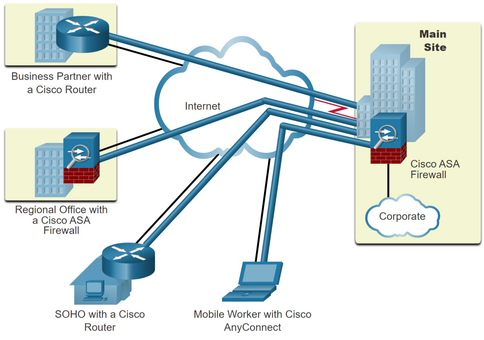
VPN Technology

8.1.1

Virtual Private Networks

To secure network traffic between sites and users, organizations use virtual private networks (VPNs) to create end-to-end private network connections. A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network. A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network.

The figure shows a collection of various types of VPNs managed by an enterprise's main site. The tunnel enables remote sites and users to access main site's network resources securely.



- A Cisco Adaptive Security Appliance (ASA) firewall helps organizations provide secure, high performance connectivity including VPNs and always-on access for remote branches and mobile users.
- SOHO stands for small office home office where a VPN-enabled router can provide VPN connectivity back to the corporate main site.
- Cisco AnyConnect is software that remote workers can use to establish client-based VPN connection with the main site.

The first types of VPNs were strictly IP tunnels that did not include authentication or encryption of the data. For example, Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco and which does not include encryption services. It is used to encapsulate IPv4 and IPv6 traffic inside an IP tunnel to create a virtual point-to-point link.

8.1.2

VPN Benefits

Modern VPNs now support encryption features, such as Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) VPNs to secure network traffic between sites.

Major benefits of VPNs are shown in the table.

Benefit	Description
Cost Savings	With the advent of cost-effective, high-bandwidth technologies, organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.
Security	VPNs provide the highest level of security available, by using advanced encryption and authentication protocols that protect data from unauthorized access.
Scalability	VPNs allow organizations to use the Internet, making it easy to add new users without adding significant infrastructure.
Compatibility	VPNs can be implemented across a wide variety of WAN link options including all the popular broadband technologies. Remote workers can take advantage of these high-speed connections to gain secure access to their corporate networks.

8.1.3

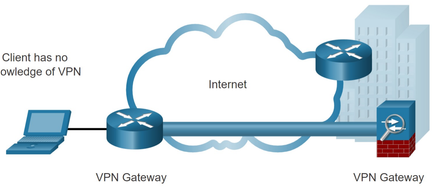
Site-to-Site and Remote-Access VPNs

VPNs are commonly deployed in one of the following configurations: site-to-site or remote-access.

Click each VPN type for more information.

Site-to-Site VPN | Remote-Access VPN

A site-to-site VPN is created when VPN terminating devices, also called VPN gateways, are preconfigured with information to establish a secure tunnel. VPN traffic is only encrypted between these devices. Internal hosts have no knowledge that a VPN is being used.



8.1.4

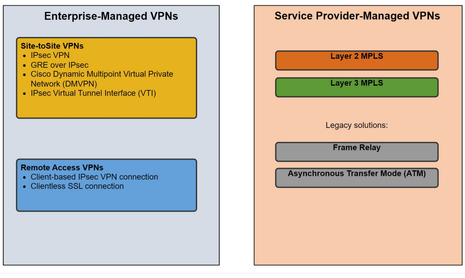
Enterprise and Service Provider VPNs

There are many options available to secure enterprise traffic. These solutions vary depending on who is managing the VPN.

VPNs can be managed and deployed as:

- **Enterprise VPNs** - Enterprise-managed VPNs are a common solution for securing enterprise traffic across the Internet. Site-to-site and remote access VPNs are created and managed by the enterprise using both IPsec and SSL VPNs.
- **Service Provider VPNs** - Service provider-managed VPNs are created and managed over the provider network. The provider uses Multiprotocol Label Switching (MPLS) at Layer 2 or Layer 3 to create secure channels between an enterprise's sites. MPLS is a routing technology the provider uses to create virtual paths between sites. This effectively segregates the traffic from other customer traffic. Other legacy solutions include Frame Relay and Asynchronous Transfer Mode (ATM) VPNs.

The figure lists the different types of enterprise-managed and service provider-managed VPN deployments that will be discussed in more detail in this module.



8.1.5

Check Your Understanding - VPN Technology

Check your understanding of VPN technology by choosing the BEST answer to the following questions.

1. Which VPN benefit allows an enterprise to easily add more users to the network?
   - ( ) Cost Savings
   - ( ) Security
   - (•) Scalability
   - ( ) Compatibility

2. Which VPN benefit allows an enterprise to increase the bandwidth for remote sites without necessarily adding more equipment or WAN links?
   - (•) Cost Savings
   - ( ) Security
   - ( ) Scalability
   - ( ) Compatibility

3. Which VPN benefit uses advanced encryption and authentication protocols to protect data from unauthorized access?
   - ( ) Cost Savings
   - (•) Security
   - ( ) Scalability
   - ( ) Compatibility

4. Which type of VPN is used to connect a mobile user?
   - ( ) Site-to-site
   - (•) Remote-access
   - ( ) GRE
   - ( ) IPsec

5. Which VPN solutions are typically managed by an enterprise? (Choose three)
   - [ ] MPLS Layer 2
   - [ ] MPLS Layer 3
   - [x] IPsec
   - [x] SSL
   - [ ] Frame Relay
   - [x] DMVPN

Check | Show Me | Reset