Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

NEW QUESTION 1
Which three methods are used by the collector agent for AD polling? (Choose three.)

A. WinSecLog
B. WMI
C. NetAPI
D. FSSO REST API
E. FortiGate polling

Answer: ABC

Explanation:
The Fortinet Single Sign-On (FSSO) Collector Agent supports three primary methods for Active Directory (AD) polling to collect user information:

- WinSecLog: Monitors Windows Security Event Logs for login events.
- WMI: Uses Windows Management Instrumentation to poll user login sessions.
- NetAPI: Utilizes the Netlogon API to query domain controllers for user session data.

These methods allow the FortiGate to gather user logon information and enforce user-based policies effectively.
References:

- FortiOS 7.4.1 Administration Guide: FSSO Configuration

NEW QUESTION 2
Refer to the exhibit, which shows a partial configuration from the remote authentication server.

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	

Why does the FortiGate administrator need this configuration?

A. To authenticate only the Training user group.
B. To set up a RADIUS server Secret
C. To authenticate and match the Training OU on the RADIUS server.
D. To authenticate Any FortiGate user groups.

Answer: A

NEW QUESTION 3
An administrator manages a FortiGate model that supports NTurbo. How does NTurbo enhance performance for flow-based inspection?

A. NTurbo offloads traffic to the content processor.
B. NTurbo creates two inspection sessions on the FortiGate device.
C. NTurbo buffers the whole file and then sends it to the antivirus engine.
D. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.

Answer: A

Explanation:
NTurbo enhances performance for flow-based inspection by offloading traffic to the content processor.

NEW QUESTION 4
Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.
B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.
C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
D. The client FortiGate requires a manually added route to remote subnets.

Answer: BC

Explanation:
For SSL VPN to function correctly between two FortiGate devices, the following settings are required:

- B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate must have a Certificate Authority (CA) certificate installed to authenticate and verify the certificate presented by the client FortiGate device.
- C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate: The client FortiGate must have a client certificate that is signed by the same CA that the server FortiGate uses for verification. This ensures a secure SSL VPN connection between the two devices.

The other options are not directly necessary for establishing SSL VPN:

- A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: This is incorrect as SSL VPN does not require a specific tunnel

interface type; it typically uses an SSL VPN client profile.

D. The client FortiGate requires a manually added route to remote subnets: While routing may be necessary, it is not specifically required for the SSL VPN functionality between two FortiGates.
References

FortiOS 7.4.1 Administration Guide - Configuring SSL VPN, page 1203.

FortiOS 7.4.1 Administration Guide - SSL VPN Authentication, page 1210.

NEW QUESTION 5
Which statement is a characteristic of automation stitches?

A. They can be run only on devices in the Security Fabric.
B. They can be created only on downstream devices in the fabric.
C. They can have one or more triggers.
D. They can run multiple actions at the same time.

Answer: C

Explanation:
Automation stitches on FortiGate can have one or more triggers, which are conditions or events that activate the automation stitch. The trigger defines when the automation stitch should execute the defined actions. Actions within a stitch can be executed sequentially or in parallel, depending on the configuration.
References:

FortiOS 7.4.1 Administration Guide: Automation Stitches

NEW QUESTION 6
Which method allows management access to the FortiGate CLI without network connectivity?

A. SSH console
B. CLI console widget
C. Serial console
D. Telnet console

Answer: C

Explanation:
The serial console method allows management access to the FortiGate CLI without relying on network connectivity. This method involves directly connecting a computer to the FortiGate device using a serial cable (such as a DB-9 to RJ-45 cable or USB to RJ-45 cable) and using terminal emulation software to interact with the FortiGate CLI. This method is essential for situations where network-based access methods (such as SSH or Telnet) are not available or feasible.
References:

FortiOS 7.4.1 Administration Guide: Console connection

NEW QUESTION 7
Refer to the exhibit showing a FortiGuard connection debug output.

FortiGuard connection debug output

```
FortiGate # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Thu Jun  9 11:26:56 2022) -=-

IP              Weight  RTT Flags TZ  FortiGuard-requests  Curr Lost Total Lost Updated Time
173.243.141.16      -8   18    DI  0                    4          0          0 Thu Jun  9 11:26:24 2022
12.34.97.18         20   30        1                    1          0          0 Thu Jun  9 11:26:24 2022
210.7.96.18        160  305        9                    0          0          0 Thu Jun  9 11:26:24 2022
```

Based on the output, which two facts does the administrator know about the FortiGuard connection? (Choose two.)

A. One server was contacted to retrieve the contract information.

B. There is at least one server that lost packets consecutively.
C. A local FortiManaqer is one of the servers FortiGate communicates with.
D. FortiGate is using default FortiGuard communication settings.

Answer: AD

Explanation:
The debug output indicates that FortiGate connected to one server (173.243.141.16) to retrieve contract information as it shows four FortiGuard requests without any packet loss, which confirms the connection to the server. Additionally, the default FortiGuard communication settings are being used, as indicated by the use of the HTTPS protocol on port 443, which is the default setting for FortiGuard connections.
References:

FortiOS 7.4.1 Administration Guide: FortiGuard Connection Settings

NEW QUESTION 8
An administrator configured a FortiGate to act as a collector for agentless polling mode.
What must the administrator add to the FortiGate device to retrieve AD user group information?

A. LDAP server
B. RADIUS server
C. DHCP server
D. Windows server

Answer: A

Explanation:
To retrieve AD user group information in agentless polling mode, the administrator must add an LDAP server to the FortiGate device.

NEW QUESTION 9
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
All traffic must be routed through the primary tunnel when both tunnels are up. The secondary tunnel must be used only if the primary tunnel goes down. In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.
Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)

A. Enable Dead Peer Detection
B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

Answer: AC

Explanation:
To configure redundant IPsec VPN tunnels on FortiGate with failover capability, the following two key configuration changes are required:

A. Enable Dead Peer Detection (DPD): Dead Peer Detection is crucial for detecting if the remote peer is unreachable. By enabling DPD, FortiGate can quickly detect a dead tunnel, ensuring a faster failover to the secondary tunnel when the primary tunnel goes down.

C. Configure a lower distance on the static route for the primary tunnel and a higher distance on the static route for the secondary tunnel: The static route with the lower distance (higher priority) will be used when both tunnels are operational. If the primary tunnel fails, the higher distance (lower priority) route for the secondary tunnel will take over, ensuring traffic is routed correctly.
The other options are not suitable:

B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels:
This option is not directly related to the requirements of failover between two IPsec VPN tunnels.

D. Configure a higher distance on the static route for the primary tunnel and a lower distance on the static route for the secondary tunnel: This would prioritize the secondary tunnel over the primary tunnel, which is opposite to the desired configuration.
References

FortiOS 7.4.1 Administration Guide - Configuring IPsec VPN, page 1320.

FortiOS 7.4.1 Administration Guide - Redundant VPN Configuration, page 1335.

NEW QUESTION 10
Refer to the exhibit.

FortiGate routing database

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
C    *> 172.16.100.0/24 is directly connected, port8
```

Which two statements are true about the routing entries in this database table? (Choose two.)

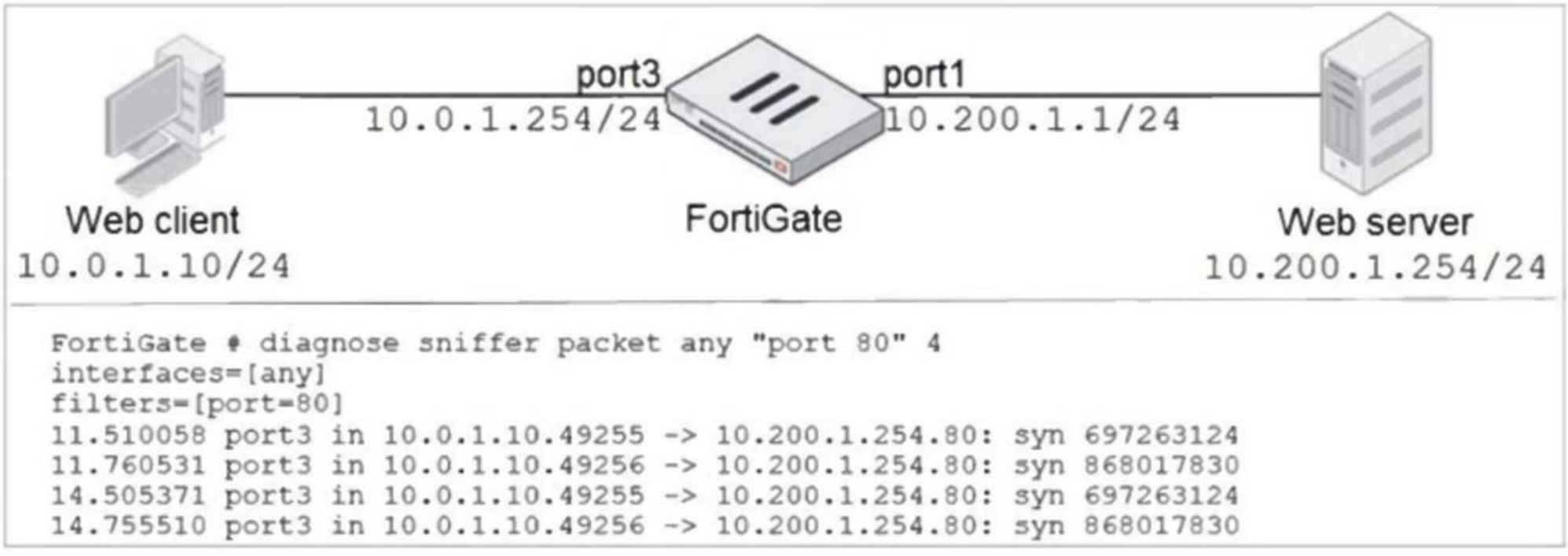
A. All of the entries in the routing database table are installed in the FortiGate routing table.
B. The port2 interface is marked as inactive.
C. Both default routes have different administrative distances.
D. The default route on porc2 is marked as the standby route.

Answer: CD

Explanation:
The routing table in the exhibit shows two default routes (0.0.0.0/0) with different administrative distances:
- The default route through port2 has an administrative distance of 20.
- The default route through port1 has an administrative distance of 10.

Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of 10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2.
Regarding the statement that the port2 interface is marked as inactive, there is no indication in the routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.
References:
- FortiOS 7.4.1 Administration Guide: Default route configuration
- FortiOS 7.4.1 Administration Guide: Routing table

NEW QUESTION 10
Refer to the exhibit.

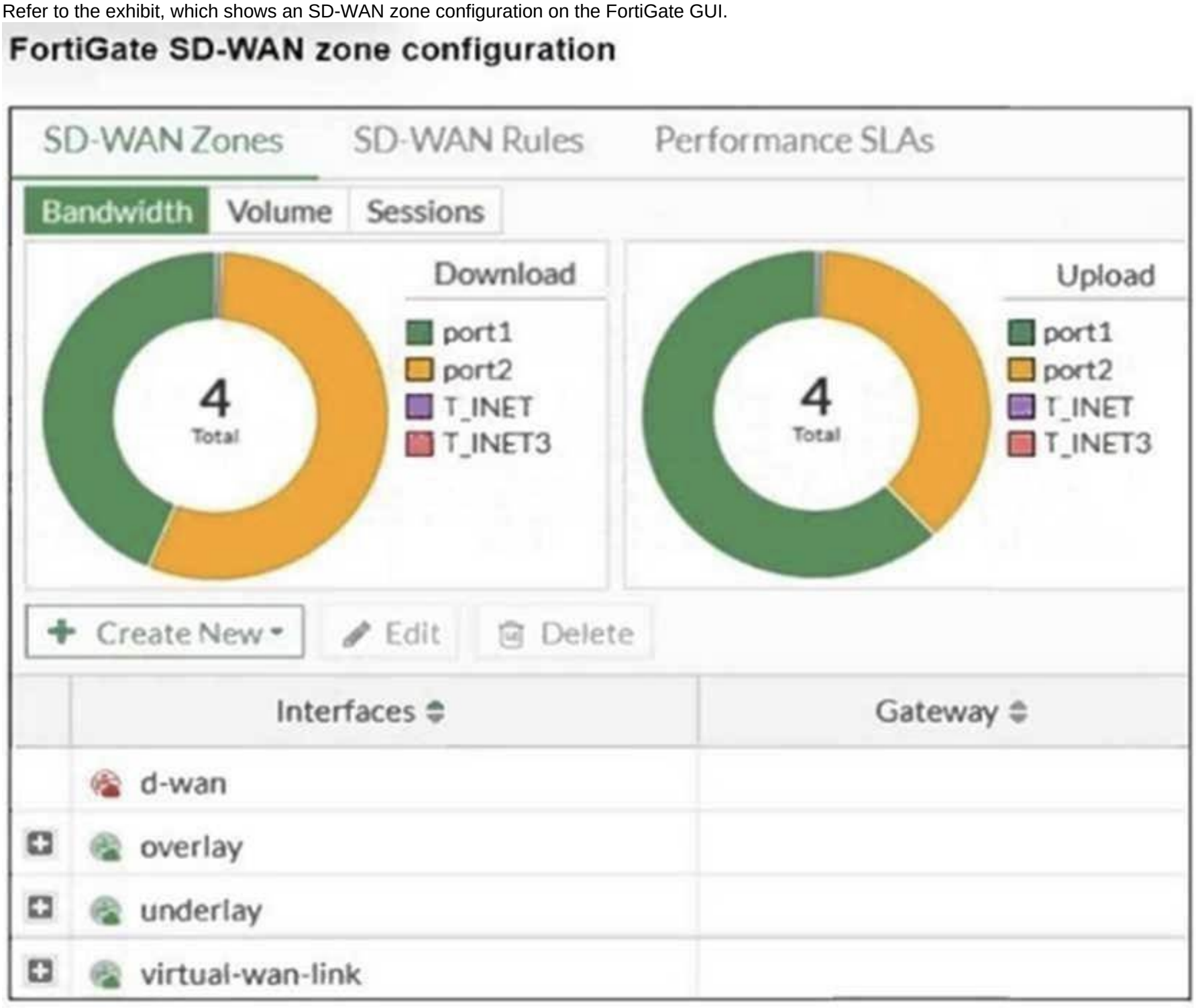


In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.
What should the administrator do next, to troubleshoot the problem?

A. Execute a debug flow.
B. Capture the traffic using an external sniffer connected to port1.
C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".
D. Run a sniffer on the web server.

Answer: A

NEW QUESTION 14
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



Based on the exhibit, which statement is true?

A. The underlay zone contains port1 and
B. The d-wan zone contains no member.
C. The d-wan zone cannot be deleted.
D. The virtual-wan-link zone contains no member.

Answer: C

Explanation:
In FortiGate's SD-WAN configuration, the d-wan zone is a system default SD-WAN zone that is automatically created and cannot be deleted. This zone is used to manage dynamic WAN links for SD-WAN
traffic balancing and routing. It ensures that multiple WAN interfaces can be grouped and managed
effectively for WAN link optimization.
Why the other options are less appropriate:
• A. The underlay zone contains port1 and: There is no mention in the exhibit about an "underlay zone" containing port1.
• B. The d-wan zone contains no member: This statement is irrelevant since the focus is on the zone's deletion, not its members.
• D. The virtual-wan-link zone contains no member: This is unrelated to the core fact that the d-wan zone cannot be deleted.
Reference:
FortiOS 7.4.1 Administration Guide: SD-WAN Zone Configuration

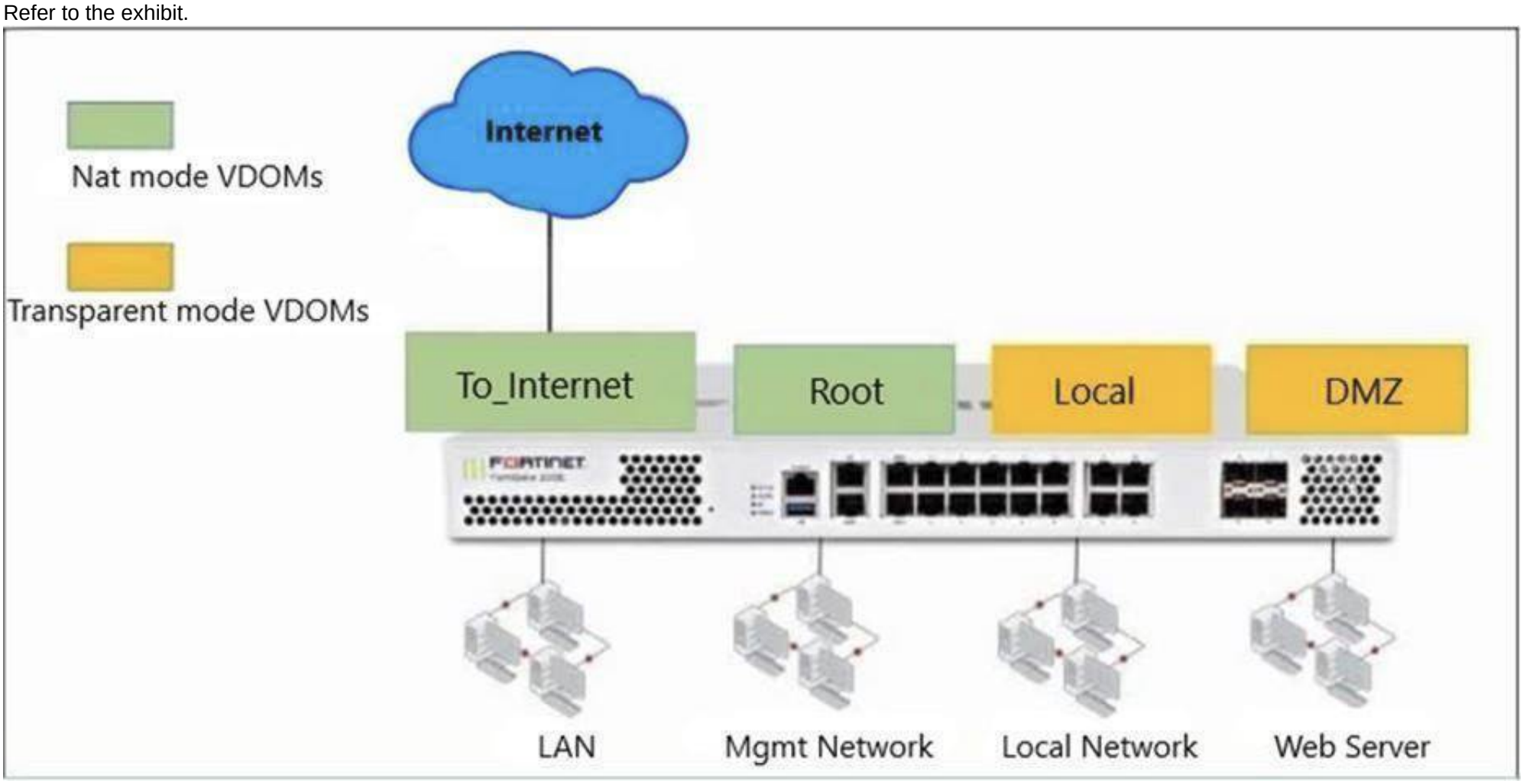
NEW QUESTION 17
Which of the following methods can be used to configure FortiGate to perform source NAT (SNAT) for outgoing traffic?

A. Configure a static route pointing to the external interface.
B. Enable the "Use Outgoing Interface Address" option in a firewall policy.
C. Create a virtual server with an external IP address.
D. Deploy an IPsec VPN tunnel with NAT enabled.

Answer: B

Explanation:
To configure source NAT (SNAT) for outgoing traffic on FortiGate, one of the most common methods is to enable the "Use Outgoing Interface Address" option in a firewall policy. This option ensures that the source IP address of packets leaving the FortiGate device is replaced by the IP address of the outgoing interface. This is typically done when traffic is exiting a private network to access the internet, requiring source NAT to translate the private IP addresses to a public IP.
Why the other options are less appropriate:
* A. Configure a static route pointing to the external interface: A static route is used to direct traffic, but it does not configure SNAT. It determines where packets are sent but does not modify the source IP.
• C. Create a virtual server with an external IP address: Virtual servers are used to provide destination NAT (DNAT) for incoming traffic, not SNAT for outgoing traffic.
• D. Deploy an IPsec VPN tunnel with NAT enabled: While IPsec VPN tunnels can be configured with NAT traversal, this is not the typical method for configuring SNAT for general outgoing internet traffic.

NEW QUESTION 19
Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
B. A default static route is not required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

Explanation:
In this scenario, multiple Virtual Domains (VDOMs) are used, and each VDOM operates either in NAT mode or transparent mode:
• Root VDOM (management) and To_Internet VDOM are in NAT mode.
• DMZ VDOM and Local VDOM are in transparent mode.
To allow traffic between different VDOMs (e.g., Local and Root), inter-VDOM links must be configured.
Since Local VDOM is in transparent mode, it functions at Layer 2, meaning it requires an inter-VDOM link to pass traffic through the Root VDOM, which operates in NAT mode at Layer 3.
Why the other options are less appropriate:
• B. A default static route is not required on the To_Internet VDOM:
A default route is required on the To_Internet VDOM to send traffic from LAN users to the internet.
• C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs:
Both Local and DMZ are in transparent mode and operate at Layer 2, so direct communication
would require inter-VDOM links if passing through another VDOM.
• D. Inter-VDOM links are not required between the Root and To_Internet VDOMs:
Even if the Root VDOM is only used for management, it still requires inter-VDOM links to communicate with other VDOMs (like To_Internet) in the Security Fabric.

NEW QUESTION 24
Consider the topology:
Application on a Windows machine <--{SSL VPN} -->FGT--> Telnet to Linux server.
An administrator is investigating a problem where an application establishes a Telnet session to a Linux
server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.
The administrator has already verified that the issue is not caused by the application or Linux server.
This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.
What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

A. Set the maximum session TTL value for the TELNET service object.
B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happenafter 90 minutes.
C. Create a new service object for TELNET and set the maximum session TTL.
D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Answer: CD

Explanation:
The issue with the idle session timing out after 90 minutes can be resolved by adjusting the session Time-
To-Live (TTL) for the TELNET service used over the SSL VPN connection. Here's how the administrator
can address the problem:
• C. Create a new service object for TELNET and set the maximum session TTL:
By creating a new service object specifically for TELNET and setting a custom maximum session TTL, the administrator can ensure that the TELNET session does not time out prematurely. This way, the session will last longer or indefinitely, depending on the configured TTL.
• D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy:
Creating a dedicated firewall policy for SSL VPN traffic and placing it above the existing one allows the administrator to apply the new TELNET service object with a longer session TTL. This will ensure the new policy with the adjusted settings takes precedence for TELNET traffic.
Why the other options are less appropriate:
• A. Set the maximum session TTL value for the TELNET service object:
This would work if you were adjusting an existing TELNET service object. However, creating a new service object for TELNET and applying it in the firewall policy (as described in options C and D) is more granular and won't affect other services using the same TELNET object.
• B. Set the session TTL on the SSLVPN policy to maximum:
While this would extend the session timeout for the entire SSL VPN traffic, it could affect other services running through the SSL VPN, which may not be desirable. This option would lack the necessary specificity for only the TELNET traffic.

NEW QUESTION 27
Which two statements correctly describe the differences between IPsec main mode and IPsec aggressive mode? (Choose two.)

A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not.
B. Main mode cannot be used for dialup VPNs, while aggressive mode can.
C. Aggressive mode supports XAuth, while main mode does not.
D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode.

Answer: AD

Explanation:
The differences between IPsec main mode and IPsec aggressive mode are mainly in the number of packets exchanged and the level of security provided during the negotiation process. Here's the breakdown:
• A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not:
In aggressive mode, the peer's identity is sent in the first packet, making the process faster but less secure because the peer's identity is not encrypted. In main mode, the peer's identity is protected and only exchanged after the encryption is established, offering more security.
• D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode:
Main mode involves a more detailed negotiation process, requiring the exchange of six packets. Aggressive mode, on the other hand, reduces this to three packets, speeding up the connection but sacrificing some security in the process.
Why the other options are less appropriate:
• B. Main mode cannot be used for dialup VPNs, while aggressive mode can:
This is incorrect. Main mode can be used for dialup VPNs as long as the peer's IP is known or configured in advance.
• C. Aggressive mode supports XAuth, while main mode does not:
Both main mode and aggressive mode can support XAuth (eXtended Authentication) if needed.

NEW QUESTION 31
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FGT_AD-7.4 Practice Exam Features:

* FCP_FGT_AD-7.4 Questions and Answers Updated Frequently

* FCP_FGT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FGT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FGT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year