

Protocols

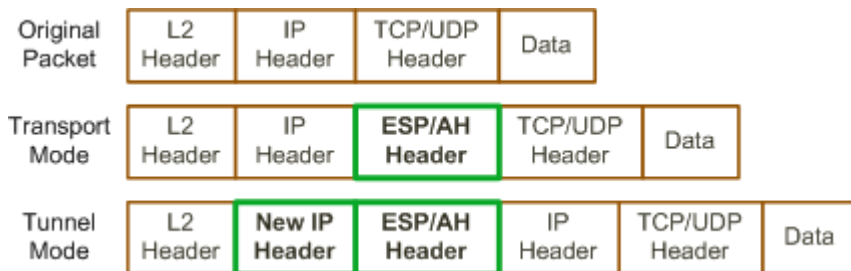
Internet Security Association and Key Management Protocol (ISAKMP) · A framework for the negotiation and management of security associations between peers

Internet Key Exchange (IKE) · Responsible for key agreement using public key cryptography; traverses TCP port 500

Encapsulating Security Payload (ESP) · Provides data encryption, data integrity, and peer authentication; IP protocol 50

Authentication Header (AH) · Provides data integrity and peer authentication, but not data encryption; IP protocol 51

IPsec Modes



Transport Mode · The ESP or AH header is inserted behind the IP header; the IP header can be authenticated but not encrypted

Tunnel Mode · A new IP header is created in place of the original; this allows for encryption of the entire original packet

Encryption Algorithms

| | Type | Key | Strength |
|-------------|------------|----------------------|----------|
| DES | Symmetric | 56-bit | Weak |
| 3DES | Symmetric | 168-bit | Medium |
| AES | Symmetric | 128, 192, or 256-bit | Strong |
| RSA | Asymmetric | 1024-bit minimum | Strong |

Hashing Algorithms

| | Length | Strength |
|--------------|---------|----------|
| MD5 | 128-bit | Medium |
| SHA-1 | 160-bit | Strong |

IKE Phases

Phase 1 · A bidirectional ISAKMP SA is established between peers to provide a secure management channel; IKE is performed in main mode or aggressive mode

Phase 1.5 (optional) · Xauth can optionally be implemented to enforce user authentication

Phase 2 · Two unidirectional IPsec SAs are established for data transfer using separate keys; IKE quick mode is used

Configuration

ISAKMP Policy

```
crypto isakmp policy 10
  encryption aes 256
  hash sha
  authentication pre-share
  group 2
  lifetime 3600
crypto isakmp key SECRET-STRING address 172.16.0.5
```

IPsec Transform Set

```
crypto ipsec transform-set F00 esp-aes 256 esp-sha-hmac
mode tunnel
```

Interesting Traffic ACL

```
access-list 123 permit ip any 10.2.0.0 0.0.255.255
```

Crypto Map

```
crypto map BRANCH-OFFICE 10 ipsec-isakmp
  set peer 172.16.0.5
  set transform-set F00
  match address 123
```

Crypto Map Application

```
interface Serial0/0
  crypto map BRANCH-OFFICE
```

Terminology

Data Integrity · Secure hashing (HMAC) is used to ensure data has not been altered in transit

Data Confidentiality · Encryption is used to ensure data cannot be intercepted by a third party

Data Origin Authentication · Peer authentication

Anti-replay · Sequence numbers are used to detect and block duplicate packets

Hash-based Message Authentication Code (HMAC) · A hash of the data and secret key used to provide message authenticity

Diffie-Hellman · A method of establishing a shared secret key over an insecure path using public and private keys

Troubleshooting

```
show crypto isakmp sa
```

```
show crypto isakmp policy
```

```
show crypto ipsec sa
```

```
show crypto ipsec transform-set
```

```
debug crypto isakmp
```

```
debug crypto ipsec
```