



## Supported VPN Standards

---

This appendix lists the VPN standards supported by PIX Firewall version 6.2. It contains the following sections:

- [IPSec](#)
- [Internet Key Exchange \(IKE\)](#)
- [Certification Authorities \(CA\)](#)

### IPSec

- **IPSec—IP Security Protocol.** IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IPSec is documented in a series of Internet RFCs, all available at the following website:

<http://www.ietf.org/html.charters/ipsec-charter.html>

The overall IPSec implementation is guided by “Security Architecture for the Internet Protocol,” RFC 2401.

- **Internet Key Exchange (IKE)**—A hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys.

IPSec as implemented in PIX Firewall supports the following additional standards:

- **AH—Authentication Header.** A security protocol that provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).

The AH protocol (RFC 2402) allows for the use of various authentication algorithms; PIX Firewall has implemented the mandatory MD5-HMAC (RFC 2403) and SHA-HMAC (RFC 2404) authentication algorithms.

- **ESP—Encapsulating Security Payload.** A security protocol that provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

The ESP protocol (RFC 2406) allows for the use of various cipher algorithms and (optionally) various authentication algorithms. The PIX Firewall implements the mandatory 56-bit DES-CBC with Explicit IV (RFC 2405); as the encryption algorithm, and MD5-HMAC (RFC 2403) or SHA-HMAC (RFC 2404) as the authentication.

## Internet Key Exchange (IKE)

IKE is implemented per “The Internet Key Exchange” (RFC 2409).

ISAKMP—The Internet Security Association and Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

ISAKMP is implemented per “Internet Security Association and Key Management Protocol (ISAKMP)” (RFC 2408).

Oakley—A key exchange protocol that defines how to derive authenticated keying material.

Skeme—A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.

The component technologies implemented for use by IKE include:

- DES—Data Encryption Standard (DES) is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. See “CBC.”
- Triple DES (3DES)—A variant of DES, which iterates three times with three separate keys, effectively doubling the strength of DES.
- CBC—Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPsec packet.
- Diffie-Hellman—A public-key cryptography protocol which allows two parties to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit and 1024-bit Diffie-Hellman groups are supported.
- MD5 (HMAC variant)—Message Digest 5 (MD5) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.
- SHA (HMAC variant)—Secure Hash Algorithm (SHA) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.
- RSA signatures—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provide non-repudiation.

IKE Extended Authentication (Xauth) is implemented per the IETF draft-ietf-ipsec-isakmp-xauth-04.txt (“extended authentication” draft). This provides this capability of authenticating a user within IKE using TACACS+ or RADIUS.

IKE Mode Configuration (IKE Mode Config) is implemented per the IETF draft-ietf-ipsec-isakmp-mode-cfg-04.txt. IKE Mode Configuration provides a method for a security gateway to download an IP address (and other network level configuration) to the VPN client as part of an IKE negotiation.

# Certification Authorities (CA)

IKE interoperates with the following standard:

X.509v3 certificates—Used with the IKE protocol when authentication requires public keys. Certificate support that allows the IPSec-protected network to scale by providing the equivalent of a digital ID card to each device. When two peers wish to communicate, they exchange digital certificates to prove their identities (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer). These certificates are obtained from a certification authority (CA). X.509 is part of the X.500 standard by the ITU.

CA supports the following standards:

- X.509v3 certificates.
- Public-Key Cryptography Standard #7 (PKCS #7)—A standard from RSA Data Security, Inc. used to encrypt and sign certificate enrollment messages.
- Public-Key Cryptography Standard #10 (PKCS #10)—A standard syntax from RSA Data Security, Inc. for certificate requests.
- RSA Keys—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA keys come in pairs: one public key and one private key.

■ Certification Authorities (CA)