Module 8

Implementing VPNs

Module Overview

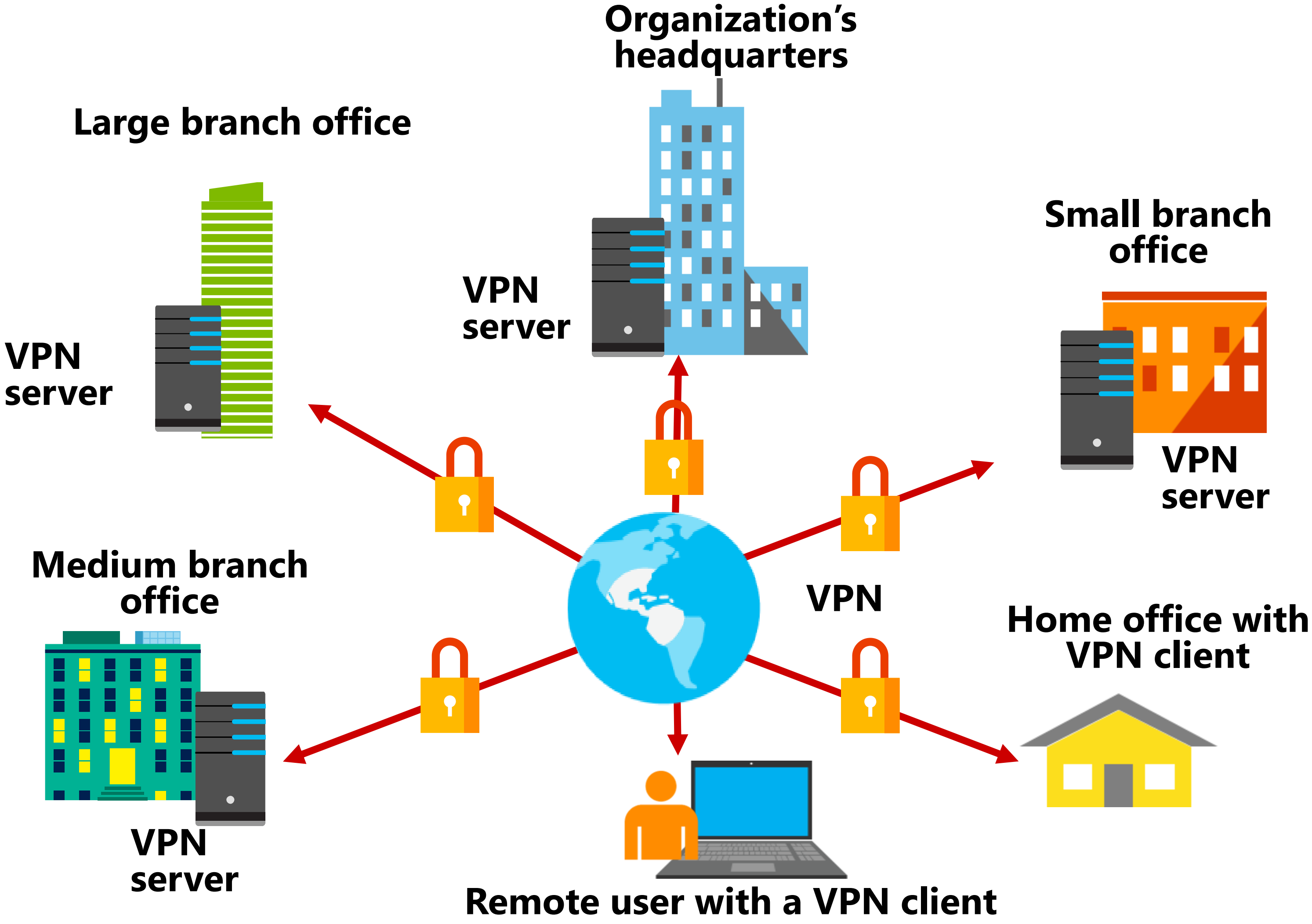
- Planning VPNs
- Implementing VPNs

Lesson 1: Planning VPNs

- VPN scenarios
- Site-to-site VPN
- Options for VPN tunneling protocols
- VPN authentication options
- What is VPN Reconnect?
- The app-triggered VPN feature

VPN scenarios

A VPN provides a point-to-point connection between a private network’s components, by using a public network, such as the Internet.



Site-to-site VPN

- Connects two portions of a private network
- The calling router (the VPN client) authenticates itself to the answering router (the VPN server)
- Requires that you create a demand-dial interface
- You can create three types of site-to-site VPNs:
  - PPTP
  - L2TP
  - IKEv2
- Can be persistent or on-demand
- You can control traffic by using either IP demand-dial filters or dial-out filters

Options for VPN tunneling protocols

Windows Server 2016 supports four VPN tunneling protocols:

Tunneling protocol	Firewall access	Description
PPTP	TCP port 1723	Provides data confidentiality, but not data integrity or data authentication
L2TP/IPsec	UDP port 500, UDP port 1701, UDP port 4500, and IP protocol ID 50	Uses either certificates or preshared keys for authentication; we recommend certificate authentication
SSTP	TCP port 443	Uses SSL to provide data confidentiality, data integrity, and data authentication
IKEv2	UDP port 500	Supports the latest IPsec encryption algorithms to provide data confidentiality, data integrity, and data authentication

VPN authentication options

Protocol	Description	Security level
PAP	Uses plaintext passwords. Typically used if the remote access client and remote access server cannot negotiate a more secure form of validation.	The least secure authentication protocol. Does not protect against replay attacks, remote client impersonation, or remote server impersonation.
CHAP	A challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme	An improvement over PAP in that the password is not sent over the PPP link Requires a plaintext version of the password to validate the challenge response. Does not protect against remote server impersonation.
MS-CHAPv2	An upgrade of MS-CHAP. Provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server to which it is dialing in to has access to the user's password.	Provides stronger security than CHAP
EAP	Allows for arbitrary authentication of a remote access connection through the use of authentication schemes, known as EAP types	Offers the strongest security by providing the most flexibility in authentication variations

What is VPN Reconnect?

- VPN Reconnect maintains connectivity across network outages
- VPN Reconnect:
  - Provides seamless and consistent VPN connectivity
  - Uses the IKEv2 technology
  - Automatically reestablishes VPN connections when connectivity is available
  - Maintains the connection if users move between different networks
  - Provides transparent connection status to users

The app-triggered VPN feature

- App-triggered VPN enables an app to trigger a VPN profile automatically
- You configure app-triggered VPN by using the **AddVpnConnectionTriggerApplication** PowerShell cmdlet
- Domain-member computers do not support app-triggered VPN
- App-triggered VPN requires that you enable split tunneling for the VPN profile

Lesson 2: Implementing VPNs

- Configuring a VPN by using the Getting Started Wizard
- Options for modifying VPN configurations
- Demonstration: Configuring VPN
- What is the Connection Manager Administration Kit?
- Demonstration: Creating a connection profile
- Distributing VPN profiles

Configuring a VPN by using the Getting Started Wizard

- Configure VPN by using the **Getting Started Wizard** in the Remote Access Management console
- Requirements for VPN server configuration include:
  - Two network interfaces (public and private)
  - IP Address allocation (static pool or DHCP)
  - Authentication provider (NPS/RADIUS or the VPN server)
  - DHCP relay agent considerations
  - Membership in the local Administrators group or equivalent

Options for modifying VPN configurations

To configure your VPN solution, you might need to:

- Configure static packet filters
- Configure services and ports
- Adjust logging levels for routing protocols
- Configure the number of available VPN ports
- Create a Connection Manager profile for users
- Add AD CS
- Increase remote access security
- Increase VPN security
- Implement VPN Reconnect

Demonstration: Configuring VPN

In this demonstration, you will learn how to:

- Verify certificate requirements for IKEv2 and SSTP
- Review the default VPN configuration
- Configure the Remote Access policies

What is the Connection Manager Administration Kit?

- CMAK:
  - Allows you to customize users’ remote connection experience by creating predefined connections on remote servers and networks
  - Creates an executable file that can be run on a client computer to establish a network connection that you have designed
- You can distribute CMAK profiles to client computers by using:
  - An operating system image
  - Removable media
  - Software distribution tools, such as Configuration Manager

Demonstration: Creating a connection profile

In this demonstration, you will learn how to:

- Install CMAK
- Create a connection profile
- Examine the profile

Distributing VPN profiles

You can create and distribute a VPN profile by using:

- Configuration Manager
- Intune
- Group Policy
- Scripts

Lab: Implementing VPN

- Exercise 1: Implementing VPN
- Exercise 2: Validating the VPN deployment
- Exercise 3: Troubleshoot VPN access

Logon Information

Virtual machines:	**20741A-LON-DC1**
	20741A-LON-SVR1
	20741A-EU-RTR
	20741A-INET1
	20741A-LON-CL1
User name:	**Adatum\Administrator**
Password:	**Pa$$w0rd**

Estimated Time: 60 minutes

Lab Scenario

The DirectAccess deployment is working very well. However, several computers that are deployed at A. Datum cannot connect to the organization's network by using DirectAccess. For example, some home users are utilizing computers that are not members of the Adatum.com domain. Other users are running operating-system versions that do not support DirectAccess. To enable remote access for these computers, you must deploy a VPN solution.

Furthermore, you must investigate why Logan cannot connect to the A. Datum VPN.

Lab Review

- In the lab, you configured the VPN server to assign IPv4 addresses by using Dynamic Host Configuration Protocol (DHCP). Are there any other options for assigning IPv4 addresses to clients?
- In exercise 1, task 3, you configured a network policy that allowed members of the IT group to connect to A. Datum´s VPN server. Would you be able to connect if you had not created that policy?
- In the troubleshooting exercise, you imported the AdatumCA Root certificate manually into the Trusted Root Certification Authority store on LON-CL1. Is it possible to automate this process?

Module Review and Takeaways

- Review Questions
- Tools
- Best Practices