Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

NEW QUESTION 1
Refer to the exhibit.

```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.
0"
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw-10.200.1.254
via port1"
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (policy 0)"
```

Why did FortiGate drop the packet?

A. It matched an explicitly configured firewall policy with the action DENY
B. It failed the RPF check.
C. The next-hop IP address is unreachable.
D. It matched the default implicit firewall policy

Answer: D

Explanation:
The debug trace output shows that the packet was "Denied by forward policy check (policy 0)." In FortiGate, policy ID 0 corresponds to the default implicit deny policy. This means that if a packet does not match any configured firewall policies, it is denied by the default implicit policy.
References:

- FortiOS 7.4.1 Administration Guide: Firewall Policies

NEW QUESTION 2
When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate.
Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

A. Allow & Warning
B. Trust & Allow
C. Allow
D. Block & Warning
E. Block

Answer: ADE

Explanation:
When FortiGate performs SSL/SSH full inspection and detects an invalid certificate, there are three valid actions it can take:

- Allow & Warning: This action allows the session but generates a warning.
- Block & Warning: This action blocks the session and generates a warning.
- Block: This action blocks the session without generating a warning.

Actions such as "Trust & Allow" or just "Allow" without additional configurations are not applicable in the context of handling invalid certificates.
References:

- FortiOS 7.4.1 Administration Guide: Configuring SSL/SSH inspection profile

NEW QUESTION 3
Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.
B. The RPF check is run on the first reply packet of any new session.
C. The RPF check is run on the first sent and reply packet of any new session.
D. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

Answer: AD

Explanation:
The Reverse Path Forwarding (RPF) check is run on the first sent packet of any new session to ensure that the packet arrives on a legitimate interface. This check protects the network from IP spoofing attacks by verifying that a return route exists from the receiving interface back to the source IP address. If the route is invalid or not found, the packet is discarded. Options B and C are incorrect because RPF checks are performed on the first sent packet, not the reply packet.
References:

- FortiOS 7.4.1 Administration Guide: Reverse Path Forwarding (RPF) Check

NEW QUESTION 4
What are two features of collector agent advanced mode? (Choose two.)

A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
B. Advanced mode supports nested or inherited groups.
C. In advanced mode, security profiles can be applied only to user groups, not individual users.
D. Advanced mode uses the Windows convention —NetBios: Domain\Username.

Answer: AD

Explanation:
Advanced mode allows for configuration as an LDAP client and supports group filtering directly on the FortiGate, as well as nested or inherited groups.

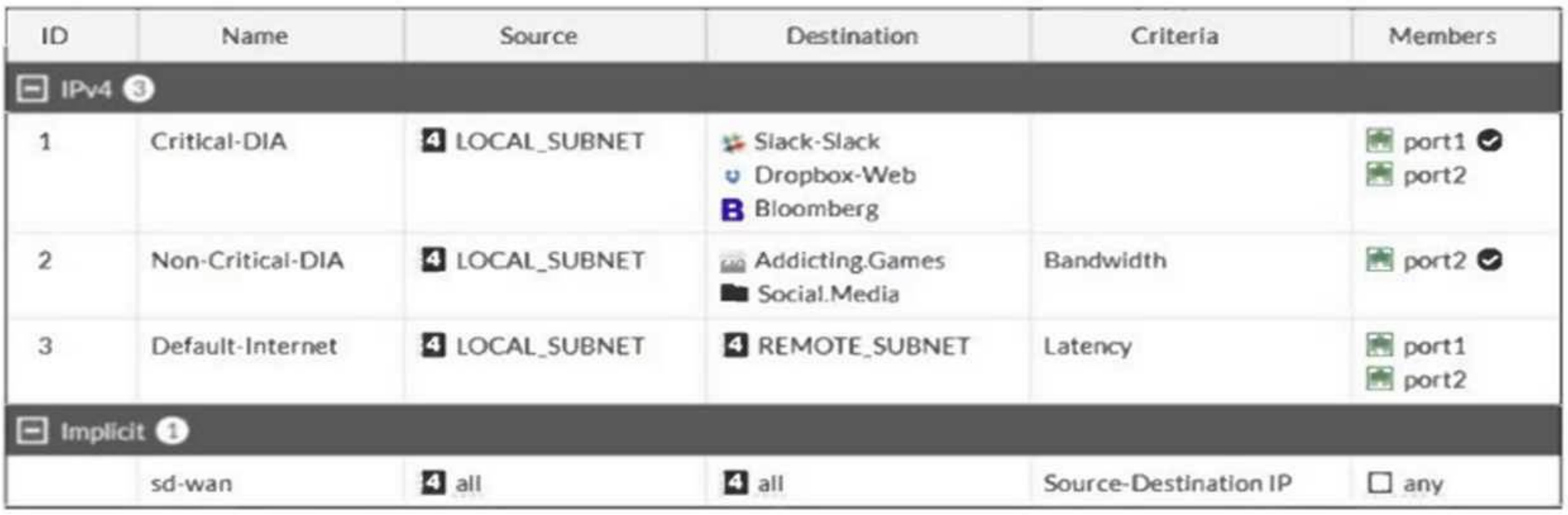
NEW QUESTION 5
Refer to the exhibit, which shows a partial configuration from the remote authentication server.

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 6
Refer to the exhibit.



Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

A. All traffic from a source IP to a destination IP is sent to the same interface.
B. Traffic is sent to the link with the lowest latency.
C. Traffic is distributed based on the number of sessions through each interface.
D. All traffic from a source IP is sent to the same interface

Answer: A

Explanation:
For traffic that does not match any of the defined SD-WAN rules, the default implicit SD-WAN rule is applied. By default, the FortiGate uses a "source-destination IP-based" algorithm, which means all traffic from a specific source IP to a specific destination IP is sent through the same interface. This ensures that a consistent path is used for traffic between the same source and destination IP addresses. Options B, C, and D do not apply because the default algorithm does not prioritize by latency, session count, or source IP alone.
References:
FortiOS 7.4.1 Administration Guide: SD-WAN Load Balancing Algorithms

NEW QUESTION 7
An administrator manages a FortiGate model that supports NTurbo. How does NTurbo enhance performance for flow-based inspection?

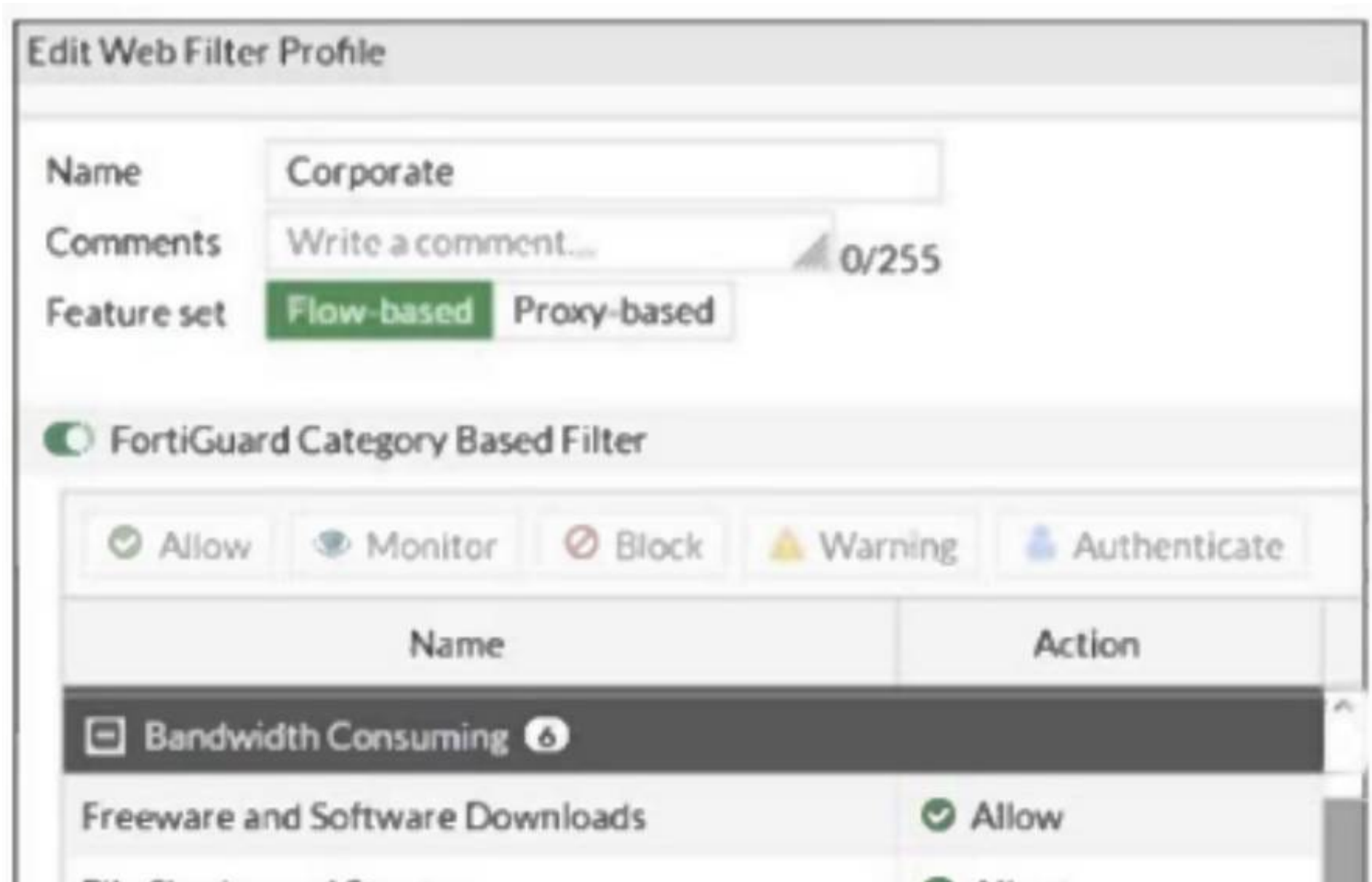
A. NTurbo offloads traffic to the content processor.
B. NTurbo creates two inspection sessions on the FortiGate device.
C. NTurbo buffers the whole file and then sends it to the antivirus engine.
D. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.

Answer: A

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

NEW QUESTION 8

Refer to the exhibit.



The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.
An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.
What are two solutions for satisfying the requirement? (Choose two.)

A. Configure a separate firewall policy with action Deny and an FQDN address object for *. download, com as destination address.
B. Set the Freeware and Software Downloads category Action to Warning
C. Configure a web override rating for download, com and select Malicious Websites as the subcategory.
D. Configure a static URL filter entry for download, com with Type and Action set to Wildcard and Block, respectively.

Answer: AD

Explanation:
To block access specifically to download.com while allowing other sites in the "Freeware and Software Downloads" category, you can create a separate firewall policy with a deny action specifically for the FQDN
*.download.com. This approach allows blocking this particular site without affecting the other sites in the same category. Alternatively, configuring a static URL filter entry with the type set to Wildcard and action set to Block will also achieve the desired effect by directly blocking the specific URL without impacting other sites in the category.
References:

FortiOS 7.4.1 Administration Guide: URL filter configuration

NEW QUESTION 9
FortiGate is integrated with FortiAnalyzer and FortiManager.
When a firewall policy is created, which attribute is added to the policy to improve functionality and to support recording logs to FortiAnalyzer or FortiManager?

A. Log ID
B. Policy ID
C. (Sequence ID
D. Universally Unique Identifier

Answer: D

Explanation:
When a firewall policy is created in FortiGate integrated with FortiAnalyzer and FortiManager, a Universally Unique Identifier (UUID) is added to the policy to support logging and management.

NEW QUESTION 10
Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

A. The host field in the HTTP header.
B. The server name indication (SNI) extension in the client hello message.
C. The subject alternative name (SAN) field in the server certificate.
D. The subject field in the server certificate.
E. The serial number in the server certificate.

Answer: BCD

Explanation:
When SSL certificate inspection is enabled on a FortiGate device, the system uses the following three pieces of information to identify the hostname of the SSL server:

Server Name Indication (SNI) extension in the client hello message (B): The SNI is an extension in the client hello message of the SSL/TLS protocol. It indicates the hostname the client is attempting to connect to. This allows FortiGate to identify the server's hostname during the SSL handshake.

Subject Alternative Name (SAN) field in the server certificate (C): The SAN field in the server certificate lists additional hostnames or IP addresses that the certificate is valid for. FortiGate inspects this field to confirm the identity of the server.

Subject field in the server certificate (D): The Subject field contains the primary hostname or domain name for which the certificate was issued. FortiGate uses this information to match and validate the server??s identity during SSL certificate inspection.
The other options are not used in SSL certificate inspection for hostname identification:

Host field in the HTTP header (A): This is part of the HTTP request, not the SSL handshake, and is not used for SSL certificate inspection.

Serial number in the server certificate (E): The serial number is used for certificate management and revocation, not for hostname identification.
References

FortiOS 7.4.1 Administration Guide - SSL/SSH Inspection, page 1802.

FortiOS 7.4.1 Administration Guide - Configuring SSL/SSH Inspection Profile, page 1799.

NEW QUESTION 10
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 15
An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

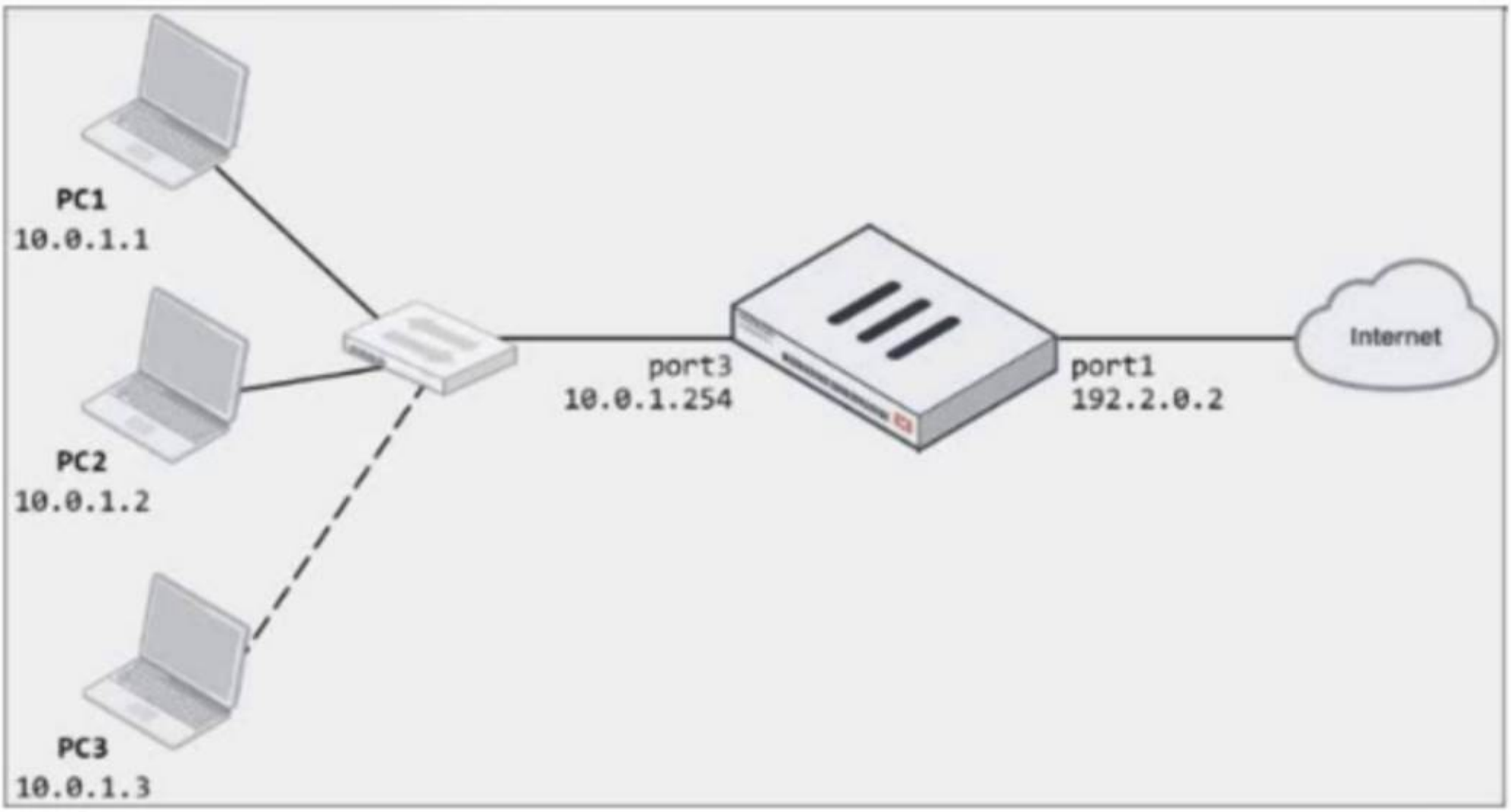
A. It uses UDP 8888.
B. It uses DNS over HTTPS.
C. It uses DNS over TLS.
D. It uses UDP 53.

Answer: D

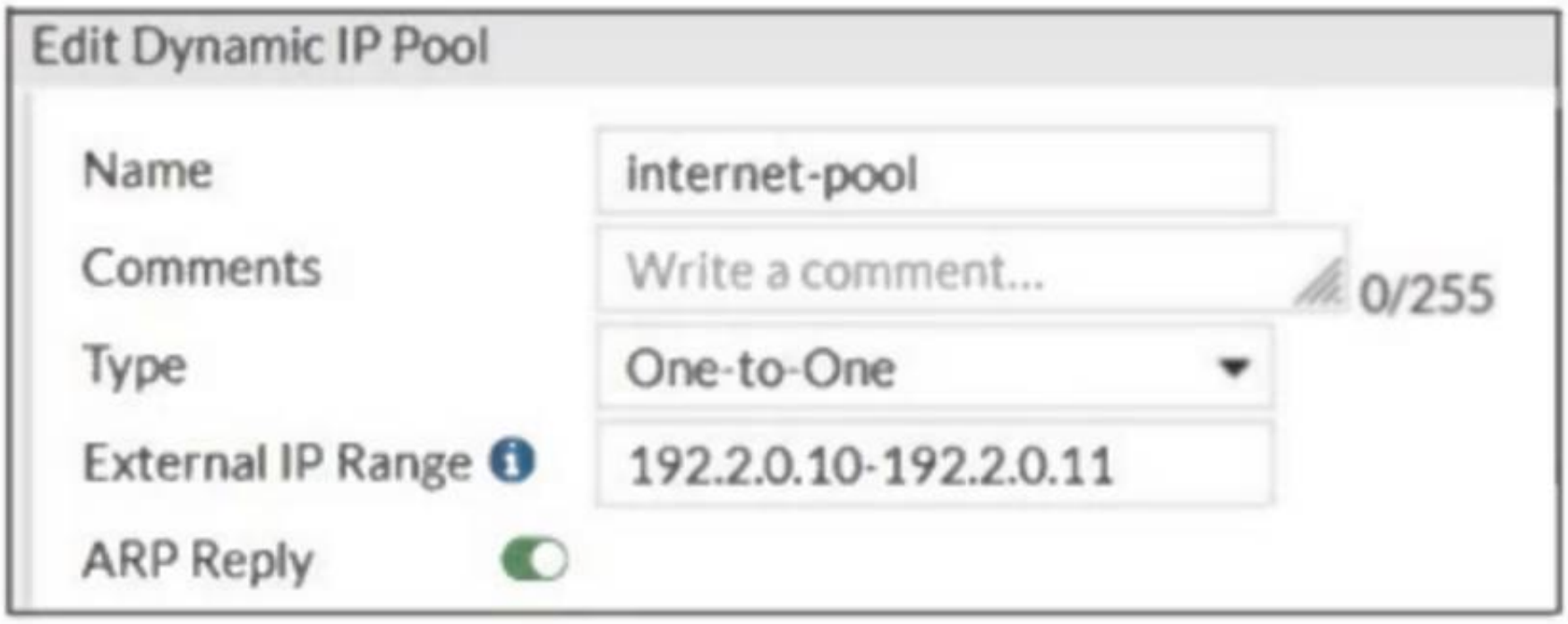
Explanation:
By default, DNS queries to FortiGuard servers use UDP port 53.

NEW QUESTION 18
Refer to the exhibits.

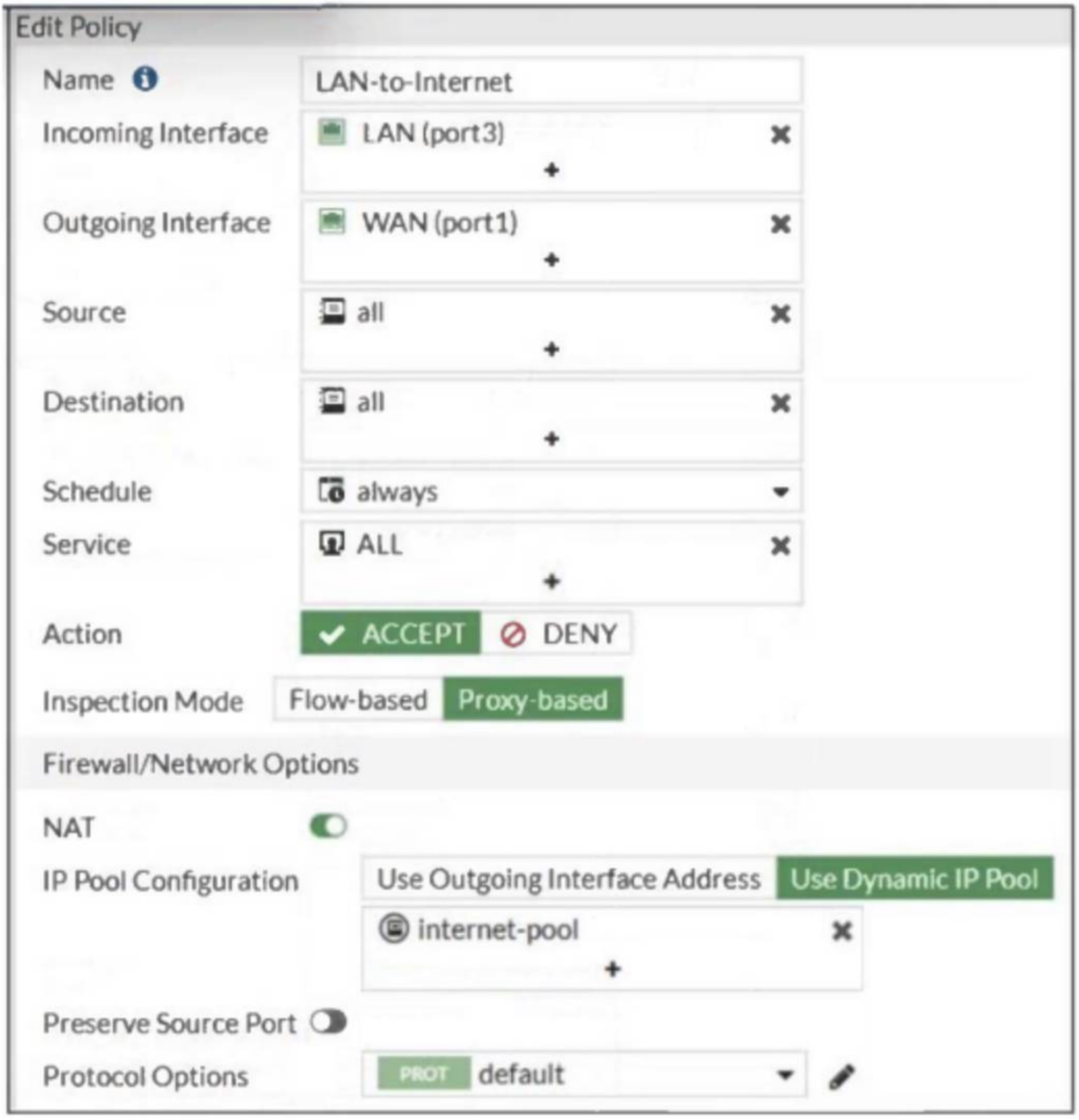
Network diagram



Dynamic IP pool



Firewall policy



The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device.
Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.
Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

A. In the firewall policy configuration, add 10.
B. 3 as an address object in the source field.
C. In the IP pool configuration, set endig to 192.2.0.12.
D. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.
E. In the IP pool configuration, set cype to overload.

Answer: BD

Explanation:
To resolve the issue of PC3 not being able to access the internet, the administrator needs to adjust the IP pool configuration or the firewall policy. The following two options will fix the connectivity issue:

B. In the IP pool configuration, set the ending IP to 192.2.0.12: The current IP pool range is 192.2.0.10-192.2.0.11, which only provides two IP addresses for network address translation (NAT). To allow PC3 to access the internet, the IP pool should be expanded to include an additional IP address by changing the end of the range to 192.2.0.12.

D. In the IP pool configuration, set type to overload: Instead of using a one-to-one NAT, changing the type to overload will allow multiple internal addresses (such as PC1, PC2, and PC3) to share a single external IP address. This will solve the issue without needing additional public IP addresses.
The other options are not suitable:

A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field: This option is unnecessary since the firewall policy already allows all addresses from the source (LAN port3).

C. Configure another firewall policy that matches only the address of PC3 as the source, and then place the policy on top of the list: This option is redundant and would not resolve the underlying issue with the IP pool configuration.
References

FortiOS 7.4.1 Administration Guide - Configuring Firewall Policies, page 512.

FortiOS 7.4.1 Administration Guide - Configuring NAT with IP Pools, page 518.

NEW QUESTION 21
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 23
Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three.)

A. Manual with load balancing
B. Lowest Cost (SLA) with load balancing
C. Best Quality with load balancing
D. Lowest Quality (SLA) with load balancing
E. Lowest Cost (SLA) without load balancing

Answer: ABC

Explanation:
FortiGate's SD-WAN rule strategies for member selection include the following:

Manual with load balancing: This strategy allows an administrator to manually configure which SD- WAN member interfaces to use for specific traffic.

Lowest Cost (SLA) with load balancing: This strategy prioritizes the link with the lowest cost that meets the SLA requirements.

Best Quality with load balancing: This strategy selects the link with the best performance metrics, such as latency, jitter, or packet loss.
Options D and E are incorrect because "Lowest Quality" is not a valid strategy, and "Lowest Cost without load balancing" contradicts the requirement for load balancing in the strategy name.
References:

FortiOS 7.4.1 Administration Guide: SD-WAN Rule Strategies

NEW QUESTION 24
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 28
Refer to the exhibit.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port3 → port1									
1	Full_Access	Remote-users LOCAL_SUB...	all	always	HTTP HTTPS ALL_ICMP	ACCEPT	NAT	Standard	Category_Monitor certificate-inspection

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt.
What is the most likely reason for this situation?

A. The Service DNS is required in the firewall policy.
B. The user is using an incorrect user name.
C. The Remote-users group is not added to the Destination.
D. No matching user account exists for this user.

Answer: A

Explanation:
Firewall authentication generally requires the DNS service to be enabled in the firewall policy to correctly resolve hostnames during the authentication process. If DNS is not allowed in the firewall policy, the FortiGate cannot resolve external domains, and as a result, the user may not be presented with the login prompt when attempting to access an external website.
References:

FortiOS 7.4.1 Administration Guide: Firewall Authentication Configuration

NEW QUESTION 29
Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

A. Pre-shared key and certificate signature as authentication methods
B. Extended authentication (XAuth)to request the remote peer to provide a username and password
C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
D. No certificate is required on the remote peer when you set the certificate signature as the authentication method

Answer: AB

Explanation:
FortiGate supports both pre-shared key and certificate signature methods for IKEv1 authentication. These methods provide flexibility depending on the security requirements of the network. Additionally, FortiGate supports Extended Authentication (XAuth), which requests a username and password from the remote peer, enhancing security by adding an extra layer of authentication. The XAuth method does not necessarily make the authentication faster; it is an additional security measure.
References:

FortiOS 7.4.1 Administration Guide: IPsec VPN Configuration

NEW QUESTION 33
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 37
What is the primary FortiGate election process when the HA override setting is disabled?

A. Connected monitored ports > Priority > System uptime > FortiGate serial number
B. Connected monitored ports > System uptime > Priority > FortiGate serial number
C. Connected monitored ports > Priority > HA uptime > FortiGate serial number
D. Connected monitored ports > HA uptime > Priority > FortiGate serial number

Answer: A

Explanation:
When the HA override setting is disabled, FortiGate uses the primary election process based on the following criteria:
- Connected monitored ports: The unit with the most monitored ports up is preferred.
- Priority: The unit with the highest priority is preferred.
- System uptime: The unit with the longest uptime is preferred.
- FortiGate serial number: Used as the final criterion to break any remaining ties.

References:

FortiOS 7.4.1 Administration Guide: HA election process

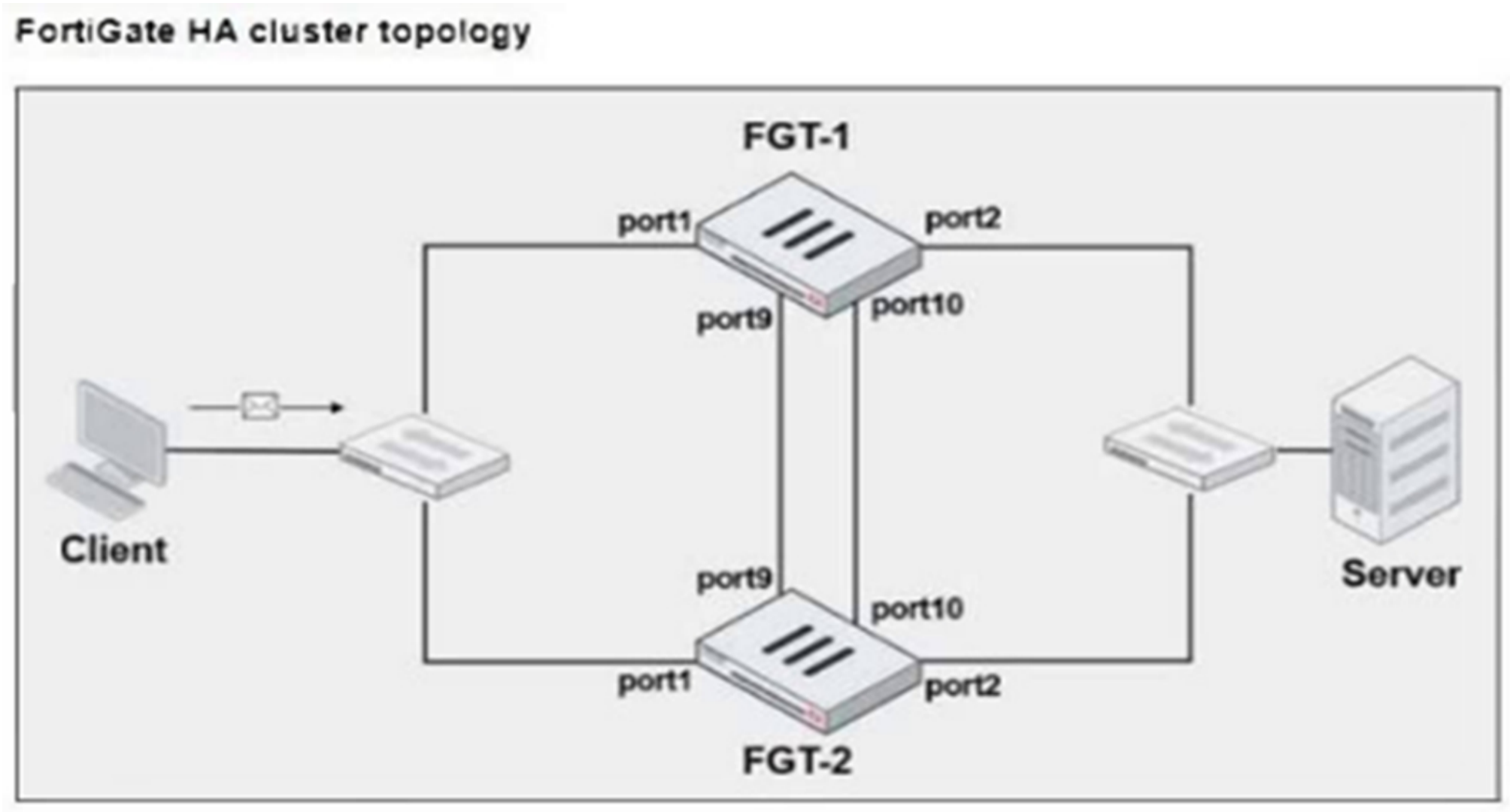
NEW QUESTION 39
An employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

A. SSL VPN idle-timeout
B. SSL VPN login-timeout
C. SSL VPN dtls-hello-timeout
D. SSL VPN session-ttl

Answer: C

Explanation:
For a high-latency internet connection, the SSL VPN setting that should be adjusted is:
* C. SSL VPN dtls-hello-timeout: This setting determines how long the FortiGate will wait for a DTLS hello message from the client. For high-latency connections, increasing this timeout will prevent SSL VPN negotiation failures caused by delays in receiving the DTLS hello message.
The other options are not suitable:
* A. SSL VPN idle-timeout: This setting controls the idle time allowed before a session is terminated, which is not relevant to the initial connection establishment.
* B. SSL VPN login-timeout: This setting controls the maximum time allowed for a user to log in, but does not affect connection negotiation.
* D. SSL VPN session-ttl: This setting controls the total time-to-live for an SSL VPN session but does not directly address issues caused by high latency.
References
FortiOS 7.4.1 Administration Guide - SSL VPN Configuration, page 1415.

NEW QUESTION 42
Refer to the exhibits.



Current HA status

```
# get system ha status
...
Configuration Status:
    FGVM010000064692(updated 4 seconds ago): in-sync
    FGVM010000064692 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
    FGVM010000065036(updated 4 seconds ago): in-sync
    FGVM010000065036 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary      : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary    : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

New FortiGate HA configuration

```
FGT-1
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override disable
    set priority 90
    set monitor port3

FGT-2
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override enable
    set priority 110
    set monitor port3
```

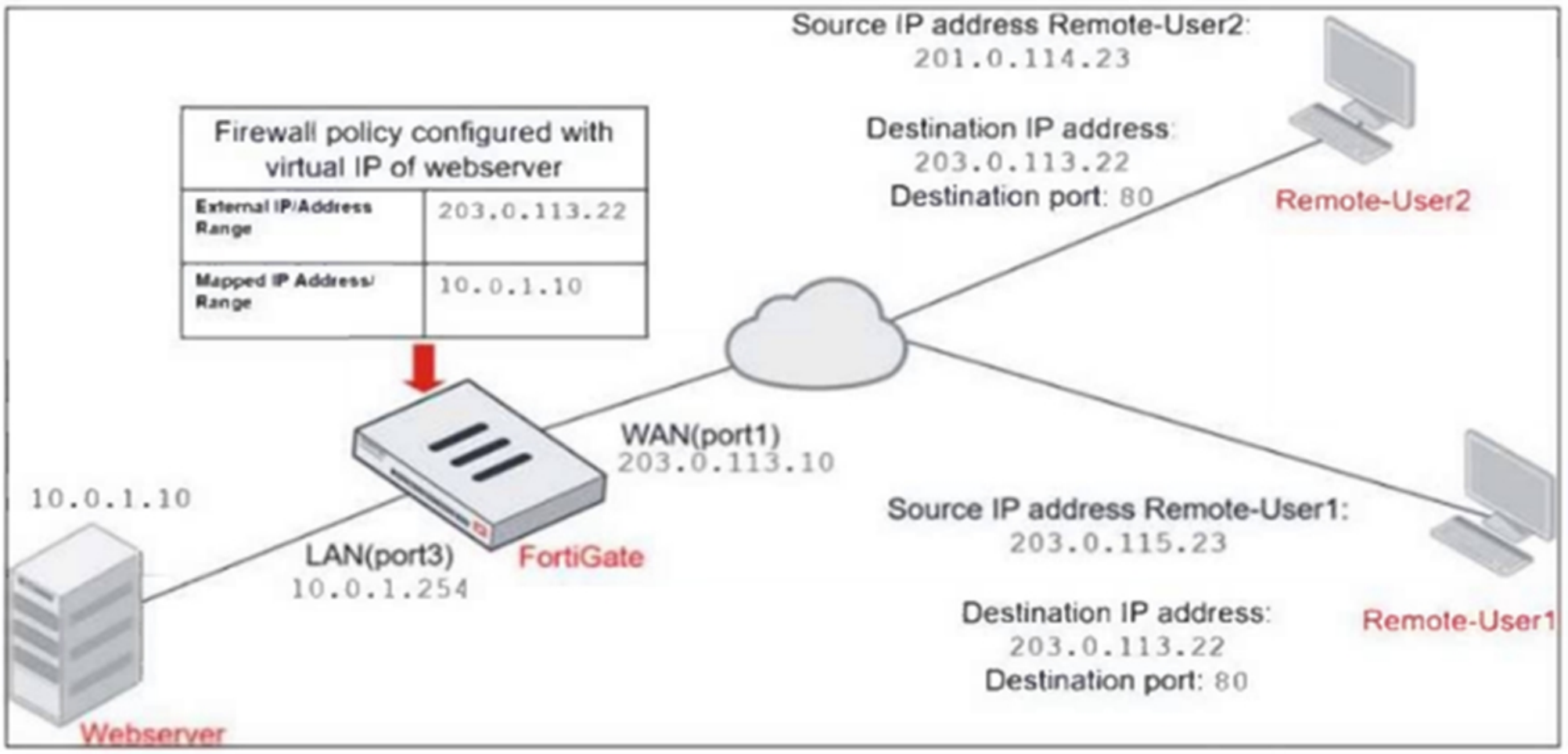
FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.
What would be the expected outcome in the HA cluster?

A. FGT-1 will remain the primary because FGT-2 has lower priority.
B. FGT-2 will take over as the primary because it has the override enable setting and higher priority than FGT-1.
C. FGT-1 will synchronize the override disable setting with FGT-2.
D. The HA cluster will become out of sync because the override setting must match on all HA members.

Answer: B

NEW QUESTION 43
Refer to the exhibits.

Network diagram



Firewall address object

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.
The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.
Which two configuration changes can the administrator make to the policy to deny Webserver access for Remote-User2? (Choose two.)

A. Enable match-vip in the Deny policy.
B. Set the Destination address as Webserver in the Deny policy.
C. Disable match-vip in the Deny policy.
D. Set the Destination address as Deny_IP in the Allow_access policy.

Answer: AB

NEW QUESTION 47
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration

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

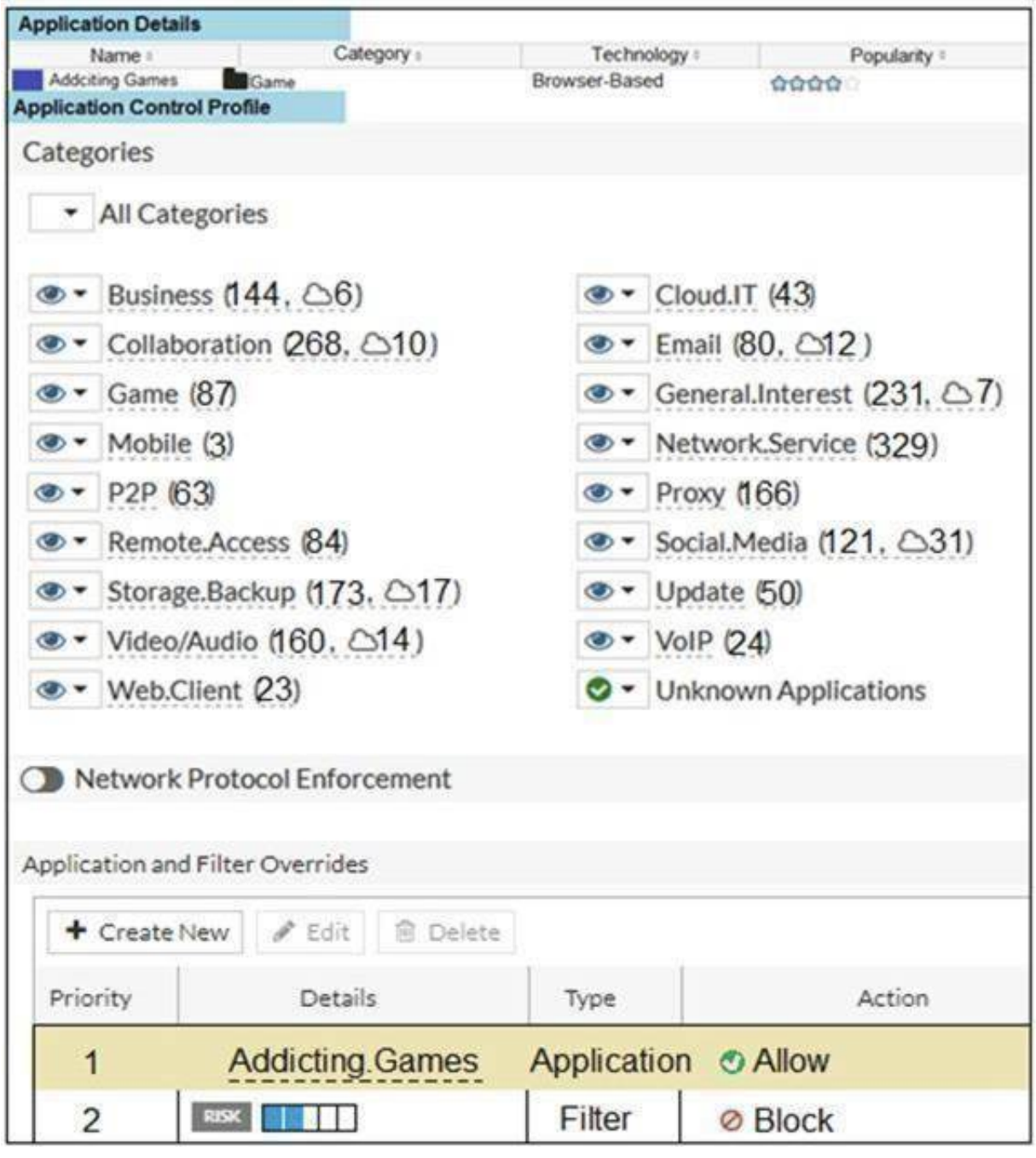
NEW QUESTION 52
Which of the following methods can be used to configure FortiGate to perform source NAT (SNAT) for outgoing traffic?

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 57
Refer to the exhibit.



A user located behind the FortiGate device is trying to go to http://www.addictinggames.com (Addicting.Games). The exhibit shows the application detains and application control profile.
Based on this configuration, which statement is true?

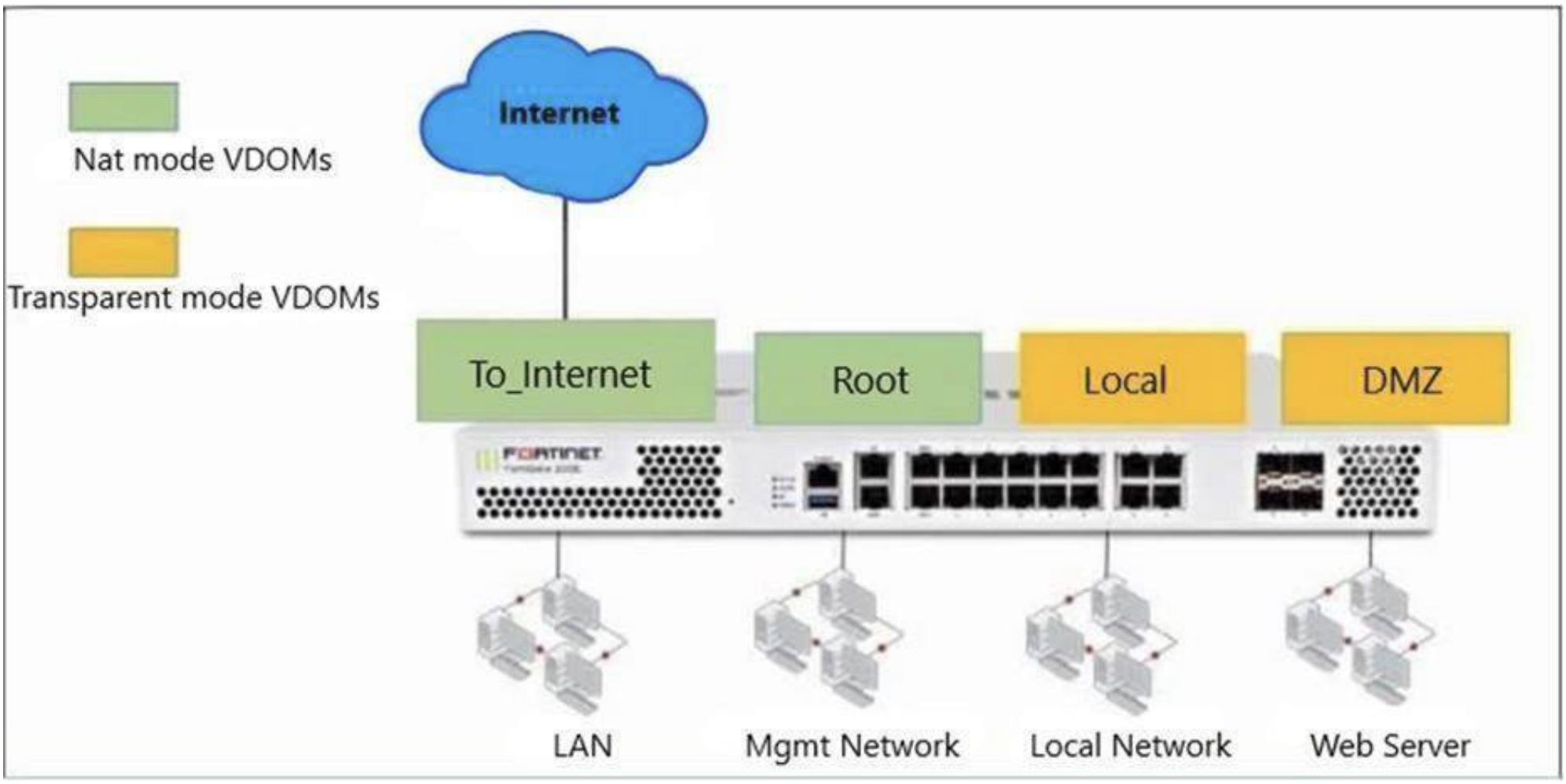
A. Addicting.Games will be blocked, based on the Filter Overrides configuration.

B. Addicting.Games will be allowed only if the Filter Overrides action is set to Learn.
C. Addicting.Games will be allowed, based on the Categories configuration.
D. Addicting.Games will be allowed, based on the Application Overrides configuration.

Answer: D

Explanation:
In the exhibit, it shows that the Application Overrides section is configured to allow the application Addicting.Games. The Application Control Profile gives priority to the application overrides, meaning that even if a category or filter would block it, the application control override would allow the specific application to proceed.
• A. Addicting.Games will be blocked, based on the Filter Overrides configuration:
This is incorrect because the Application Overrides take precedence over other filters.
• B. Addicting.Games will be allowed only if the Filter Overrides action is set to Learn:
This is not applicable as the action is based on Application Overrides, not filter overrides.
• C. Addicting.Games will be allowed, based on the Categories configuration:
This is not correct because the application is being allowed due to the Application Overrides, not the category settings.
Thus, the correct explanation is that Addicting.Games will be allowed due to the Application Overrides configuration.

NEW QUESTION 61
Refer to the exhibit.



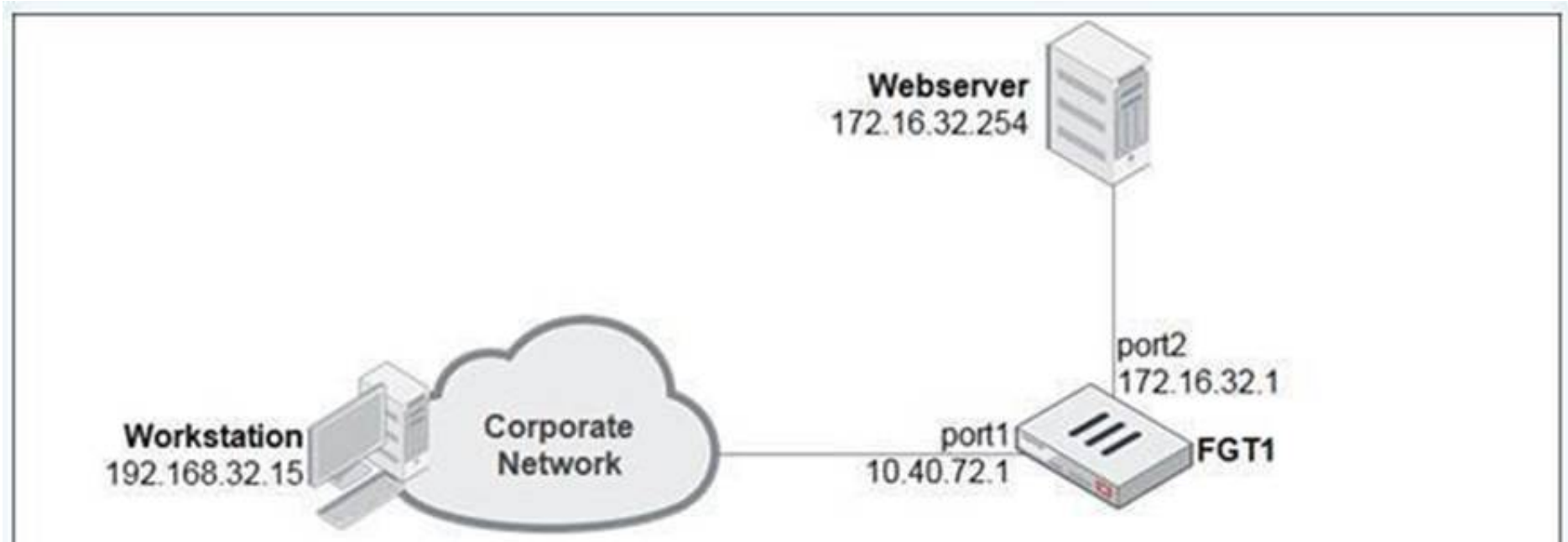
The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected 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 64
View the exhibit.
A user at 192.168.32.15 is trying to access the web server at 172.16.32.254.




```
FGT1 # get router info routing-table all
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
       * - candidate default

Routing table for VRF=0
S       0.0.0.0/0 [10/0] via 10.40.72.2, port1, [1/0]
C       172.16.32.0/24 is directly connected, port2
C       10.40.72.0/30 is directly connected, port1
```

Which two statements best describe how the FortiGate will perform reverse path forwarding (RPF) checks on this traffic? (Choose two.)

A. Strict RPF check will deny the traffic.
B. Loose RPF check will allow the traffic.
C. Strict RPF check will allow the traffic.
D. Loose RPF check will deny the traffic.

Answer: BC

Explanation:
When FortiGate performs reverse path forwarding (RPF) checks, it can operate in two modes: Strict RPF and Loose RPF. Here??s how these two checks work:
In strict RPF, FortiGate checks whether the best route back to the source IP of the packet (in this case, 192.168.32.15) goes through the same interface on which the packet was received. If the best return path uses a different interface, the packet is denied. Based on the scenario:
o C. Strict RPF check will allow the traffic:
If the return path for 192.168.32.15 matches the interface where the traffic was received, the strict RPF check will allow the traffic.
• Loose RPF Check:
In loose RPF, FortiGate only checks if there is any route back to the source IP of the packet, regardless of the interface. This is a more permissive check, and if a route exists, the packet will be allowed.
o B. Loose RPF check will allow the traffic:
Since loose RPF requires only that a valid route to the source exists, the traffic is allowed.
Why the other options are less appropriate:
• A. Strict RPF check will deny the traffic:
This would only happen if the return route didn??t match the incoming interface, which is not indicated here.
• D. Loose RPF check will deny the traffic:
Loose RPF is more permissive, so it will not deny the traffic as long as a valid route to the source IP exists.

NEW QUESTION 66
.....

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