

IPv4 IPSec – Internet Key Exchange

RFC 2409 - Internet Key Exchange (IPv1)
RFC 4306 - Internet Key Exchange (IPv2)

Used for performing mutual authentication and establishing and maintaining security associations (SAs) between two parties, Initiator and Responder, a two-phase negotiation process

IKE is considered "Hybrid" protocol

ISAKMP – Internet Security Association and Key Management Protocol
(Framework for exchanging encryption keys and Security Associations (SA))

IKE uses two exchange protocols:

- Oakley, most of the IKE key exchange is based on OAKLEY
- SKEME IKE uses some functions of SKEME and its fast re-keying features

ISAKMP Phase 1 (Main/Aggressive mode) - Setup stage - agree on how to exchange further information securely - creates a SA for the ISAKMP itself - an ISAKMP SA, also called the **control SA**, the SA used for securely exchanging more detailed information in phase 2.

(Three two-way exchanges between initiator and receiver)

Phase 1 includes the negotiation of the following attributes:

- An encryption algorithm to be used, such as 3DES-CBC
- A hash algorithm (MD5 or SHA, as used by AH or ESP).
- An authentication method, such as a pre-shared key or X.509 Certificate.
- Using a Diffie-Hellman exchange to generate shared secret keying material used to generate shared secret keys and to pass nonce, (random numbers).

ISAKMP Phase 2 (Quick mode) - ISAKMP phase 1 SA is used to create SAs for other security protocols - The "real" SAs for the ESP protocol is negotiated, called the **child SA**. Also used to renegotiate a new IPSec SA when the lifetime expires.

ISAKMP Main-mode – Phase 1
6-exchanges

Initiator **Responder**

HDR,[SA] proposal(s) →
HDR,[SA] choice ←

Parameter negotiation is completed; an agreement is reached

HDR,[KE]_i,[NONCE]_i →
HDR,[KE]_r,[NONCE]_r ←

Both DH public keys exchange

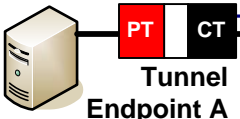
DH Key-exchange payloads [KEs] and **Nonces** are derived from the KEs by both the initiator and the responder. The nonces are exchanged at this point to defeat replay.

HDR*,[ID]_i,[AUTH]_i →
HDR*,[ID]_r,[AUTH]_r ←

IDs have been exchanged. Each party has exchanged information and authentication. The IDs and AUTHs are used to verify the other party. The algorithms used are agreed upon.

The computation of the shared secret key is performed according to RFC 2409 d

(In ISAKMP **aggressive-mode** 3-exchanges, the negotiation and the key exchange at the same time. Identity protection or PSK Hash protection is transmitted in plaintext)

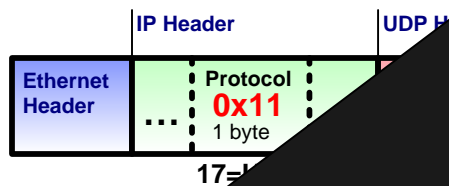


Black (CT)
"unsecure"
network

The IKE protocol uses **UDP** 4-6 packets with 2-3 tunnels. IKE uses a **Diffie-Hellman** session secret.

When peers negotiate a main mode SA across a **NAT**, only the initial IKE message from the initiating IPsec peer uses UDP port 500. **All other IKE traffic is sent over UDP port 4500.**

IPsec NAT-T
UDP port 4500



IKE Payload Header

Next Payload Type
1 byte

IKEv2

payload

SA payload (proposals / transforms / cert / notify, ...)

Bit 2 Authentication Only (Notify)