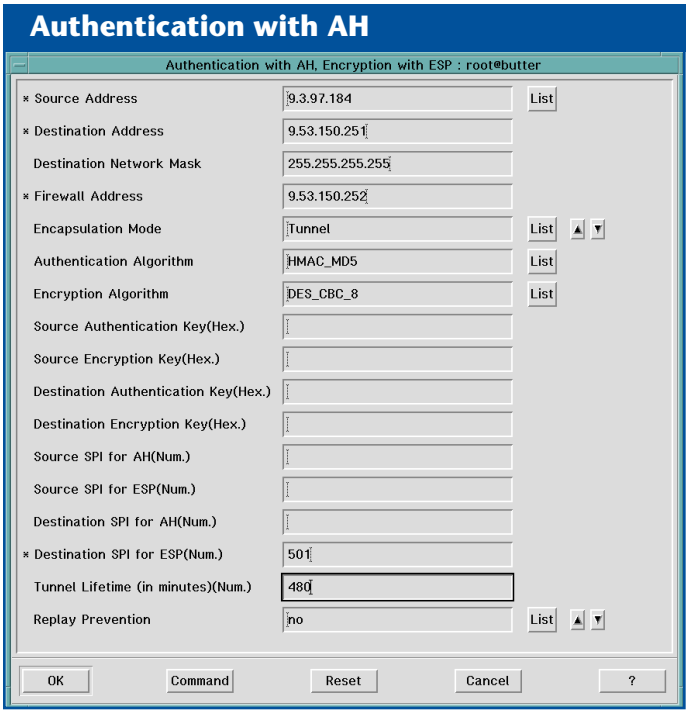


Figure 6. AH authentication

permitted, denied, or sent through a tunnel. The rule criteria are compared to the packet characteristics until a match is found or the default rule is reached. Figure 8 shows a listing of the filter rule.

The first three general rules (not specific to any configured tunnel) allow AH, ESP, and IBM tunnel session traffic to flow. Rules 4 and 5 are the rules for tunnel number 1, which is the first manual tunnel shown earlier (see Figure 5). Rules 6 and 7 allow traffic for tunnel number 2, as shown in Figure 6. Rule number 0 (last rule to match), the default rule, shows the permit default action on packets that do not match any prior rules.

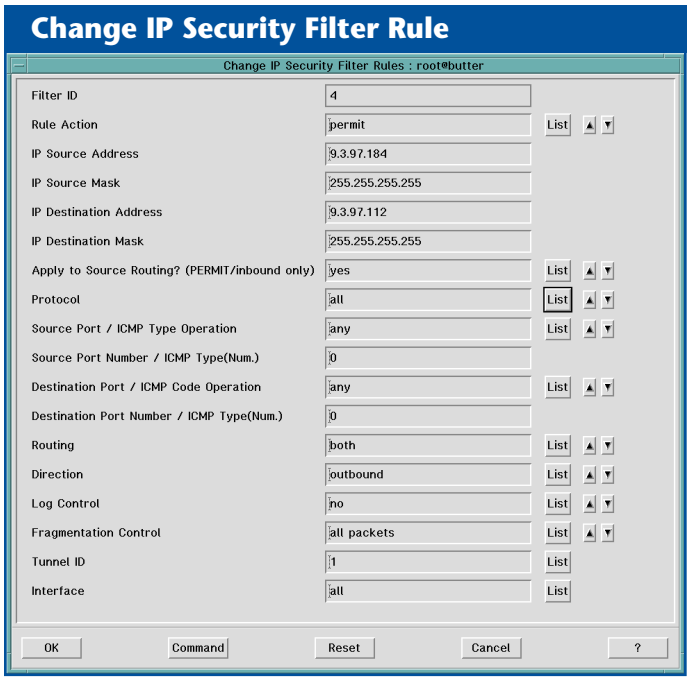


Figure 7. Filter rule for change IP security

VPN Scenarios and IP Security Solutions

Three obvious VPN scenarios today include:

- Remote and secure access
- Extranet with business partner or supplier intranet
- Branch office intranet

Figure 9 highlights these scenarios.

Remote Secure Access

The remote access environment is one in which a mobile computer is connected to the corporate network. These connections are primarily handled by dial-up links, such as point-to-point protocol (PPP). Multiple

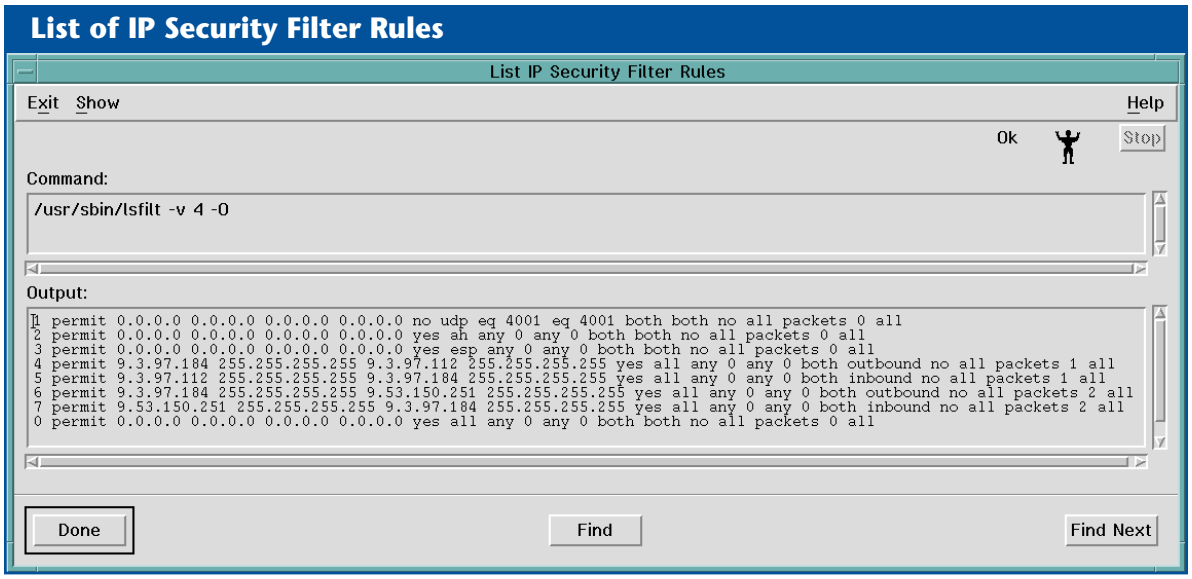


Figure 8. Filter rules for IP security

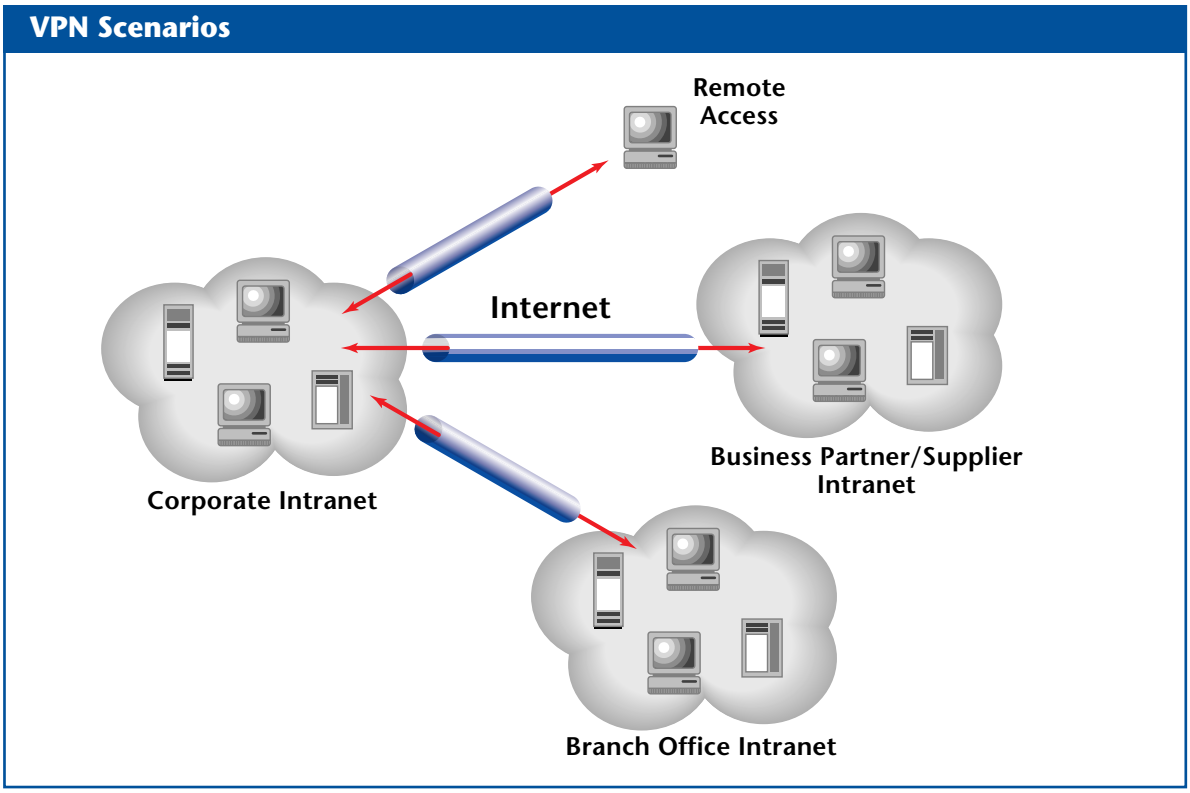


Figure 9. VPN Scenarios

modem banks provide the incoming connection, often with long distance carrier charges.

The IP security function of VPN lets users dial the local calling number of the Internet Service Provider (ISP), where end-to-end security is achieved by creating a separate tunnel between a remote mobile computer to the server inside the corporate network. This is end-to-end tunnel flow through the ISP and corporate firewall to the destination server.

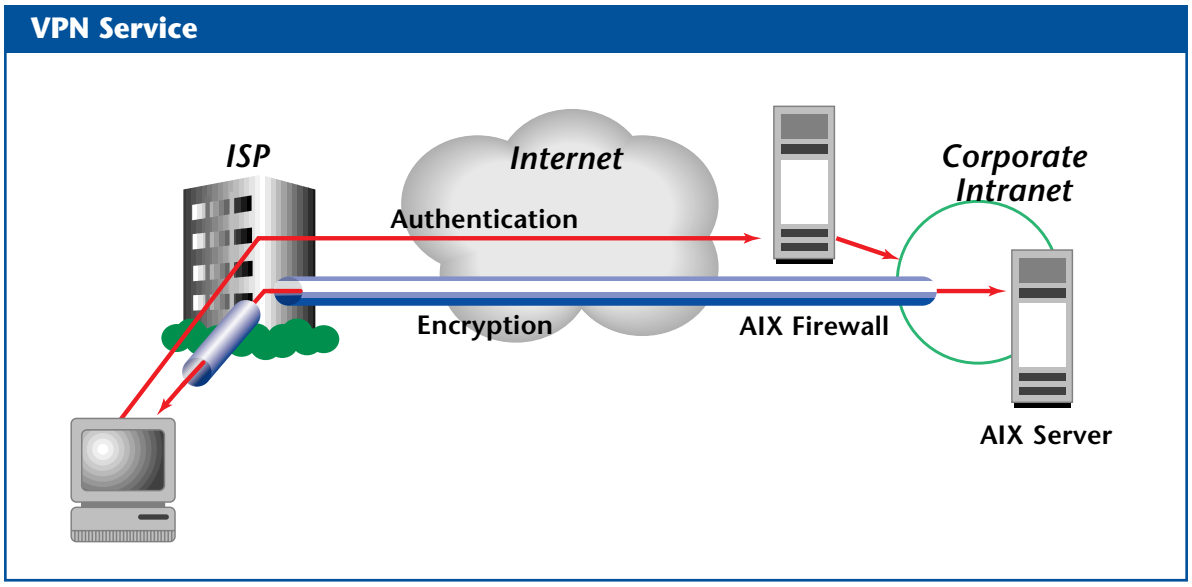


Figure 10. VPN Service

Extranet with Business Partner/Supplier

The extranet environment interconnects the corporate intranet to intranets from business partners and/or suppliers via the Internet. Many corporations have created and maintained a separate security policy and a private data network. Often when companies merge or when they must communicate with suppliers, the setup and operational costs are prohibitably high for smaller business partners because of the high costs of maintaining the network charges (such as leased T1 lines). The VPN based on IP Security provides a cost-effective, secure, end-to-end communication over the Internet.

Branch Office Intranet

A branch office intranet is a secure interconnection between the branch intranet and the corporate intranet. Unlike the supplier network, it is expected to have a similar setup in types of networks and applications. It generally requires expensive leased-line connections or on-demand dial connections to the home office. A VPN with IP Security provides 24-hour ease-of-use connectivity via inexpensive Internet links.

Solutions with IP Security

Each scenario described above highlights the problems facing businesses today. AIX IP Security addresses these situations with authenticity and confidentiality. It works with most firewall products to support popular mobile or desktop clients with an IP security solution.

Conclusion

The VPN provides end-to-end secure connectivity over the Internet. AIX IP Security is a robust, IETF standards-conforming product implementing a VPN solution with ease-of-use, policy-based management.

VPN is built-in to both AIX Version 4.3 and the IBM Firewall product. Popular client products, such as Microsoft® Windows™, have available offerings from IBM add-on or third-party vendors.

One important consideration is that using the Internet as a dedicated private network requires a service level agreement (SLA) to guarantee quality of service that the Internet lacks. Vendors must develop a service to provide functions that the business demands and expects. Since the Internet consists of loosely interconnected heterogeneous networks, it only guarantees a service level at best basis. Service providers, such as IBM Global Services, must add extra services for the VPN to provide availability, performance, and reachability. IBM began the SLA initiative to help solve these problems faced by companies using the Internet.

***Kay Chang**, IBM Corporation, 11400 Burnet Road, Austin, TX 78758. Ms. Chang is a senior programmer in AIX communication architecture working on AIX Connections and the Network Computer. She has an MS in Computer Science from Wright State University in Dayton, Ohio.*

***Jackie Wilson**, IBM Corporation, 11400 Burnet Road, Austin, TX 78758. Ms. Wilson is the project lead and a programmer on the AIX implementation of IP Security shipped in AIX 4.3. Since joining IBM in 1982, she has programmed and led projects in wide area networks, developed device drivers and adapter software for X.25, SDLC, bisync and modem support. She has a BSEE in Electrical Engineering and Computer Science from Princeton University and an MBA from St. Edwards University. She is also the inventor of three software patents in network programming.*

***Xinhua (Jason) Wu**, IBM Corporation, 11400 Burnet Road, Austin, TX 78758. Mr. Wu is an advisory programmer with AIX Development. He has an MS in Computer Science from the University of Southern California.*