Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FGT_AD-7.4/

NEW QUESTION 1
A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad. Which IPsec Wizard template must the administrator apply?

A. Remote Access
B. Site to Site
C. Dial up User
D. iHub-and-Spoke

Answer: A

Explanation:
For configuring an IPsec VPN tunnel for a sales employee traveling abroad, the "Remote Access" template is the most appropriate choice. This template is designed to allow remote users to securely connect to the internal network of an organization from any location using FortiClient or a compatible client. The other options, such as "Site to Site," "Dial up User," and "iHub-and-Spoke," are used for connecting different networks or sites, not individual remote users.
References:

FortiOS 7.4.1 Administration Guide: IPsec Wizard Template Types

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
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

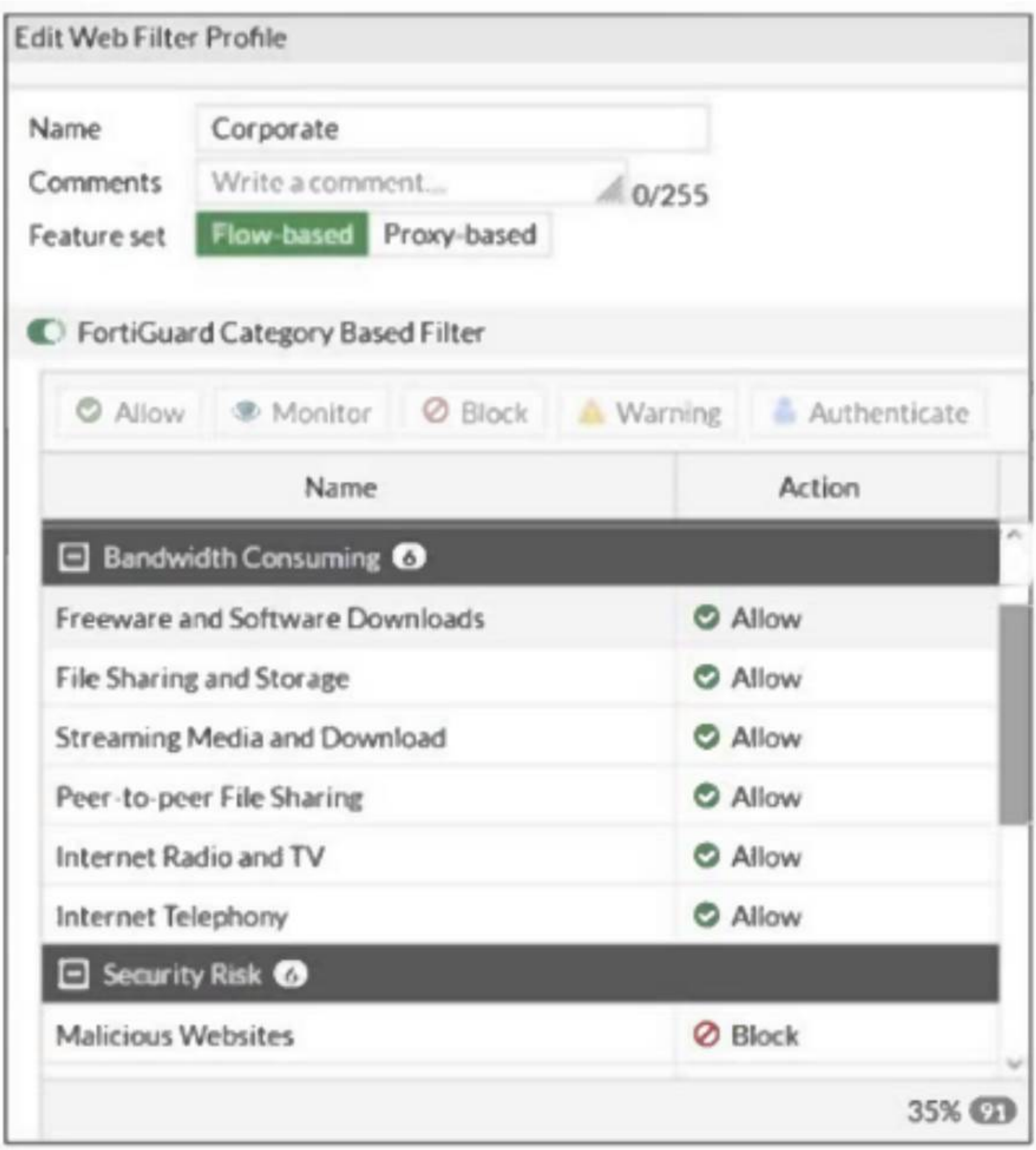
NEW QUESTION 5
An administrator manages a FortiGate model that supports NTurbo. How does NTurbo enhance performance for flow-based inspection?

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 6
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 7
Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

A. Checksums of devices are compared against each other to ensure configurations are the same.
B. Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.
C. Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster
D. Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

Answer: AB

Explanation:
In FortiGate HA (High Availability) configuration, checksums of device configurations are compared to ensure they are synchronized and identical across the cluster. Incremental synchronization can only happen from changes made on the primary device to ensure consistency and integrity across the cluster members. Changes made on non-primary devices do not initiate synchronization.
References:
FortiOS 7.4.1 Administration Guide: HA Configuration Synchronization

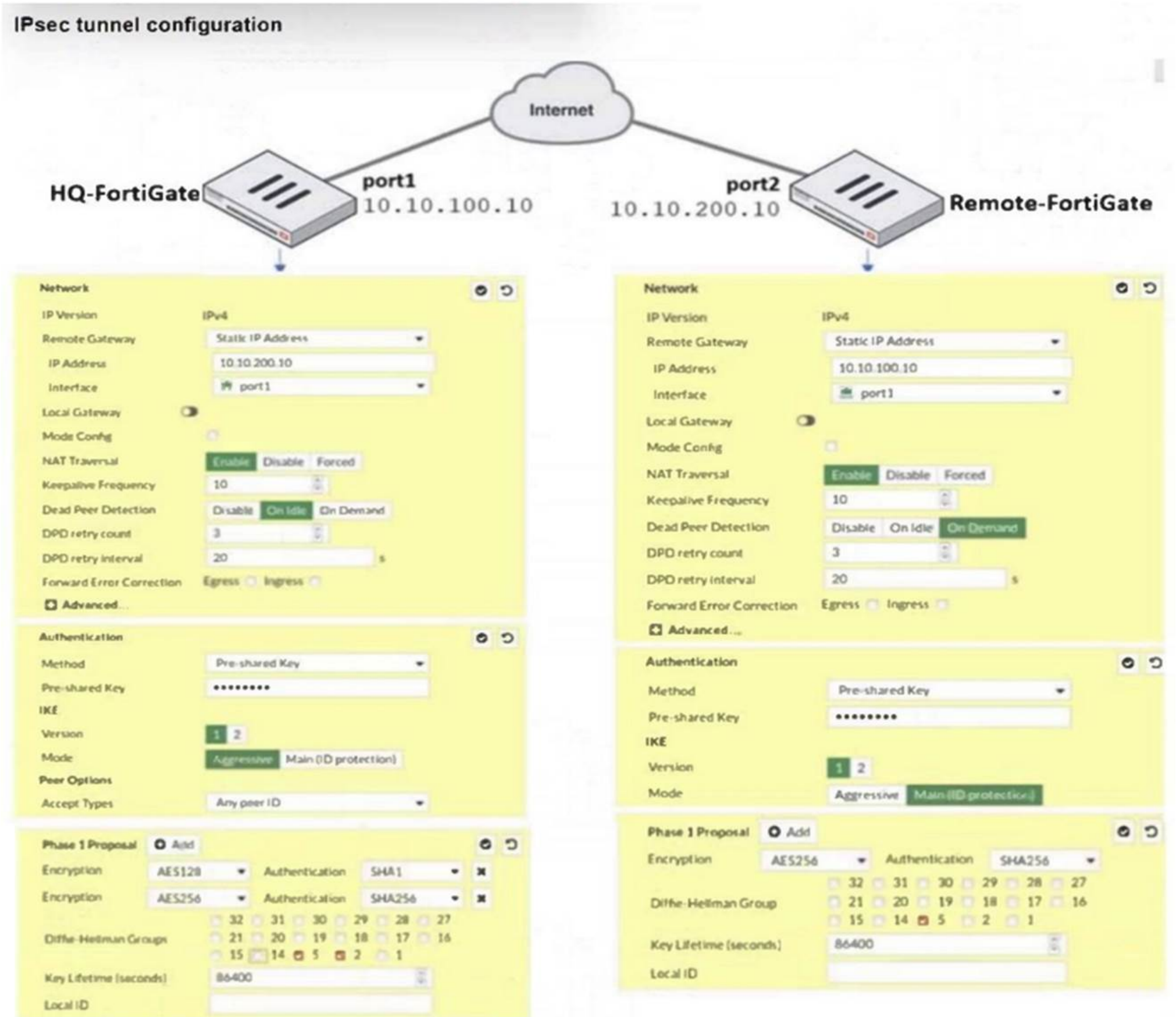
NEW QUESTION 8
Which statement is a characteristic of automation stitches?

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 9
Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 failed to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.
Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes can the administrator make to bring phase 1 up? (Choose two.)

A. On HQ-FortiGate, disable Diffie-Helman group 2.
B. On Remote-FortiGate, set port2 as Interface.
C. On both FortiGate devices, set Dead Peer Detection to On Demand.
D. On HQ-FortiGate, set IKE mode to Main (ID protection).

Answer: CD

Explanation:
To bring Phase 1 up, the following changes can be made:

A. On HQ-FortiGate, disable Diffie-Helman group 2: This is incorrect because Diffie-Hellman group 2 is already selected on both devices. Disabling it would not help.

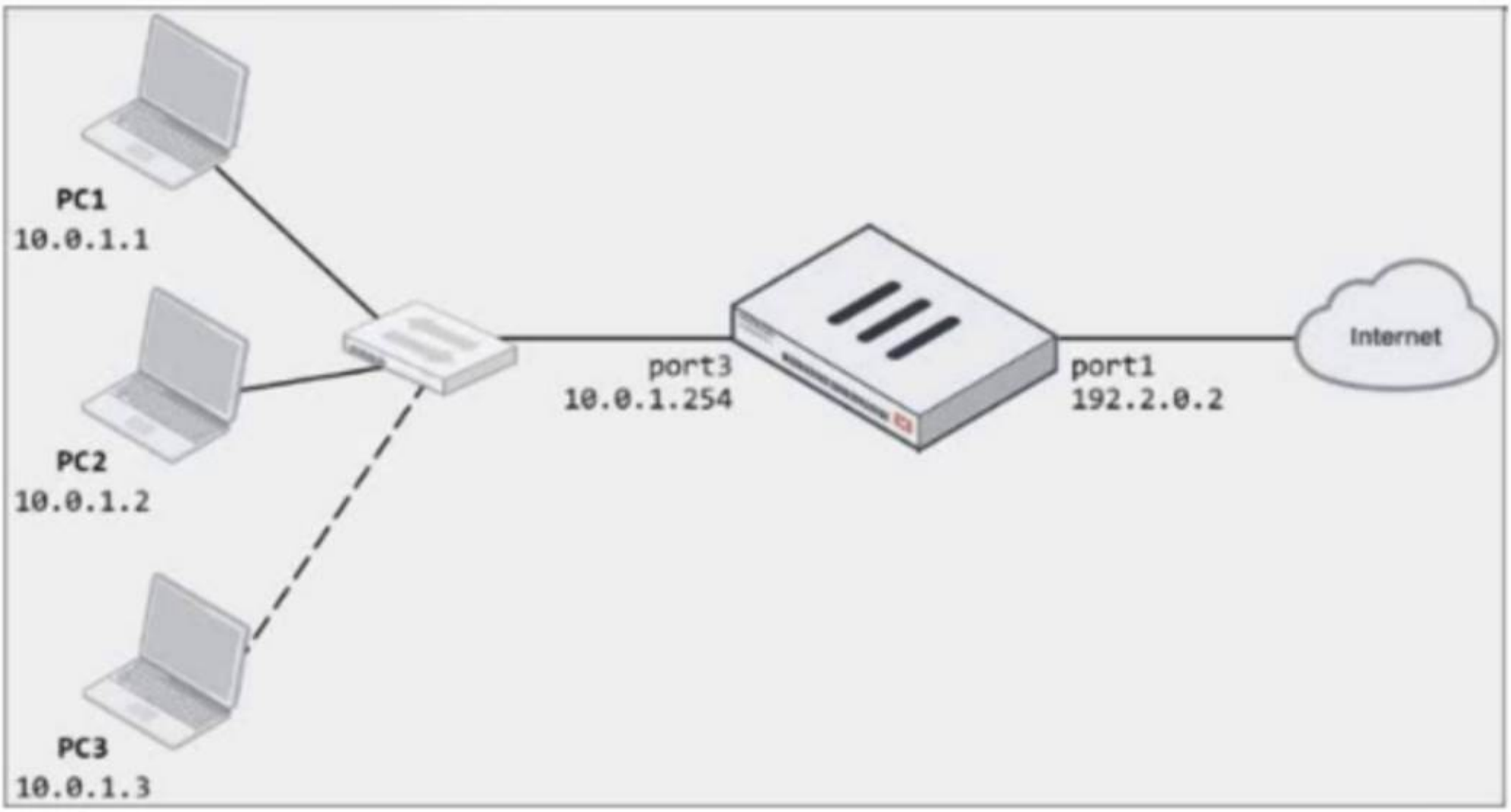
B. On Remote-FortiGate, set port2 as Interface: This is incorrect as both sides should be consistent in their interface settings for the IPsec tunnel, and the interface is correctly set to port1 on both FortiGates in the IPsec configuration.

C. On both FortiGate devices, set Dead Peer Detection to On Demand: This is a valid option.
Setting Dead Peer Detection (DPD) to "On Demand" helps maintain the IPsec connection by checking if the peer is still available, which can help in some cases where the connection fails due to timeouts.

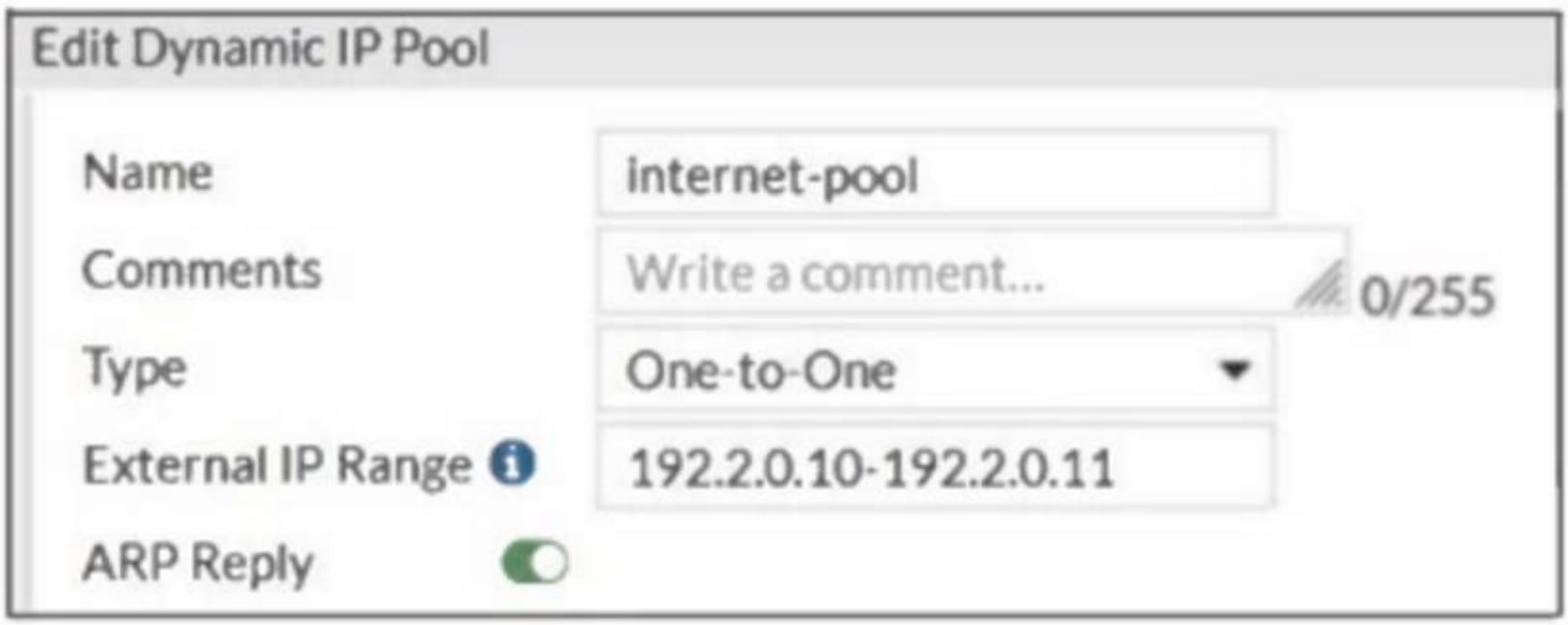
D. On HQ-FortiGate, set IKE mode to Main (ID protection): This is also a valid option because the Remote-FortiGate is already set to Main mode (ID protection). Ensuring that both ends use the same mode is crucial for successful phase 1 negotiation.
Thus, the correct answers are:C. On both FortiGate devices, set Dead Peer Detection to On Demand.D. On HQ-FortiGate, set IKE mode to Main (ID protection).

NEW QUESTION 10
Refer to the exhibits.

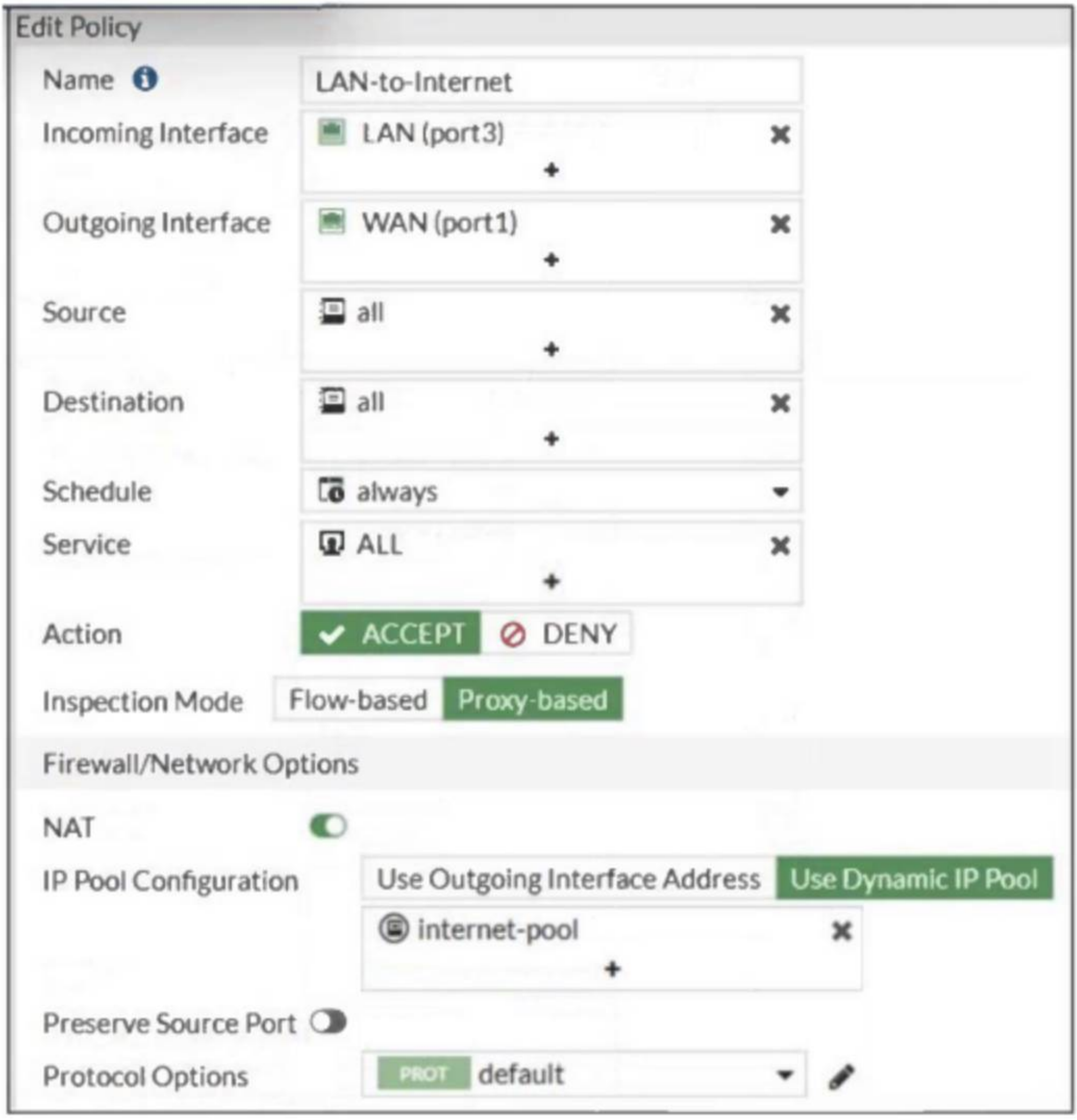
Network diagram



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 10
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	WEB Category_Monitor SSL 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 13
Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

A. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.
B. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
C. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP
D. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.

Answer: AD

Explanation:
When SD-WAN is enabled on FortiGate, the load balancing algorithm for Equal-Cost Multi-Path (ECMP) is configured using the load-balance-mode parameter under SD-WAN settings. However, if SD-WAN is disabled, the ECMP load balancing algorithm can be configured under config system settings. This flexibility allows FortiGate to control traffic routing behavior based on the network configuration and requirements.
References:

FortiOS 7.4.1 Administration Guide: ECMP Configuration

NEW QUESTION 16
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.

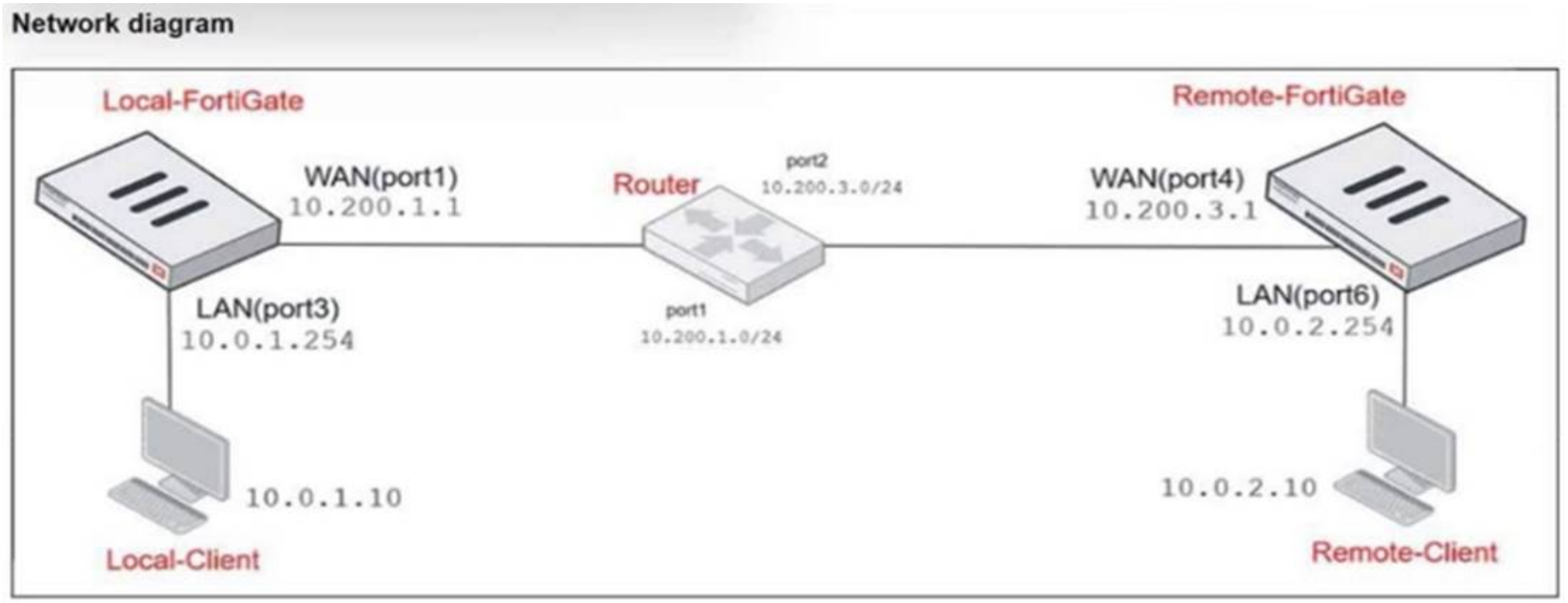
System uptime: The unit with the longest uptime is preferred.

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 18
Refer to the exhibits.



NAT IP pool configuration

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49 - 10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149 - 10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99 - 10.200.1.99	Overload	Enabled

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port3) → WAN (port1)								
2	TCP traffic	all	REMOTE_FORTIGATE	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
6	PING traffic	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
7	IGMP traffic	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.
The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IPaddress 10.0.1.254/24.
Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

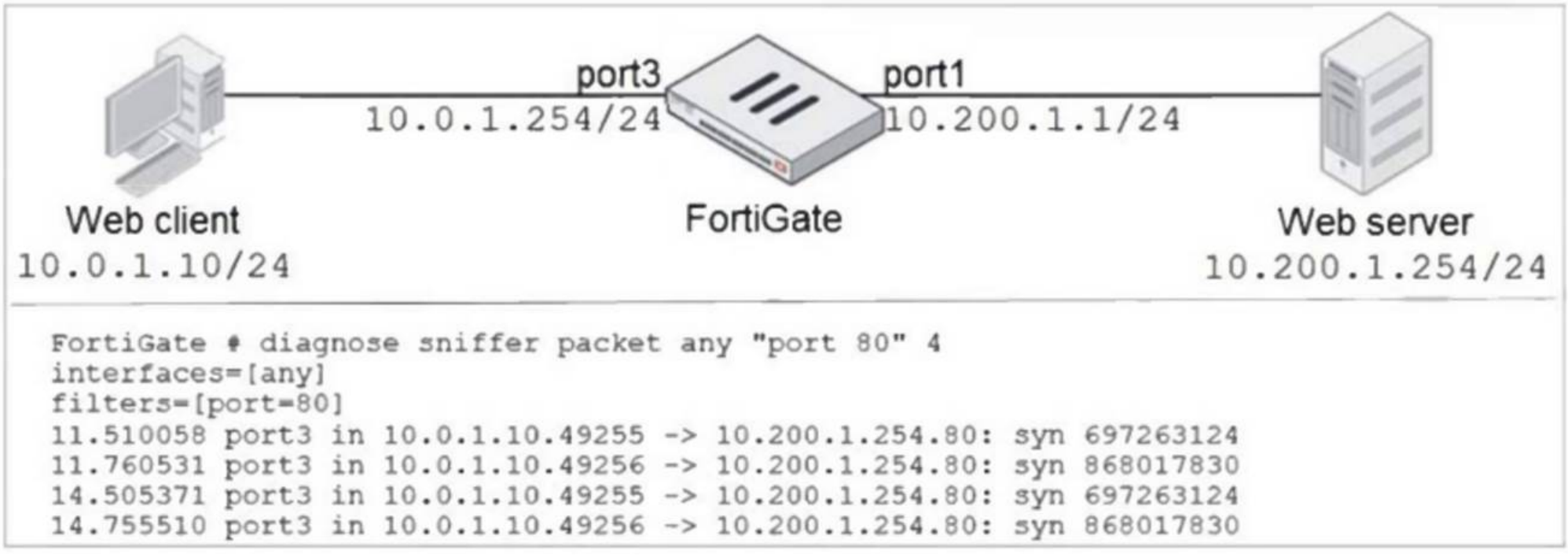
A. 10.200.1.1B.10.200.1.149C.10.200.1.99
B. 10.200.1.49

Answer: C

Explanation:
The traffic from the user on Local-Client (10.0.1.10) pinging the IP address of Remote-FortiGate (10.200.3.1) will match the firewall policy with the service "PING traffic". According to the firewall policy:

Policy ID 6 is set for PING traffic and uses the NAT IP pool "SNAT-Remote1", which is defined as 10.200.1.99.

NEW QUESTION 19
Refer to the exhibit.

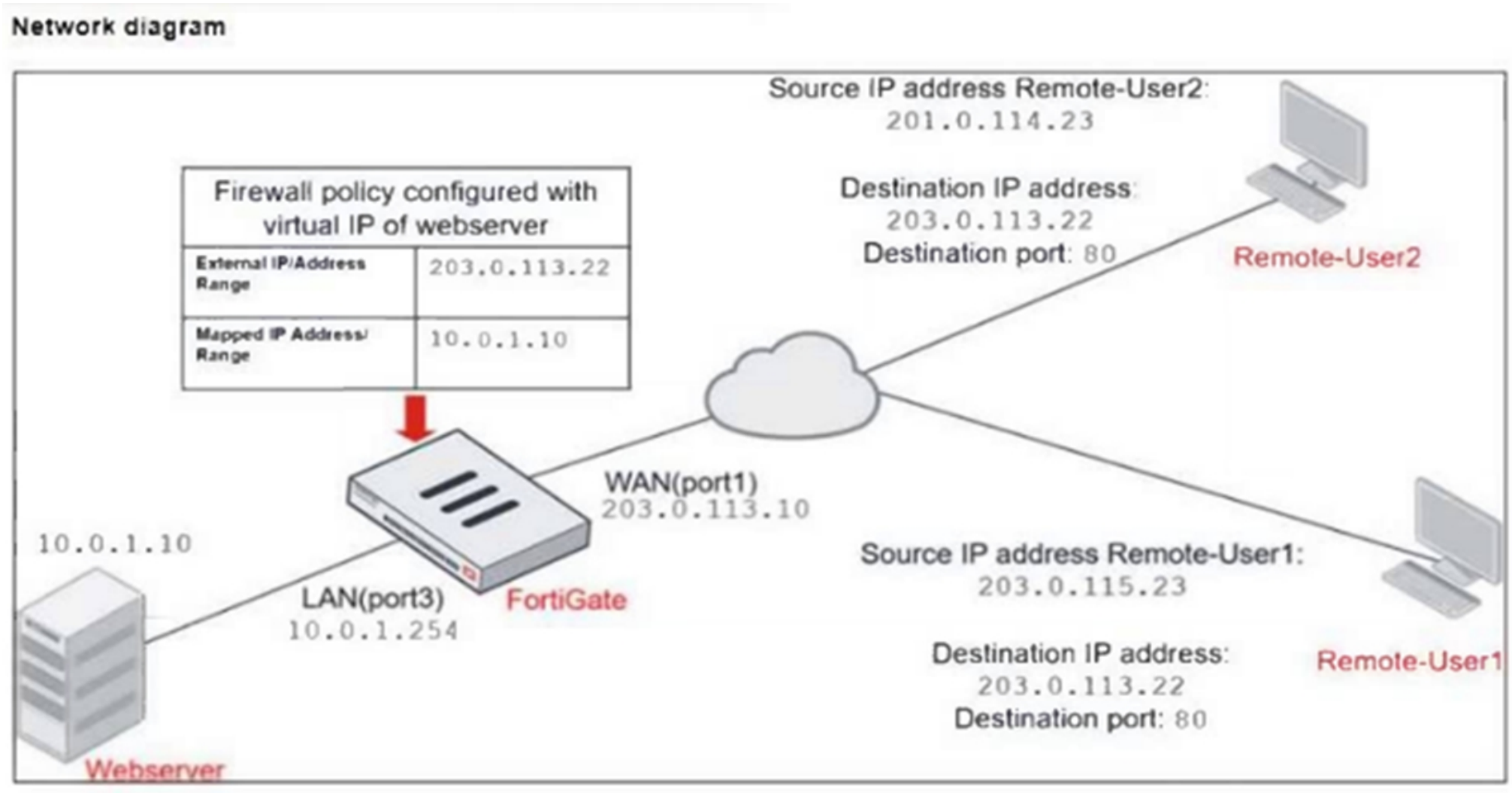


In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.
What should the administrator do next, to troubleshoot the problem?

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 22
Refer to the exhibits.



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 24
Refer to the exhibit.

```
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 172.20.121.2, port1, [1/0]
C       172.20.121.0/24 is directly connected, port1
C       172.20.168.0/24 is directly connected, port2
C       172.20.167.0/24 is directly connected, port3
S       10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
S       10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
S       10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
```

Which route will be selected when trying to reach 10.20.30.254?

A. 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]

Answer: A

Explanation:
The correct route selected when trying to reach 10.20.30.254 is 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0].
Prefix Length: The routing process prioritizes routes with the most specific (longest) prefix. In this case, 10.20.30.0/24 has a shorter prefix than 10.20.30.0/26 (option C), but it still matches the target address 10.20.30.254. The /24 subnet includes all addresses from 10.20.30.0 to 10.20.30.255, so 10.20.30.254 falls within this range.
• Administrative Distance and Metric: In the exhibit, all routes have the same administrative distance (AD) and metric, meaning they are considered equal in terms of preference. Hence, the prefix length becomes the primary factor for route selection.
Why the other options are less appropriate:

B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
• This route is for a different subnet, 10.30.20.0/24, which does not include the target address 10.20.30.254. Therefore, it is not a valid match.

C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
• Although this has a more specific prefix (/26), which means it should cover a smaller range of addresses, the /26 subnet only includes addresses from 10.20.30.0 to 10.20.30.63. The target address 10.20.30.254 does not fall within this range, so this route will not be selected.

D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]
• This is a default route (0.0.0.0/0) used for any address that doesn??t match a more specific route. Since 10.20.30.254 matches the 10.20.30.0/24 route (option A), the default route will not be selected.

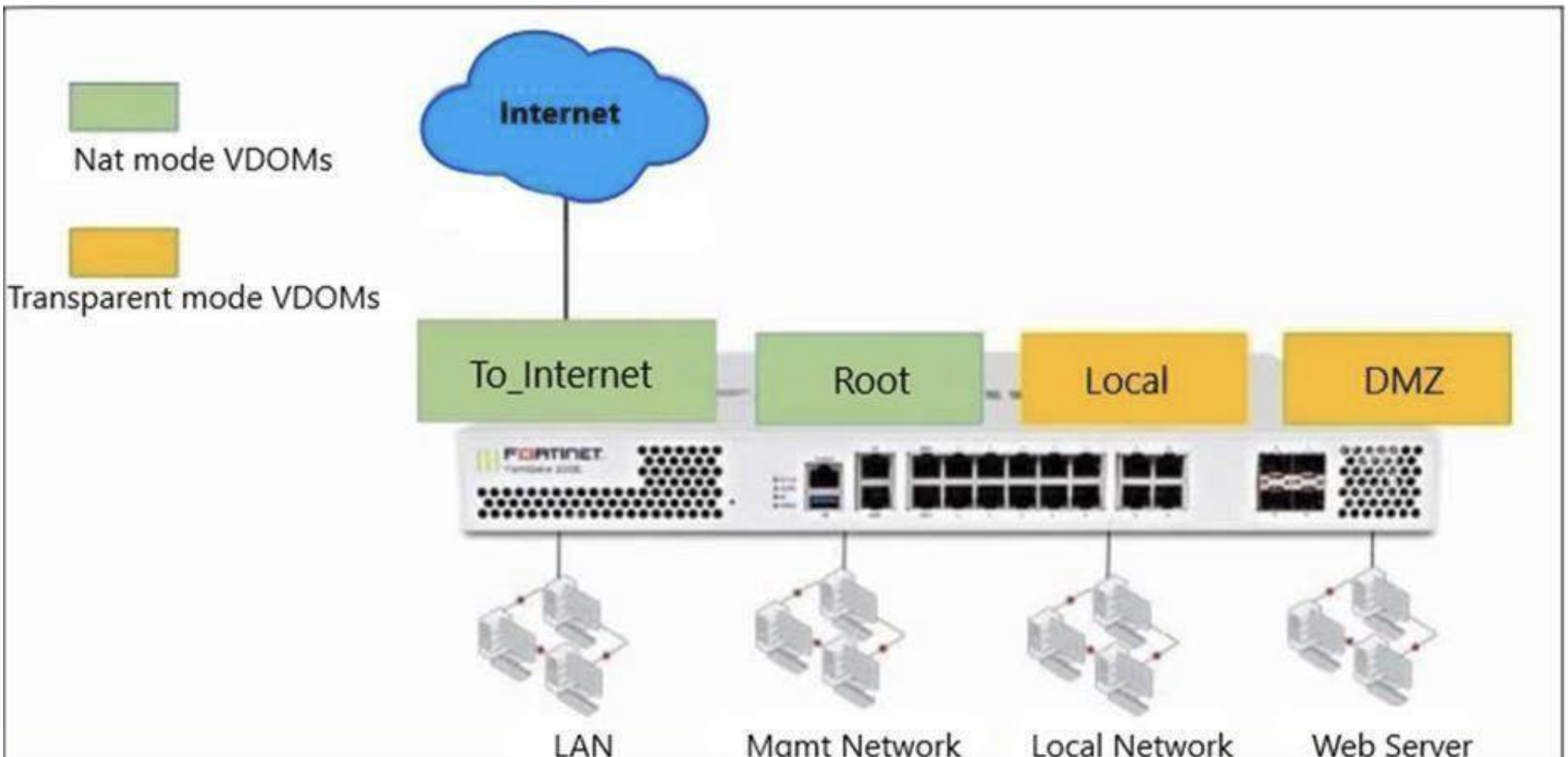
NEW QUESTION 28
Which two IP pool types are useful for carrier-grade NAT deployments? (Choose two.)

A. Port block allocation
B. Fixed port range
C. One-to-one
D. Overload

Answer: AB

Explanation:
In carrier-grade NAT (CGNAT) deployments, specific IP pool types are used to manage large-scale NAT translations efficiently. The correct IP pool types for CGNAT are:
• A. Port block allocation: This type of IP pool allocates a block of ports from a single public IP to multiple clients. It allows efficient use of a limited number of public IPs by distributing port ranges among users, which is crucial for carrier-grade NAT environments where a large number of users need access to the internet.
• B. Fixed port range: In this type, each client is assigned a fixed range of ports, ensuring that the same public IP and port range are used consistently. This helps in reducing the complexity and overhead of managing dynamic port assignments, which is particularly useful in large-scale CGNAT setups.
Why the other options are less appropriate:
• C. One-to-one: One-to-one NAT is used for mapping a single private IP address to a single public IP address. This is not efficient for carrier-grade NAT because CGNAT is designed to allow multiple clients to share a smaller number of public IPs.
• D. Overload: Overload, also known as PAT (Port Address Translation), maps multiple private IPs to a single public IP by differentiating connections based on port numbers. While commonly used in regular NAT setups, CGNAT benefits more from port block allocation and fixed port range due to th

NEW QUESTION 30
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 31
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 34
Which three criteria can FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Services defined in the firewall policy
B. Highest to lowest priority defined in the firewall policy
C. Destination defined as Internet Services in the firewall policy
D. Lowest to highest policy ID number
E. Source defined as Internet Services in the firewall policy

Answer: ACE

Explanation:
• A. Services defined in the firewall policy: FortiGate uses the service specified in the firewall policy to match traffic. Services define the types of traffic (like HTTP, FTP) that the policy will apply to.
• C. Destination defined as Internet Services in the firewall policy: Policies can be matched based on the destination being categorized as Internet Services, allowing specific handling of such traffic.
• E. Source defined as Internet Services in the firewall policy: Similarly, traffic from sources categorized as Internet Services can be matched and processed according to the policy configuration.
Why the other options are less relevant:
• B. Highest to lowest priority defined in the firewall policy: Policies are processed from top to bottom, not by priority. The highest priority policy is processed first, but this is about the order of policy processing rather than criteria for matching traffic.
• D. Lowest to highest policy ID number: Policies are processed from the top of the list (the lowest policy ID) to the bottom (the highest policy ID), which is about the processing order rather than matching criteria.

NEW QUESTION 35
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FGT_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FGT_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FGT_AD-7.4/

Money Back Guarantee

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