VPN Planning Design (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 activity is best completed in small groups. It can then be shared with another group, the class, or the instructor (as a group project).

Scenario

Your small- to medium-sized business has received quite a few new contracts lately. This has increased the need for teleworkers and workload outsourcing. The new contract vendors and clients will also need access to your network as the projects progress.

As network administrator for the business, you recognize that VPNs must be incorporated as a part of your network strategy to support secure access by the teleworkers, employees, and vendors or clients.

To prepare for implementation of VPNs on the network, you devise a planning checklist to bring to the next department meeting for discussion.

Resources

- World Wide Web access
- Packet Tracer software
- Word processing software

Step 1: Visit the VPN Discovery Tool, or any other Internet site with VPN-implementation, or planning checklist examples.

Step 2: Use Packet Tracer to draw the current topology for your network; no device configurations are necessary. Include:

- Two branch offices: the Internet cloud and one headquarters location
- Current network devices: servers, switches, routers/core routers, broadband ISR devices, and local user workstations

Step 3: On the Packet Tracer topology, indicate:

a. Where you would implement VPNs?

b. What types of VPNs would be needed?

1) Site to site

2) Remote access

Step 4: Using a word processing software program, create a small VPN planning checklist based on your research from Step 1.

Step 5: Share your work with the class, another group, or your instructor.

Suggested Activity Example Solution:

VPN Project Goals: (Write "1" beside the most important goal, "2" beside the next most-important goal, etc.)

_____Reduce existing telecommunications costs
_____Provide a secure VPN communications system for teleworkers, mobile users, and customers
_____Use existing equipment with a minimum of redesign (cost consideration)
_____Take advantage of new technologies (software and hardware)

Timeline Goal:

☐ 3 months ☐ 6 months ☐ 9 months ☐ 1 year
Phased-in approach: ☐ Yes ☐ No

VPN Factors to Support: (1=Most Important, 2=Very Important, 3=Somewhat Important, 4=Not Important)

Factor	Hardware	Software
Scalability		
Cost		
Interoperability		
Security		
Quality of Service		
Network Maintenance		
Applications Support		

VPN Users and Applications to Support:

Internal Network Users	Customers/Vendors	Teleworkers
Number of users: _____	Approximate number of users: _____	Number of Users: _____

Type of VPN Connection:

_____Site-to-Site _____Remote Access (Internet)

Network resources available to VPN users:

_____Software Applications/Files _____Servers (FTP, Web, Mail, etc.)

VPN Protocols to be used:

_____ SSL _____IPsec _____Both

Network protocols to be used:

_____EIGRP _____OSPF

Technologies currently in use:

_____Network Address Translation (NAT) _____Packet Filtering (ACLs) _____DHCP _____DNS

Authentication to be used:

_____Digital Certificates _____Shared Secrets _____SSL _____Passwords _____IPsec

Encryption to be used:

_____DES _____3DES _____AES

HASH message method to be used:

_____MD-5 _____SHA-1

Encryption key exchange method to be used:

_____Internet Key Exchange (IKE) _____Manual Exchange

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

- VPN network planning
- VPN topology types
- Security methods
  - Authentication
  - Encryption
  - HASH message type
  - Key exchange type