VPNs at a Glance (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Objective

Explain the use of VPNs in securing site-to-site connectivity in a small- to medium-sized business network.
Instructor Note: This is an individual, student-based activity which then moves into a small, group-based activity for discussion and design purposes. Once the small, group-based activity is completed, students will deliver a presentation to the entire class.

Scenario

A small- to medium-sized business is growing and needs customers, teleworkers, and wired/wireless employees to be able to access the main network from any location. As the network administrator for the business, you have decided to implement VPNs for security, network access ease, and cost savings.

It is your job to ensure that all of the network administrators start the VPN planning process with the same knowledge set.

Four basic VPN informational areas need to be researched and presented to the network administrative team:

- Concise definition of VPNs
- Some general VPN facts
- IPsec as a VPN security option
- Ways VPNs use tunneling

Resources

- World Wide Web access
- Word processing or presentation software

Directions

Step 1: Individual students research all four of the following topics and take notes on their research:

a. Topic 1: A concise definition of VPNs
b. Topic 2: Five general facts about VPNs
c. Topic 3: IPsec defined as a security option when using VPNs
d. Topic 4: A graphic showing how VPNs use tunneling

Step 2: After students research their topics, groups of four students will be formed to discuss their individual research.

a. Each group will agree on
    1) One concise VPN definition
    2) Five facts describing VPNs
    3) One definition of IPsec as a VPN security option
    4) One graphic showing a VPN network using tunneling

Step 3: Each group will design a four-slide presentation (one slide per topic) to deliver to the class for discussion.

Instructor – Example Activity Solution (all group presentations will vary)

Topic 1 - VPN Definition - How VPNs Work

A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote site or employee. By using a VPN, businesses ensure security -- anyone intercepting the encrypted data can't read it.

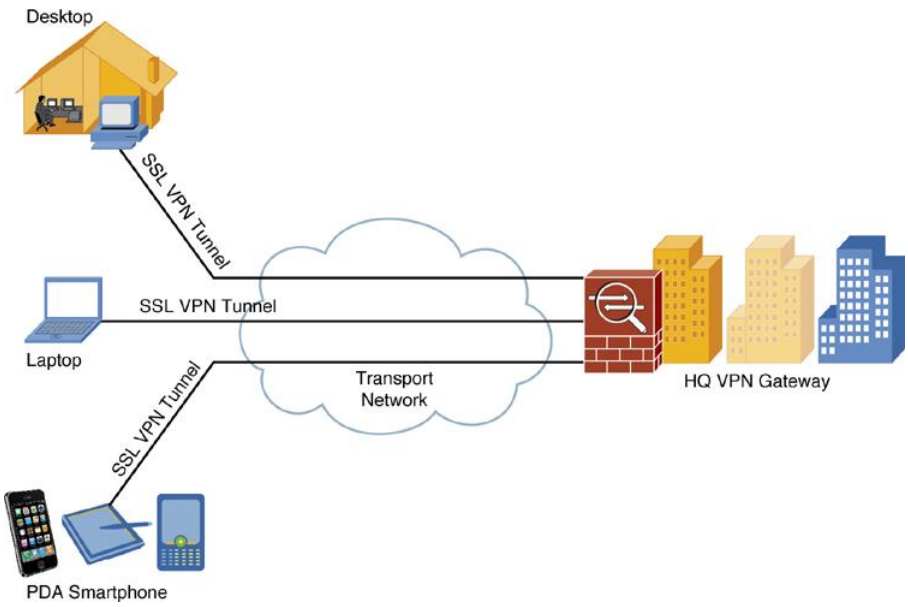
Topic 2 - Five general facts about VPNs - VPN - Virtual Private Network

- A VPN uses public networks to send and receive private network data using special protocols.
- VPNs utilize a client and server approach.
- VPN clients authenticate users.
- Data is encrypted over most VPN systems.
- VPNs use servers to configure tunneling on the network.

Topic 3 - IPsec as a security option - Encryption and Security Protocols in a VPN

IPsec is a widely used protocol for securing traffic on IP networks, including the Internet. IPsec can encrypt data between various devices, including router to router, firewall to router, desktop to router, and desktop to server.

Topic 4 - A graphic showing a VPN using tunneling - Deploying Cisco ASA AnyConnect Remote-Access SSL VPN Solutions



Identify elements of the model that map to IT-related content:

- VPN definition
- VPN facts
- Security as related to VPNs (IPsec)
- VPN tunneling