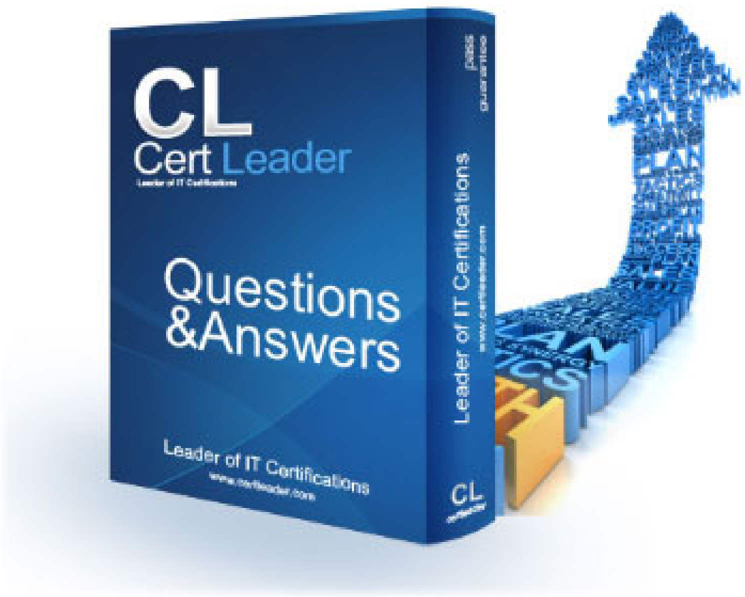
FCP_FGT_AD-7.4 Dumps

FCP - FortiGate 7.4 Administrator

https://www.certleader.com/FCP_FGT_AD-7.4-dumps.html



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?

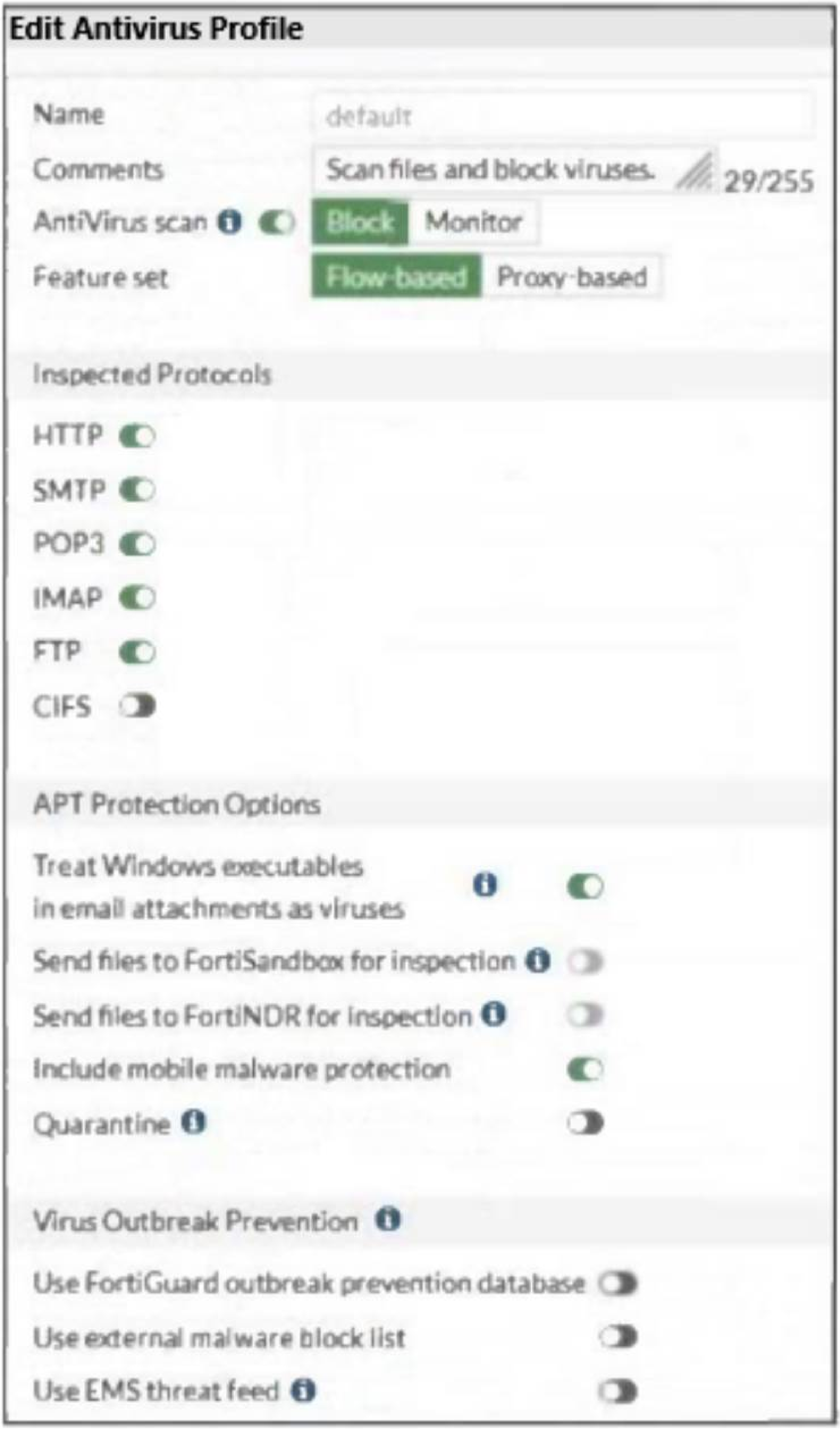
A. Remote Access
B. Site to Site
C. Dial up User
D. iHub-and-Spoke

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



Edit Antivirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: enabled — Block | Monitor (Block selected)

Feature set: Flow-based | Proxy-based (Flow-based selected)

Inspected Protocols

- HTTP: enabled
- SMTP: enabled
- POP3: enabled
- IMAP: enabled
- FTP: enabled
- CIFS: disabled

APT Protection Options

- Treat Windows executables in email attachments as viruses: enabled
- Send files to FortiSandbox for inspection: disabled
- Send files to FortiNDR for inspection: disabled
- Include mobile malware protection: enabled
- Quarantine: disabled

Virus Outbreak Prevention

- Use FortiGuard outbreak prevention database: disabled
- Use external malware block list: disabled
- Use EMS threat feed: disabled

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 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 5
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 6
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 7

A network administrator has configured an SSL/SSH inspection profile defined for full SSL inspection and set with a private CA certificate. The firewall policy that allows the traffic uses this profile for SSL inspection
and performs web filtering. When visiting any HTTPS websites, the browser reports certificate warning errors.
What is the reason for the certificate warning errors?

A. The SSL cipher compliance option is not enabled on the SSL inspection profil
B. This setting is required when the SSL inspection profile is defined with a private CA certificate.
C. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
D. The browser does not recognize the certificate in use as signed by a trusted CA.
E. With full SSL inspection it is not possible to avoid certificate warning errors at the browser level.

Answer: C

Explanation:
The certificate warning errors occur because the SSL inspection profile is configured to use a private CA certificate that is not recognized by the browser as being signed by a trusted CA. For the browser to trust the FortiGate's re-signed certificates, the CA certificate used by FortiGate for SSL inspection must be installed in the browser's trusted certificate store. Until the browser recognizes the certificate authority (CA) as trusted, it will continue to display warning errors when accessing HTTPS websites.
References:

- FortiOS 7.4.1 Administration Guide: SSL/SSH Inspection Configuration

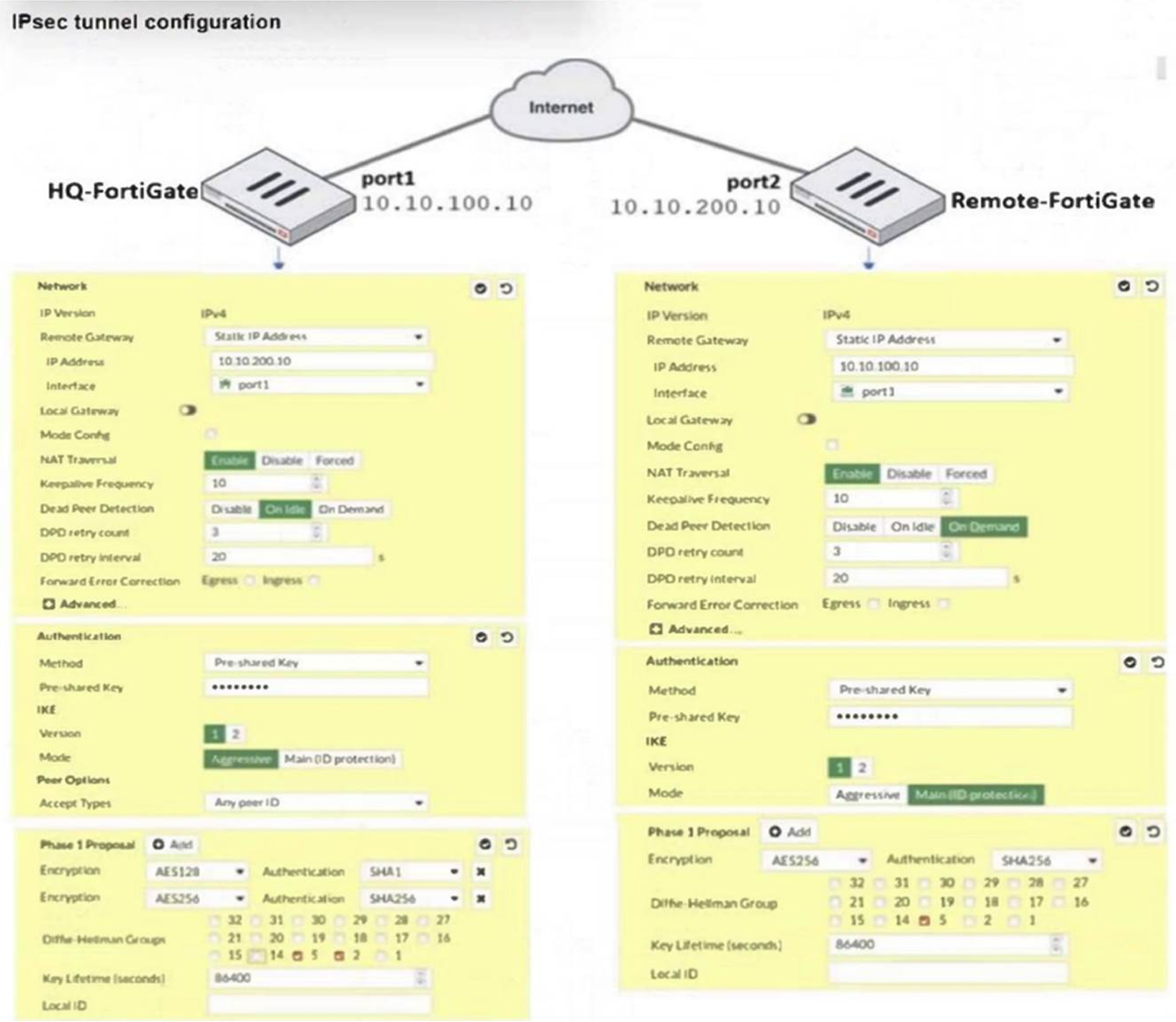
NEW QUESTION 8
An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

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 9
Refer to the exhibit.



HQ-FortiGate

Network	
IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	10.10.200.10
Interface	port1
Local Gateway	
Mode Config	□
NAT Traversal	[✓ Enable] Disable Forced
Keepalive Frequency	10
Dead Peer Detection	Disable [✓ On Idle] On Demand
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress □ Ingress □
Advanced...	
Authentication	
Method	Pre-shared Key
Pre-shared Key	••••••••
IKE	
Version	[✓ 1] 2
Mode	[✓ Aggressive] Main (ID protection)
Peer Options	
Accept Types	Any peer ID
Phase 1 Proposal	Add
Encryption	AES128 Authentication SHA1
Encryption	AES256 Authentication SHA256
Diffie-Hellman Groups	□ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 ☑ 2 □ 1
Key Lifetime (seconds)	86400
Local ID	

Remote-FortiGate

Network	
IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	10.10.100.10
Interface	port1
Local Gateway	
Mode Config	□
NAT Traversal	[✓ Enable] Disable Forced
Keepalive Frequency	10
Dead Peer Detection	Disable On Idle [✓ On Demand]
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress □ Ingress □
Advanced...	
Authentication	
Method	Pre-shared Key
Pre-shared Key	••••••••
IKE	
Version	[✓ 1] 2
Mode	Aggressive [✓ Main (ID protection)]
Phase 1 Proposal	Add
Encryption	AES256 Authentication SHA256
Diffie-Hellman Group	□ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 □ 2 □ 1
Key Lifetime (seconds)	86400
Local ID	

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.

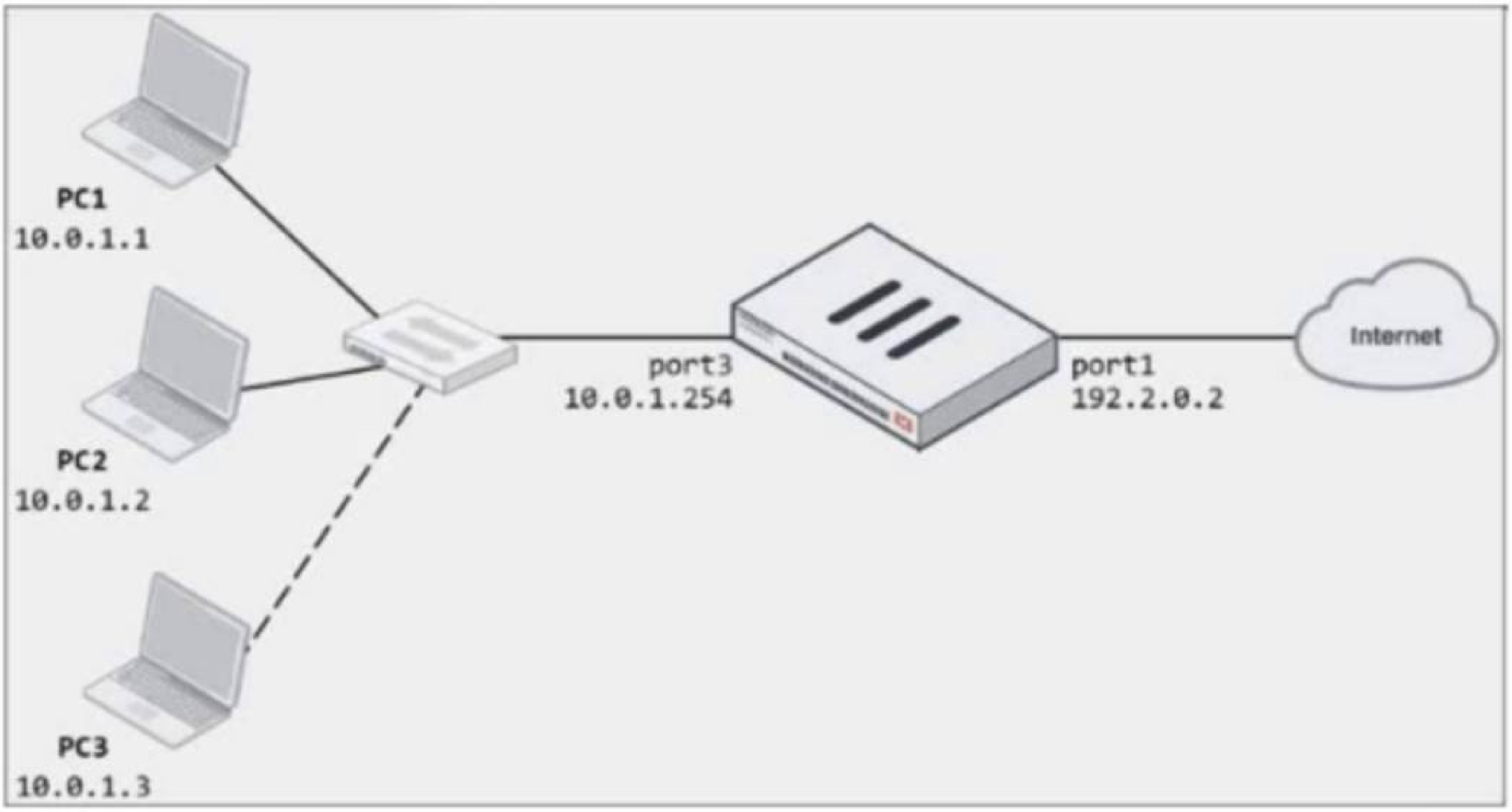
- B. On Remote-FortiGate, set port2 as Interface: This is incorrect as both sides should be consistent in their interface settings for the IPsec tunnel, and the interface is correctly set to port1 on both FortiGates in the IPsec configuration.

- 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.

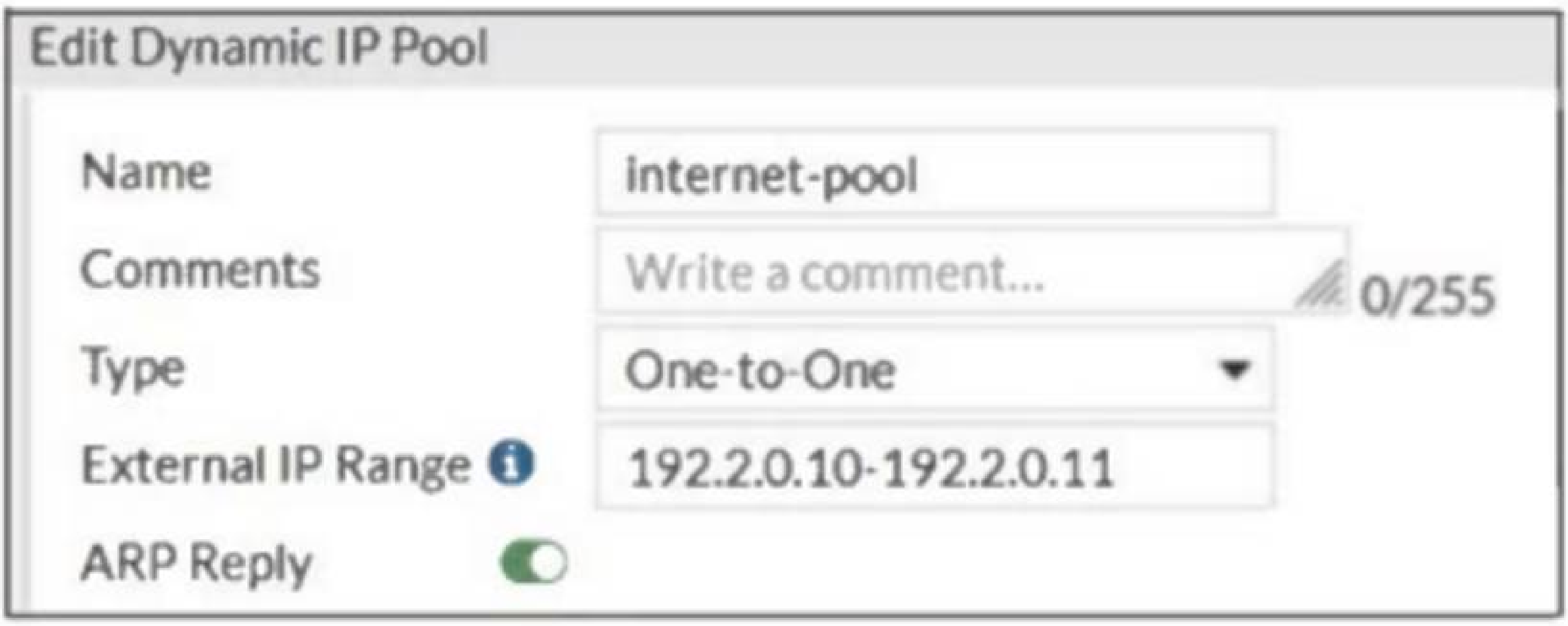
- D. On HQ-FortiGate, set IKE mode to Main (ID protection): This is also a valid option because the Remote-FortiGate is already set to Main mode (ID protection). Ensuring that both ends use the same mode is crucial for successful phase 1 negotiation.
Thus, the correct answers are:C. On both FortiGate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



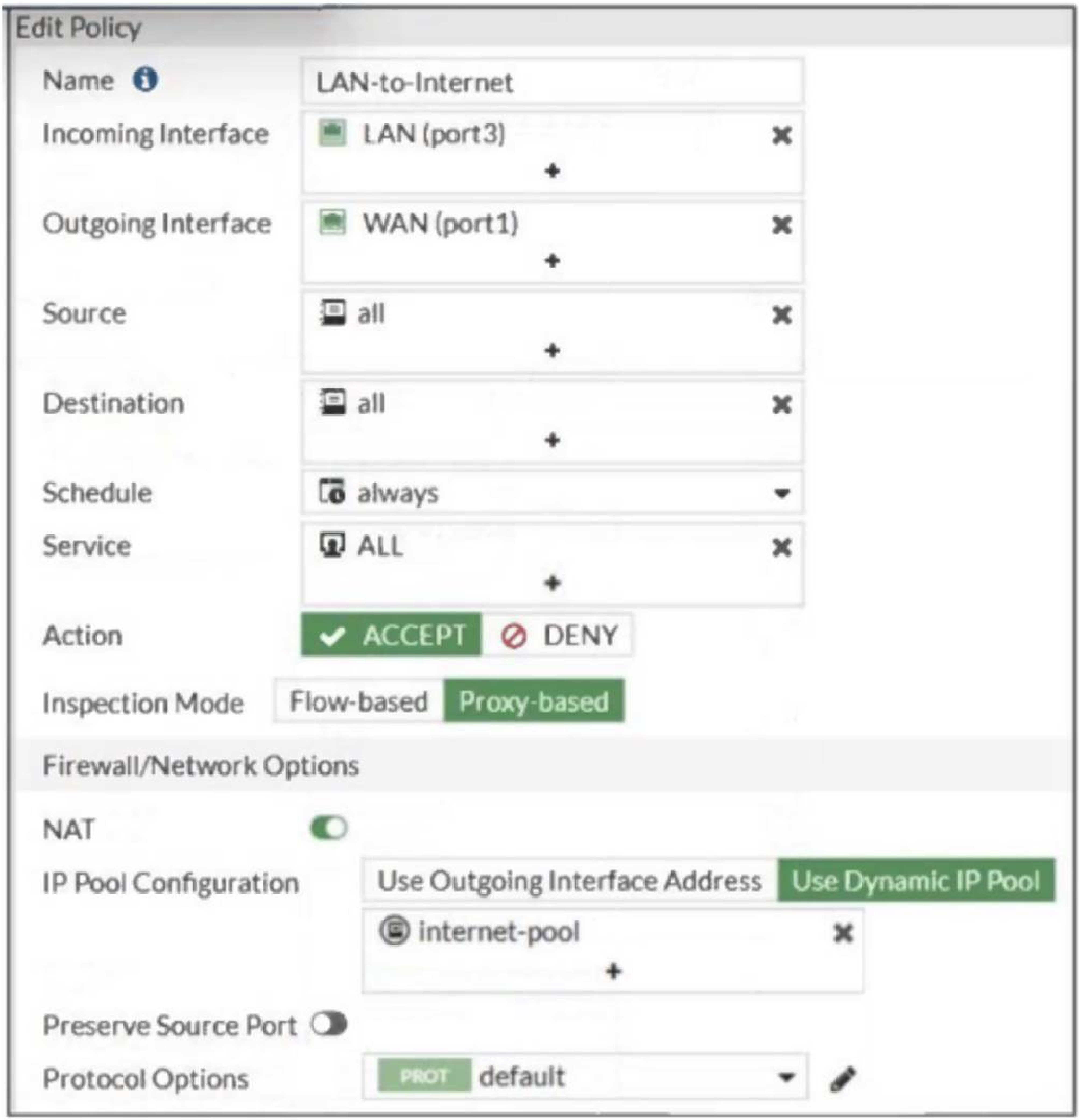
Dynamic IP pool



Edit Dynamic IP Pool

Name	internet-pool
Comments	Write a comment... 0/255
Type	One-to-One
External IP Range	192.2.0.10-192.2.0.11
ARP Reply	●

Firewall policy



Edit Policy

Name	LAN-to-Internet
Incoming Interface	LAN (port3)
Outgoing Interface	WAN (port1)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY
Inspection Mode	Flow-based [✓ Proxy-based]

Firewall/Network Options

NAT	●
IP Pool Configuration	Use Outgoing Interface Address [✓ Use Dynamic IP Pool] internet-pool
Preserve Source Port	○
Protocol Options	PROT default

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

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 15

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.

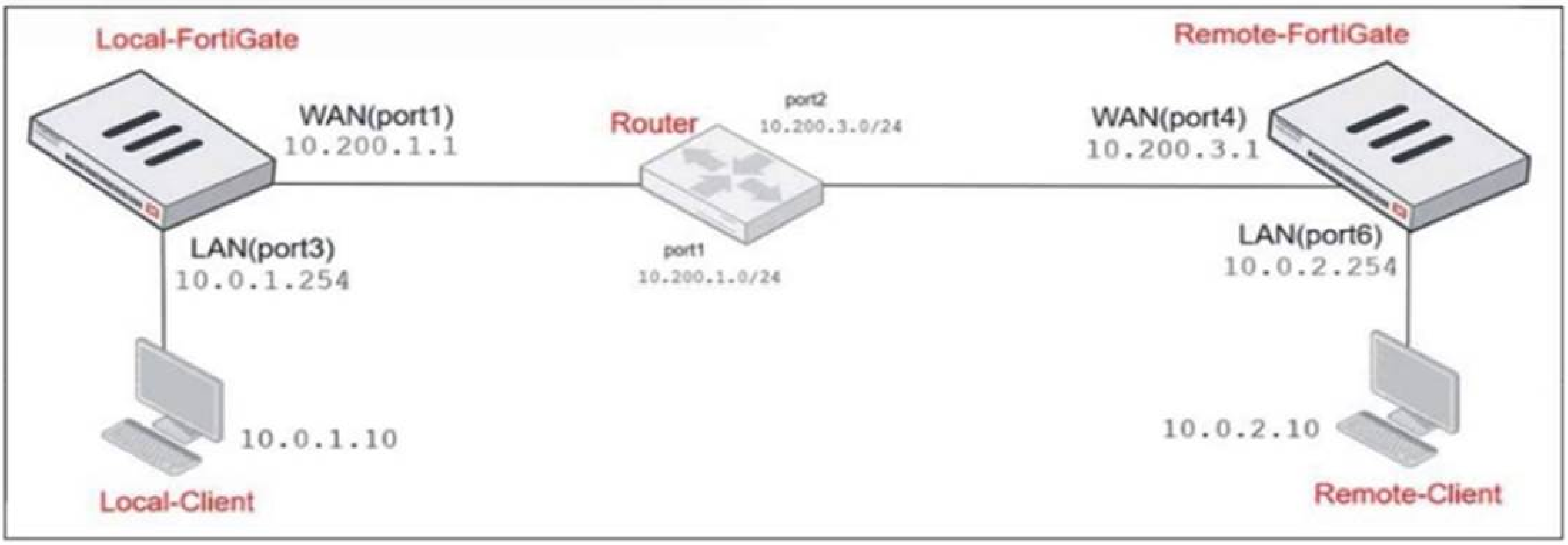
References:

- FortiOS 7.4.1 Administration Guide: HA election process

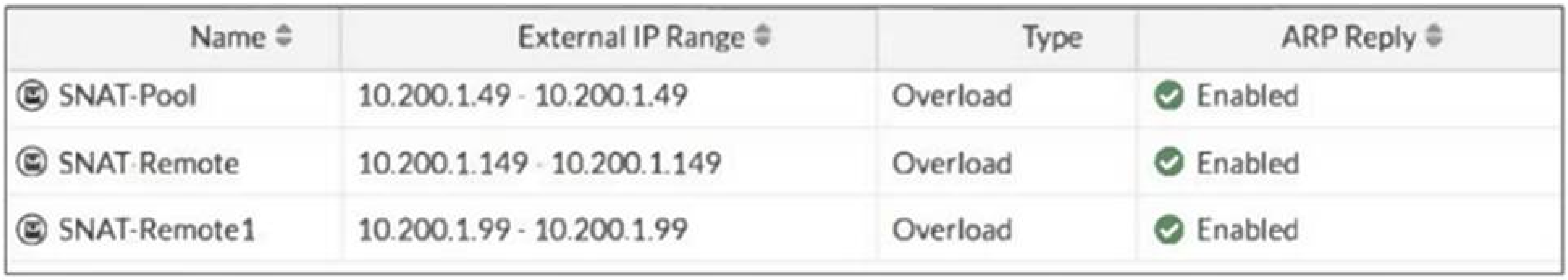
NEW QUESTION 19

Refer to the exhibits.

Network diagram

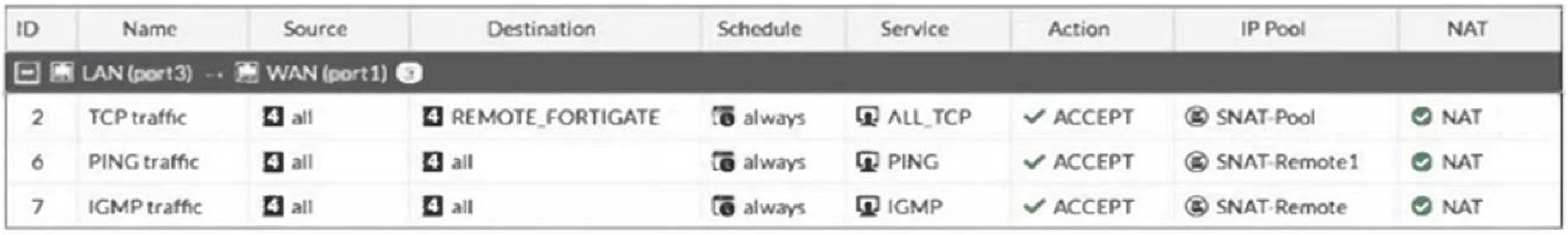


NAT IP pool configuration



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) 3								
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)?

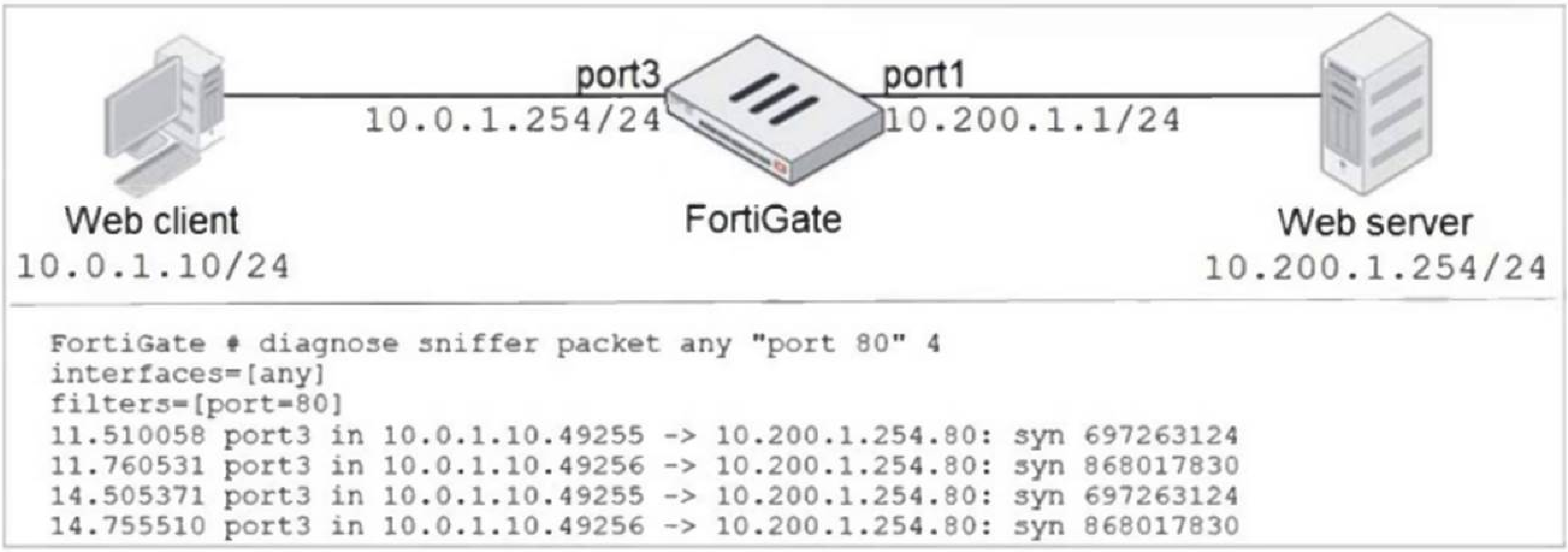
A. 10.200.1.1B.10.200.1.149C.10.200.1.99
B. 10.200.1.49

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 20
Refer to the exhibit.



```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port=80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
14.755510 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
```

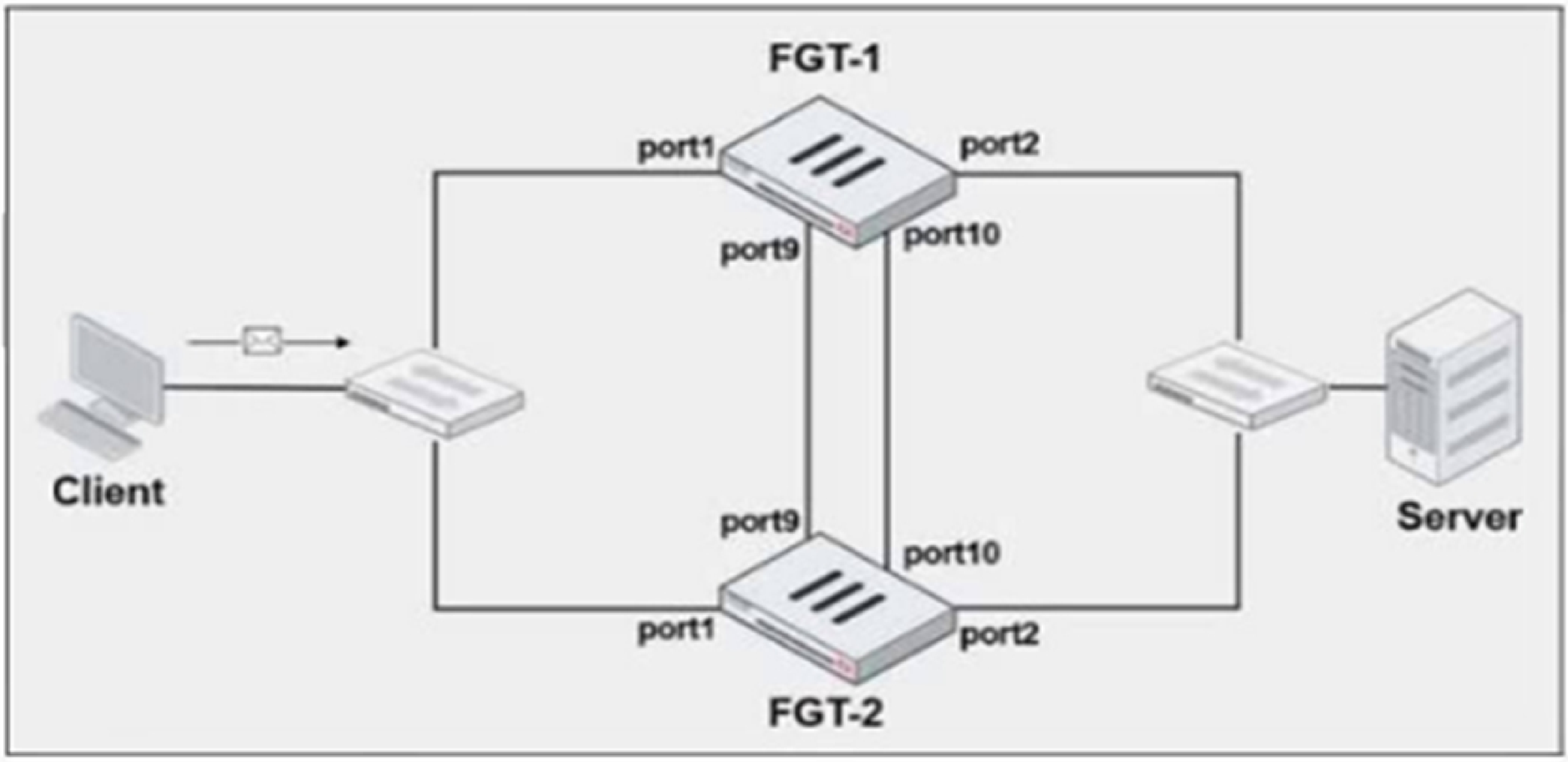
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.
What should the administrator do next, to troubleshoot the problem?

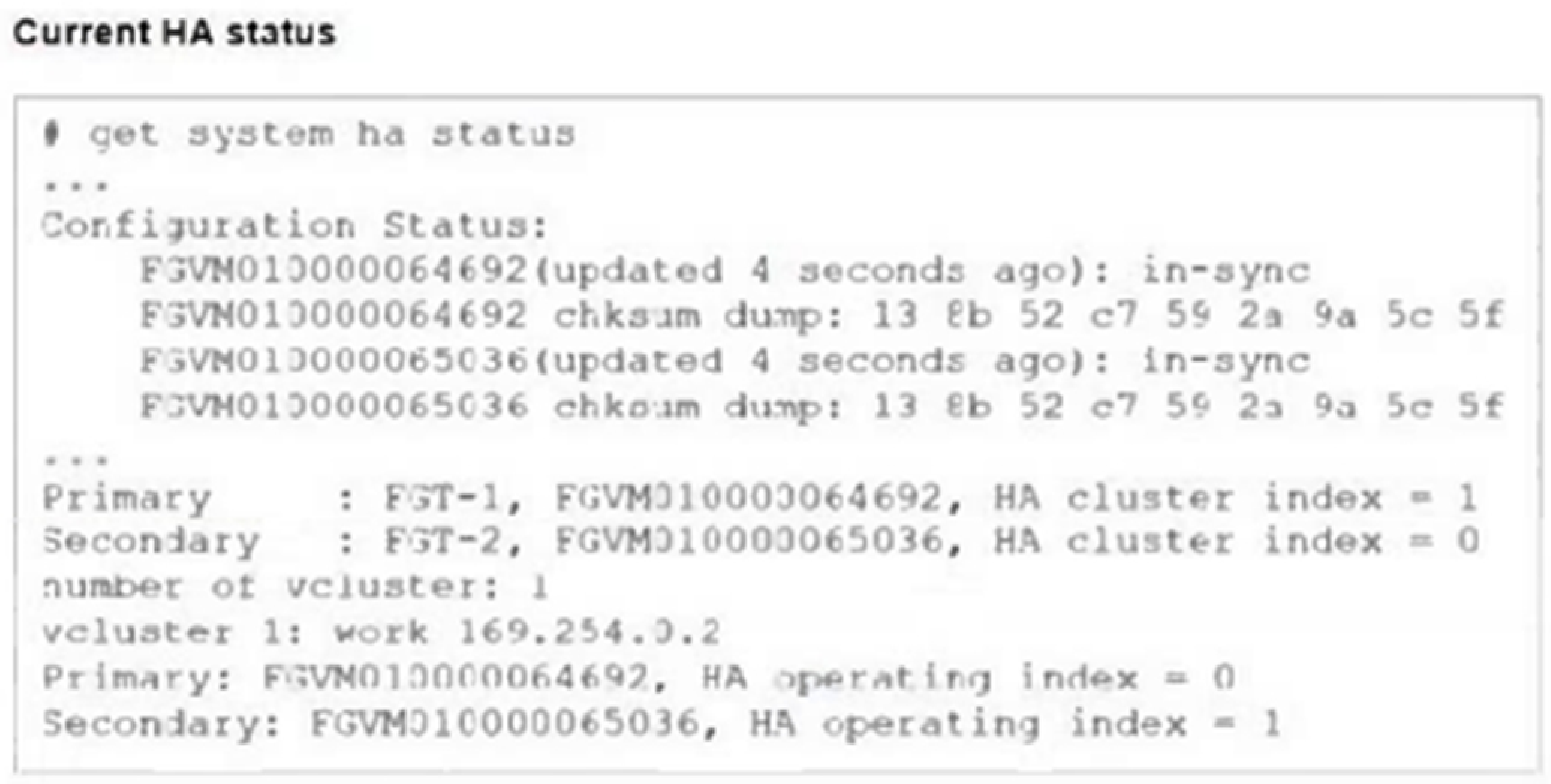
A. Execute a debug flow.
B. Capture the traffic using an external sniffer connected to port1.
C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".
D. Run a sniffer on the web server.

Answer: A

NEW QUESTION 22
Refer to the exhibits.

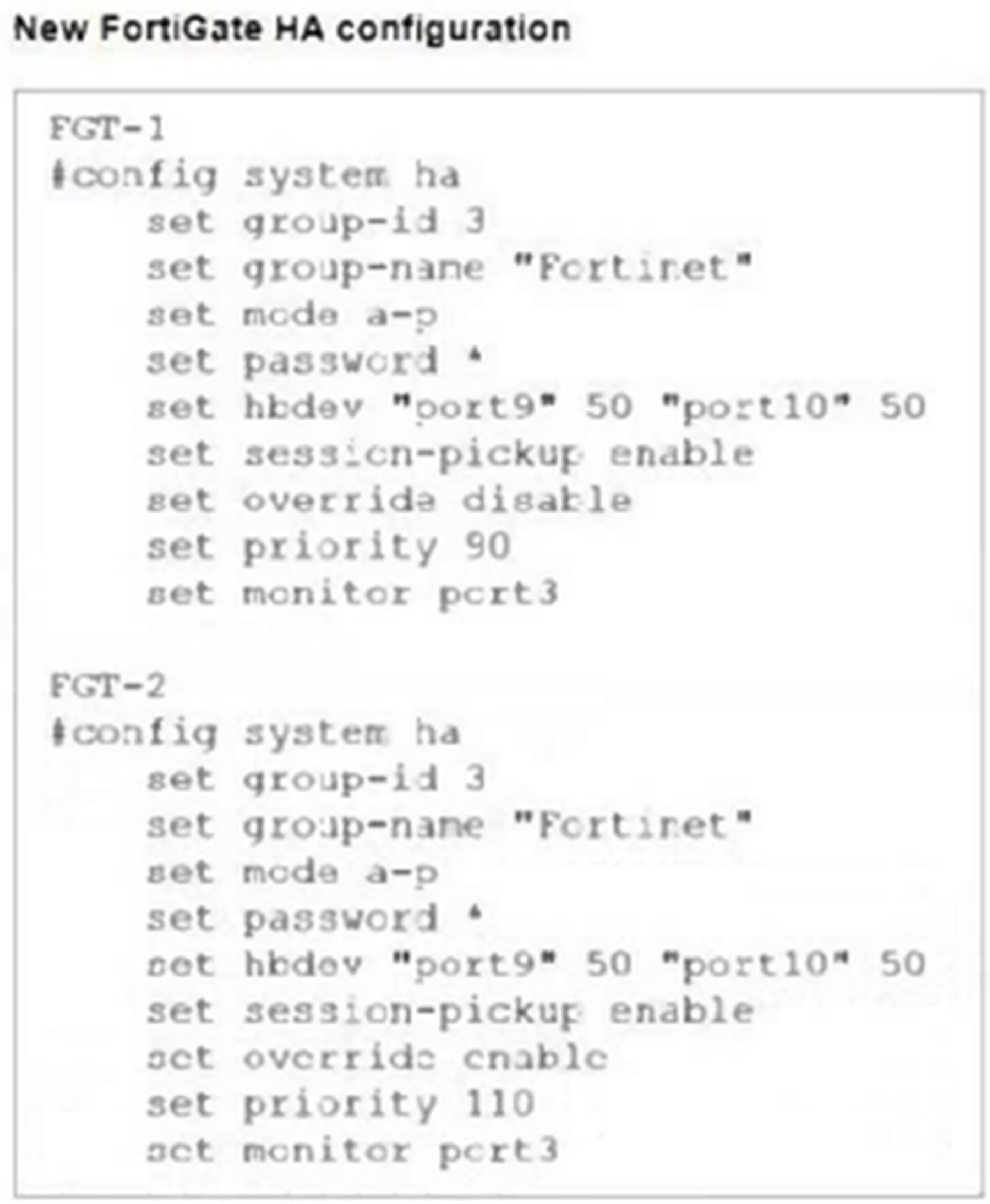
FortiGate HA cluster topology





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

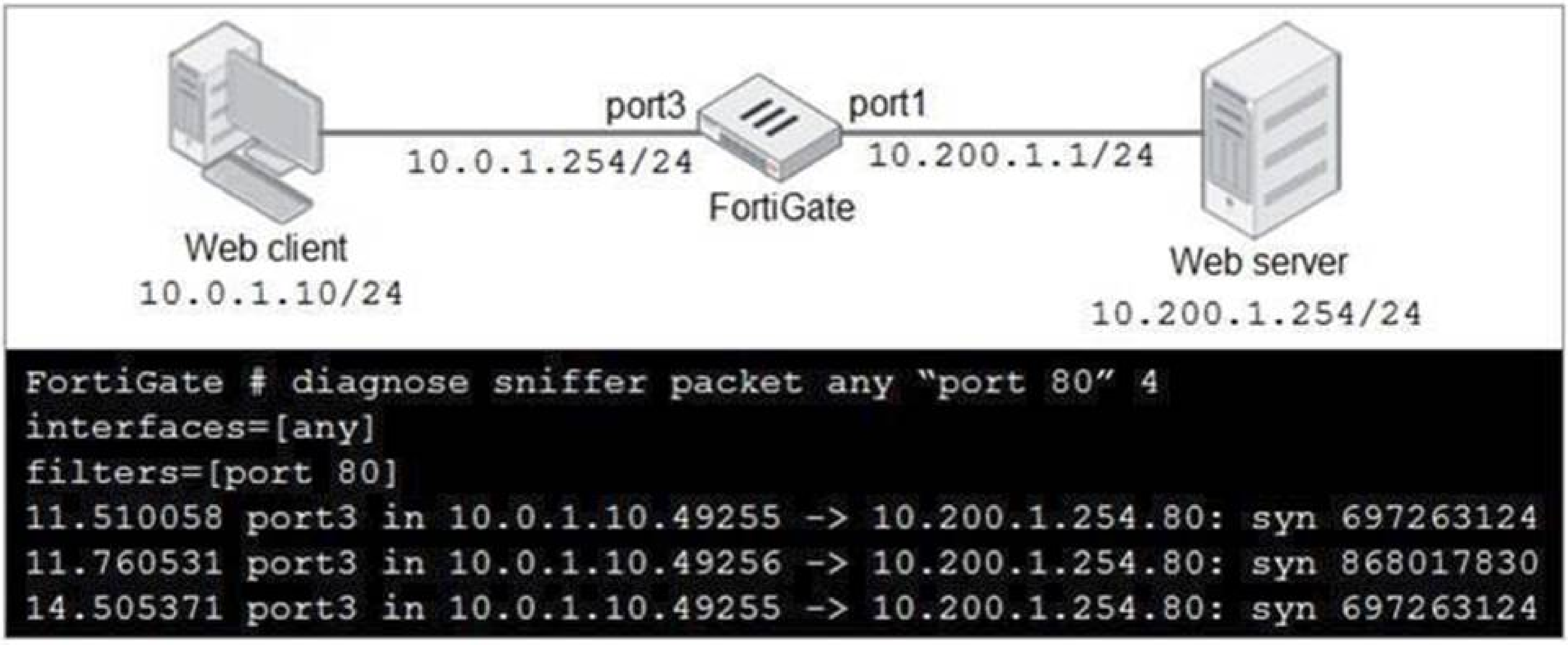
```
FGT-1
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override disable
    set priority 90
    set monitor port3

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 24
Refer to the exhibit.



```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
```

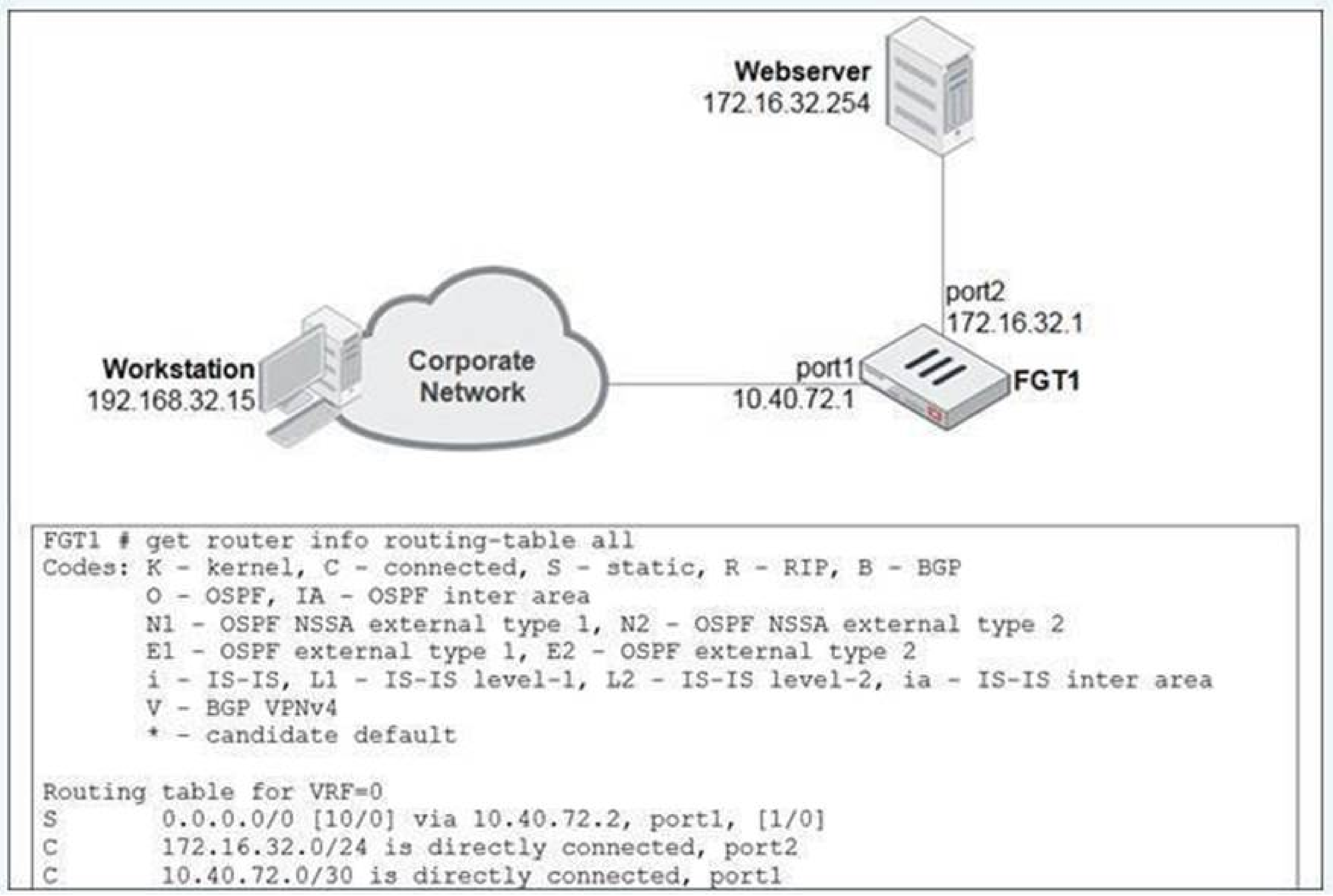
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

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

Answer: D

Explanation:
The next step for troubleshooting the problem would be to execute a debug flow on the FortiGate. The debug flow command provides detailed insights into how FortiGate handles the traffic, including whether the traffic is being dropped, allowed, or forwarded to the correct interface. It helps in identifying issues like firewall policy misconfigurations, routing issues, or NAT problems.
• A. Run a sniffer on the web server: While this might help diagnose server-side issues, the initial focus should be on the FortiGate, as the problem might lie in the firewall configuration or traffic handling.
• B. Capture the traffic using an external sniffer connected to port1: This may provide packetlevel information, but it's more useful to first analyze FortiGate's internal decision-making process with a debug flow.
• C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??: Running a sniffer on the specific host might give more packet details, but the debug flow provides more comprehensive information on how the firewall processes the packets.
Thus, using the debug flow will offer a more direct understanding of how the traffic is being processed or
blocked within FortiGate.

NEW QUESTION 29
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 33
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
......