Document Name: IPsec
IPsec or Internet Protocol Security is a standards-based security framework that has a lot of RFCs attached to it see some notable ones below.

- RFC 2408 (ISAKMP)
- RFC 2409 (IKE)
- RFC 4301 (IPsec Architecture)
- RFC 4302 (Auth Header)
- RFC 4303 (ESP)
- RFC 5996 (IKEv2)

IPsec has a few main features going for it those being:

- Data origin authentication
- Data integrity
- Data confidentiality
- Anti-replay

Here are some reasons why you might choose to use IPsec.

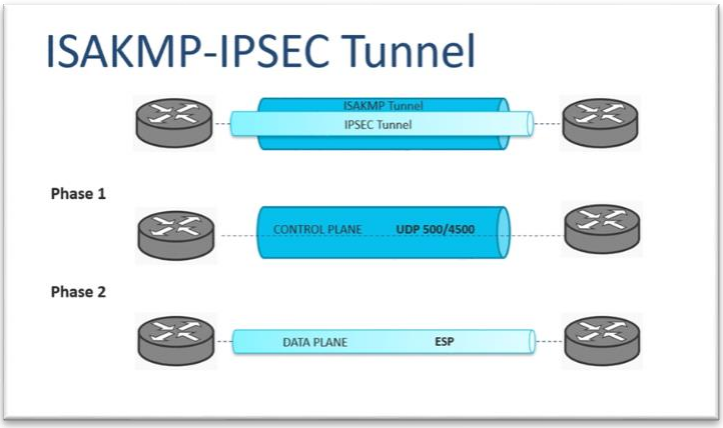
- Does not need static provisioning like MPLS
- Only requires IPv4/IPv6 transport
- Includes both site-to-site and remote access features
- Data Protection

IPsec has a couple protocols associated with it.

- **ISAKMP or Internet Security Key Management Protocol** – Provides a secure way to exchange keys.
- **ESP or Encapsulating Security Protocol** – Used to provide confidentiality, data origin authentication, connectionless integrity, and anti-replay services.
- **AH or Authentication Header** – Provides authentication

ISAKMP uses **IKE or Internet Key Exchange** which provides the means for ISAKMP to exchange keys by negotiating **SAs or Security Associations**. There are two version of IKE.

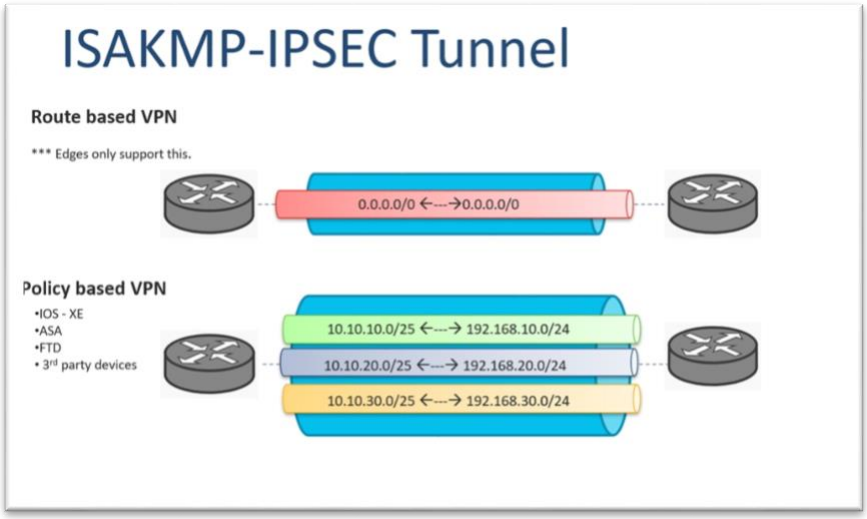
- **IKEv1** – Has two modes Main mode (six messages) and Aggressive mode (three messages). Uses symmetric encryption. IKEv1 has two phases:
    - Phase 1: Establishes the secure tunnel uses to secure the ISAKMP negotiation messages. This is where Main and Aggressive mode come in. Think control plane.
    - Phase 2: Negotiates the materials and algorithms for the SAs to allow data to be transferred. Think data plane.



- **IKEv2** – Is an enhancement of IKEv1 and uses asymmetric encryption and sends less messages during the exchange. IKEv2 has two initial phases of negotiation:
    - IKE_SA_INIT – Initial exchange used to build an encrypted tunnel between both peers.
    - IKE_AUTH – Once the IKE_SA_INIT exchange is complete the IKEv2 SA is encrypted but the remote peer is unauthenticated. ISAKMP is then used to authenticate the peer and setup the IPsec SA.

Policy vs Route based VPNs

- **Policy** – A policy is used to encrypt a subset of traffic per the policy that is written. An ACL is used to match specific traffic to be encrypted and then sent out to its destination. This can create multiple IPsec SAs and "sub-tunnels" for each SA within the same tunnel.
- **Route** – A tunnel interface is used as the endpoints between the two peers. This configuration allows the use of dynamic routing protocols. So, any traffic passing over the tunnel is encrypted.



Diffie-Hellman Group (DH Group) Selection

Not every device will support each DH group. When possible, configure the most secure highest common denominator on all your peers.

DH Group	Key Size (Bits)	Notes
1	768-bit	Avoid
2	1024-bit	Avoid
5	1536-bit	Avoid
14	2048-bit	Less Preferable
15	3072-bit	Less Preferable
16	4096-bit	Less Preferable
17	6144-bit	Less Preferable
18	8192-bit	Less Preferable
19	256-bit elliptic curve	Preferable
20	384-bit elliptic curve	Preferable
21	512-bit elliptic curve	Preferable
24	2048-bit, 256-bit subgroup	Most Preferable

Configuration

A ISAKMP policy is created, and a transform-set is configured. Then the ISAKMP policy and the transform-set are applied to a crypto map.

- **ISAKMP Policy** – Defines the parameters to use during the IKE negotiation process.
- **Transform-set** – Defines the encryption and algorithms to be used, this covers ESP and AH.
- **Crypto Map** – Tells the device what traffic to encrypt and what transform-set to use.

Router-01

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key cisco address 100.64.0.4
!
crypto ipsec transform-set R1_TSET esp-aes esp-sha-hmac
 mode transport
!
crypto map CRYPTO_MAP 10 ipsec-isakmp
 set peer 100.64.0.4
 set transform-set R1_TSET
 match address GRE-IN-IPSEC
!
interface Tunnel1
 ip address 192.168.47.1 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 100.64.0.4
!
interface GigabitEthernet0/0
 ip address 100.64.0.3 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 crypto map CRYPTO_MAP
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
router eigrp 100
 network 172.16.0.0 0.0.0.255
 network 192.168.47.0 0.0.0.3
!
ip access-list extended GRE-IN-IPSEC
 permit gre any any
!
```

Router-02

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key cisco address 100.64.0.3
!
crypto ipsec transform-set R2_TSET esp-aes esp-sha-hmac
 mode transport
!
crypto map CRYPTO_MAP 10 ipsec-isakmp
 set peer 100.64.0.3
 set transform-set R2_TSET
 match address GRE-IN-IPSEC
!
interface Tunnel1
 ip address 192.168.47.2 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 100.64.0.3
!
interface GigabitEthernet0/0
 ip address 100.64.0.4 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 crypto map CRYPTO_MAP
!
interface GigabitEthernet0/1
 ip address 172.17.0.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
router eigrp 100
 network 172.17.0.0 0.0.0.255
 network 192.168.47.0 0.0.0.3
!
ip access-list extended GRE-IN-IPSEC
 permit gre any any
!
```

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html