What is IPsec?

IPsec is a protocol that provides security for internet protocol communications. It can be used to encrypt data and to authenticate communications. IPsec can be used in a number of different ways, but is most commonly used in virtual private networks (VPNs)

Can you explain how an IPsec VPN works -

IPsec VPNs work by creating a secure, encrypted tunnel between two devices. This tunnel is used to send data back and forth between the devices, and any data that is sent through the tunnel is protected from being read or tampered with by anyone who does not have the proper encryption key

What are the main components of IPsec VPNs

IPsec VPNs have three main components: the Authentication Header (AH), the Encapsulating Security Payload (ESP), and the Internet Key Exchange (IKE). The AH provides authentication for the data being sent, while the ESP encrypts the data. The IKE is responsible for establishing the connection and negotiating the security parameters

Use of encryption and authentication -

The use of encryption and authentication helps to ensure that only authorized users are able to access the network and that the data passing through the network is not accessible to unauthorized individuals. By encrypting the data, it becomes much more difficult for someone to intercept and read the data as it is passing through the network. Authentication helps to ensure that only authorized users are able to access the network in the first place

Virtual private network (VPN) is?

A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. VPNs use “virtual” connections routed

through the Internet from the organization’s private network to the remote site or employee. From the user’s perspective, the VPN is a point-to-point connection between the user’s computer and the corporate network

What is IPSEC Encapsulating Security Payload (ESP)?

Encapsulating Security Payload (ESP) is a security protocol used to provide confidentiality, integrity, and authentication for data in transit. It can be used in conjunction with a variety of other protocols but is most commonly used with the IPsec protocol. ESP uses a variety of encryption algorithms to encrypt data, and can also provide authentication for data integrity

What is AH or Authentication Header in context with IPsec?

The Authentication Header is used to provide integrity and authentication for IPsec data packets. AH uses a hashing algorithm to create a message digest, which is then used to verify the integrity of the data packet. AH also provides authentication by using a shared secret key to encrypt the message digest

What is Diffie-Hellman and RSA key exchange algorithms?

The Diffie-Hellman key exchange algorithm allows two parties to generate a shared secret key that can be used to encrypt and decrypt communications between them. This key is generated by each party using their own private key and the other party’s public key. The RSA key exchange algorithm is similar in that it also allows two parties to generate a shared secret key, but the key is generated using the RSA public-key encryption algorithm

Understanding of IKE Phase 1?

IKE phase 1 is responsible for creating a secure, authenticated channel between two devices. This is typically done by exchanging public keys and then using a Diffie-Hellman key exchange to generate a shared secret key.

This shared secret key is then used to encrypt all further communication between the two devices

Which two mode ESP can operate -

ESP can operate in two modes: transport mode and tunnel mode. Transport mode is typically used for end-to-end communication, while tunnel mode is used for communication between two security gateways. I would recommend using transport mode, as it is more efficient and secure

What is NAT Traversal?

NAT Traversal is a technique used to allow IPsec-encrypted traffic to pass through a network that is using Network Address Translation (NAT). NAT Traversal allows a VPN client that is behind a NAT device to connect to a VPN server that is also behind a NAT device.

What is VTI?

VTI is a Virtual Tunnel Interface. It is a tunnel interface that uses IPsec to secure the traffic that is passing through it

Various phases involved in IPsec VPN setup?

There are three phases involved in IPsec VPN setup:

1. The first phase is the IKE phase, which is responsible for setting up the security association (SA) between the two VPN endpoints.

2. The second phase is the ESP phase, which is responsible for encrypting and decrypting the data that is being sent between the two VPN endpoints.

3. The third and final phase is the AH phase, which is responsible for authenticating the data that is being sent between the two VPN endpoints.

Difference between Transport and Tunnel Mode -

-->> IPsec Transport Mode

Advantage --

The main advantage of IPsec transport mode is that it is more compatible with certain firewalls and it offers higher levels of security. In addition, transport mode does not require a secure connection to be established between two endpoints and has less overhead because it does not encapsulate packets

Disadvantage--

The main disadvantage of IPsec transport mode is the difficulties it has with NAT traversal or UDP encapsulation. The User Datagram Protocol (UDP) is a technique of adding network headers to the packets and helps with load balancing to better distribute network traffic

--->> IPsec Tunnel Mode

Advantage --

The main advantage of IPsec tunnel mode is that it creates a secure connection between two endpoints by encapsulating packets in an additional IP header. Tunnel mode also provides better security over transport mode because the entire original packet is encrypted.

Disadvantage --

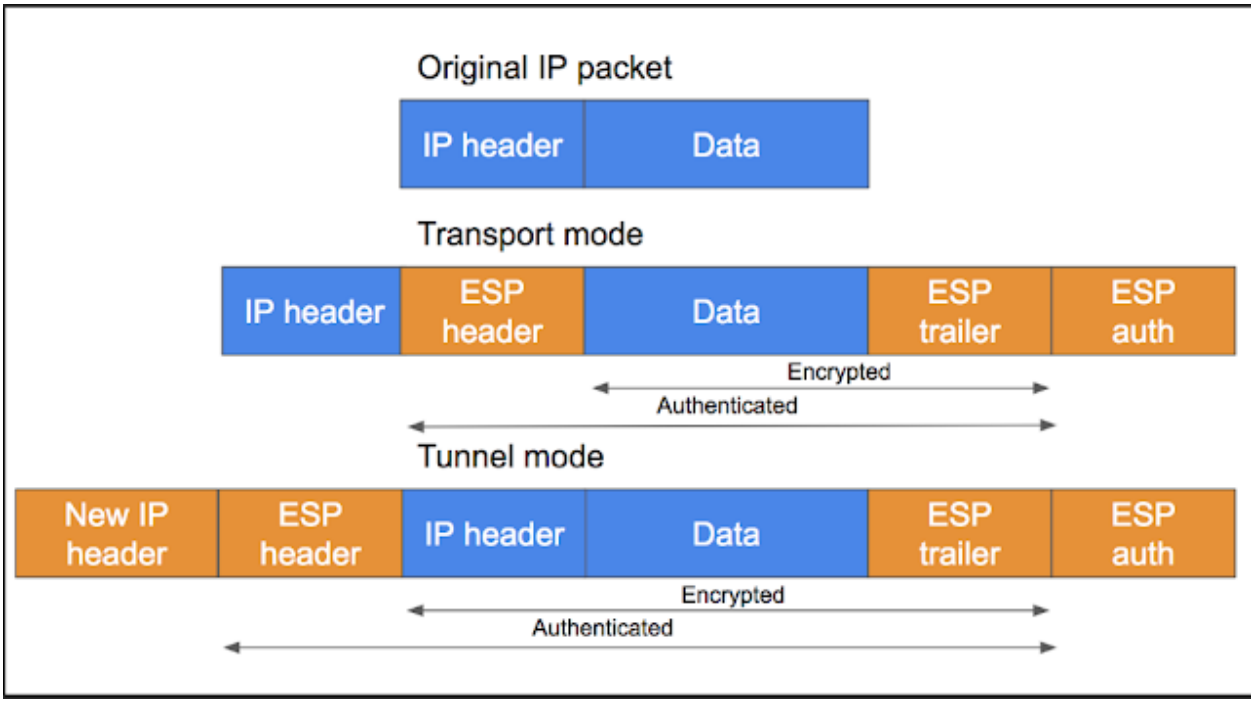
The main disadvantage of the IPsec tunnel mode is that it requires a secure connection to be established between two endpoints and tends to create more overhead because the entire original packet must be encapsulated. In addition, transport mode may perform better than tunnel mode on some types of networks and with certain firewalls

IPSec / IKEv2 use port -

use ports **500** and **1500 UDP** we will have to open both ports. This VPN protocol does not allow port switching, it is the standard

IPSEC uses port **500** (for AH and ESP) in the Control plane and Protocol numbers 50 and 51

NAT use port **4500** for both the Control and Data Plane.

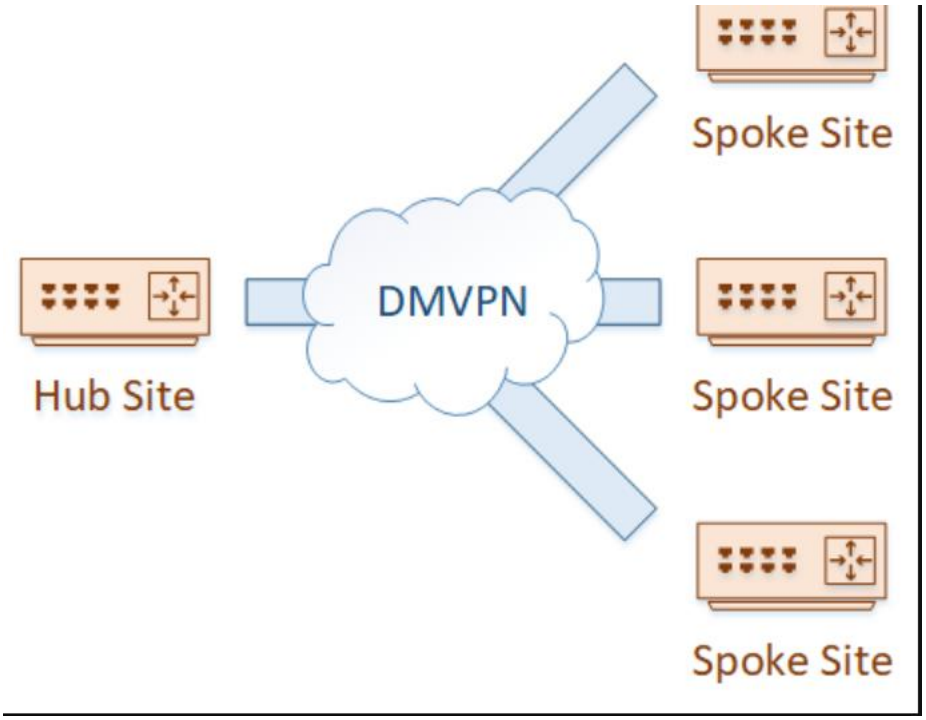


What is CIA --

- **Confidentiality** is the property of restricting everyone from accessing systems or data except authorized users. Essentially, keeping data confidential means keeping it a secret.
- **Integrity** means that data must be complete and accurate, and that it hasn't been corrupted or tampered with.
- **Availability** refers to the data being accessible when it is required.

What is Dynamic multipoint virtual private network (DMVPN)?

A dynamic multipoint virtual private network (DMVPN) is a secure network that exchanges data between sites/routers without passing traffic through an organization's virtual private network (VPN) server or router, located at its headquarters. A DMVPN allows organizations to build a VPN network with multiple sites, without the need to configure devices statically.



DMVPN consists of four key components -

Multipoint GRE tunnel interfaces

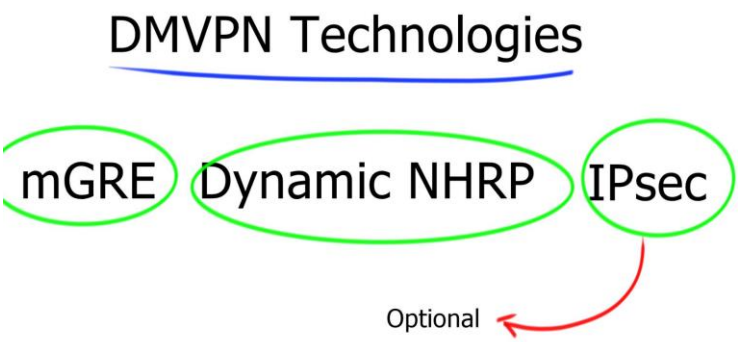
For an enterprise network where sites need to connect, internet connections with multiple GRE tunnel interfaces can get messy and be difficult to scale. DMVPN and multipoint GRE (mGRE) allow a business to add multiple destinations, with only one tunnel interface on each router.

mGRE features a single GRE interface on each router with the possibility of multiple destinations. This interface secures multiple IPsec tunnels and reduces the overall scope of the DMVPN configuration.

NHRP --

The NHRP can deploy spokes with assigned IP addresses. These spokes can be connected from the central DMVPN hub

This protocol is required by one branch router to find the public IP address of the second branch router. NHRP uses a "server-client" model, where one router functions as the NHRP *server*, while the other routers are the NHRP *clients*



DMVPN phases -

Phase 1

In phase 1, the DMVPN spokes are registered with the hub. In this early phase, there is no direct communication between the spokes, so all traffic goes through the hub. Each spoke uses regular point-to-point GRE tunnel interfaces and requires only a summary or default route to the hub to reach other spokes. As a result, the routing configuration in this phase is simple.

Phase 2

This phase allows spoke-to-spoke tunnel deployment with all spoke routers using multipoint GRE tunnels. These spoke-to-spoke tunnels are on demand, i.e., triggered based on the spoke traffic. This means the data does not have to travel to a central hub first. While the hub is used for the control plane, it is not necessarily in the data plane. This key fact differentiates Phase 2 from Phase 1.

Phase 3

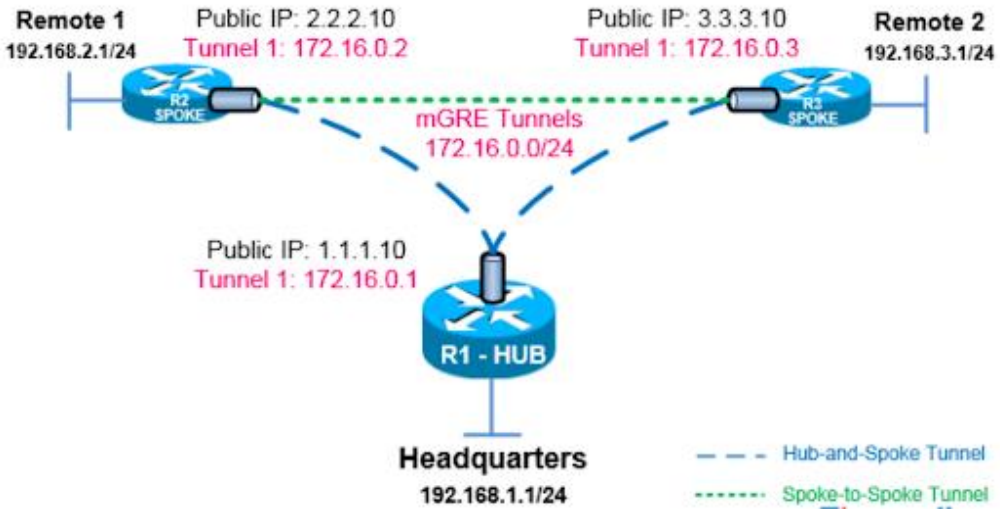
In phase 3, the spoke-to-spoke tunnels are deployed without using specific pre-made routes. To secure those routes on the fly, this phase uses NHRP traffic indication messages (*redirect* and *shortcuts*) from the hub. This phase improves the scalability of phase 2

	Phase I	Phase II	Phase III
Spoke-to-Spoke Communication	NO	YES Creates invalid CEF at first	YES Uses NHRP route
Distance Vector Summarization	YES	NO	YES
Distance Vector Summarization	YES	Not on hub	YES
EIGRP Routing	All routes from hub	"Reflect" routes to spokes	All routes from hub
OSPF Routing	P2MP Network	Broadcast Hub is DR (No BDR)	Broadcast Hub is DR (No BDR)

DMVPN benefits -

DMVPN, multiple tunnel interfaces for each branch (spoke) VPN are not required. Instead, the simple hub-and-spoke configuration provides on-demand mesh connectivity with dynamic routing and IP multicast. DMVPN also supports "zero touch" deployment to add more remote sites

DMVPN and the NHRP, spokes can be deployed using dynamically assigned public IP addresses. Each spoke can make a VPN tunnel with other spokes by finding their public IP addresses. It does this by querying the NHRP database for the real IP addresses of the destination spokes



Difference between Route based VPN and Policy based VPN

PARAMETER	POLICY-BASED VPN	ROUTE-BASED VPN
Terminology	Policy-based VPNs encrypt and encapsulate a subset of traffic flowing through an interface according to a defined policy (an access list).	A route based VPN creates a virtual IPSec interface, and whatever traffic hits that interface is encrypted and decrypted according to the phase 1 and phase 2 IPSec settings.
Scalability	Numbers of VPN tunnels are limited by the number of policies specified	Numbers of VPN tunnels are limited to either route entries or number of tunnel interface specified which are supported by the device.
Dynamic Routing support	The exchange of dynamic routing information is not supported in policy-based VPNs.	Supports dynamic routing over the tunnel interface.
Policy Control	"Deny" of traffic flowing through the VPN tunnel can't be configured.	"Deny" of traffic flowing through the VPN tunnel can't be configured.
Network topology	Supports P2P network topology while Hub and Spoke topology is not supported	Supports Hub-spoke , P2P and P2MP network topologies
Security Association status	Forms SAs in response to interesting traffic matching policy (and will eventually tear down the SAs in the absence of such traffic).	The SAs for a route-based VPN are always maintained, till corresponding tunnel interface is up.