
Networkforyou
Welcome
To
Network for you
VPN
Networkforyou

VPN (Virtual Private Network):

- A VPN, or virtual private network, is a private network that encrypts and transmits data while it travels from one place to another on the internet.
- It helps to establish a secure connection over insecure network, such as the Internet.
- It is a great alternative to private WAN connection since internet access is cheaper and it available everywhere.
- VPN create tunnels that allows users or systems to connect securely.
- VPN using network security protocols like IPSec to provide privacy and Data Integrity.

VPNS Provides following features as given below:

- Confidentiality: Preventing anyone to read our data **-- With Encryption**
- Authentication: Verifying that the router or firewall or remote user that is sending VPN traffic is authorize
- Integrity: Verifying that the VPN packet was not changed somehow during transit.
- Anti-Reply: Preventing someone from capturing traffic and resending it.

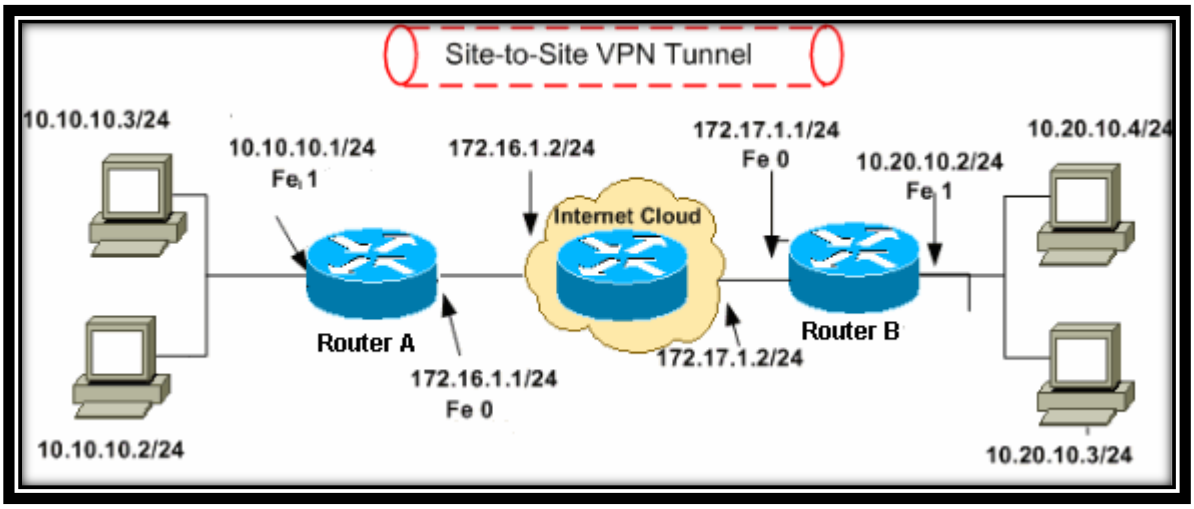
Common VPN types that we use as given below

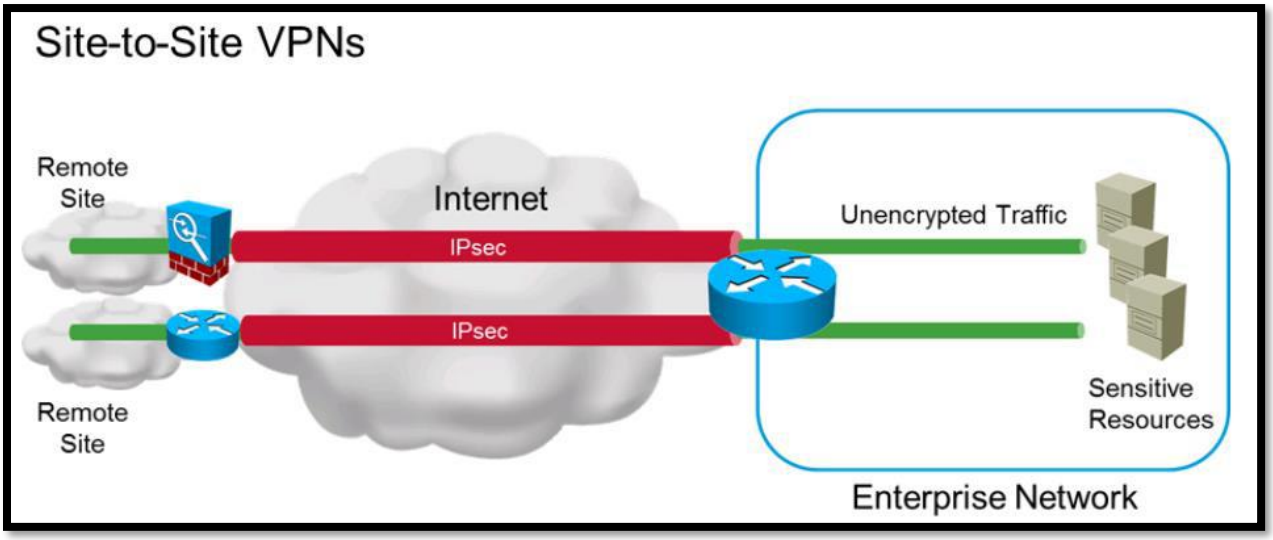
1. Site to Site VPN
2. Remote user VPN (Client to site)

Site to Site VPN:

- In Site to site VPN we have a network device at each site between this network device we can build a VPN Tunnel.

- Each end of the VPN tunnel will be encrypted with original IP packet and add a VPN header a new ip header then it will forward the encrypted packet to the other end of the tunnel.
- A VPN connection that allows connecting two LANs is called a Site-to-Site VPN.
- Connect two private LAN over Public Network, Private to Private over Public Network.
- It is also called Site-to-Site VPN, LAN-to-LAN VPN or Hub-and-Spoke VPN.
- Many organizations use IPsec, GRE, and MPLS VPN as Site-to-Site VPN protocols.
- Site-to-Site VPNs can connect branch office network to company Head-Office Network.
- VPN allows secure connection of corporate office with branch offices or remote offices.
- Site-to-Site, VPN are built over Internet between two or more office locations.
- Site-to-Site Virtual Private Network (VPN) connect entire networks to each other.

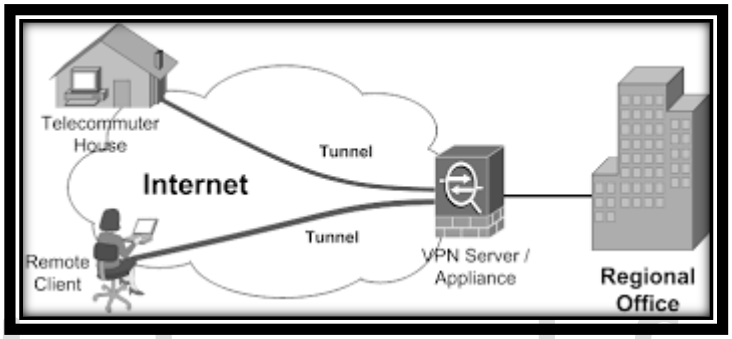


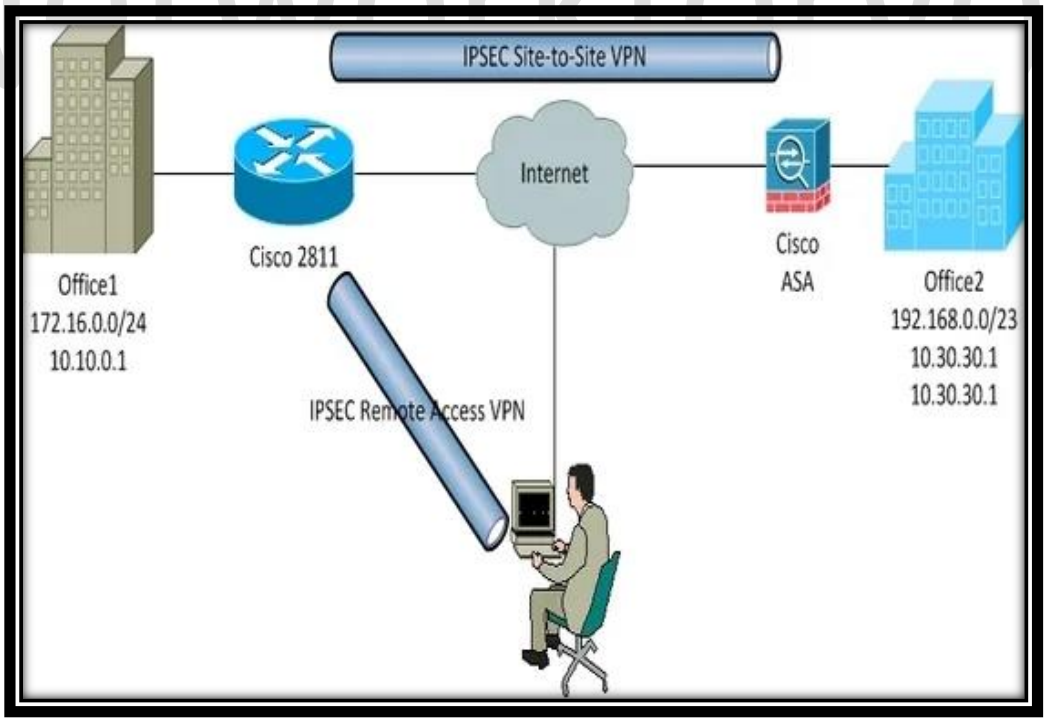


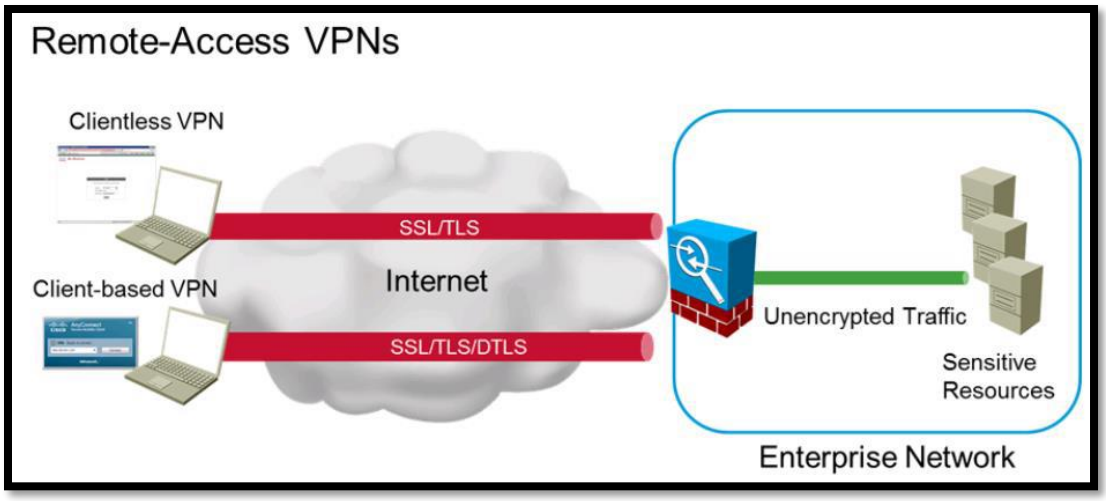
Remote user VPN:

- It is also known also Client to site VPN.
- In this user installs a VPN client on his computer and VPN Tunnel is established between the user's device and the remote network device.
- Enable users to work from remote locations such as their homes & other premises.
- Remote-Access VPNs connect client devices to LAN over the Internet infrastructure.
- Individual hosts or clients, access a company network securely over the Internet.
- Each host typically has VPN client software loaded or uses a web-based client.
- Whenever the host send any information, the VPN client software encapsulates it.
- It allows individual users to establish secure connections with a remote network.

- Remote-Access VPN tunnels are formed between a VPN device & an end-user PC.
- The remote user requires the Cisco Virtual Private Network (VPN) client software.
- Remote access Virtual Private Network connect individual users to private networks.







VPN Protocols:

There are some VPN Protocols use as given below.

- IPSec (Internet protocol security): A Framework that provides security on layer three of the OSI Model.
- L2TP (Layer two traffic): a VPN protocol that tunnels layer two traffic does not offer any encryption so should be used together with IPsec
- SSL (Secure Socket layer): uses SSL (HTTPs) to create a secure connection with the web browser.
- PPTP (Point to point Tunneling Protocol): An old VPN Protocol that uses PPP and GRE, insecure and should not be used any more.

Advantages of VPNs:

- Cost savings
- Scalability
- Security
- Compatibility

- Better Performance
- Flexible and Reliable

Encryption Algorithms for VPN:

The following are the typical encryption (Confidentiality) algorithms:

Data Encryption Standard (DES)	064 bits long
Triple Data Encryption Standard (3DES)	168 bits long
Advanced Encryption Standard (AES)	128 bits long
Advanced Encryption Standard (AES)	192 bits long
Advanced Encryption Standard (AES)	256 bits long

Hashing Algorithms for VPN:

The following are the Hashing (Integrity) algorithms:

Secure Hash Algorithm	SHA
Message Digest Algorithm	5 MD5

Authentication Algorithms for VPN: The following are common authentication methods:

Pre-Shared Keys	Digital Certificates