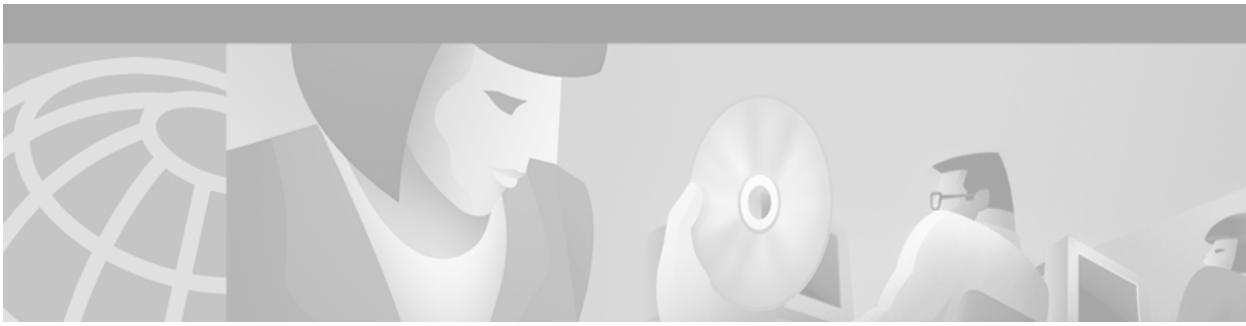

IP Security and Encryption Overview

This chapter briefly describes the following security features and how they relate to each other:

- IPSec Network Security
- Certification Authority Interoperability
- Internet Key Exchange Security Protocol

IPSec Network Security

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards:

- IPSec
- Internet Key Exchange (IKE)
- Data Encryption Standard (DES)
- MD5 (HMAC variant)
- SHA (HMAC variant)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

IPSec services provide a robust security solution that is standards-based. IPSec also provides data authentication and anti-replay services in addition to data confidentiality services.

For more information regarding IPSec, refer to the chapter "Configuring IPSec Network Security."

IPSec Encryption Technology

IPSec protects sensitive data that travels across unprotected networks. IPSec security services are provided at the network layer, so you do not have to configure individual workstations, PCs, or applications. This benefit can provide a great cost savings. Instead of providing the security services you do not need to deploy and coordinate security on a per-application, per-computer basis, you can simply change the network infrastructure to provide the needed security services.

IPSec encryption offers a number of additional benefits:

- Because IPSec is standards-based, enables Cisco devices to interoperate with other IPSec-compliant networking devices to provide the IPSec security services. IPSec-compliant devices could include both Cisco devices and non-Cisco devices such as PCs, servers, and other computing systems.

  Cisco and its partners, including Microsoft, are planning to offer IPSec across a wide range of platforms, including Cisco IOS software, the Cisco PIX Firewall, and Windows 2000.

- Enables a mobile user to establish a secure connection back to the office. For example, the user can establish an IPSec "tunnel" with a corporate firewall—requesting authentication services—in order to gain access to the corporate network; all of the traffic between the user and the firewall will then be authenticated. The user can then establish an additional IPSec tunnel—requesting data privacy services—with an internal router or end system.
- Provides support for the Internet Key Exchange (IKE) protocol and for digital certificates. IKE provides negotiation services and key derivation services for IPSec. Digital certificates allow devices to be automatically authenticated to each other without manual key exchanges.

Certification Authority Interoperability

Certification Authority (CA) interoperability is provided in support of the IPSec standard. It permits Cisco IOS devices and CAs to communicate so that your Cisco IOS device can obtain and use digital certificates from the CA. Although IPSec can be implemented in your network without the use of a CA, using a CA provides manageability and scalability for IPSec.

For more information regarding CA interoperability, refer to the chapter "Configuring Certification Authority Interoperability."

Internet Key Exchange Security Protocol

Internet Key Exchange (IKE) security protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

For more information regarding IKE, refer to the chapter "Configuring Internet Key Exchange Security Protocol."