
Important Protocols

IpSec

What is IpSec?

RFC 6071(IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap)

IPsec is a protocol that provides a secure tunnel between two computers. It is used to protect data that is transmitted over the internet.

IPsec helps mitigation against:

- eavesdropping
- theft
- replay attacks,
- Data corruption.

Ipsec operates in 2 different modes: tunnel mode and transport mode.

In **tunnel mode**, everything is encapsulated in IPsec datagram. when data is transmitted, the layer 3 devices only use IPsec header to route the packet.

This is used basically in the site-to-site VPN and remote access VPN.

in **transport mode**, all of the data is protected but the original IP header is not. Payload is protected by IPsec. This is used generally in P2P applications.

Ipsec building Blocks:

Ipsec Suite either uses **Authentication Header(AH)** or **Encapsulating Security Payload (ESP)**. One difference is that in the former, the data is encrypted.

ESP and AH both come with options of transport and tunnel.

In the AH transport mode, the payload is encrypted and the original IP header is not protected. In the tunnel mode, the payload is encrypted and the original IP header is protected. A new IP header is appointed to the packet in tunnel mode.

ESP transport and Tunnel modes can be used as it is or with AH.

ESP encapsulates the data so we have both header and trailer in the packet in Transport mode and in Tunnel mode.

in ESP header, different than AH header, there is no next header field and payload length field.

After the headers, there is **Security Association (SA)**.

Security Association in IPsec suite is a **unidirectional connection** that gives devices the capability to use AH or ESP services. for a bidirectional comms, a pair of SA is needed.

In order SA to be established, the following steps are needed:

- **SPI:** Security Parameter Index. It is a unique number that is used to identify the SA.
- **Security Protocol Identifier:** It is a number that identifies the protocol that is used in the SA. (50 for AH or 51 for ESP)
- **Destination IP Address**

For key management, it is either done manually or automated using IKEv1 or IKEv2.

IKE (Internet Key Exchange) is a protocol that is used to establish a key management between two computers. default one is IKEv2.

Next building block is **Crypto Algorithm**. These are used for Encryption , Authentication , Integrity and Pseudorandom Number Generation.

====

for SA establishment, there are couple of different protocols that are used.

- **ISAKMP** (Internet Security Association Key Management Protocol) : Used for procedures and formats to establish SA. It helps us build the SA.
- **OAKLEY** (One-Way Authentication Key Exchange Protocol) : gives key-exchange mechanism. Used to exchange key over insecure connection using Diffie-Hellman.
- **SKEME** (Security Key Exchange Method) : gives anonymity and reputability through key-exchange techniques.
- **IKE** (Internet Key Exchange) : Uses combination of ISAKMP, OAKLEY, and SKEME

=====

Ipsec in Enterprise

In enterprise level, there are 2 main uses of IPsec:

- Site-to-Site VPN

connect 2 or more sites together. One type of Site-to-Site VPN is **DMVPN** (Dynamic Multicast VPN).

logically connects sites, protects **entire** network, provides corporate resources to other sites.

- Remote Access VPN

logically connect endpoint to another network. IPsec using the OS IP stack. protects **individual** devices.

useful in wifi hotspots.

Bu mesela bir isci evden calisirken isyerinin agina ulassin diye kullanilan vpn. ticari bireysel VPNler de bu tip, hotspotshield, NordVPN gibi.

as for IPsec implementations, there are 2 main types:

- GRE over IPsec

way more common.

encapsulates entire packet. this is essentially DMVPN over IPsec.

- IPsec over GRE

much less common. only the payload is protected via IPsec. routing information stays visible in the GRE portion of the datagram.

IKEv2

What is IKE?

IKE is Internet Key Exchange that uses ISAKMP, OAKLEY, and SKEME for establishing SA for securing network traffic.

Although IKEv1 is still used, IKEv2 is the new standard and IKEv1 is obsolete.

V2 brought these:

- new authentication method EAP (Extensible Authentication Protocol) alongside PKS and PKI
- brought MOBIKE (Multicast Opportunistic Key Exchange) which allows dynamically change IP addresses without needing to re-establish the SA.
- in V1, SA lifetime was negotiated, in V2, SA lifetime is configured locally and faster negotiation.
- Flexible traffic selection per SA.

Some benefits of IKEv2 are:

- **It is more reliable:**

message flow system uses requests followed by responses. Initiator sends a request, and the responder sends a response. If the initiator does not receive a response, it will retry or drops the request. the reliability is on the initiator side.

- **It is more Mobile:**

using MOBIKE, keeps VPN connection active when changing IP addresses. thanks to **multihoming**, when interface drops, the traffic is moved to another interface.

- **it enables High Availability:**

IKEv2 comes with **redirection** feature. if one server for VPN is taken down or went down, the users can be redirected to another server.

For authentication, IKEv2 uses **Pre-Shared Key** (PSK) and **Certificate Authentication**. Apart from that uses EAP.

MacSec

While IPsec is encryption at Layer 3, MacSec is encryption at Layer 2 which is Ethernet layer.

Remember this : ==> **IEEE 802.1AE**

Compared to IPsec:

- MacSec provides STRONGER ENCRYPTION performance at HIGHER SPEEDS.
- Macsec can encrypt user data at UP TO 800Gig Ethernet Speeds without any hardware offloading.
- Application to any network that relies on Ethernet so can be used in many places => so Data Center, Corporate environment, Service Provider, etc.

Packet Structure:

A captured MacSec packet has some options and payloads.

-> **802.1AE Security Tag.**

This Tag has some option flags like VER, ES, E.

E flag is set to 1 if the packet is **encrypted**.

-> **ICV Value**

ICV is a checksum that is used to verify the integrity of the packet.

-> **Port Identifier.**

shows on what port the packet was captured on.

-> **Data**

Data is the encrypted payload. looks like a random hash value.

MacSec Terminology:

1. **MacSec Key Agreement Protocol**

Used to discover Macsec capable peers and used to negotiate encryption keys. These keys are for **data encryption** and **Security Association Key Encryption**(SAK)

2. **Connectivity Association (CA)**

Similar to **IPSec SA** but for MacSec. Defines a secure relationship between MacSec peers.

3. ****Connectivity Association Key(CAK)****

Static or Dynamic Key exchanged by macsec speakers. This can be seen as **primary key** that is used to device all other session keys.

So CAK is used to derive SAK keys and this SAK keys are used to encrypt the user data.

So this CAK can be statically configured or can be distributed by the server.

4. **Connectivity Association Key Name (CKN) **

Any name that defines a CAK.

5. **Primary and Fallback Keys **

Primary key is used to negotiate an MKA if this fails, Fallback key is used.

6. ** Security Association Keys(SAK) **

Derived from CAK used to encrypt data as mentioned earlier.

A **Key Server** generates SAK. If you have if you have one switch connected to another switch on ethernet link and MacSec is enabled on this switch, one of these switches will be a Key Server.

ArpSec