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
Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

A. The intrusion prevention security profile must be enabled when using flow-based inspection mode.
B. The option to send files to FortiSandbox for inspection is enabled.
C. The firewall policy performs a full content inspection on the file.

D. Flow-based inspection is used, which resets the last packet to the user.

Answer: D

Explanation:
In flow-based inspection mode, FortiGate sends a reset (RST) packet to the client instead of providing a replacement message, which causes the block message not to be displayed.

NEW QUESTION 3
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 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
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 6
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 7
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.

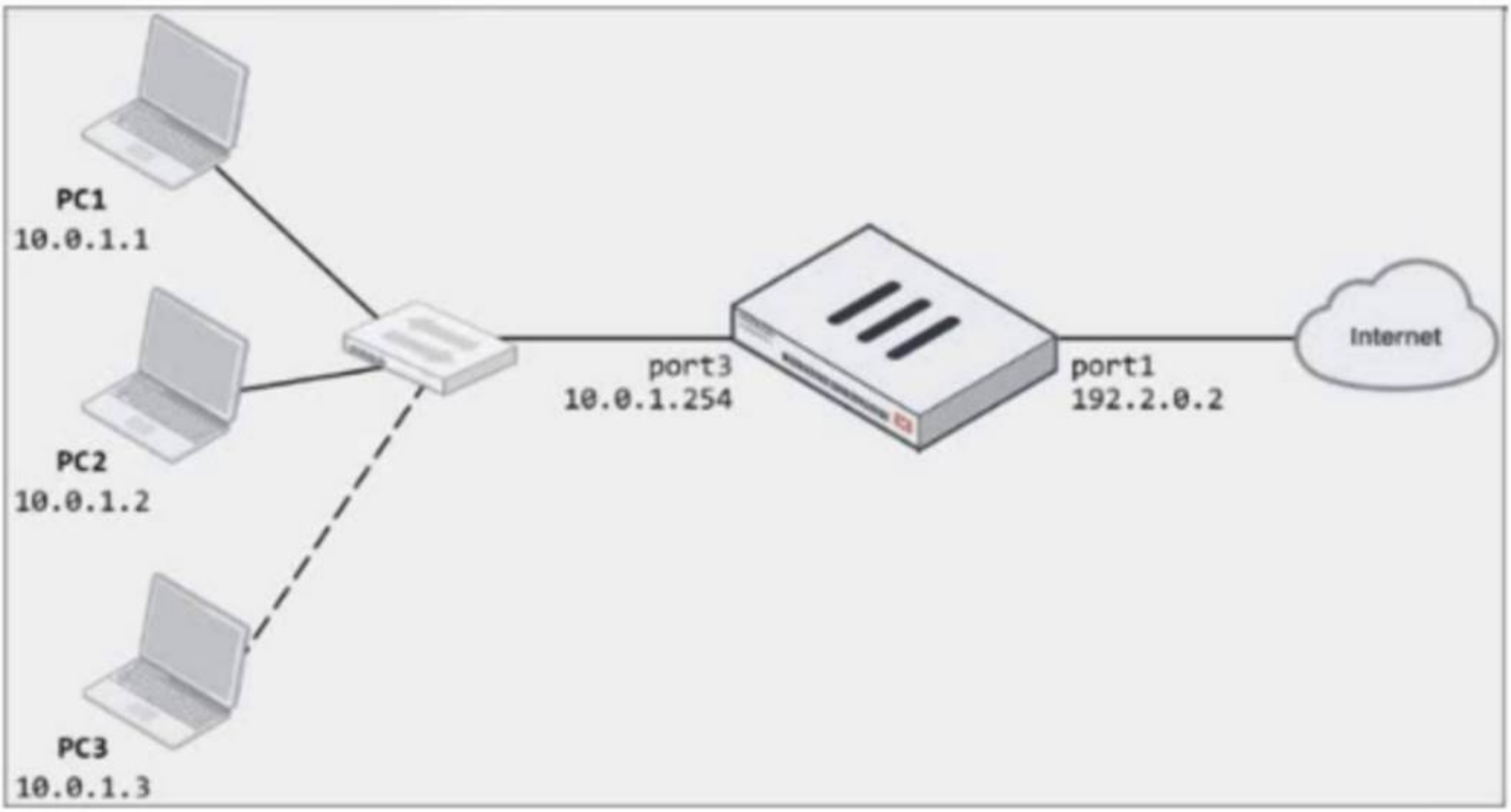
Answer: C

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:

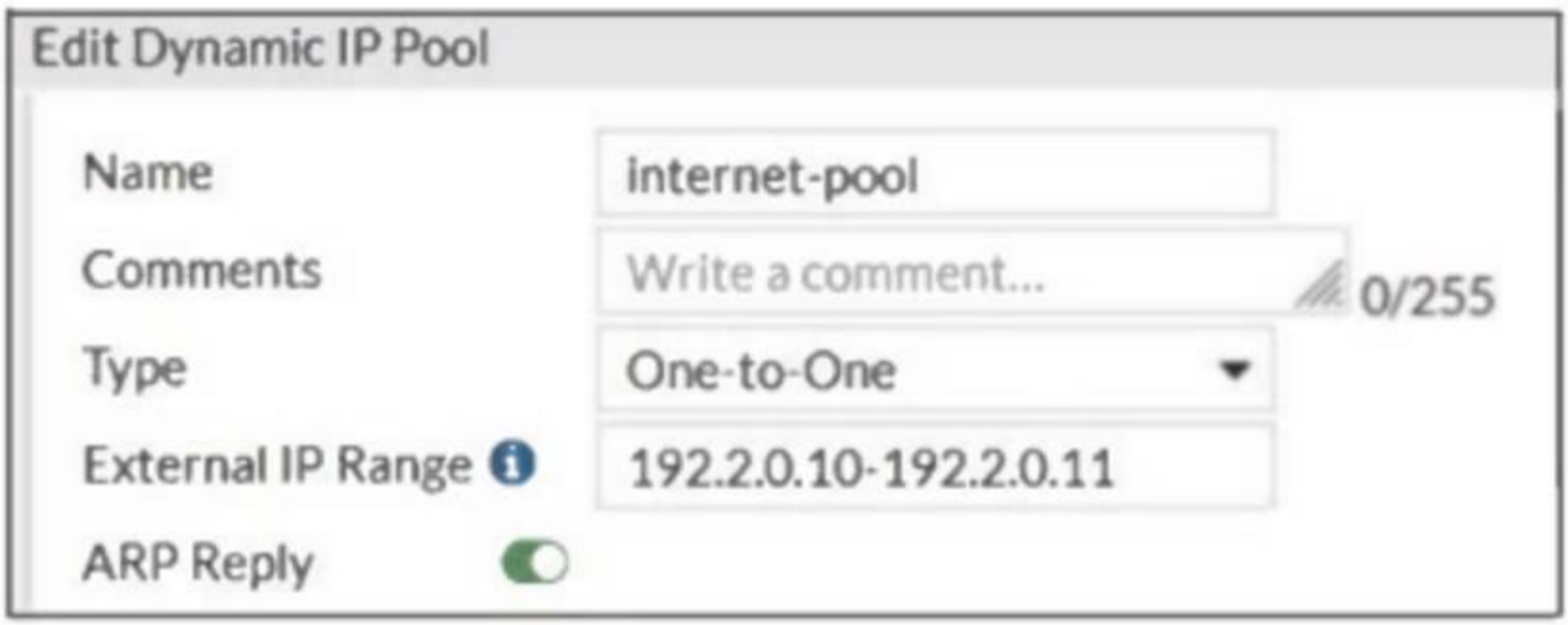
- FortiOS 7.4.1 Administration Guide: Automation Stitches

NEW QUESTION 8
Refer to the exhibits.

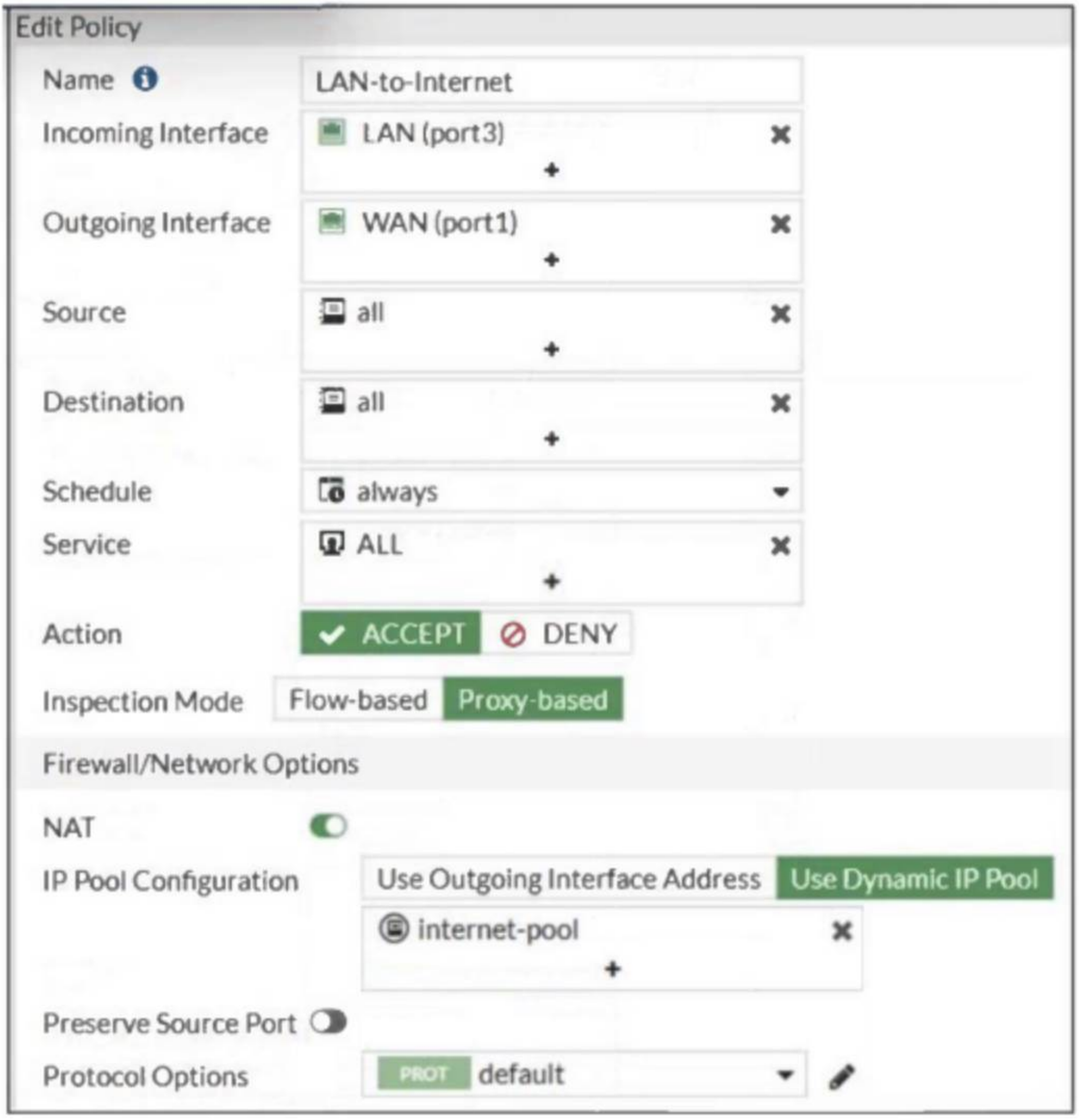
Network diagram



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 9
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 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 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 14
An administrator must enable a DHCP server on one of the directly connected networks on FortiGate. However, the administrator is unable to complete the process on the GUI to enable the service on the interface.
In this scenario, what prevents the administrator from enabling DHCP service?

A. The role of the interface prevents setting a DHCP server.

B. The DHCP server setting is available only on the CLI.
C. Another interface is configured as the only DHCP server on FortiGate.
D. The FortiGate model does not support the DHCP server.

Answer: A

Explanation:
FortiGate interfaces can be configured in different roles, such as WAN or LAN. If an interface is set as a "WAN" role, you cannot configure it to act as a DHCP server through the GUI. The interface role must be set to "LAN" or "Undefined" to allow DHCP server configuration.
References:

- FortiOS 7.4.1 Administration Guide: DHCP Server Configuration

NEW QUESTION 19
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:

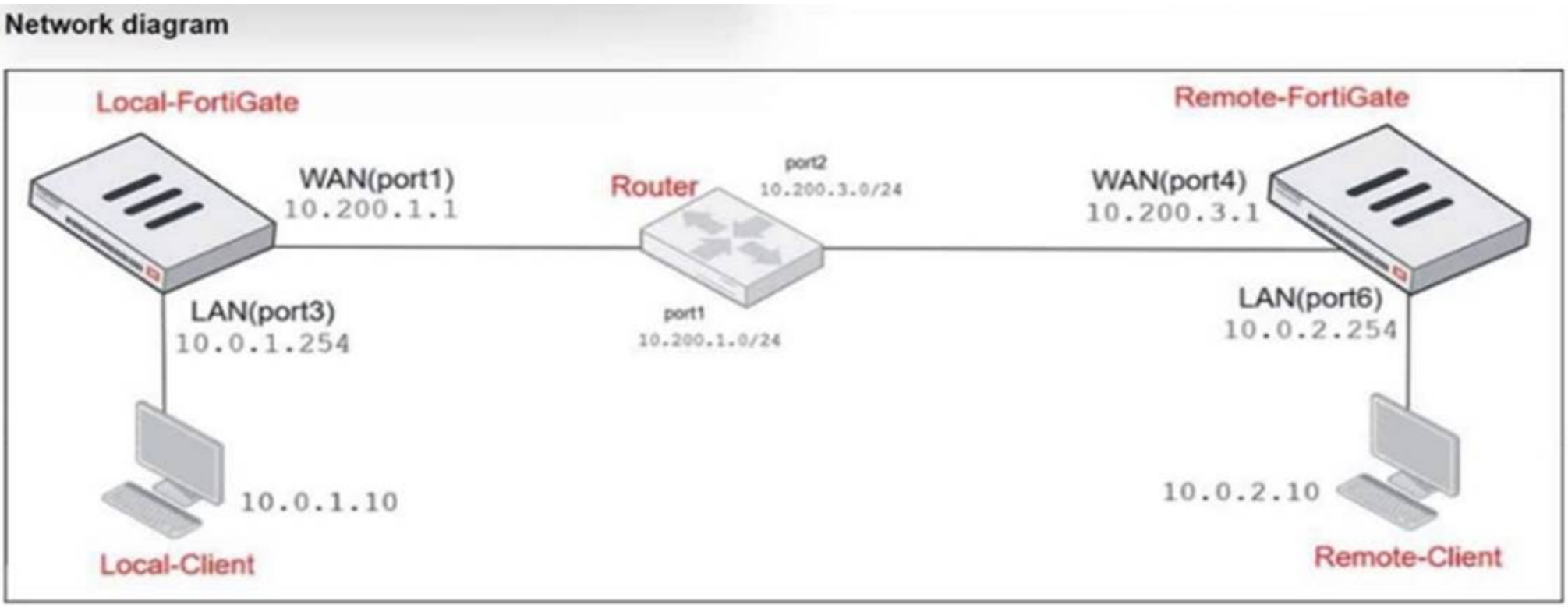
- Connected monitored ports: The unit with the most monitored ports up is preferred.
- Priority: The unit with the highest priority is preferred.
- System uptime: The unit with the longest uptime is preferred.
- FortiGate serial number: Used as the final criterion to break any remaining ties.

References:

- FortiOS 7.4.1 Administration Guide: HA election process

NEW QUESTION 24
Refer to the exhibits.

Network diagram



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 29
Refer to the exhibit.

Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

Which statement about this firewall policy list is true?

A. The Implicit group can include more than one deny firewall policy.
B. The firewall policies are listed by ID sequence view.
C. The firewall policies are listed by ingress and egress interfaces pairing view.
D. LAN to WA
E. WAN to LA
F. and Implicit are sequence grouping view lists.

Answer: C

Explanation:
The firewall policy list in the exhibit is arranged in the "Interface Pair View," where policies are grouped by their incoming (ingress) and outgoing (egress) interface pairs. Each section (LAN to WAN, WAN to LAN, etc.) groups policies based on these interface pairings. This view helps administrators quickly identify which policies apply to specific traffic flows between network interfaces. Options A and D are incorrect because the Implicit group typically does not include more than one deny policy, and there is no "sequence grouping view" in FortiGate. Option B is incorrect as the list is not displayed strictly by ID sequence.
References:
FortiOS 7.4.1 Administration Guide: Firewall Policy Views

NEW QUESTION 31
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?

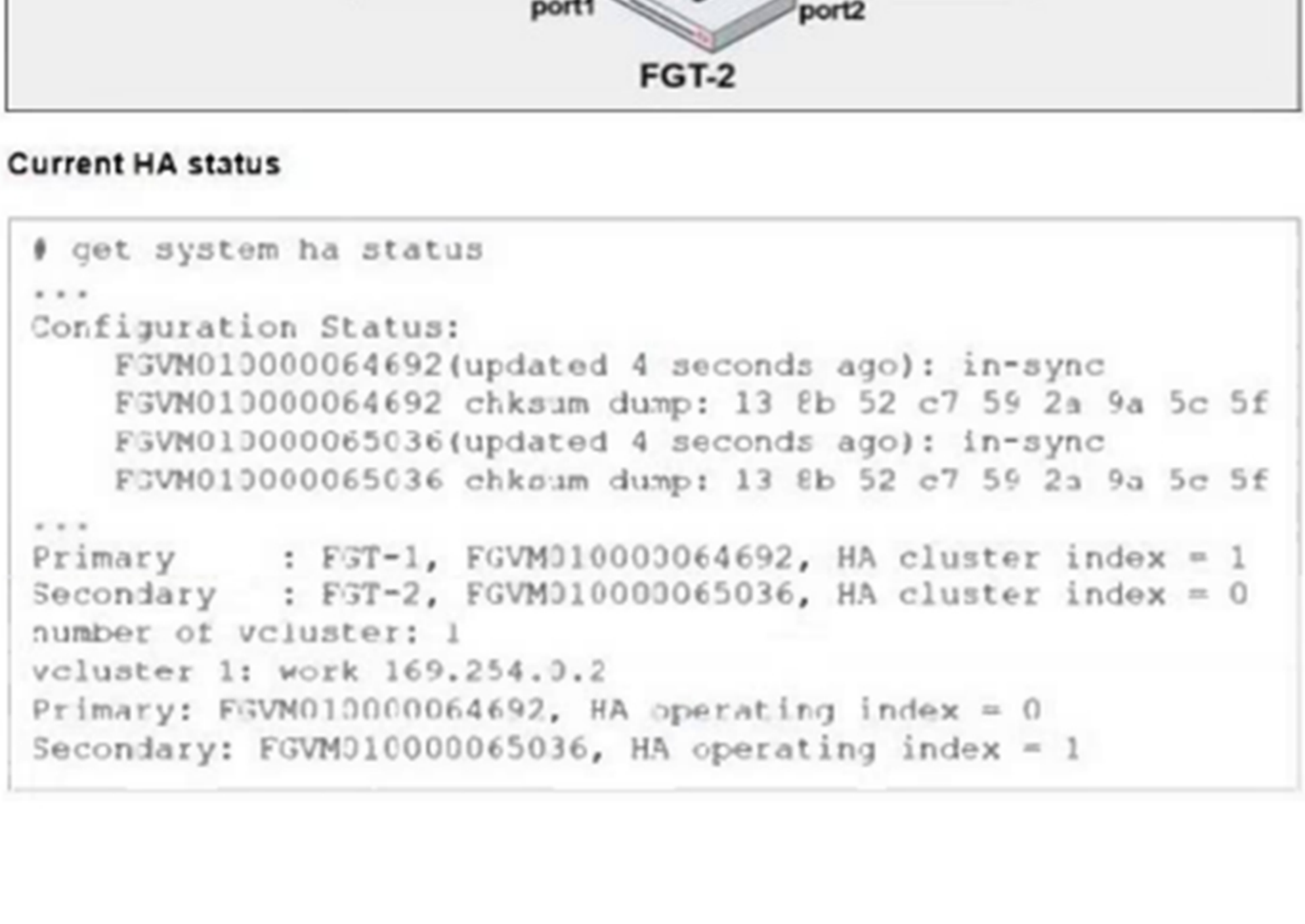
A. SSL VPN idle-timeout
B. SSL VPN login-timeout
C. SSL VPN dtls-hello-timeout
D. SSL VPN session-ttl

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 34
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
```

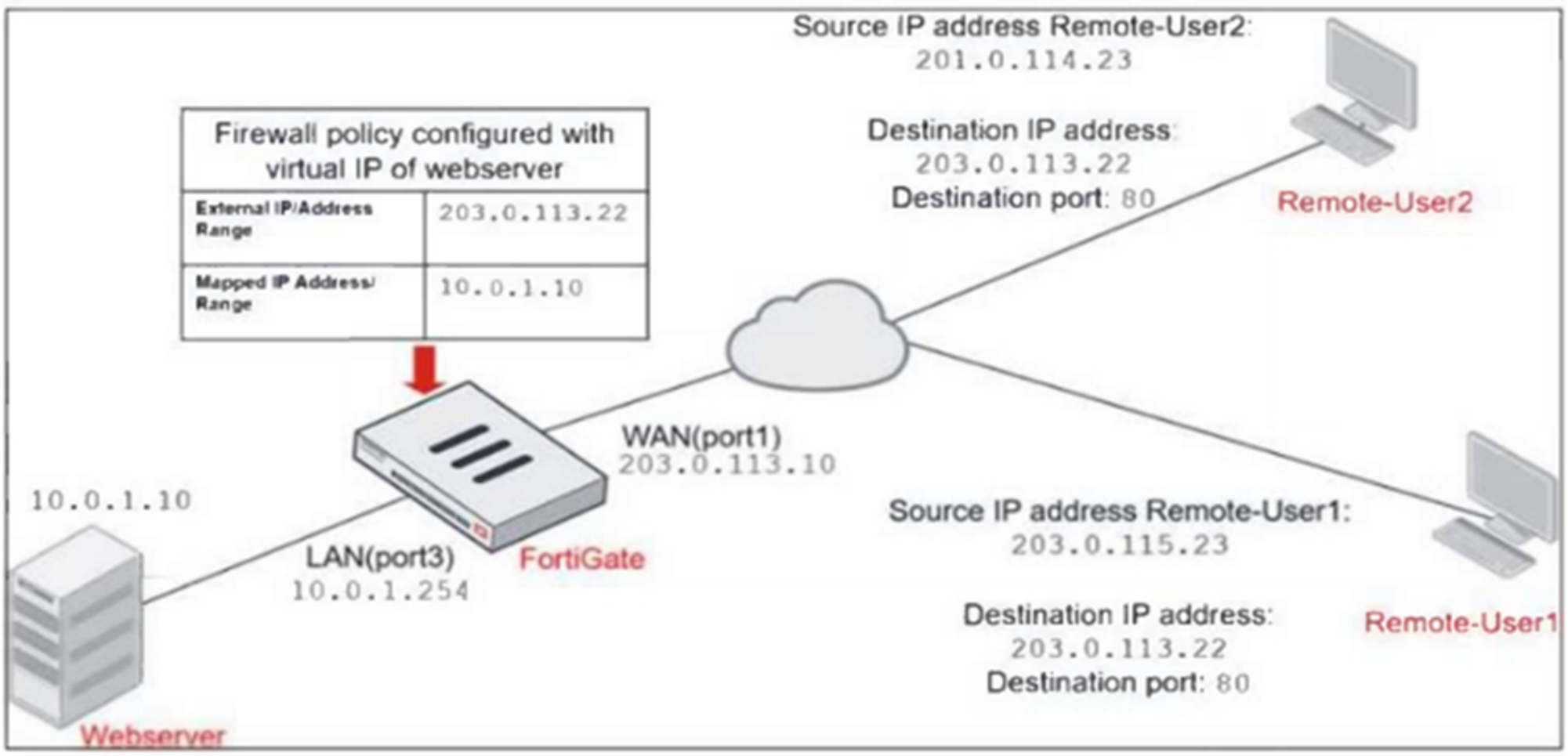
FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.
What would be the expected outcome in the HA cluster?

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 37
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 42
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 45
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 48
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 53
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 56
.....

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