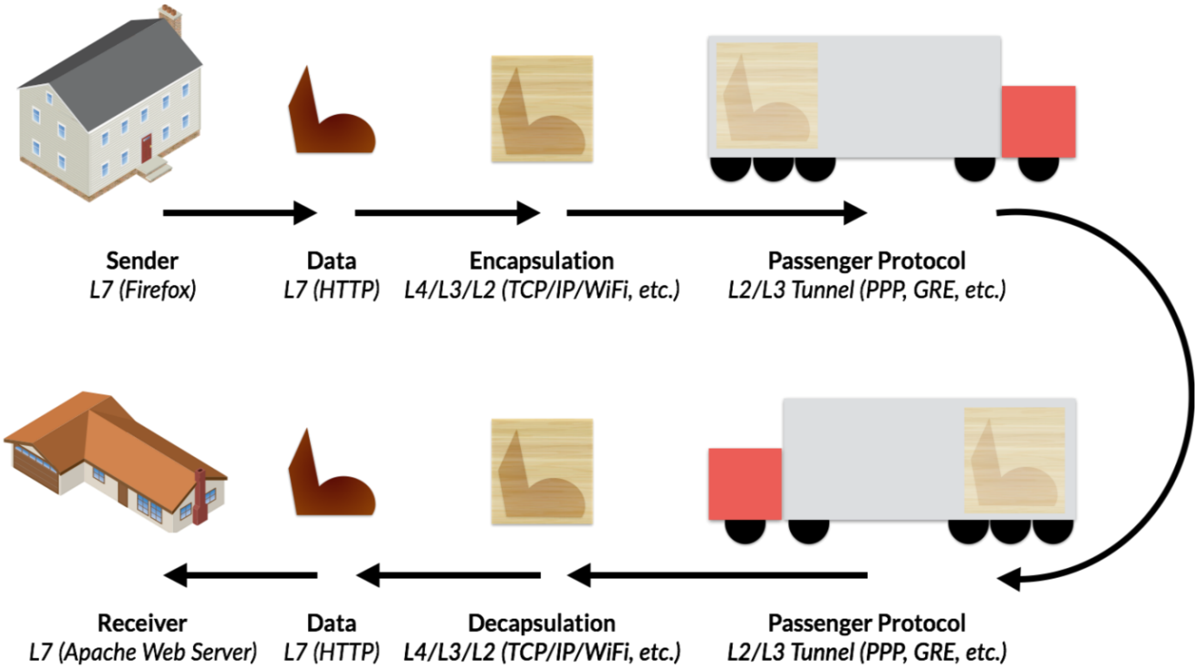
VPN Concept:

- VPN is a network term, which is stands for Virtual Private Network.
- VPN allows creating secure connection to another network over the Internet.
- VPNs create tunnels that allow users and systems to connect securely.
- Virtual Private Network (VPN) is a secure private tunnel over an insecure path.
- There are different technologies available for Wide Area Network (WAN) connectivity.
- Main drawback of many Wide Area Network (WAN) connectivity solutions is "Cost".
- VPN is a Network Security Technology, to secure private network traffic over a public.
- VPN ensures Privacy for network data from the source device to destination device.
- VPN ensures Data Integrity for network data from the source device to destination device.
- VPN using network security protocols like IPSec to provide Privacy and Data Integrity.
- IPSec VPN provide Data Confidentiality by encrypting the data at the sending device.
- IPSec VPN provide Data Confidentiality by decrypting the data at receiving end.
- IPSec VPN also provides Data Integrity by using Hashing Algorithms like MD5 and SHA.
- Cisco supports several types of VPN implementations on the ASA IPSec & SSL based.
- Virtual Private Network (VPN) technology relies on the concept of tunneling.
- VPN tunneling involves establishing and maintaining a logical network association.
- Public network is a network to which anyone can connect and anyone can use.
- Private network is any network to which access is restricted and not for public use.



VPN Classification:

Classification Based on Deployment:

1. Site to Site VPN
2. Remote-Access VPN

Classification Based on OSI Layers:

1. Layer 4/7 VPN - WebVPN
2. Layer 3 VPN - IPSec, GRE, DMVPN, SSL VPN, L2TPV3
3. Layer 2 VPN - L2TP, PPTP, MPPE, Frame Relay, X.25, ATM

Classification Based on Trust Level:

1. Intranet VPN
2. Extranet VPN
3. Remote VPN

Classifications Based on Customer Point of View:

1. Traditional VPN:

   1. Frame-Relay (L2 VPN)
   2. ATM VPN (L2 VPN)

2. CPE Based VPN:

   1. L2TP and PPTP (Layer 2 VPN)
   2. IPSec VPN (Layer 3 VPN)

3. Provider Provisioned VPN:

   1. BGP/MPLS (L2/L3 VPN)

4. Session Based VPN:

   1. SSLVPN/WebVPN (L4/L7 VPN)

Classification Based on Security Level:

1. Secure VPN
2. Trusted VPN
3. Hybrid VPN

Classification based on Cleartext VPNs:

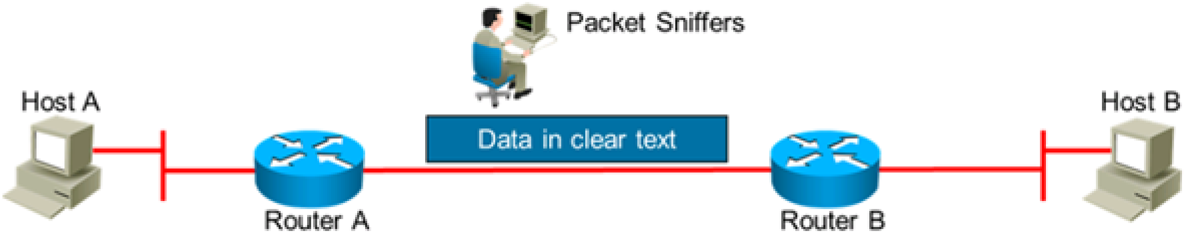
1. MPLS,VPLS
2. L2VPN, L3VPN
3. PPTP, L2F,L2TP

Advantages of VPNs:

Cost Savings	Organizations can use VPNs to reduce connectivity costs.
Scalability	Organizations can use the Internet to easily interconnect new offices.
Security	Advanced encryption and authentication protocols protect data.
Compatibility	VPNs can be implemented across a wide variety of WAN link options.
Better Performance	VPNs provide better performance.
Flexible & Reliable	VPNs is flexible and reliable.

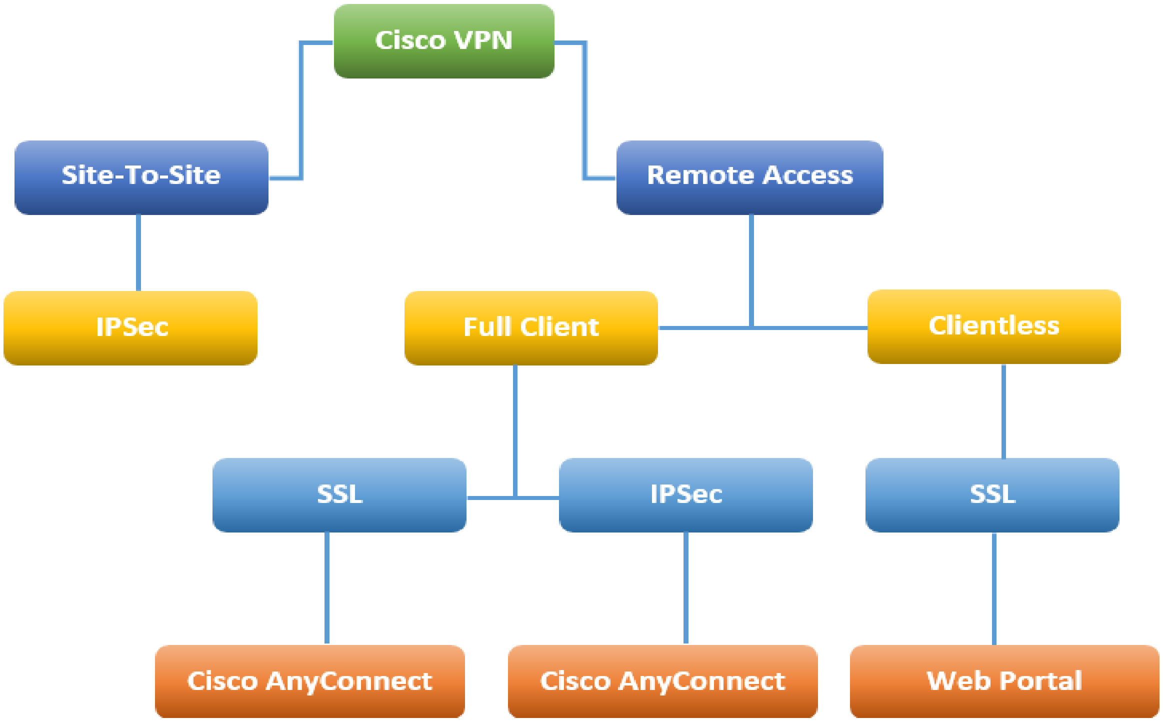
Why Use Secure VPN:

Eavesdropping Attacks	Traffic can be sniffed from unsecured lines.
Network Spoofing Attacks	Attacker can sniff the encrypted data over the public network and use it to make itself as a legitimate VPN peer.
Man-in-The-Middle-Attacks	Attacker gets in-line with normal flow of traffic just to sniff the critical information.



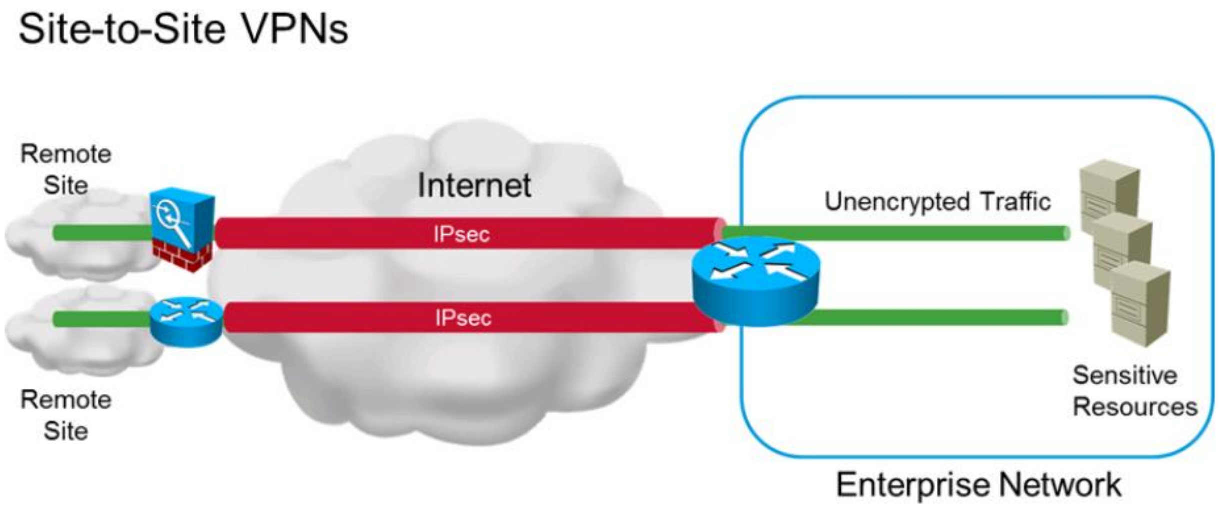
Type of VPNs:

There are two main types or categories of VPNs, Site-to-Site VPNs and Remote-Access VPNs.



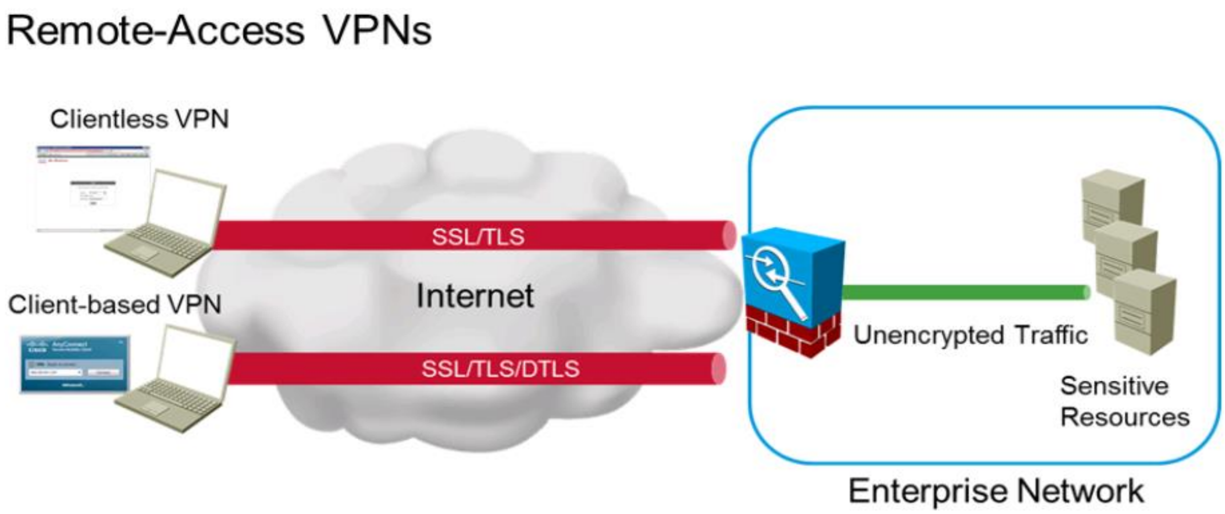
Site-to-Site VPNs:

- 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.
- The VPNs may be placed in the enterprise internet edge, enterprise WAN edge or branch.



Remote-Access VPNs:

- 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.
- Whenever the host send any information, the VPN client software also encrypts 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.
- Remote-access Virtual Private Network connects individual host to company Network.



Protocols for VPN:

The following are different protocols use for VPN implementation:

Point-to-Point Tunneling Protocol	PPTP
Layer 2 Forwarding Protocol	L2FP
Layer 2 Tunneling Protocol	L2TP
Generic Routing Encapsulation Protocol	GRE
Multiprotocol Label Switching	MPLS
Internet Protocol Security	IPSec
Secure Sockets Layer	SSL

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:

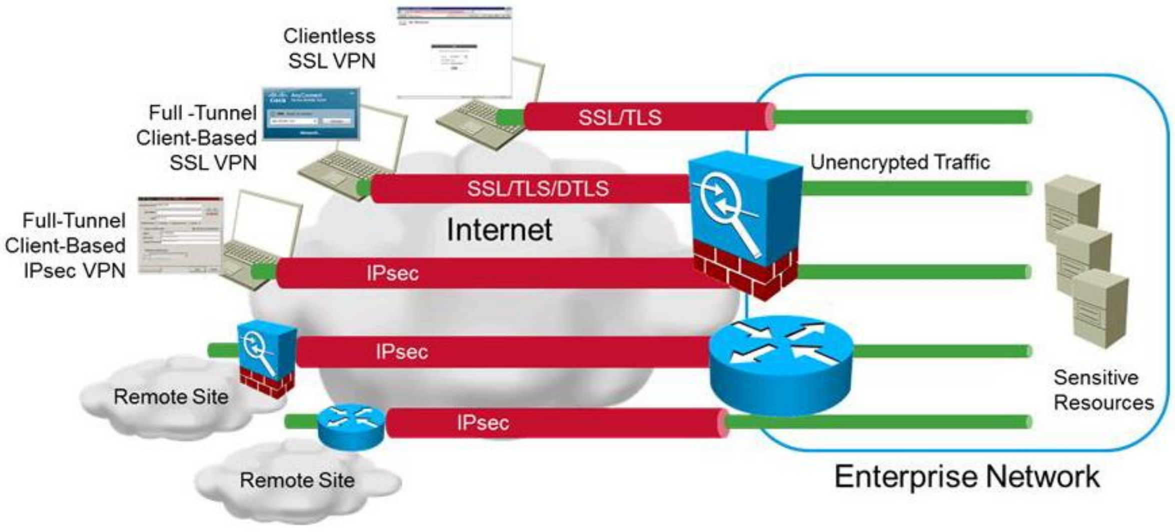
The following are common authentication methods:

Pre-Shared Keys	Digital Certificates

Virtual Private Networks (VPNs):

- VPNs are a way to establish private connections over another network.
- VPNs protect data that is transmitted over internet from threats.

Confidentiality	Prevent others from reading data traffic
Integrity	Ensure data traffic has not been modified
Authentication	Prove identity of remote peer and packets
Anti-replay	Prevent replay of encrypted traffic



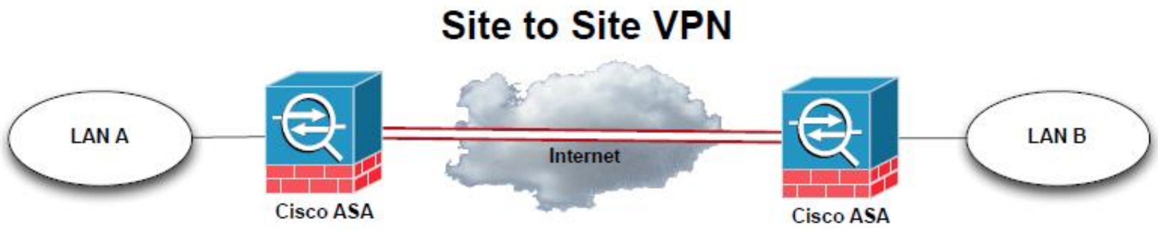
VPN Support for IOS and ASA Devices:

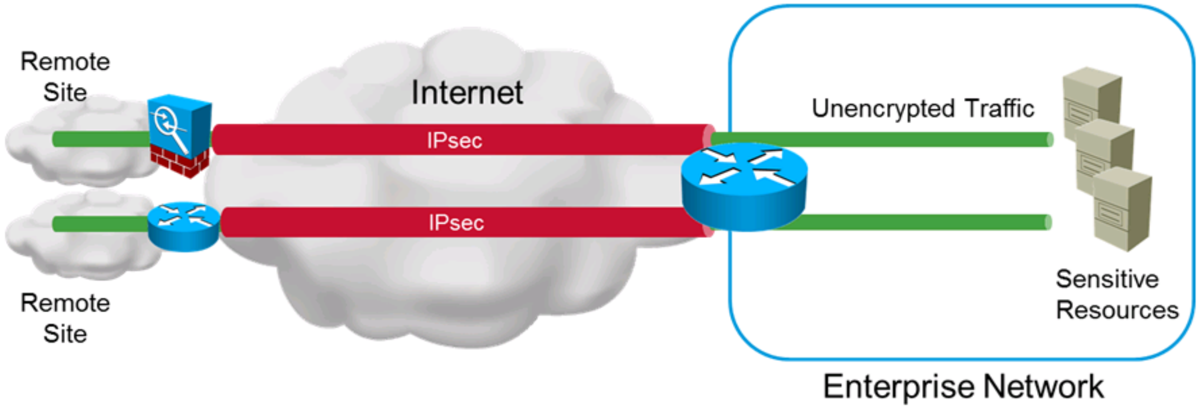
- The table below lists which types of VPNs are supported on each major device type:

VPN	Cisco IOS	Cisco ASA Firewall
Site-To-Site	Yes	Yes
Remote Access	Yes	Yes
SSL	Yes	Yes
DMVPN	Yes	No
GETVPN	Yes	No
FlexVPN	Yes	No

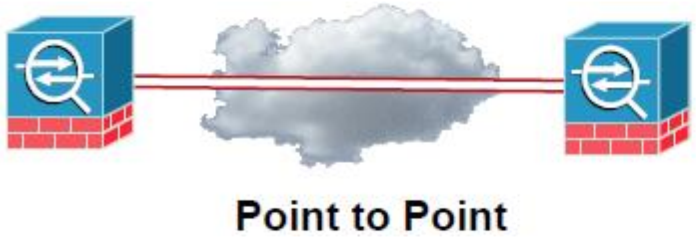
Site-to-Site VPN:

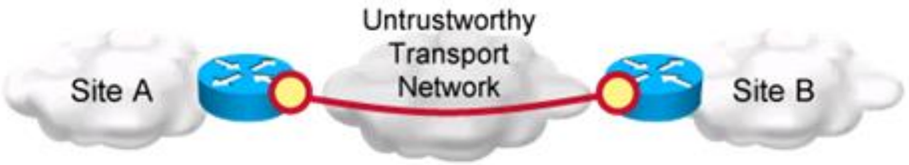
- Site-to-Site VPNs are used to connect two or more sites together.
- Used instead of private WAN connections or to improve security.
- VPN devices may be Cisco routers or Cisco ASA firewalls.
- Site-to-Site VPN Utilizes IPSec IKEv1 and IPSec IKEv2 .
- They are often used to connect a branch office to the main office
- Site-to-Site VPN Supports hub and spoke designs



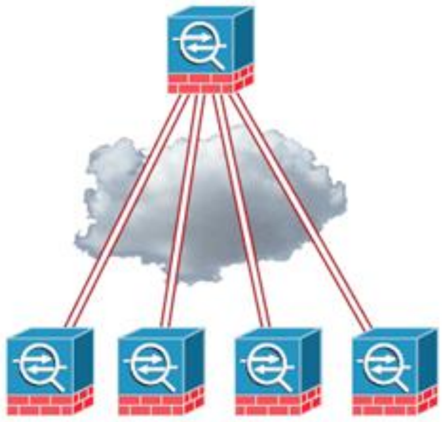


Site-to-Site VPN Types:

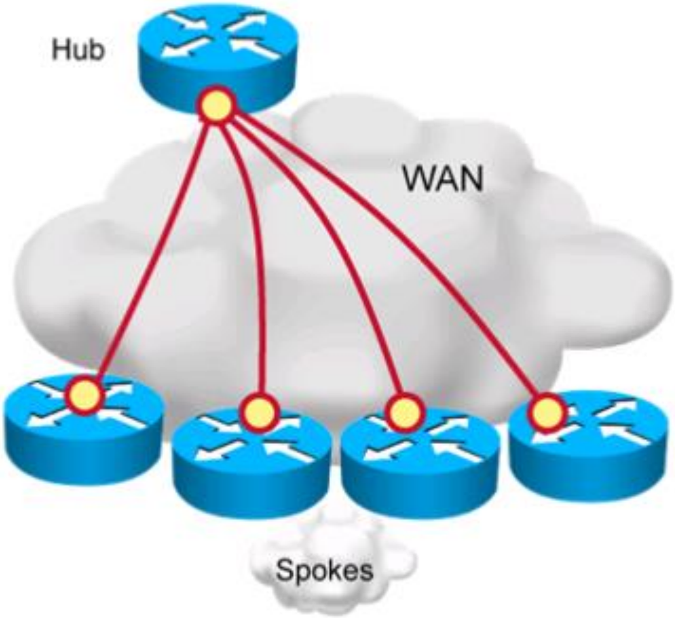


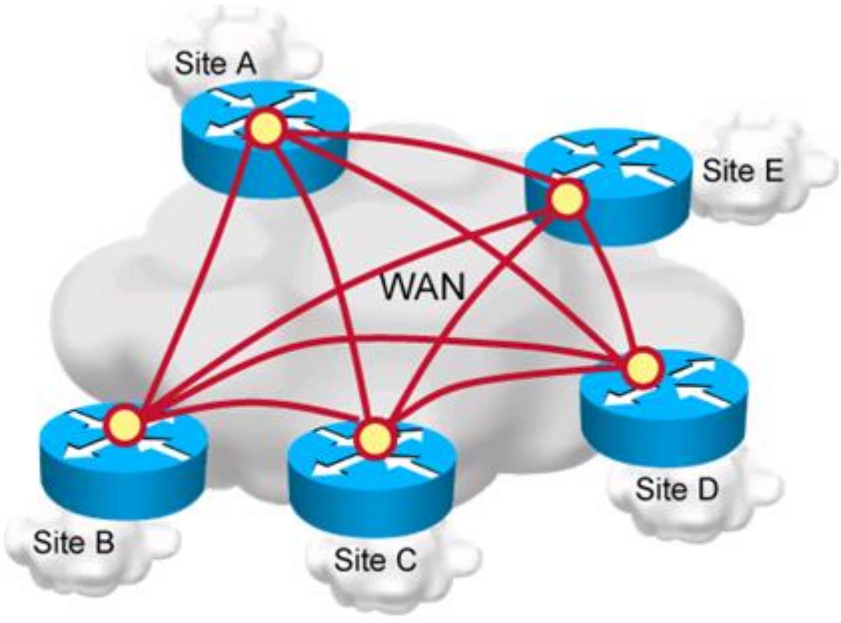


Individual Point-to-Point Tunnels



Hub and Spoke

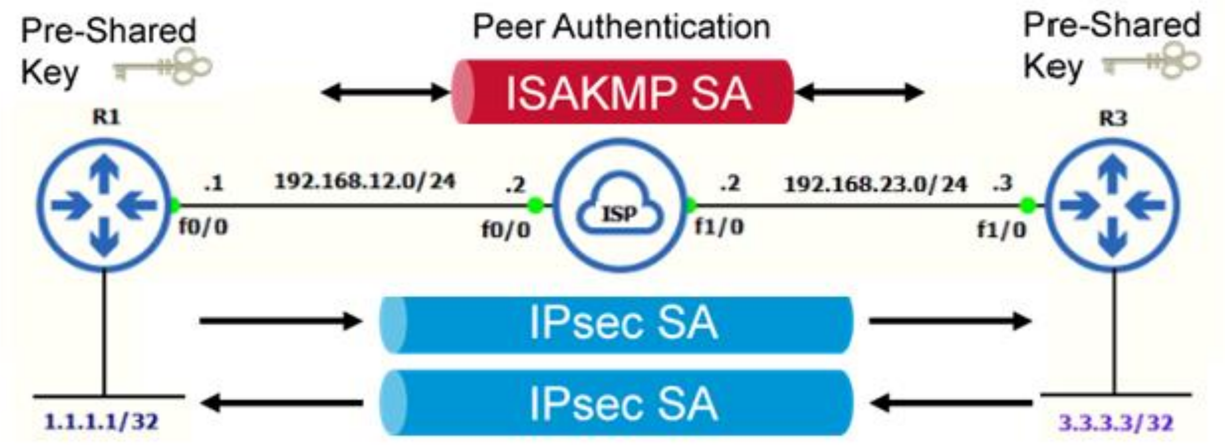




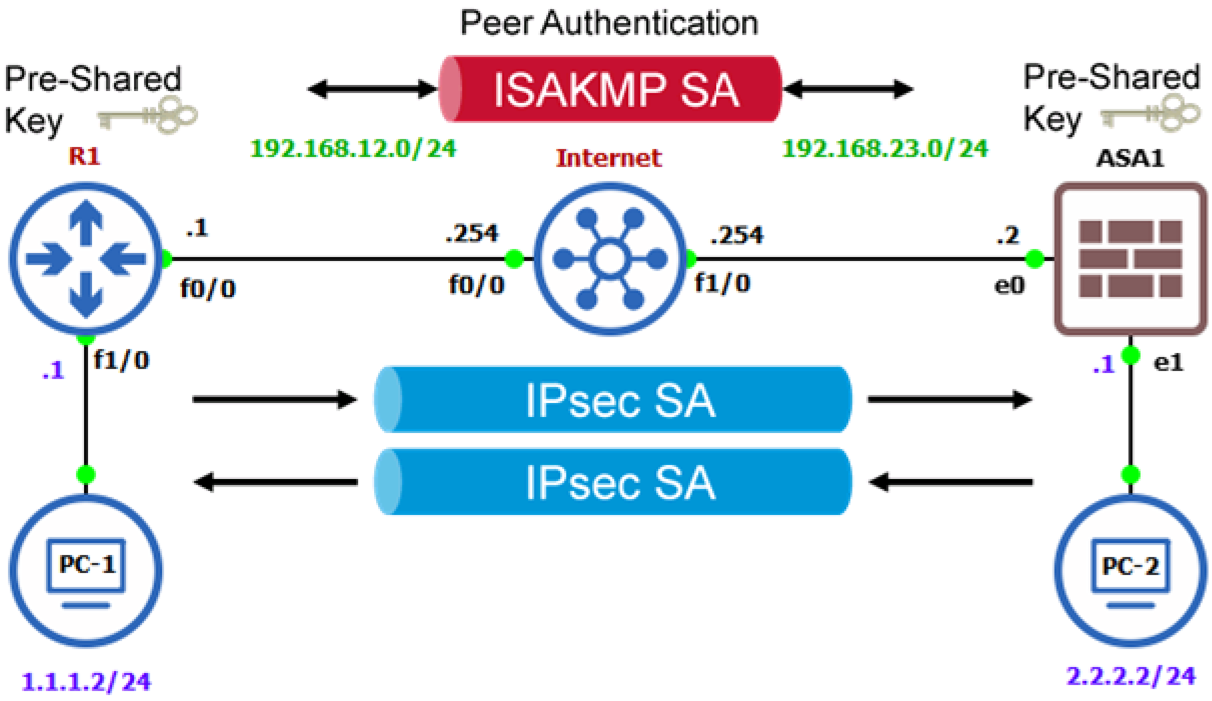
Full Mesh

Site-to-Site VPN:

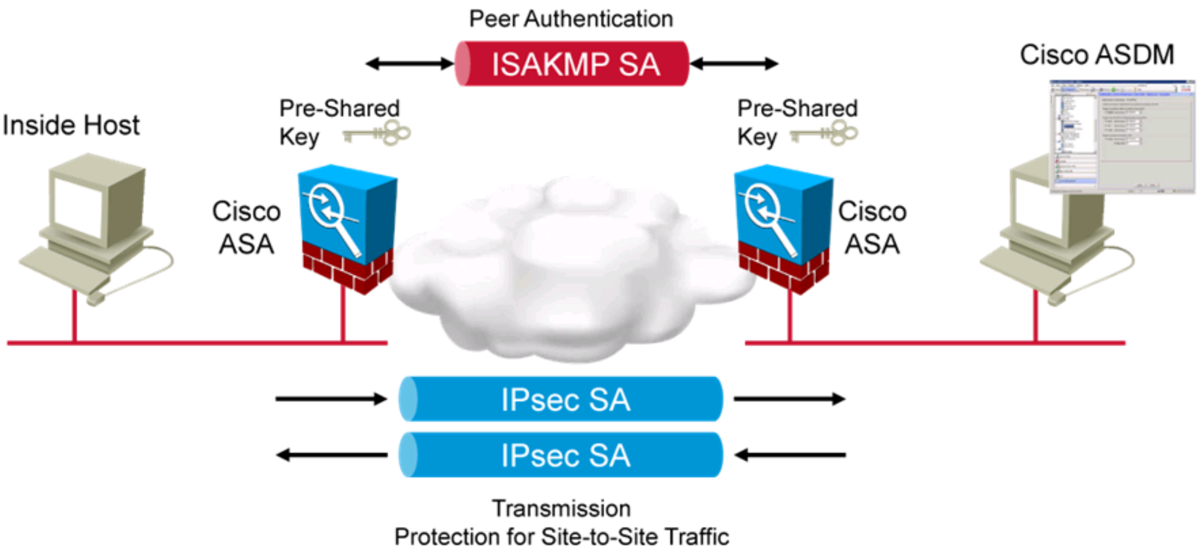
- Site to Site VPN With Pre share key with Main Mode.
- Site to Site VPN With Pre share key with Aggressive Mode.



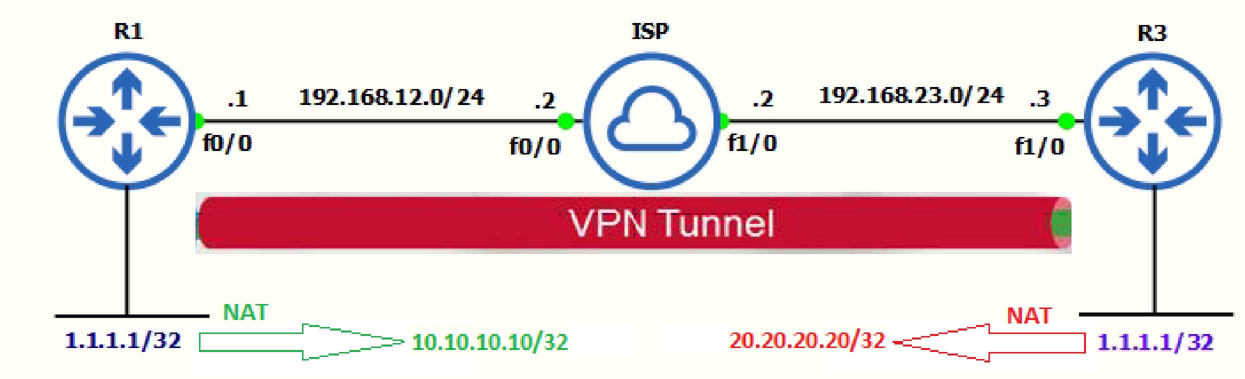
- Site to Site VPN With Cisco ASA and Cisco IOS Router.



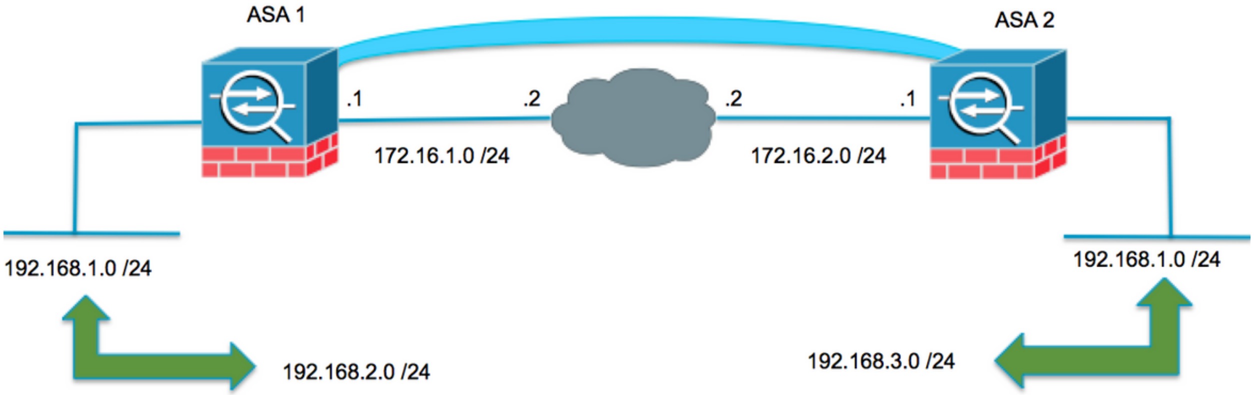
- Site to Site VPN With Pre share key on Cisco ASA Firewalls.



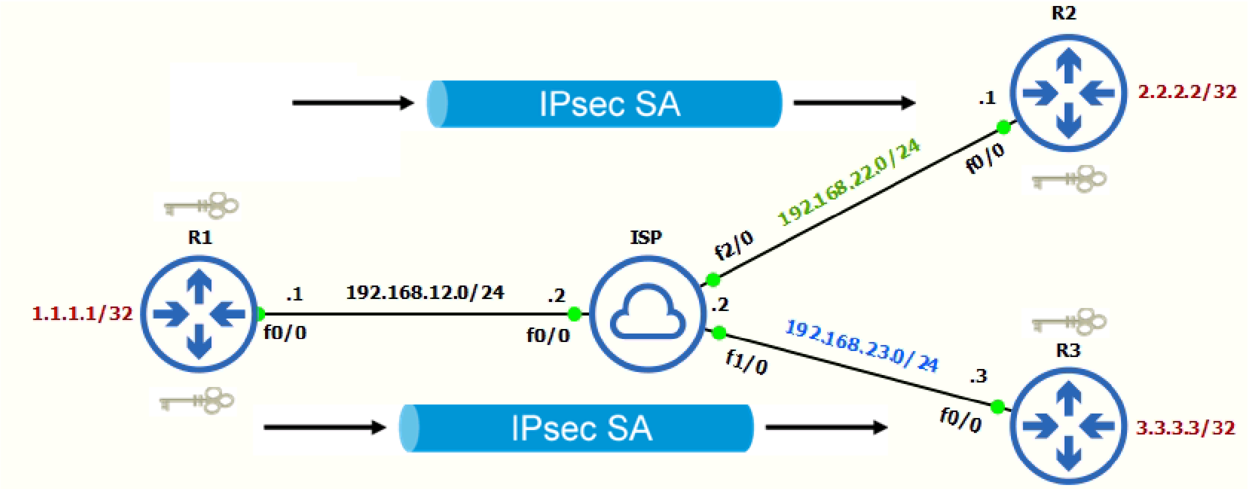
- Site to Site VPN on Cisco IOS Router with Overlapping Subnet.



- Site to Site VPN on Cisco ASA with Overlapping Subnet.



- Site to Site VPN on Cisco IOS with CA Server.
- Site to Site Hub-to-Spoke VPN on Cisco IOS Router.



Remote Access VPN:

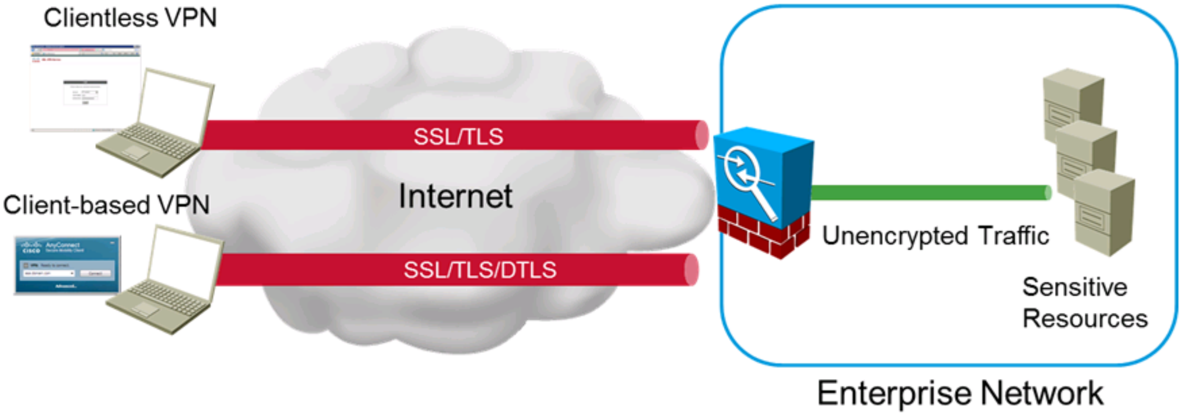
- Connects single user to a remote network via gateway such as an ASA.
- Utilizes IPsec or Secure Sockets Layer (SSL).

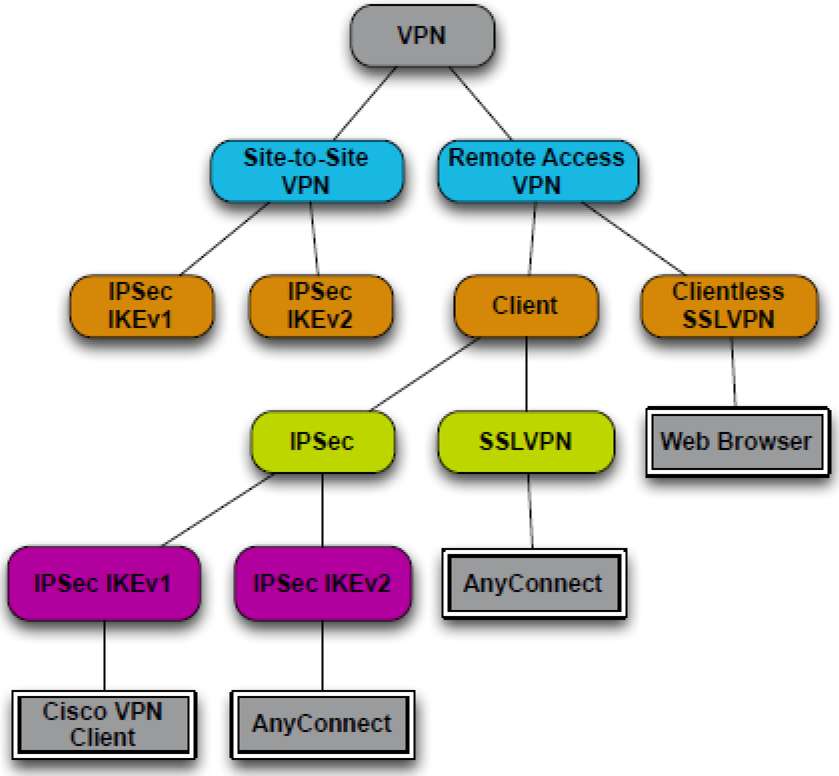
Client-based VPN:

- Remote access using client like Cisco AnyConnect.
- Permits “full tunnel” access.

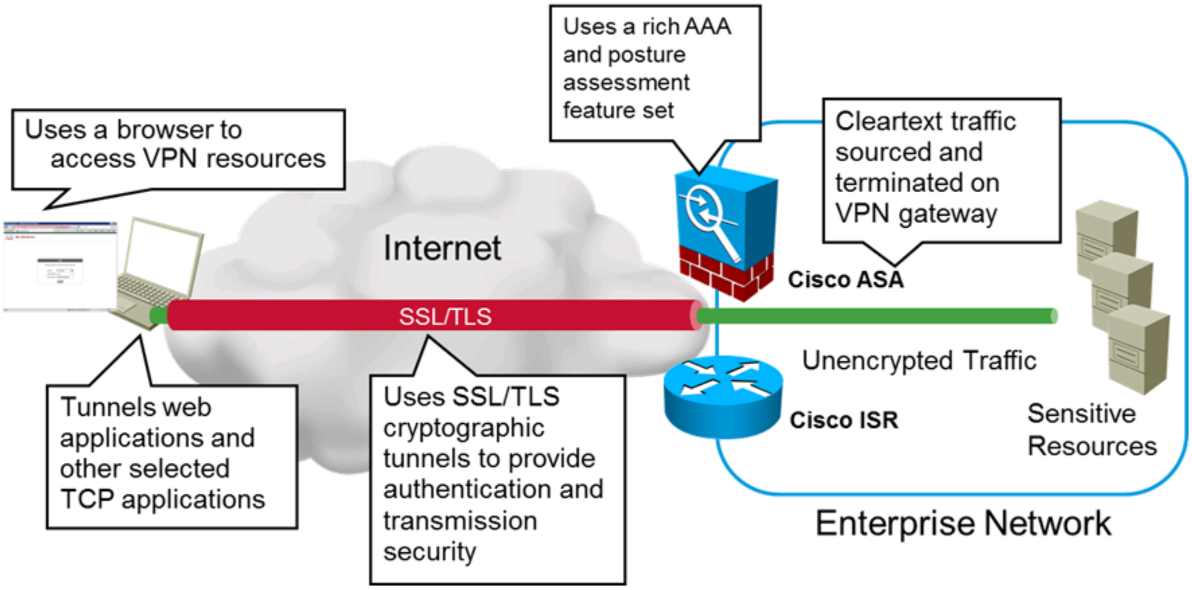
Clientless VPN:

- Leverages the web browser’s SSL encryption for protection.
- Permits limited access but no footprint required.

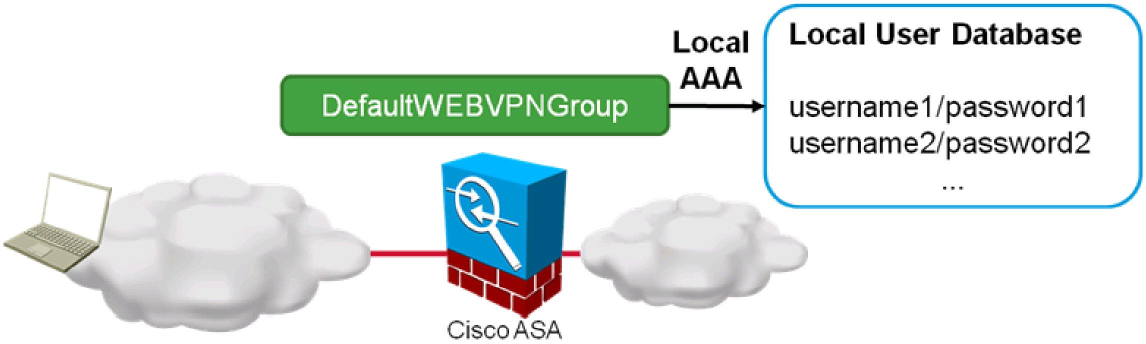




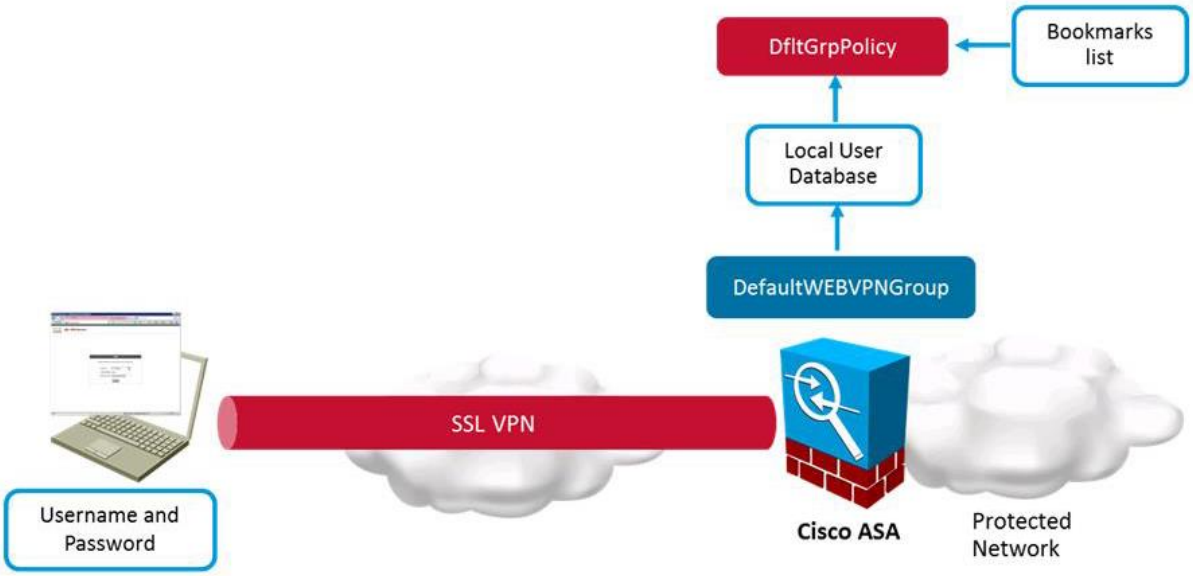
Clientless SSL VPN:


Uses a browser to access VPN resources
Uses a rich AAA and posture assessment feature set
Cleartext traffic sourced and terminated on VPN gateway
Internet
Cisco ASA
SSL/TLS
Unencrypted Traffic
Cisco ISR
Sensitive Resources
Tunnels web applications and other selected TCP applications
Uses SSL/TLS cryptographic tunnels to provide authentication and transmission security
Enterprise Network

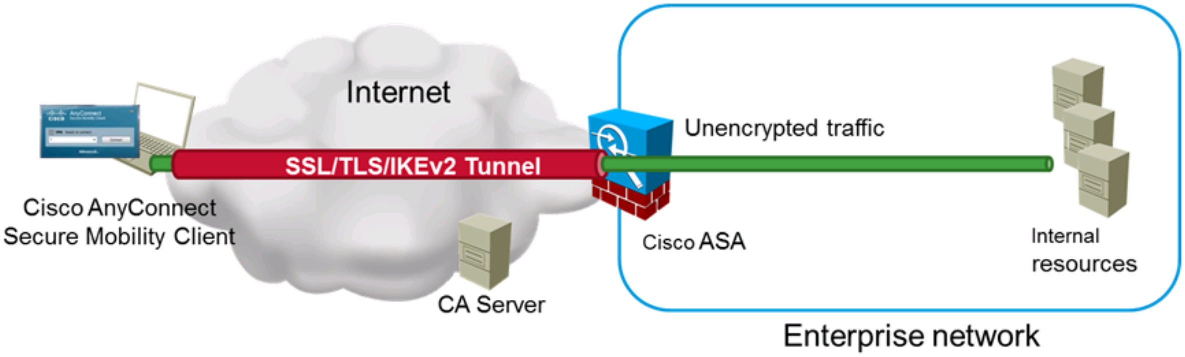
Clientless SSL VPN Authentication Local user database:



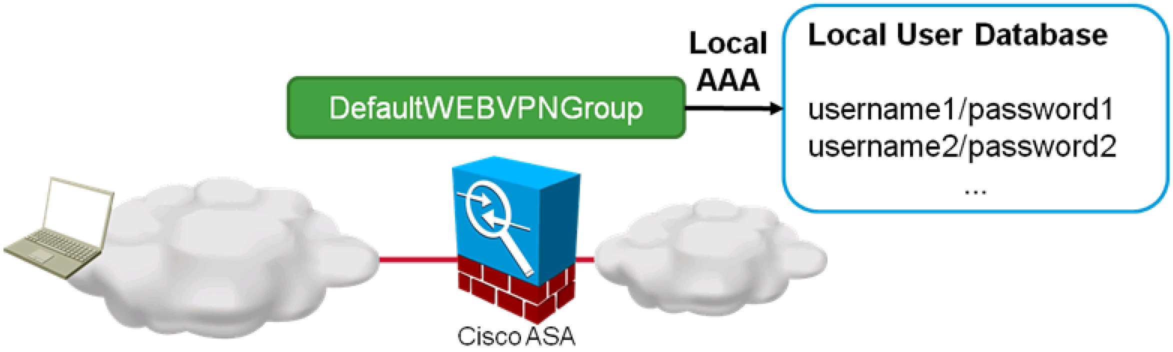
Clientless SSL VPN Configuration Scenario:



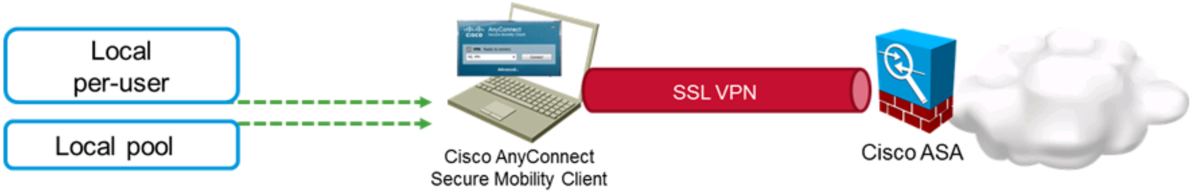
Cisco AnyConnect SSL VPN on ASA:



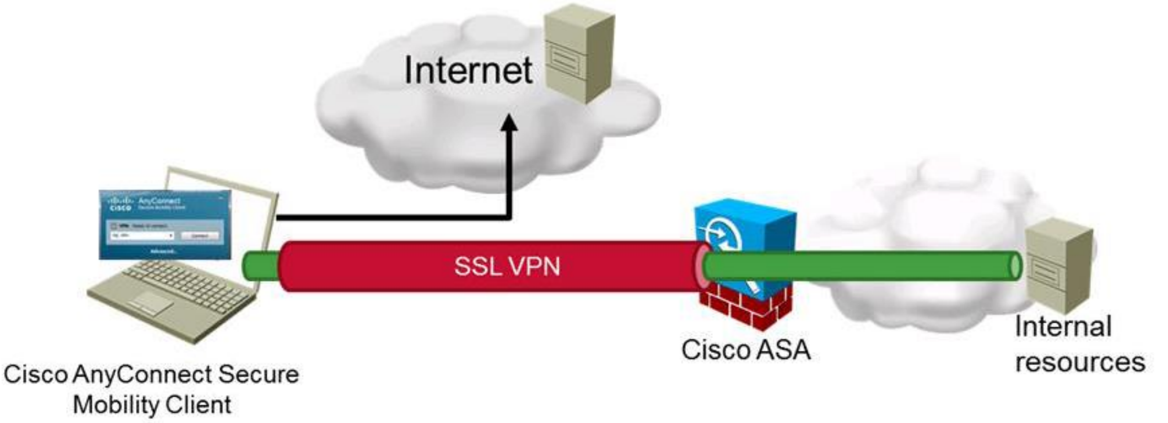
AnyConnect Full-Tunnel Password-Based Users:



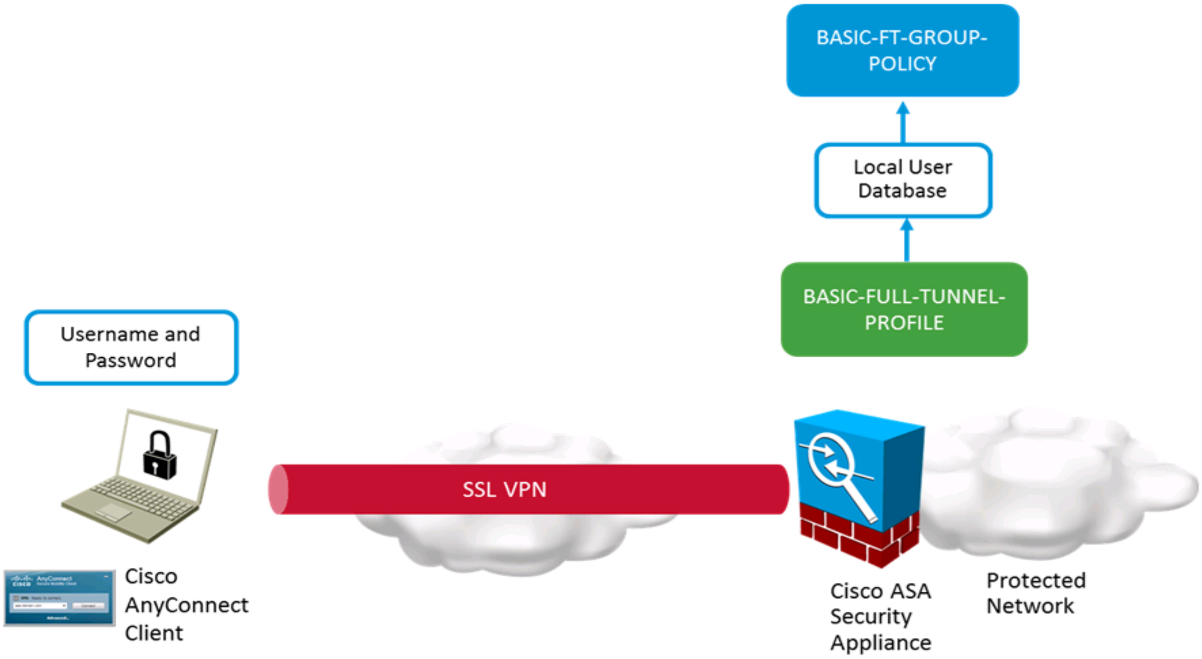
SSL VPN Clients IP Address Assignment Using Local Pool:



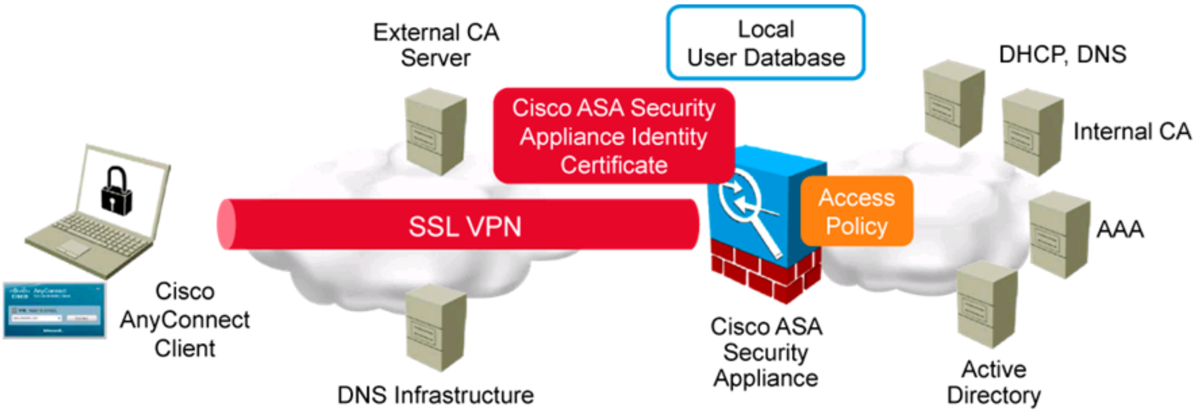
SSL VPN Split Tunneling Policy:



AnyConnect SSL VPN Configuration Scenario:



AnyConnect SSL VPN Solution Components:


External CA Server
Local User Database
DHCP, DNS
Internal CA
Cisco ASA Security Appliance Identity Certificate
SSL VPN
Access Policy
AAA
Cisco AnyConnect Client
Cisco ASA Security Appliance
Active Directory
DNS Infrastructure