# 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

## Encryption Algorithms

<table>
<thead>
<tr>
<th>Type</th>
<th>Key Length (Bits)</th>
<th>Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>Symmetric 56</td>
<td>Weak</td>
</tr>
<tr>
<td>3DES</td>
<td>Symmetric 168</td>
<td>Medium</td>
</tr>
<tr>
<td>AES</td>
<td>Symmetric 128/192/256</td>
<td>Strong</td>
</tr>
<tr>
<td>RSA</td>
<td>Asymmetric 1024+</td>
<td>Strong</td>
</tr>
</tbody>
</table>

## Hashing Algorithms

<table>
<thead>
<tr>
<th>Length (Bits)</th>
<th>Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5 128</td>
<td>Medium</td>
</tr>
<tr>
<td>SHA-1 160</td>
<td>Strong</td>
</tr>
</tbody>
</table>

## 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}`

## IPsec Modes

<table>
<thead>
<tr>
<th>Original Packet</th>
<th>L2</th>
<th>IP</th>
<th>TCP/UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Mode</td>
<td>L2</td>
<td>IP</td>
<td>ESP/AH</td>
</tr>
<tr>
<td>Tunnel Mode</td>
<td>L2</td>
<td>New IP</td>
<td>ESP/AH</td>
</tr>
</tbody>
</table>

## 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
```