

70-642: Windows Server 2008 Network Infrastructure, Configuring

1

Your network contains one Active Directory domain. You have a member server that runs Windows Server 2008.

You need to immediately disable all incoming connections to the server.

What should you do?

- A. From the Services snap-in, disable the IP Helper.
- B. From the Services snap-in, disable the Netlogon service.
- C. From Windows Firewall, enable the **Block all connections** option on the Public Profile.
- D. From Windows Firewall, enable the **Block all connections** option on the Domain Profile.

2

You deploy a Windows Server 2008 VPN server behind a firewall. Remote users connect to the VPN by using portable computers that run Windows Vista with the latest service pack.

The firewall is configured to allow only secured Web communications.

You need to enable remote users to connect as securely as possible. You must achieve this goal without opening any additional ports on the firewall.

What should you do?

- A. Create an IPsec tunnel.
- B. Create an SSTP VPN connection.
- C. Create a PPTP VPN connection.
- D. Create an L2TP VPN connection.

3

Your network contains one Active Directory domain. You have a member server named Server1 that runs Windows Server 2008. The server has the Routing and Remote Access Services role service installed.

You implement Network Access Protection (NAP) for the domain.

You need to configure the Point-to-Point Protocol (PPP) authentication method on Server1.

Which authentication method should you use?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Extensible Authentication Protocol (EAP)
- C. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)
- D. Password Authentication Protocol (PAP)

4

Your company has Active Directory Certificate Services (AD CS) and Network Access Protection (NAP) deployed on the network.

You need to configure the wireless network to accept smart cards.

What should you do?

- A. Configure the wireless network to use WPA2, PEAP, and MSCHAP v2.
- B. Configure the wireless network to use WPA2, 802.1X authentication and EAP-TLS.
- C. Configure the wireless network to use WEP, 802.1X authentication, PEAP, and MS-CHAP v2.
- D. Configure the wireless network to use WPA, PEAP, and MS-CHAP v2 and also require strong user passwords.

5

Your company has users who connect remotely to the main office through a Windows Server 2008 VPN server.

You need to ensure that users cannot access the VPN server remotely from 22:00 to 05:00.

What should you do?

- A. Create a network policy for VPN connections. Modify the **Day and time restrictions**.
- B. Create a network policy for VPN connections. Apply an IP filter to deny access to the corporate network.
- C. Modify the **Logon hours** for all user objects to specify only the VPN server on the **Computer restrictions** option.
- D. Modify the **Logon Hours** for the default domain policy to enable the **Force logoff when logon hours expire** option.

6

Your company has Active Directory Certificate Services (AD CS) and Network Access Protection (NAP) deployed on the network.

You need to ensure that NAP policies are enforced on portable computers that use a wireless connection to access the network.

What should you do?

- A. Configure all access points to use 802.1X authentication.
- B. Configure all portable computers to use MS-CHAP v2 authentication.
- C. Use the Group Policy Management Console to access the wireless Group Policy settings, and enable the **Prevent connections to ad-hoc networks** option.
- D. Use the Group Policy Management Console to access the wireless Group Policy settings, and disable the **Prevent connections to infrastructure networks** option.

7

Your company has deployed Network Access Protection (NAP).

You configure secure wireless access to the network by using 802.1X authentication from any access point.

You need to ensure that all client computers that access the network are evaluated by NAP.

What should you do?

- A. Configure all access points as RADIUS clients to the Remediation Servers.
- B. Configure all access points as RADIUS clients to the Network Policy Server (NPS).
- C. Create a Network Policy that defines Remote Access Server as a network connection method.
- D. Create a Network Policy that specifies EAP-TLS as the only available authentication method.

8

Your network contains a server that runs Windows Server 2008. The server has the Network Policy and Access Services server role installed.

You need to allow only members of a global group named Group1 VPN access to the network.

What should you do?

- A. Add Group1 to the RAS and IAS Servers group.
- B. Add Group1 to the Network Configuration Operators group.
- C. Create a new network policy and define a group-based condition for Group1. Set the access permission of the policy to **Access granted**. Set the processing order of the policy to **1**.
- D. Create a new network policy and define a group-based condition for Group1. Set the access permission of the policy to **Access granted**. Set the processing order of the policy to **3**.

9

Your company's corporate network uses Network Access Protection (NAP).

Users are able to connect to the corporate network remotely.

You need to ensure that data transmissions between remote client computers and the corporate network are as secure as possible.

What should you do?

- A. Apply an IPsec NAP policy.
- B. Configure a NAP policy for 802.1X wireless connections.
- C. Configure VPN connections to use MS-CHAP v2 authentication.
- D. Restrict Dynamic Host Configuration Protocol (DHCP) clients by using NAP.

10

Your company has deployed Network Access Protection (NAP) enforcement for VPNs.

You need to ensure that the health of all clients can be monitored and reported.

What should you do?

- A. Create a Group Policy object (GPO) that enables Security Center and link the policy to the domain.
- B. Create a Group Policy object (GPO) that enables Security Center and link the policy to the Domain Controllers organizational unit (OU).
- C. Create a Group Policy object (GPO) and set the **Require trusted path for credential entry** option to **Enabled**. Link the policy to the domain.
- D. Create a Group Policy object (GPO) and set the **Require trusted path for credential entry** option to **Enabled**. Link the policy to the Domain Controllers organizational unit (OU).

11

Your company has 10 servers that run Windows Server 2008. The servers have Remote Desktop Protocol (RDP) enabled for server administration. RDP is configured to use default security settings. All administrators' computers run Windows Vista.

You need to ensure the RDP connections are as secure as possible.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Set the security layer for each server to the RDP Security Layer.
- B. Configure the firewall on each server to block port 3389.
- C. Acquire user certificates from the internal certification authority.
- D. Configure each server to allow connections only to Remote Desktop client computers that use Network Level Authentication.

12

You have a DHCP server that runs Windows Server 2008.

You restore the DHCP database by using a recent backup.

You need to prevent DHCP clients from receiving IP addresses that are currently in use on the network.

What should you do?

- A. Add the DHCP server option 15.
- B. Add the DHCP server option 44.
- C. Set the Conflict Detection value to **0**.
- D. Set the Conflict Detection value to **2**.

13

Your network uses IPv4.

You install a server that runs Windows Server 2008 at a branch office. The server is configured with two network interfaces.

You need to configure routing on the server at the branch office.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Install the Routing and Remote Access Services role service.
- B. Run the **netsh ras ip set access ALL** command.
- C. Run the **netsh interface ipv4 enable** command.
- D. Enable the **IPv4 Router** Routing and Remote Access option.

14

You have a Windows Server 2008 computer that has an IP address of 172.16.45.9/21.

The server is configured to use IPv6 addressing.

You need to test IPv6 communication to a server that has an IP address of 172.16.40.18/21.

What should you do from a command prompt?

- A. Type **ping 172.16.45.9::::::**
- B. Type **ping ::9.45.16.172**.
- C. Type **ping** followed by the Link-local address of the server.
- D. Type **ping** followed by the Site-local address of the server.

15

You have a DHCP server that runs Windows Server 2008.

You need to reduce the size of the DHCP database.

What should you do?

- A. From the DHCP snap-in, reconcile the database.
- B. From the folder that contains the DHCP database, run **jetpack.exe dhcp.mdb temp.mdb**.
- C. From the properties of the dhcp.mdb file, enable the **File is ready for archiving** attribute.
- D. From the properties of the dhcp.mdb file, enable the **Compress contents to save disk space** attribute.

16

Your company has an IPv4 Ethernet network.

A router named R1 connects your segment to the Internet. A router named R2 joins your subnet with a segment named Private1. The Private1 segment has a network address of 10.128.4.0/26.

Your computer named WKS1 requires access to servers on the Private1 network.

The WKS1 computer configuration is as shown in the following table.

Network	Addresses
IPv4 Address	10.128.64.113
Subnet mask	255.255.252.0
Default Gateway	10.128.64.1

The routers are configured as shown in the following table.

Router ID	Addresses
R1 - interface 1	10.128.64.1
R1 - interface 2 (To Internet)	131.107.108.37
R2 - interface 1	10.128.64.10
R2 - interface 2	10.128.4.1

WKS1 is unable to connect to the Private1 network by using the current configuration.

You need to add a persistent route for the Private1 network to the routing table on WKS1.

Which command should you run on WKS1?

- A. **Route add -p 10.128.4.0/22 10.128.4.1**
- B. **Route add -p 10.128.4.0/26 10.128.64.10**
- C. **Route add -p 10.128.4.0 mask 255.255.255.192 10.128.64.1**
- D. **Route add -p 10.128.64.10 mask 255.255.255.192 10.128.4.0**

17

You have a DHCP server named Server1 and an application server named Server2. Both servers run Windows Server 2008. The DHCP server contains one scope.

You need to ensure that Server2 always receives the same IP address. Server2 must receive its DNS settings and its WINS settings from DHCP.

What should you do?

- A. Create a multicast scope.
- B. Assign a static IP address to Server2.
- C. Create an exclusion range in the DHCP scope.
- D. Create a DHCP reservation in the DHCP scope.

18

Your network consists of a single Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2008. All client computers run Windows Vista. All computers are members of the Active Directory domain.

You assign the Secure Server (Require Security) IPsec policy to Server1 by using a Group Policy object (GPO).

Users report that they fail to connect to Server1.

You need to ensure that users can connect to Server1. All connections to Server1 must be encrypted.

What should you do?

- A. Restart the IPsec Policy Agent service on Server1.
- B. Assign the Client (Respond Only) IPsec policy to Server1.
- C. Assign the Server (Request Security) IPsec policy to Server1.
- D. Assign the Client (Respond Only) IPsec policy to all client computers.

19

Your company has computers in multiple locations that use IPv4 and IPv6. Each location is protected by a firewall that performs symmetric NAT.

You need to allow peer-to-peer communication between all locations.

What should you do?

- A. Configure dynamic NAT on the firewall.
- B. Configure the firewall to allow the use of Teredo.
- C. Configure a link local IPv6 address for the internal interface of the firewall.
- D. Configure a global IPv6 address for the external interface of the firewall.