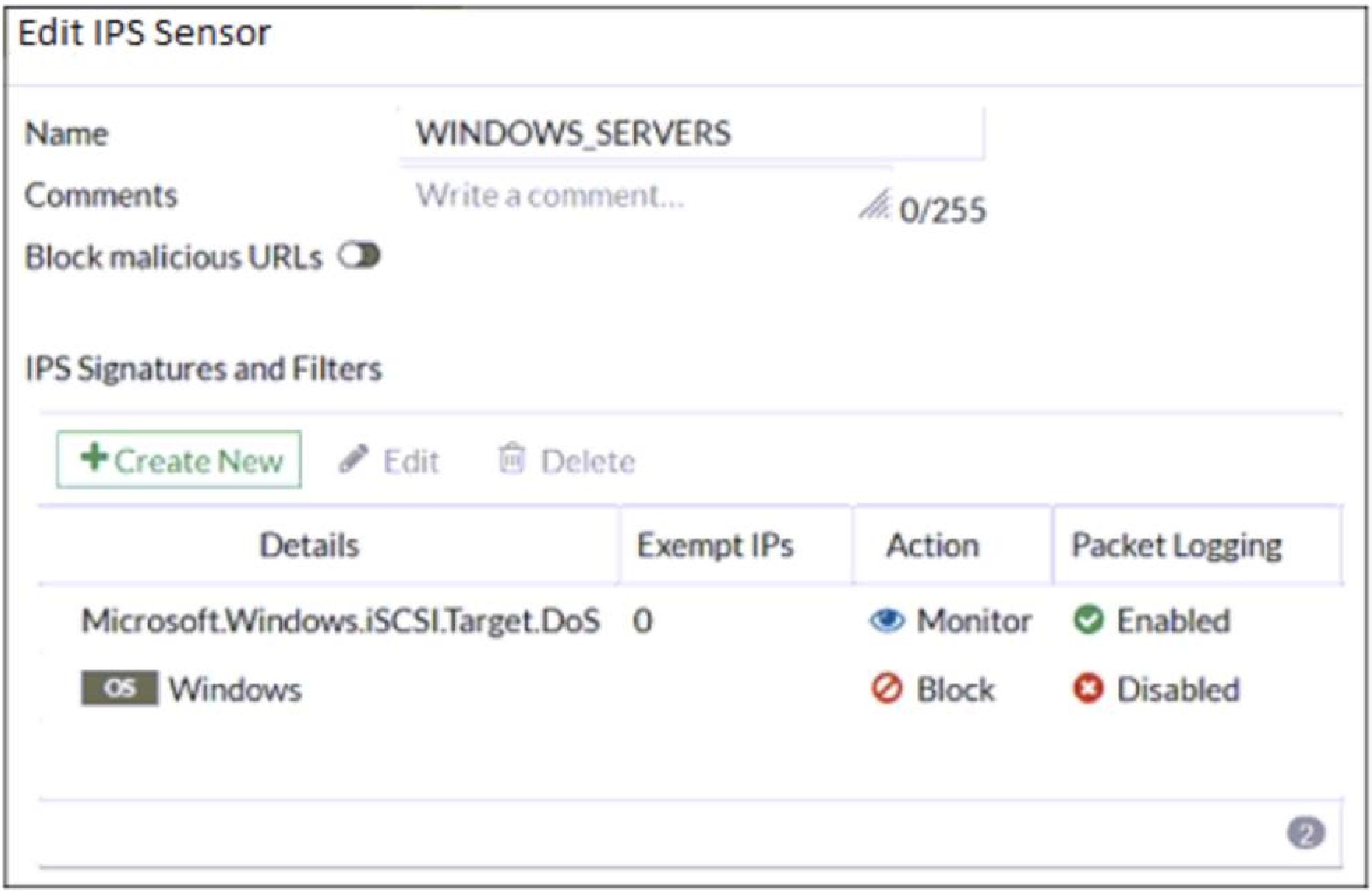
Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

NEW QUESTION 1
Refer to the exhibit, which shows the IPS sensor configuration.



Edit IPS Sensor

Name: WINDOWS_SERVERS
Comments: Write a comment... 0/255
Block malicious URLs ○

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
Microsoft.Windows.iSCSI.Target.DoS	0	Monitor	✓ Enabled
OS Windows		⊘ Block	✕ Disabled

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will gather a packet log for all matched traffic.
B. The sensor will reset all connections that match these signatures.
C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.
D. The sensor will block all attacks aimed at Windows servers.

Answer: AC

Explanation:
The IPS sensor configuration shows that:

- The Microsoft.Windows.iSCSI.Target.DoS signature is set to "Monitor" with packet logging enabled, meaning that while traffic matching this signature will be allowed, it will also be logged for further analysis.
- The generic Windows filter is set to "Block," meaning that all other attacks matching this filter will be blocked. However, the sensor will not reset connections or log packets unless specified.

Therefore, the sensor will allow attackers matching the specific DoS signature while blocking other attacks against Windows.
References:

- FortiOS 7.4.1 Administration Guide: IPS Configuration

NEW QUESTION 2
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

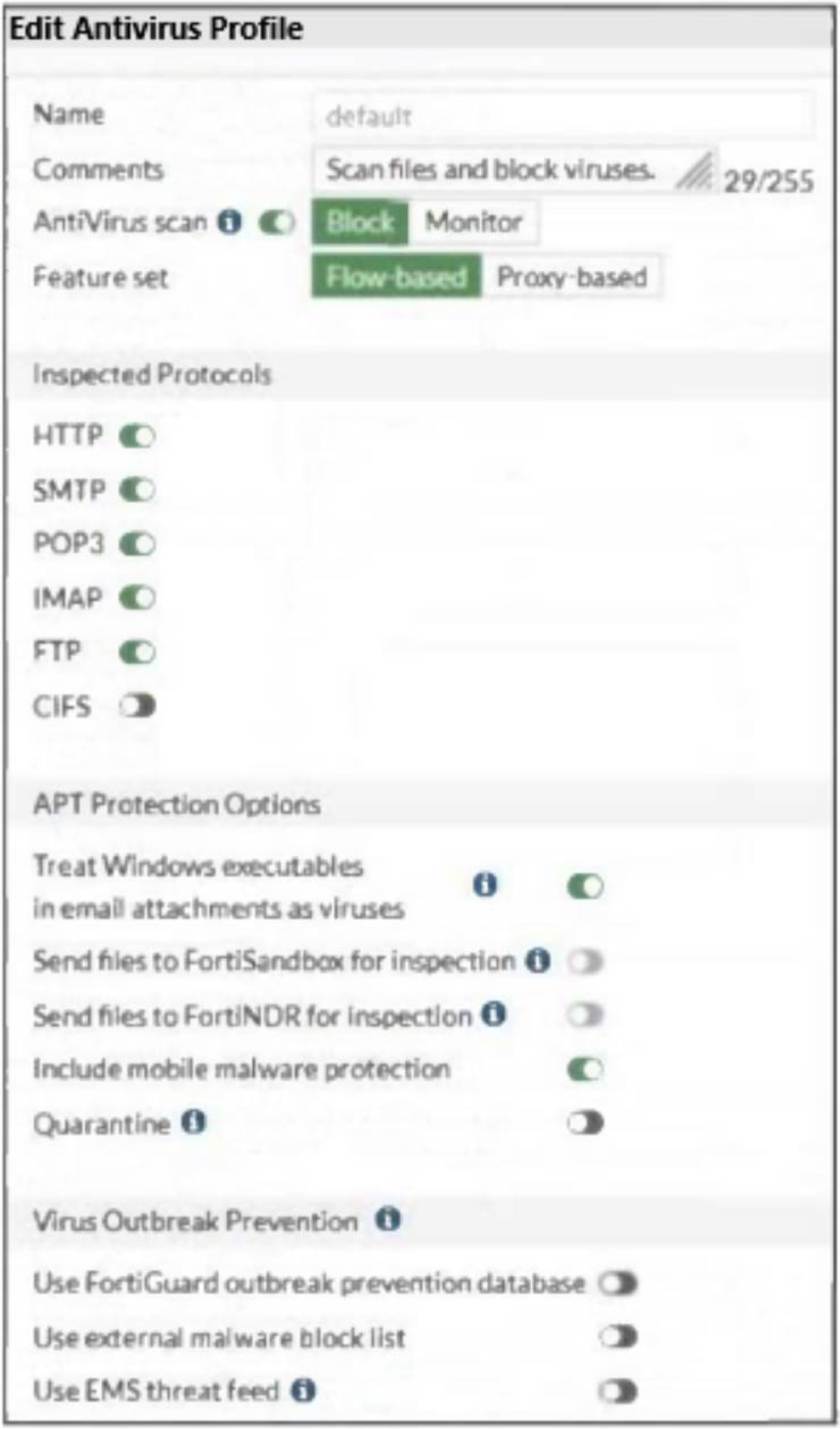
Answer: A

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 3

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: ● Block | Monitor

Feature set: ● Flow-based | Proxy-based

Inspected Protocols

HTTP: on
SMTP: on
POP3: on
IMAP: on
FTP: on
CIFS: off

APT Protection Options

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

Virus Outbreak Prevention

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

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 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
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 6
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 7
Which inspection mode does FortiGate use for application profiles if it is configured as a profile-based next- generation firewall (NGFW)?

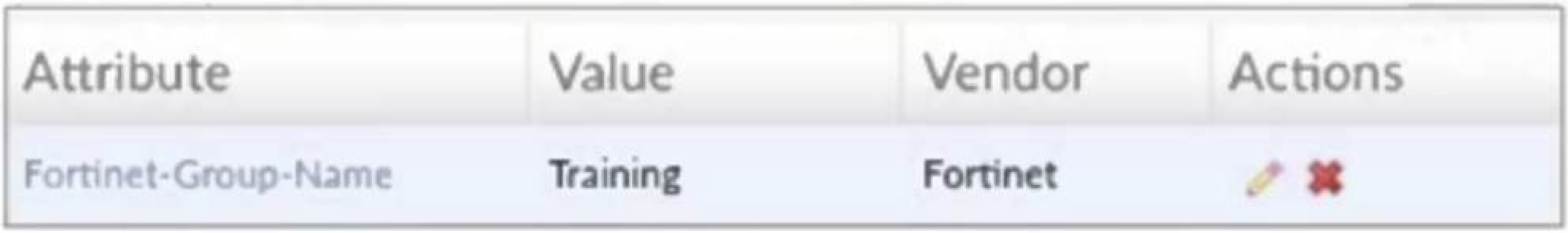
A. Full content inspection
B. Proxy-based inspection
C. Certificate inspection
D. Flow-based inspection

Answer: D

Explanation:
When FortiGate is configured in NGFW profile-based mode, it primarily uses flow-based inspection for application profiles. Flow-based inspection provides faster processing and lower latency by inspecting traffic in real-time without buffering, making it suitable for scenarios where performance is a priority.
References:

FortiOS 7.4.1 Administration Guide: Inspection Modes

NEW QUESTION 8
Refer to the exhibit, which shows a partial configuration from the remote authentication server.



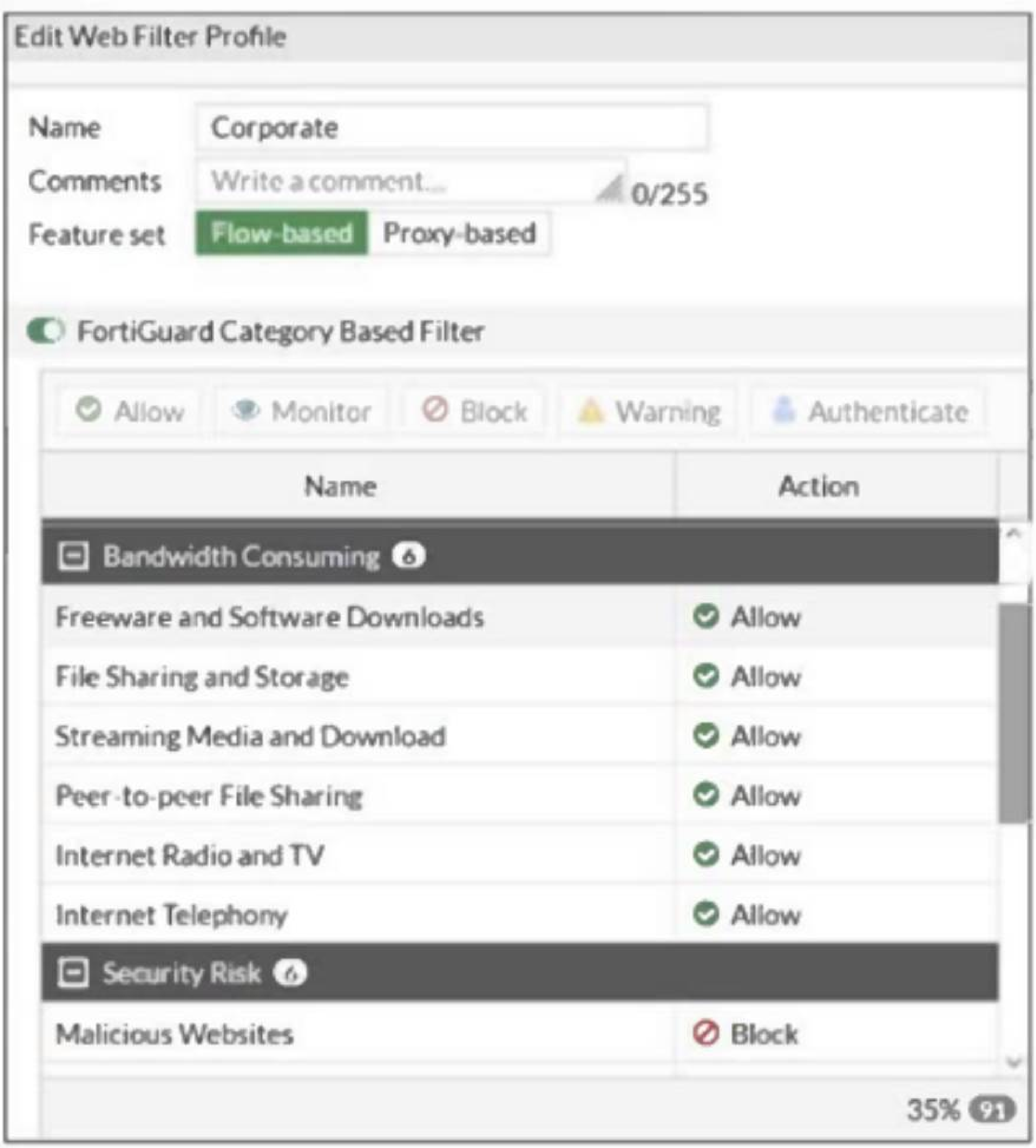
Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	✎ ✖

Why does the FortiGate administrator need this configuration?

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

Answer: A

NEW QUESTION 9
Refer to the exhibit.



Edit Web Filter Profile

Name: Corporate

Comments: Write a comment... 0/255

Feature set: Flow-based | Proxy-based

FortiGuard Category Based Filter

Name	Action
Bandwidth Consuming 6	
Freeware and Software Downloads	✓ Allow
File Sharing and Storage	✓ Allow
Streaming Media and Download	✓ Allow
Peer-to-peer File Sharing	✓ Allow
Internet Radio and TV	✓ Allow
Internet Telephony	✓ Allow
Security Risk 6	
Malicious Websites	⊘ Block

35% 91

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 10
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.

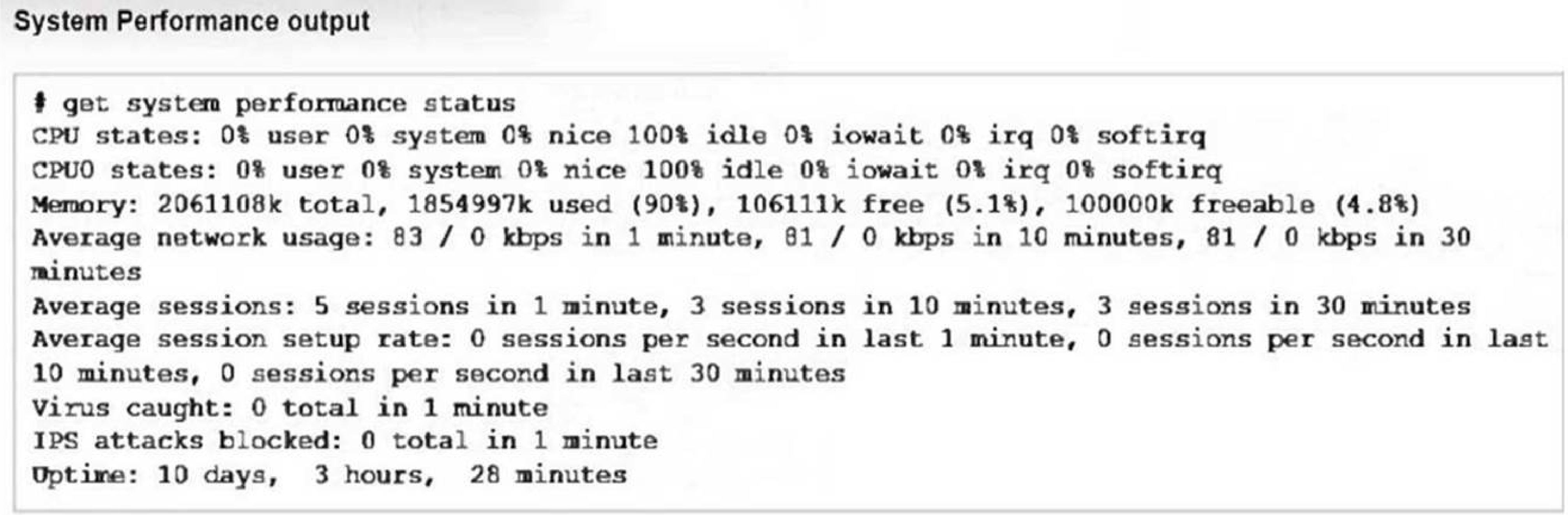
The other options are not directly necessary for establishing SSL VPN:

- 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

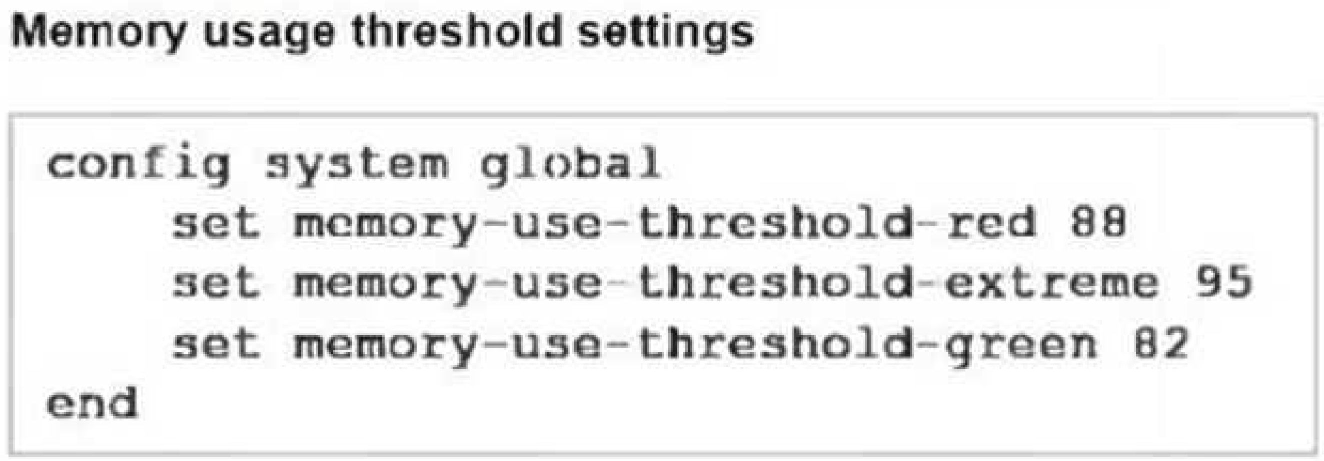
- FortiOS 7.4.1 Administration Guide - Configuring SSL VPN, page 1203.
- FortiOS 7.4.1 Administration Guide - SSL VPN Authentication, page 1210.

NEW QUESTION 10
Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.



System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```



Memory usage threshold settings

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, what can be the two possible outcomes? (Choose two.)

A. FortiGate will start sending all files to FortiSandbox for inspection.
B. FortiGate has entered conserve mode.
C. Administrators cannot change the configuration.
D. Administrators can access FortiGate onlythrough the console port.

Answer: BC

Explanation:
Based on the system performance output provided, the memory usage on the FortiGate device is at 90%, which is above the green threshold (82%) but below the red threshold (88%). Given this high memory usage, the FortiGate device will enter "conserve mode" to prevent further resource exhaustion. In conserve mode:

- B. FortiGate has entered conserve mode: When the memory usage reaches or exceeds certain thresholds (in this case, the green and red thresholds), the FortiGate enters conserve mode to protect itself from running out of memory entirely. This mode limits some functionalities to reduce memory usage and avoid a potential system crash.

- D. Administrators can access FortiGate only through the console port: During conserve mode, administrative access might be restricted, and administrators may only be able to connect to the device via the console port. This restriction is in place to ensure that the FortiGate can be managed directly, even under low resource conditions.

The other options are not correct:

- A. FortiGate will start sending all files to FortiSandbox for inspection: This is unrelated to memory usage and conserve mode.
- C. Administrators cannot change the configuration: While access may be limited, configuration changes can still be made via the console port.

References

- FortiOS 7.4.1 Administration Guide - Monitoring System Resources and Performance, page 325.
- FortiOS 7.4.1 Administration Guide - Conserve Mode, page 330.

NEW QUESTION 12

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.

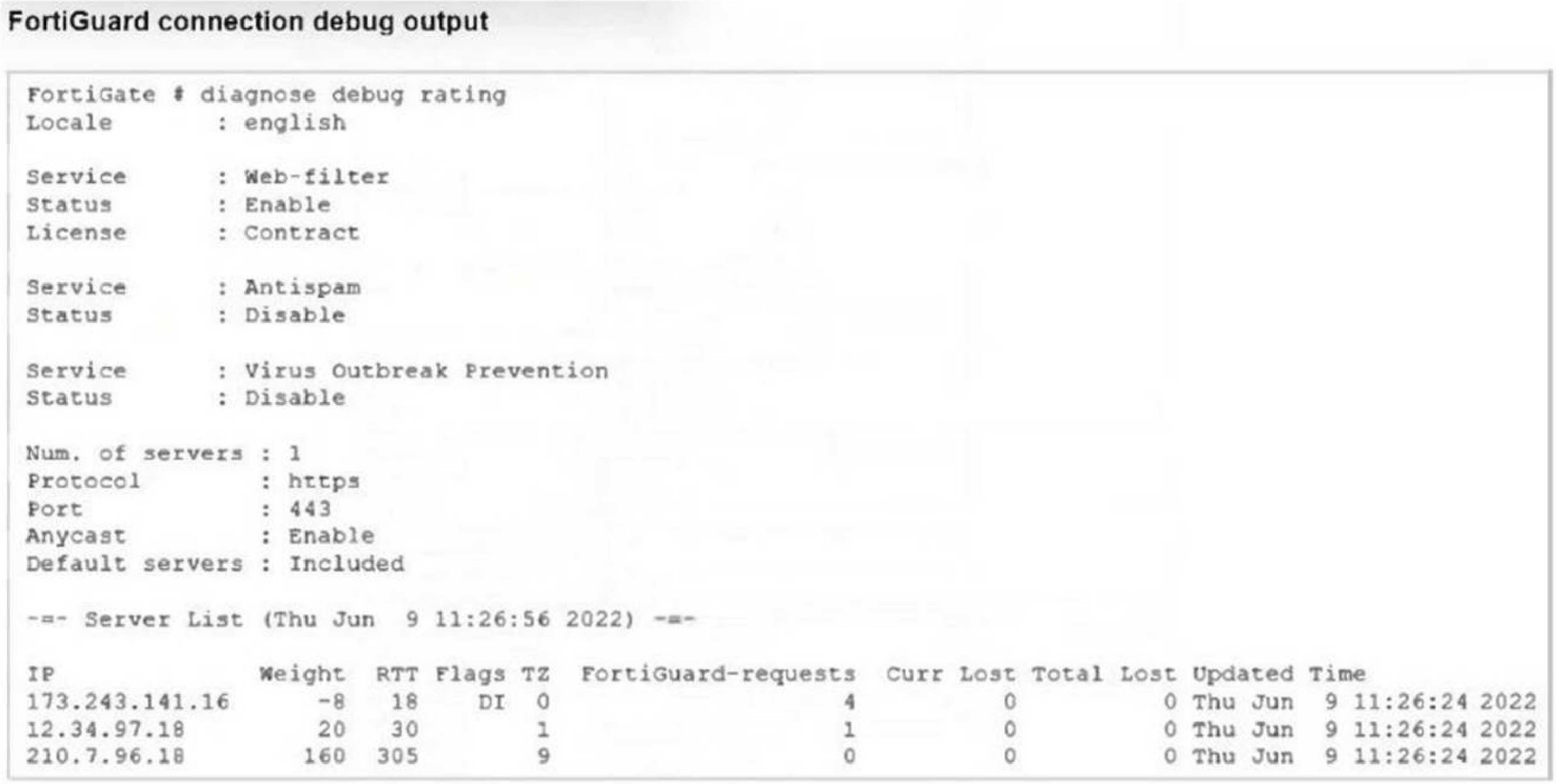
Answer: D

Explanation:

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

NEW QUESTION 15

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 17

An administrator configured a FortiGate to act as a collector for agentless polling mode.

What must the administrator add to the FortiGate device to retrieve AD user group information?

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

Answer: A

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

NEW QUESTION 18
Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

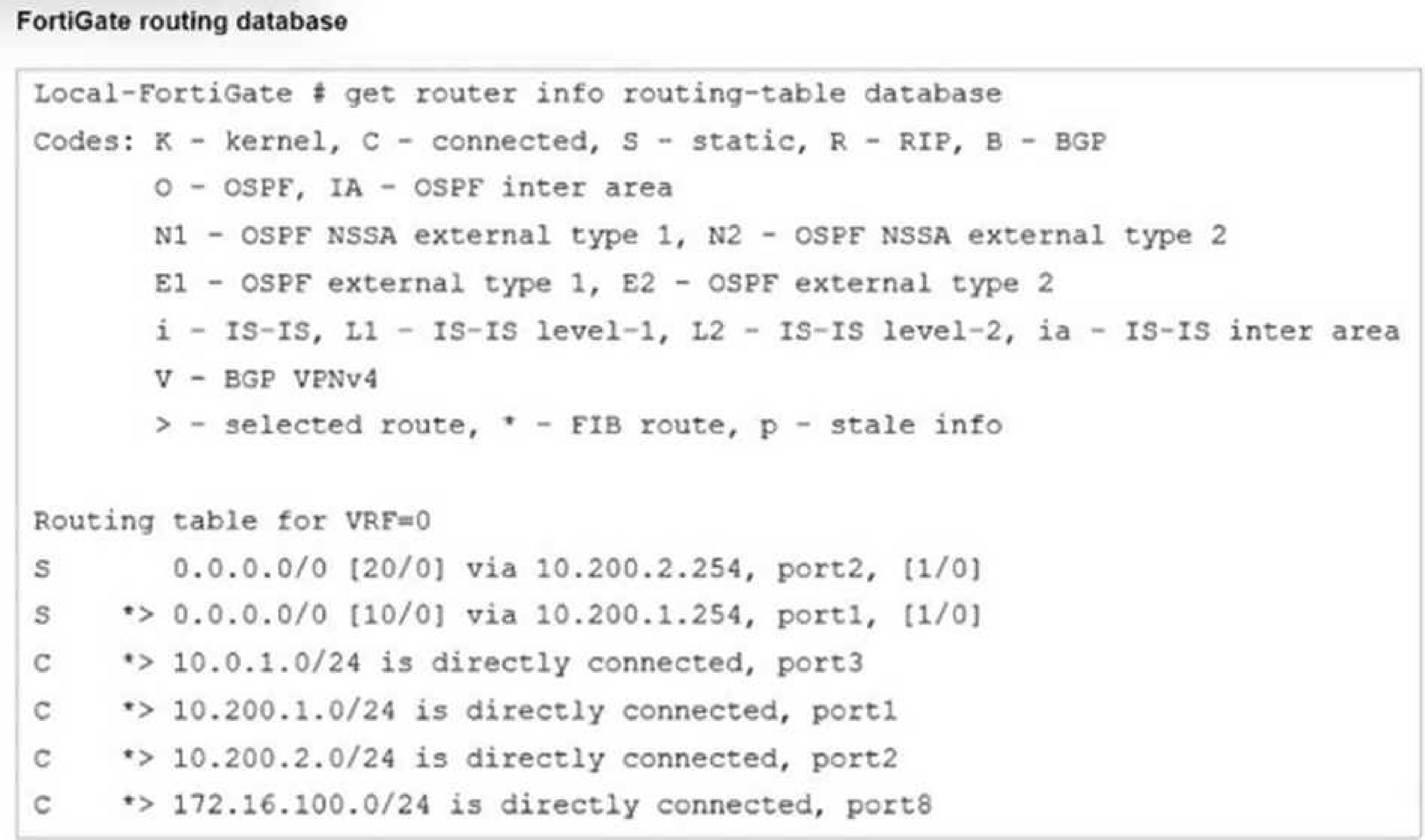
A. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.
B. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
C. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP
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 22
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 25

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:

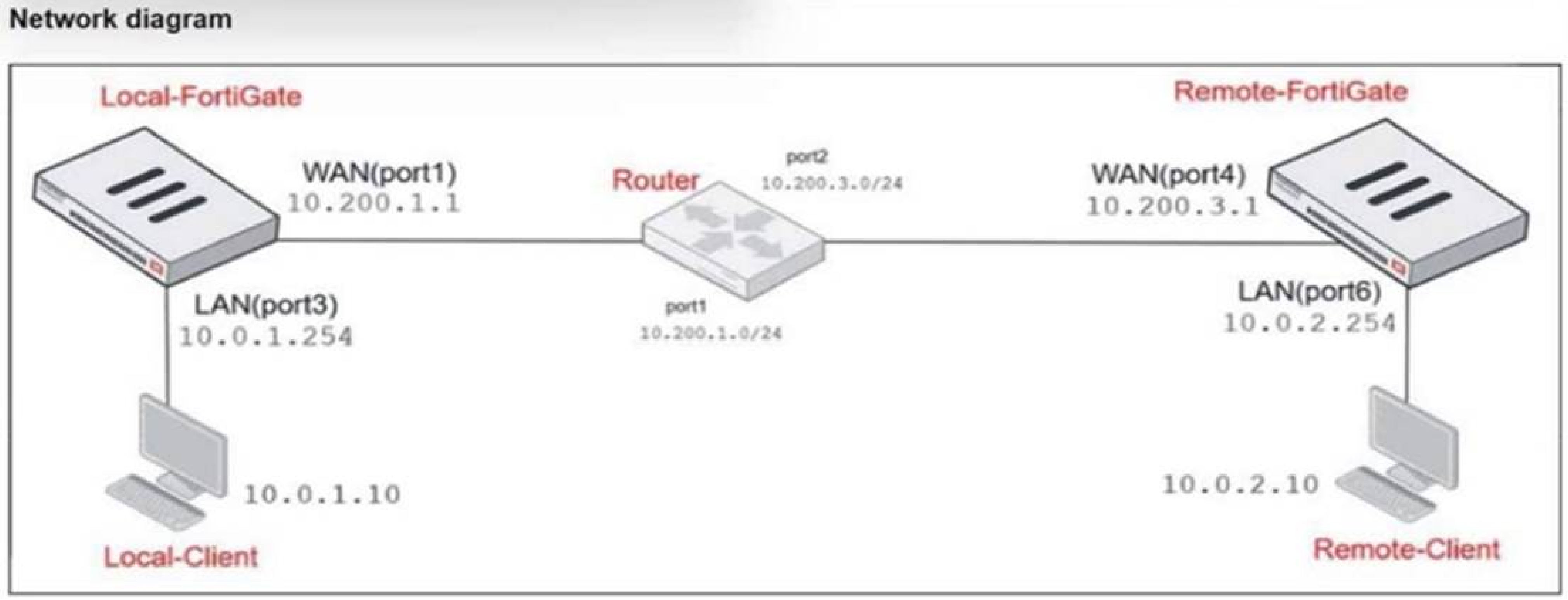
- Connected monitored ports: The unit with the most monitored ports up is preferred.
- Priority: The unit with the highest priority is preferred.
- System uptime: The unit with the longest uptime is preferred.
- FortiGate serial number: Used as the final criterion to break any remaining ties.

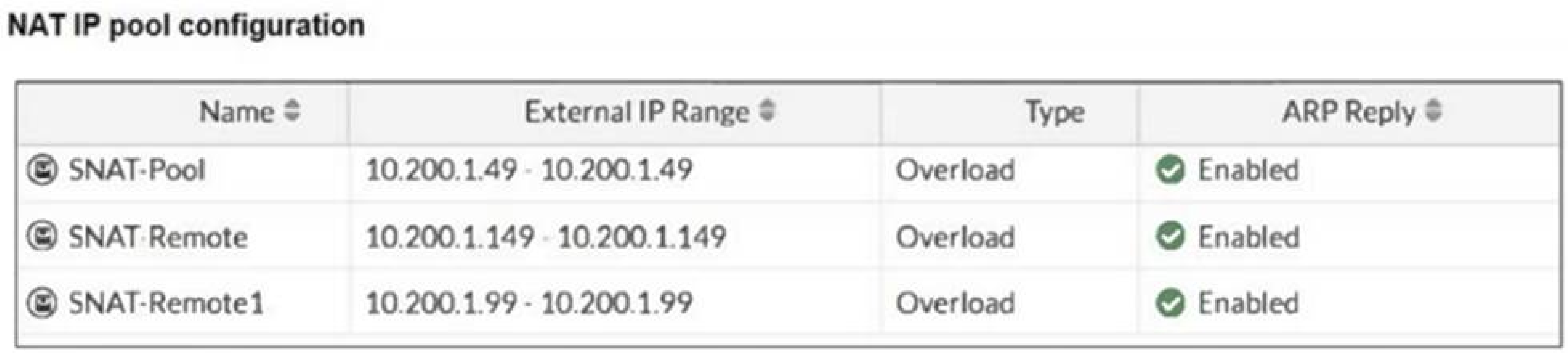
References:

- FortiOS 7.4.1 Administration Guide: HA election process

NEW QUESTION 27

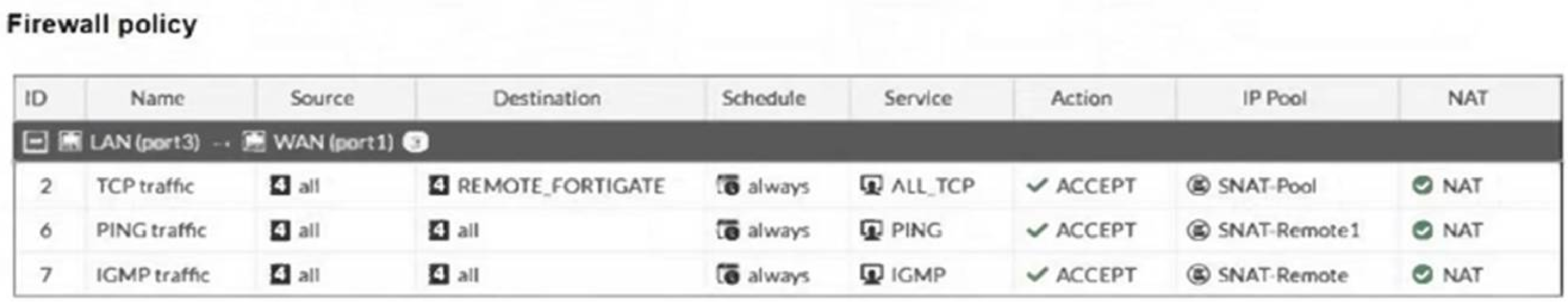
Refer to the exhibits.





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) 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)?

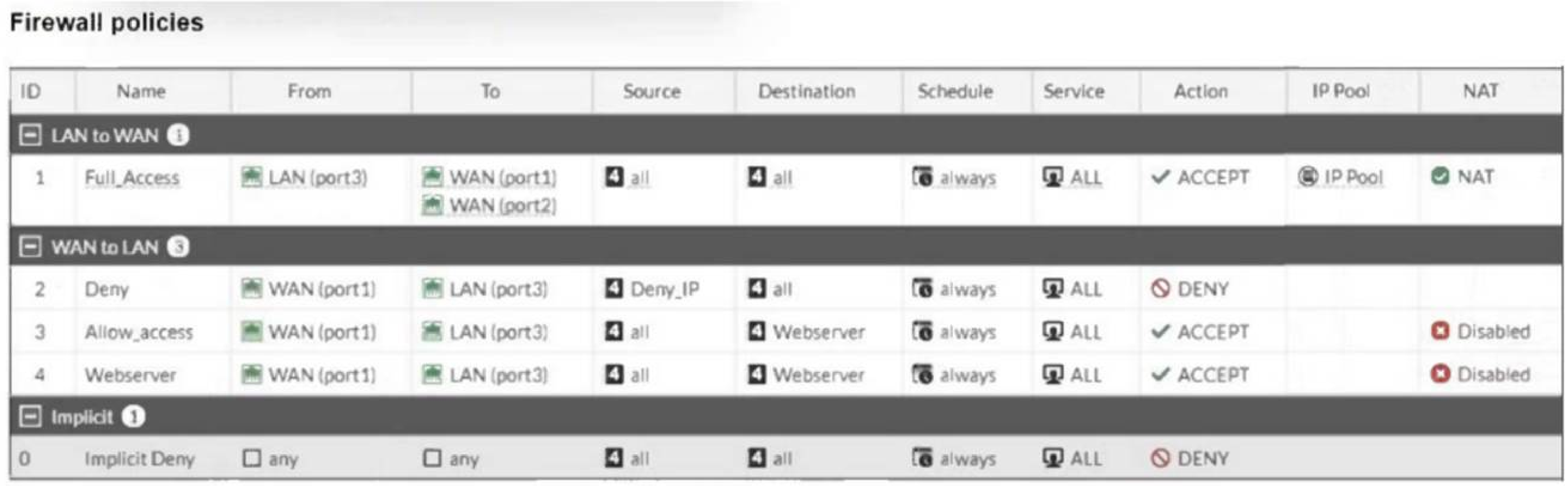
A. 10.200.1.1B.10.200.1.149C.10.200.1.99
B. 10.200.1.49

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 31
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?

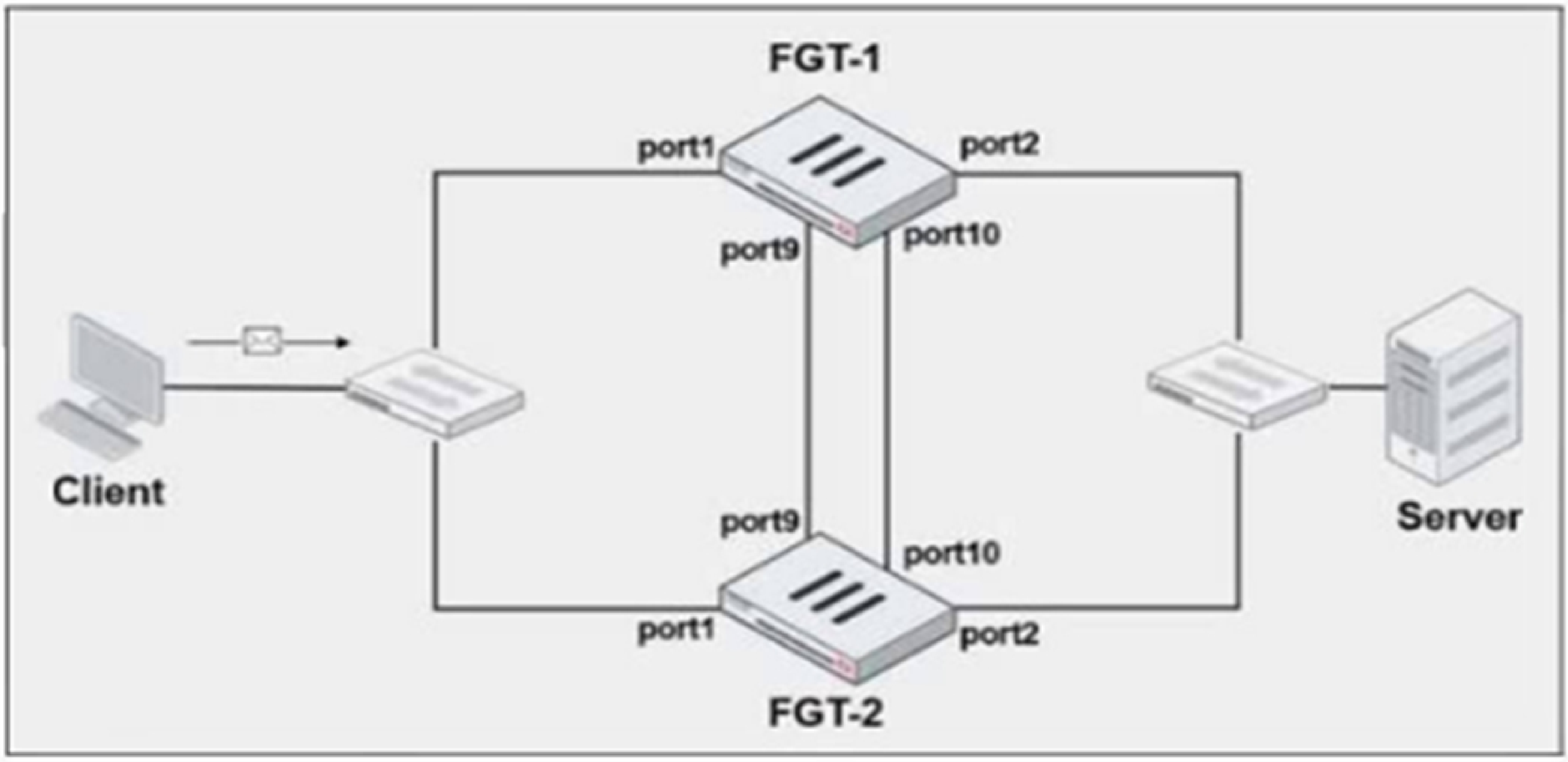
A. The Implicit group can include more than one deny firewall policy.
B. The firewall policies are listed by ID sequence view.
C. The firewall policies are listed by ingress and egress interfaces pairing view.
D. LAN to WA
E. WAN to LA
F. and Implicit are sequence grouping view lists.

Answer: C

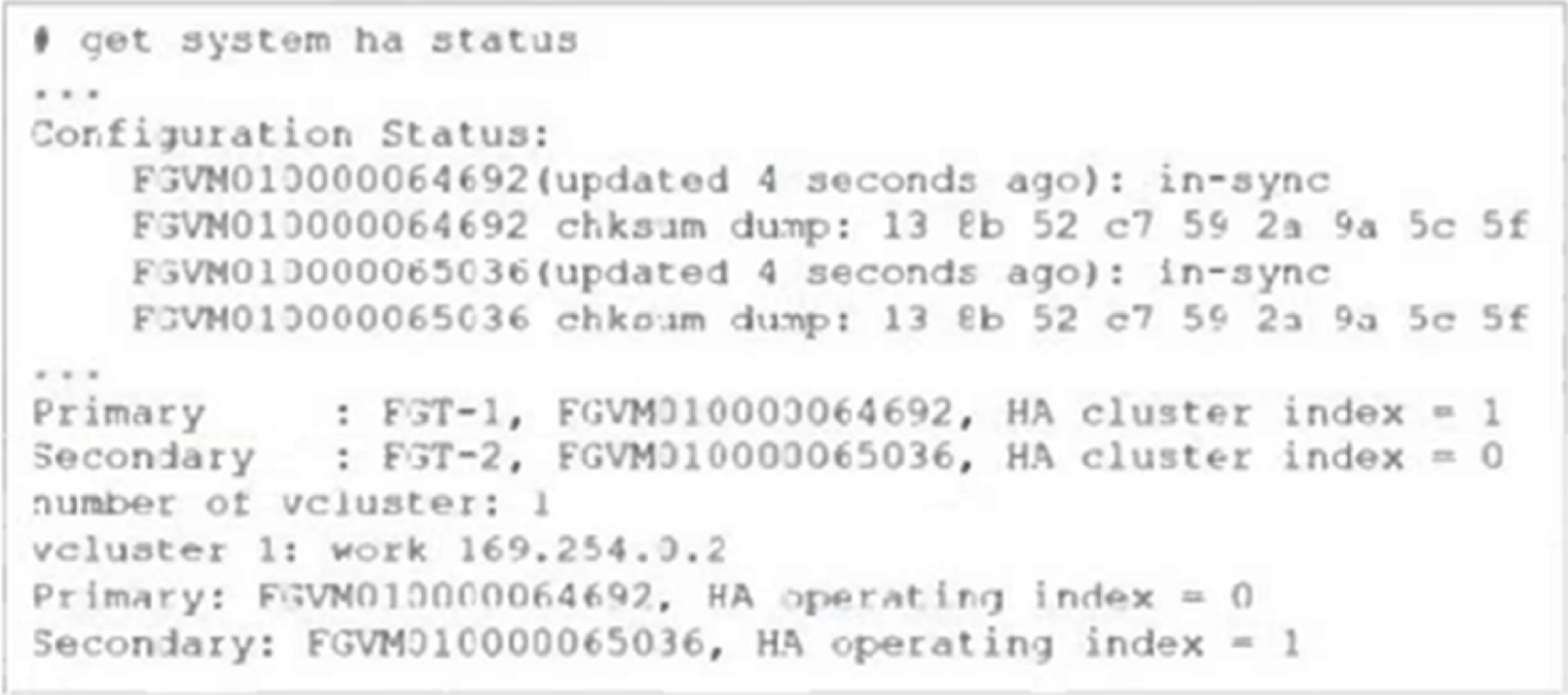
Explanation:
The firewall policy list in the exhibit is arranged in the "Interface Pair View," where policies are grouped by
their incoming (ingress) and outgoing (egress) interface pairs. Each section (LAN to WAN, WAN to LAN,
etc.) groups policies based on these interface pairings. This view helps administrators 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 35
Refer to the exhibits.

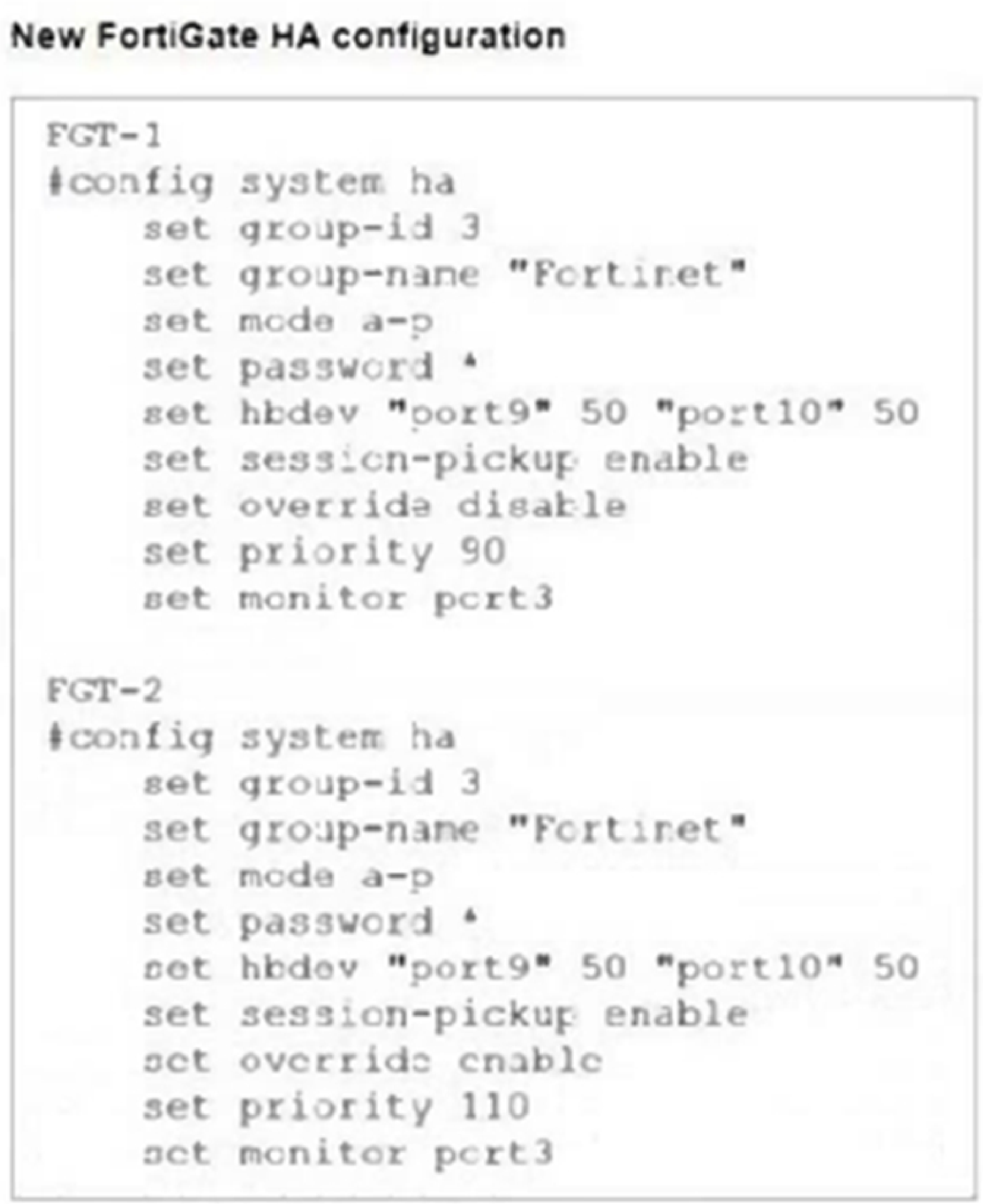
FortiGate HA cluster topology



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
```

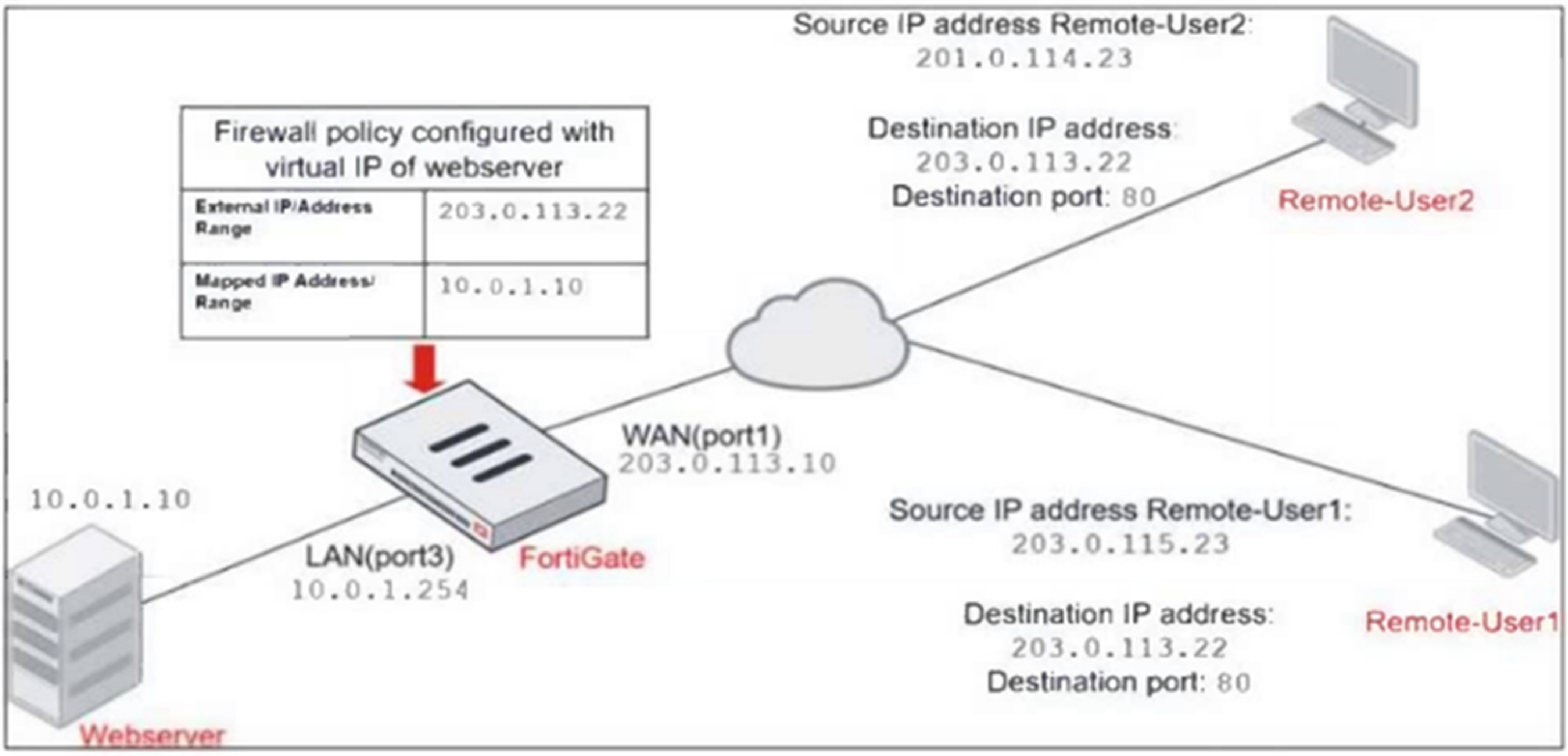
FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.
What would be the expected outcome in the HA cluster?

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.

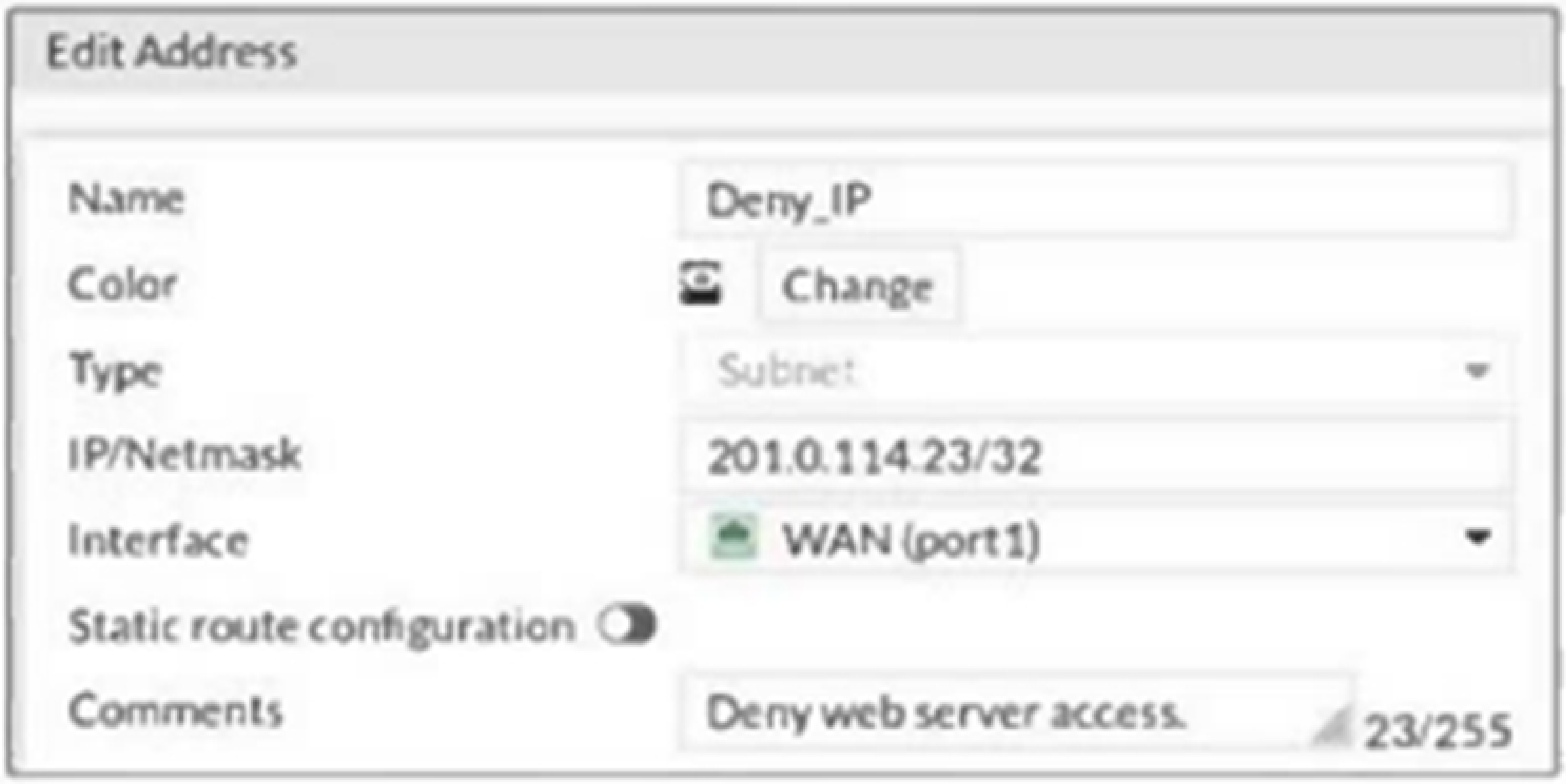
Answer: B

NEW QUESTION 37
Refer to the exhibits.

Network diagram



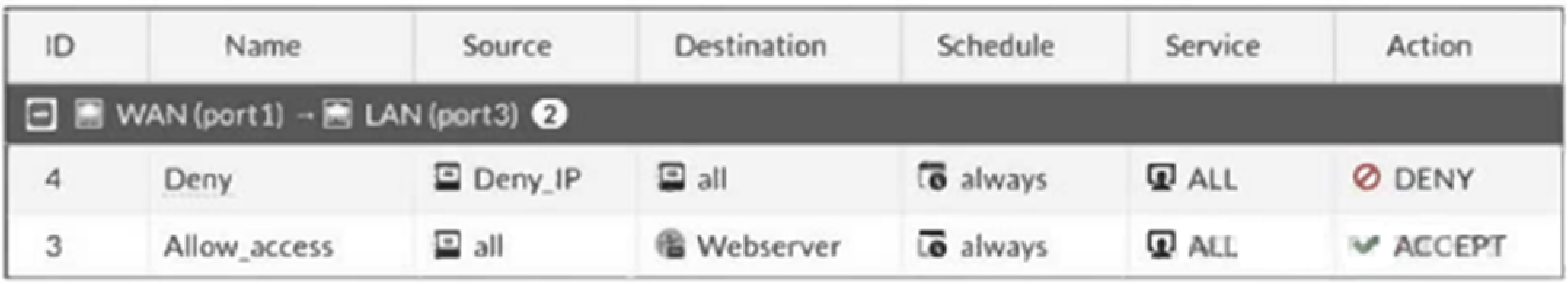
Firewall address object



Edit Address

Name	Deny_IP
Color	Change
Type	Subnet
IP/Netmask	201.0.114.23/32
Interface	WAN (port1)
Static route configuration	○
Comments	Deny web server access. 23/255

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

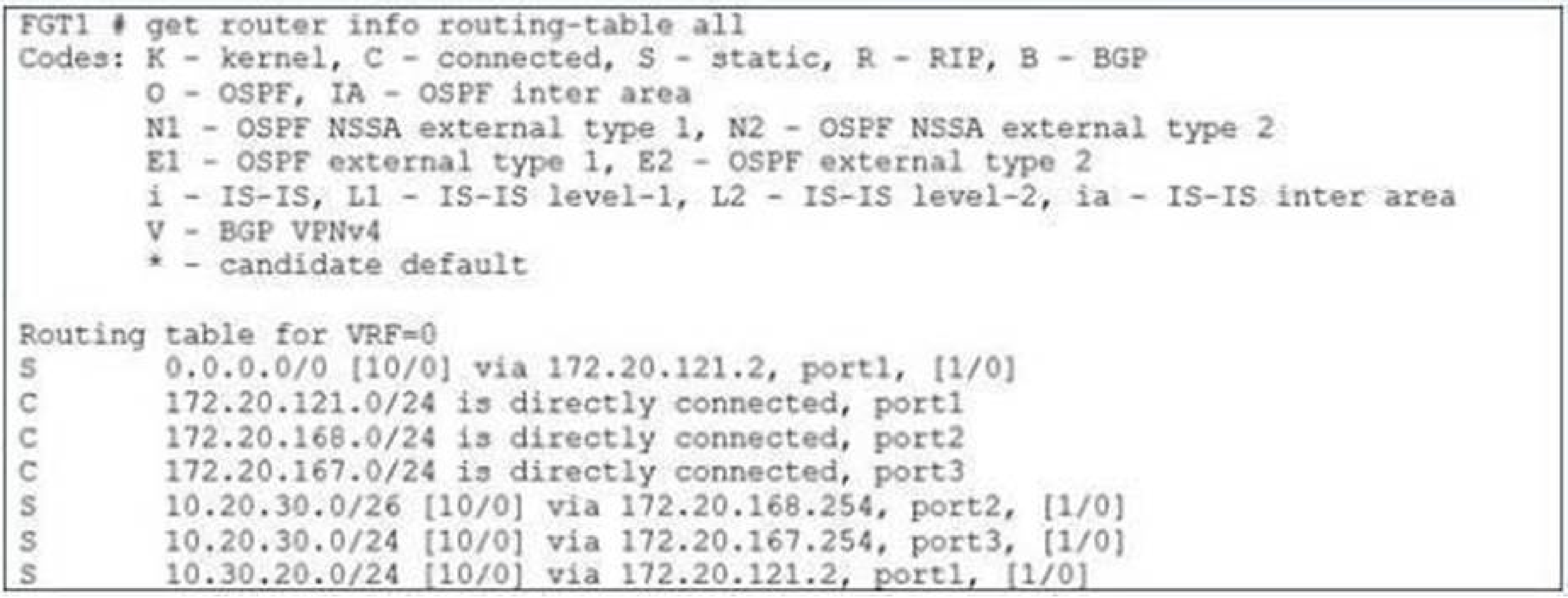
The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.
The policy should work such that Remote-User1 must be able to access the Webserver while 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 39
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:

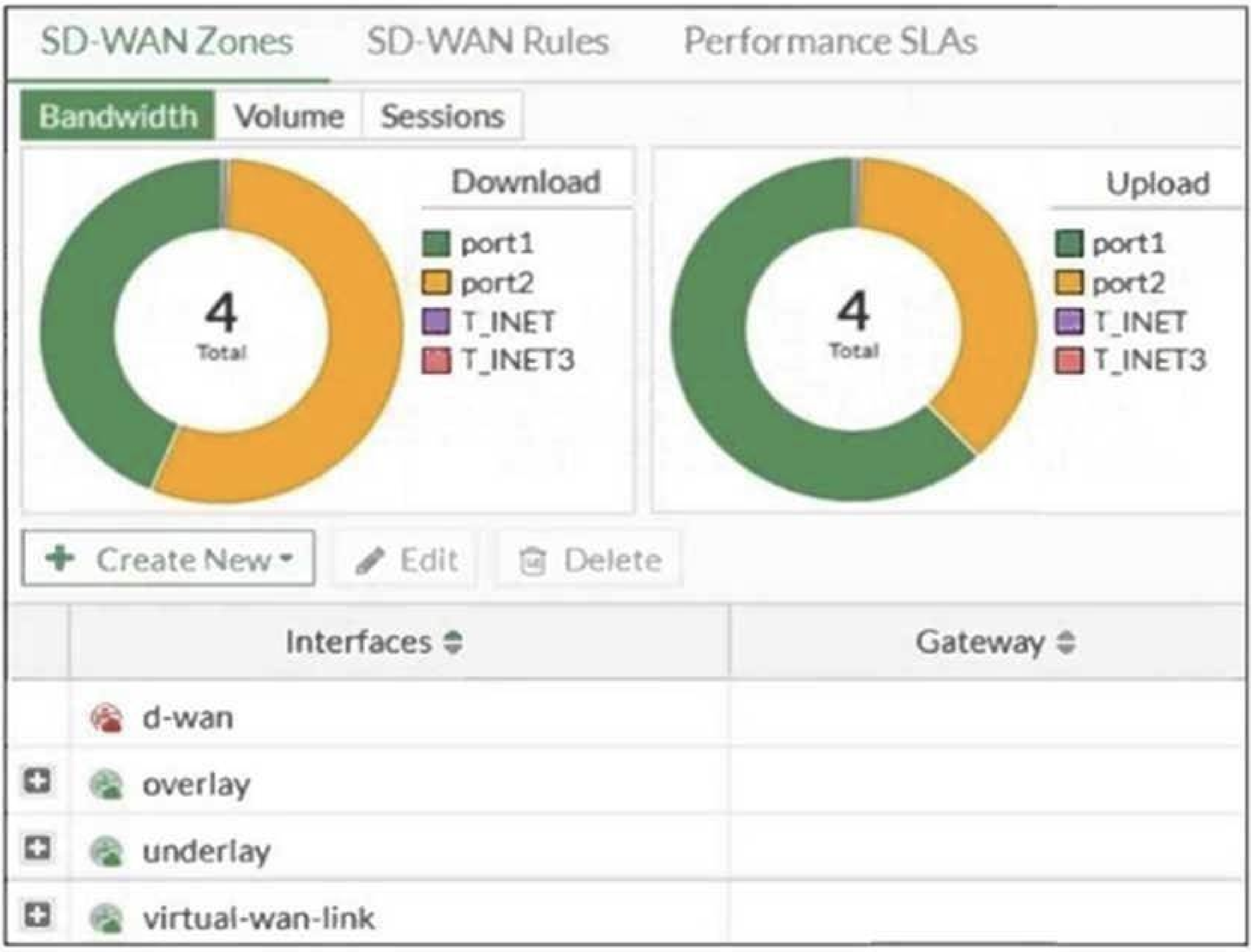
B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
• This route is for a different subnet, 10.30.20.0/24, which does not include the target address 10.20.30.254. Therefore, it is not a valid match.

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 41
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration



	Interfaces	Gateway
	d-wan	
⊞	overlay	
⊞	underlay	
⊞	virtual-wan-link	

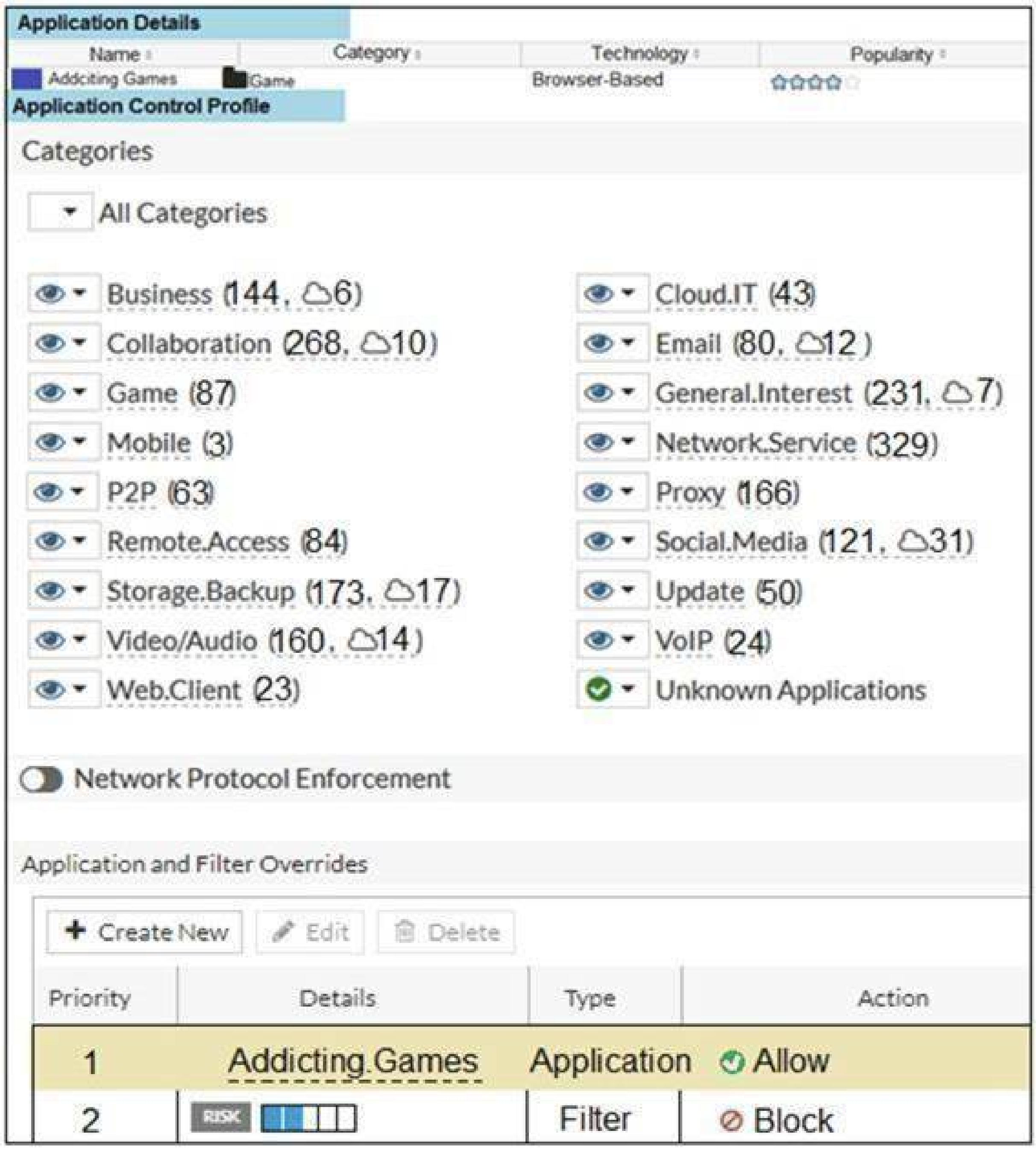
Based on the exhibit, which statement is true?

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 42
Refer to the exhibit.



Application Details

Name	Category	Technology	Popularity
Addicting Games	Game	Browser-Based	★★★★☆

Application Control Profile

Categories

All Categories

Business (144, ☁6)	Cloud.IT (43)
Collaboration (268, ☁10)	Email (80, ☁12)
Game (87)	General.Interest (231, ☁7)
Mobile (3)	Network.Service (329)
P2P (63)	Proxy (166)
Remote.Access (84)	Social.Media (121, ☁31)
Storage.Backup (173, ☁17)	Update (50)
Video/Audio (160, ☁14)	VoIP (24)
Web.Client (23)	✓ Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	Addicting.Games	Application	✓ Allow
2	RISK ▮▯▯▯	Filter	⊘ Block

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

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

Answer: D

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

NEW QUESTION 46
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 47
......