IPsec

Protocols

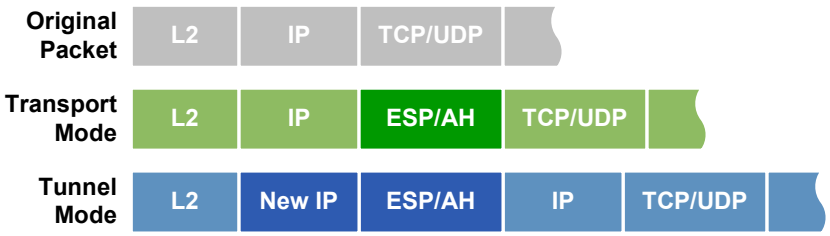
Internet Security Association and Key Management Protocol (ISAKMP)
A framework for the negotiation and management of security associations between peers (traverses UDP/500)

Internet Key Exchange (IKE)
Responsible for key agreement using asymmetric cryptography

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

Configuration

ISAKMP Policy

```
crypto isakmp policy 10
 encryption aes 256
 hash sha
 authentication pre-share
 group 2
 lifetime 3600
```

ISAKMP Pre-Shared Key

```
crypto isakmp key 1 MySecretKey address 10.0.0.2
```

IPsec Transform Set

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

IPsec Profile

```
crypto ipsec profile MyProfile
 set transform-set MyTS
```

Virtual Tunnel Interface

```
interface Tunnel0
 ip address 172.16.0.1 255.255.255.252
 tunnel source 10.0.0.1
 tunnel destination 10.0.0.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile MyProfile
```

Encryption Algorithms

	Type	Key Length (Bits)	Strength
DES	Symmetric	56	Weak
3DES	Symmetric	168	Medium
AES	Symmetric	128/192/256	Strong
RSA	Asymmetric	1024+	Strong

Hashing Algorithms

	Length (Bits)	Strength
MD5	128	Medium
SHA-1	160	Strong

IKE Phases

Phase 1
A bidirectional ISAKMP SA is established between peers to provide a secure management channel (IKE in main 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)

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
Authentication of the SA peer

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

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

Diffie-Hellman Exchange
A shared secret key is established 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 | ipsec}
```