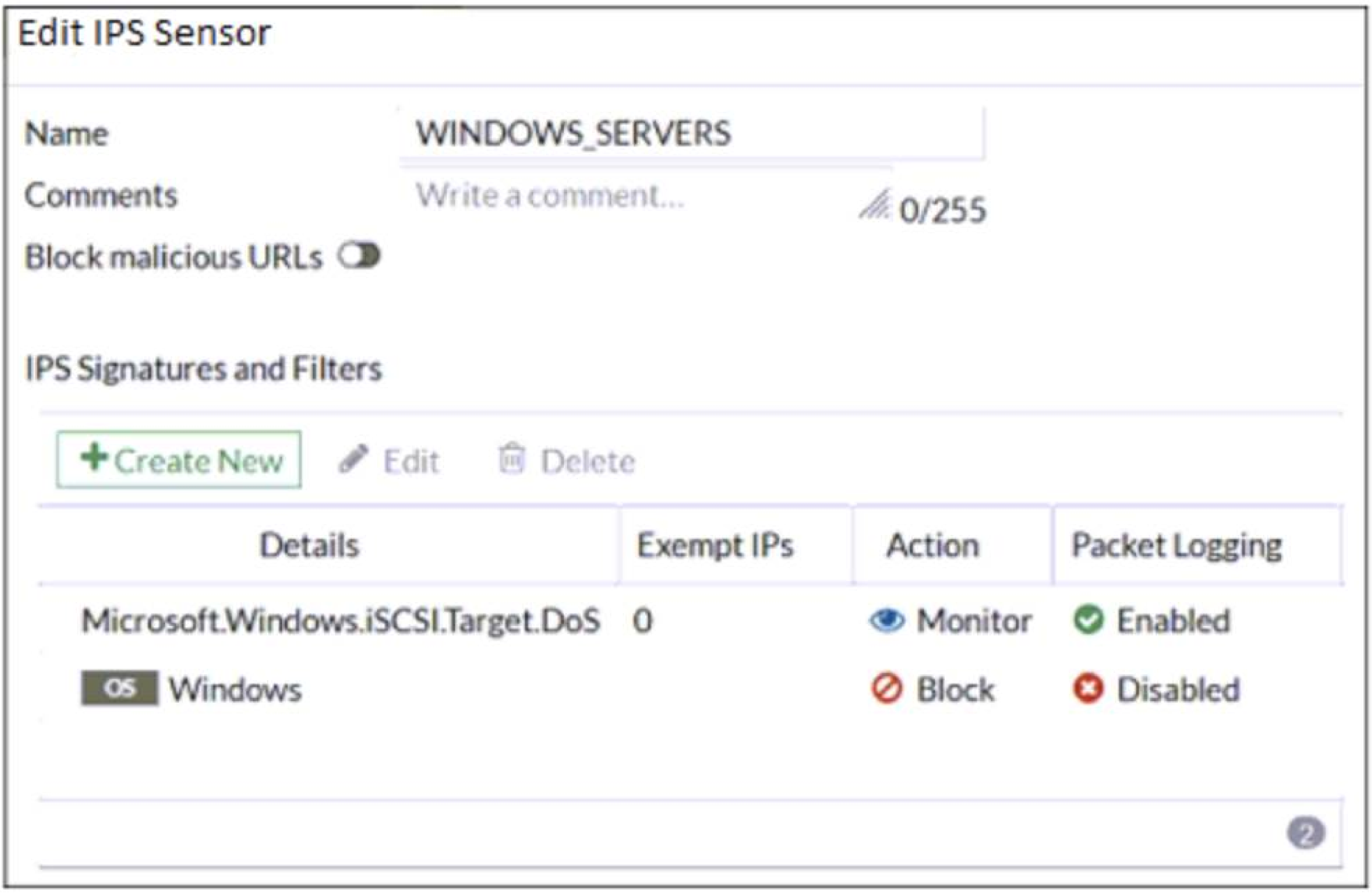
Fortinet

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

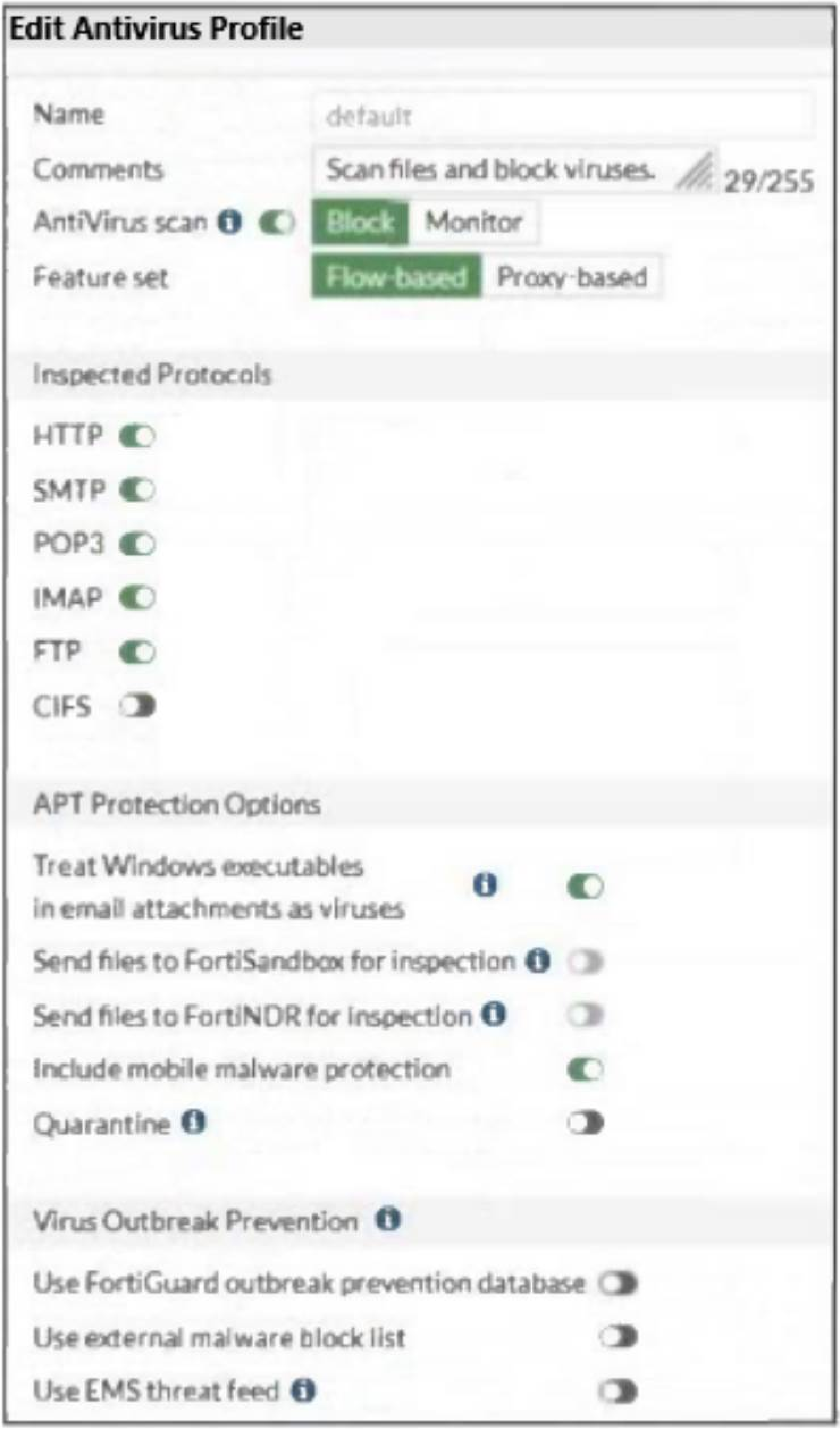
Explanation:
The IPS sensor configuration shows that:

- 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
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 ☑

SMTP ☑

POP3 ☑

IMAP ☑

FTP ☑

CIFS ☐

APT Protection Options

Treat Windows executables in email attachments as viruses ☑

Send files to FortiSandbox for inspection ☐

Send files to FortiNDR for inspection ☐

Include mobile malware protection ☑

Quarantine ☐

Virus Outbreak Prevention

Use FortiGuard outbreak prevention database ☐

Use external malware block list ☐

Use EMS threat feed ☐

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

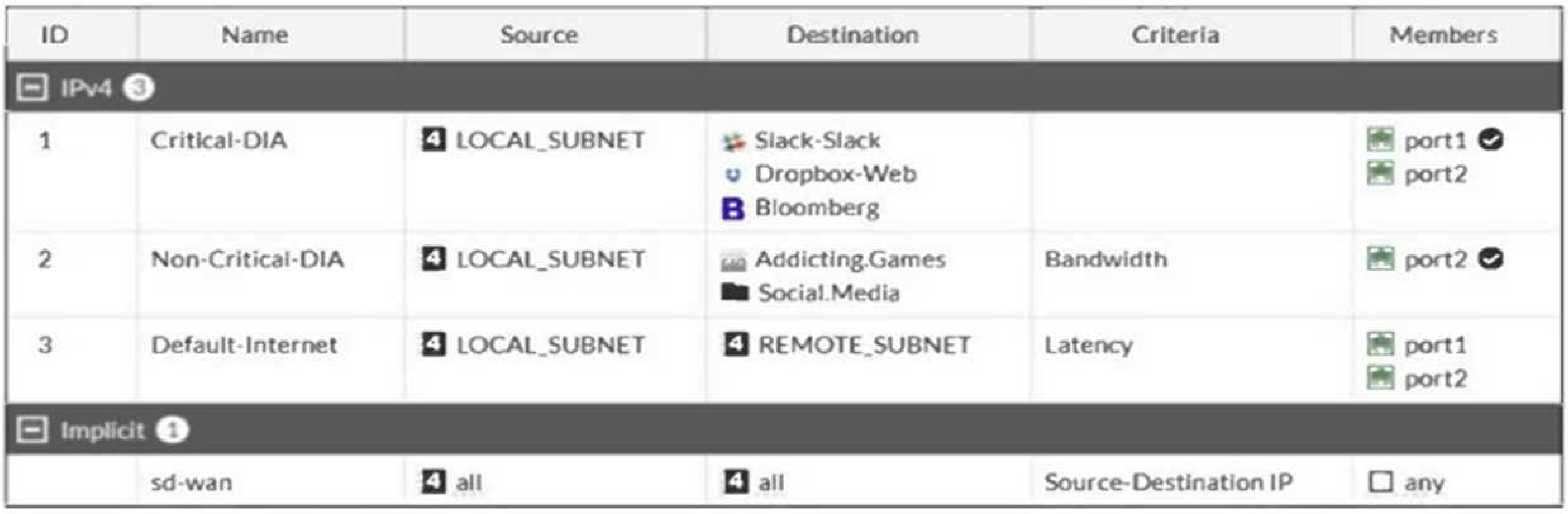
NEW QUESTION 4
What are two features of collector agent advanced mode? (Choose two.)

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

Answer: AD

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

NEW QUESTION 5
Refer to the exhibit.



ID	Name	Source	Destination	Criteria	Members
⊟ IPv4 3					
1	Critical-DIA	LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 ✓ port2
2	Non-Critical-DIA	LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2 ✓
3	Default-Internet	LOCAL_SUBNET	REMOTE_SUBNET	Latency	port1 port2
⊟ Implicit 1					
	sd-wan	all	all	Source-Destination IP	□ any

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

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

Answer: A

Explanation:
For traffic that does not match any of the defined SD-WAN rules, the default implicit SD-WAN rule is applied. By default, the FortiGate uses a "source-destination IP-based" algorithm, which means all traffic from a specific source IP to a specific destination IP is sent through the same interface. This ensures that a consistent

path is used for traffic between the same source and destination IP addresses. Options B, C, and D do not apply because the default algorithm does not prioritize by latency, session count, or source IP alone.
References:

- FortiOS 7.4.1 Administration Guide: SD-WAN Load Balancing Algorithms

NEW QUESTION 6
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 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?

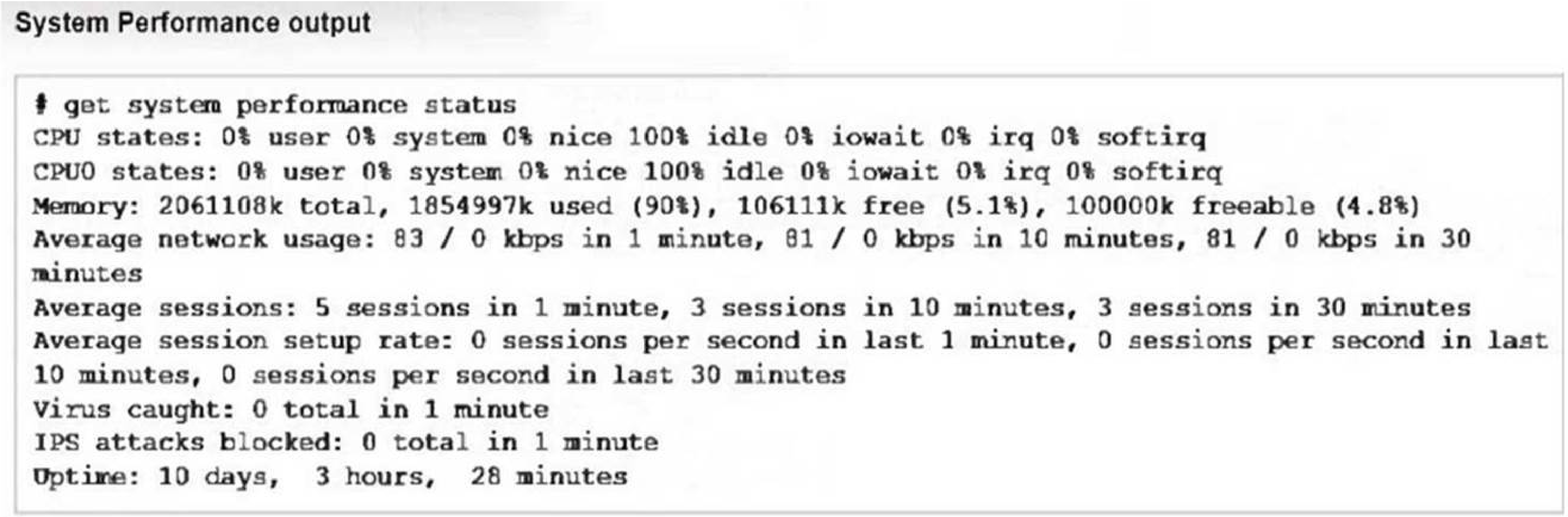
A. The SSL cipher compliance option is not enabled on the SSL inspection profil
B. This setting is required when the SSL inspection profile is defined with a private CA certificate.
C. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
D. The browser 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:

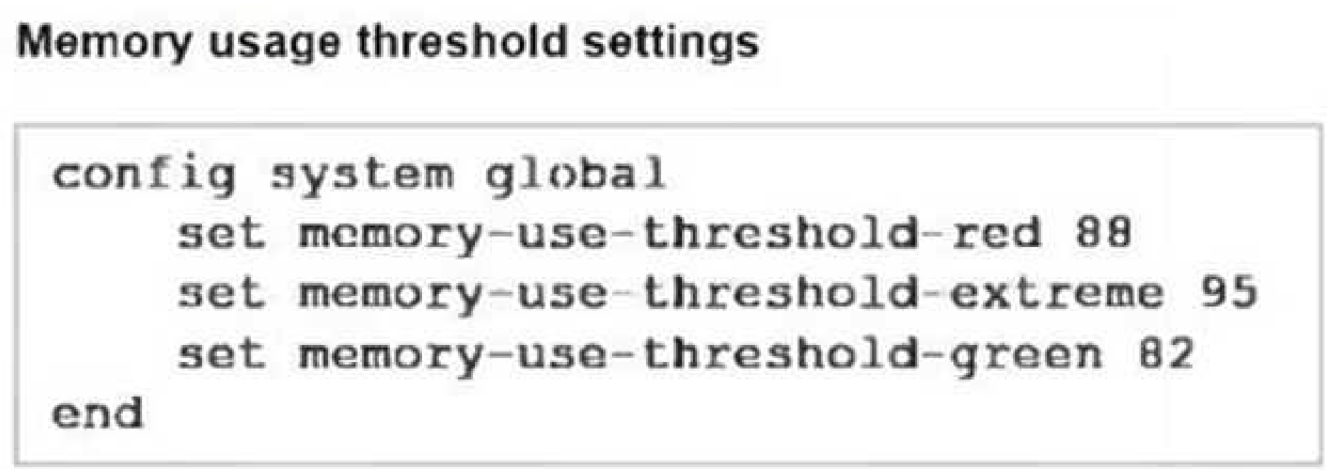
- FortiOS 7.4.1 Administration Guide: SSL/SSH Inspection Configuration

NEW QUESTION 8
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 9
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
All traffic must be routed through the primary tunnel when both tunnels are up. The secondary tunnel must be used only if the primary tunnel goes down. In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.
Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)

A. Enable Dead Peer Detection
B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

Answer: AC

Explanation:
To configure redundant IPsec VPN tunnels on FortiGate with failover capability, the following two key configuration changes are required:

- A. Enable Dead Peer Detection (DPD): Dead Peer Detection is crucial for detecting if the remote peer is unreachable. By enabling DPD, FortiGate can quickly detect a dead tunnel, ensuring a faster failover to the secondary tunnel when the primary tunnel goes down.

- C. Configure a lower distance on the static route for the primary tunnel and a higher distance on the static route for the secondary tunnel: The static route with the lower distance (higher priority) will be used when both tunnels are operational. If the primary tunnel fails, the higher distance (lower priority) route for the secondary tunnel will take over, ensuring traffic is routed correctly.

The other options are not suitable:

- B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels:

This option is not directly related to the requirements of failover between two IPsec VPN tunnels.

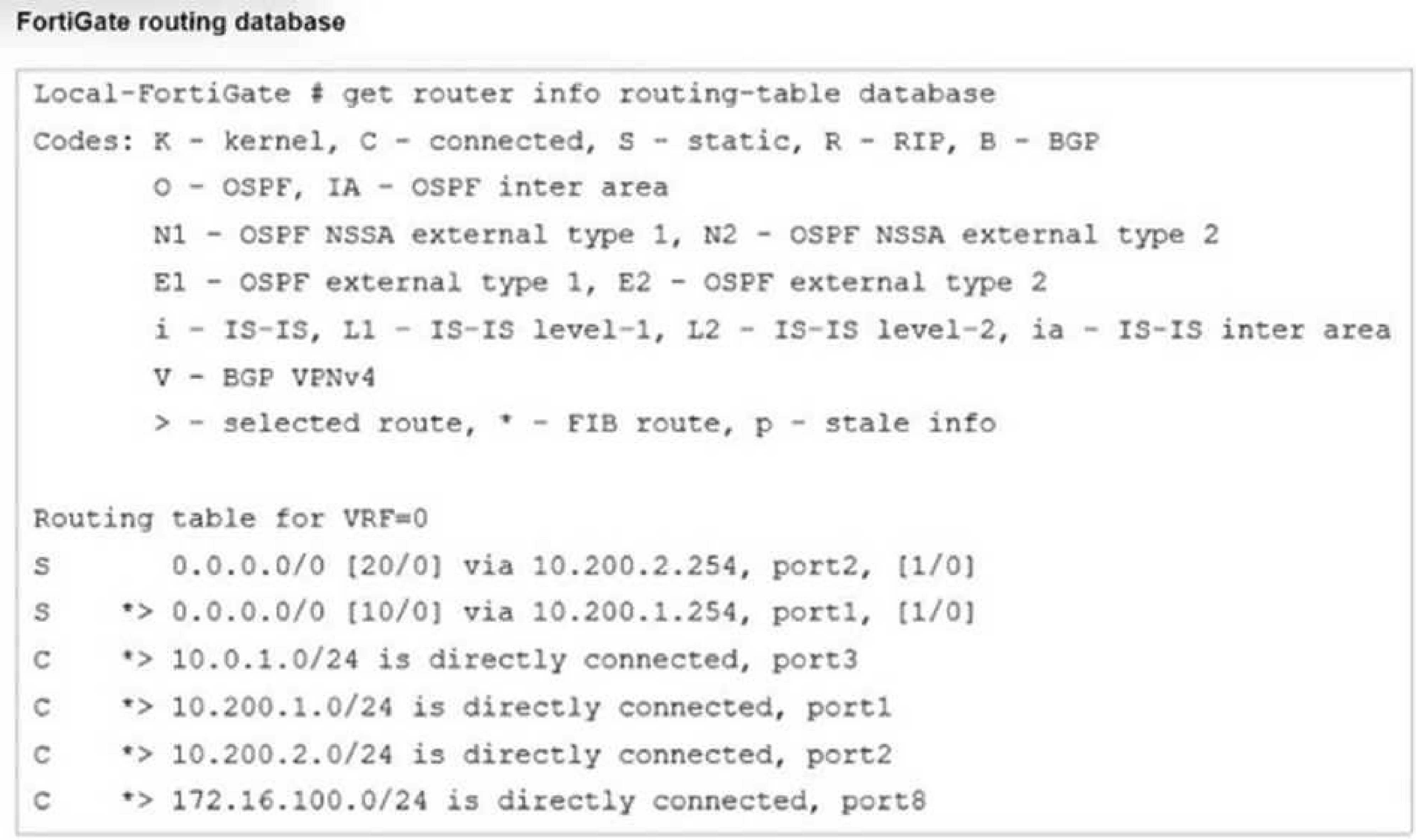
- D. Configure a higher distance on the static route for the primary tunnel and a lower distance on the static route for the secondary tunnel: This would prioritize the secondary tunnel over the primary tunnel, which is opposite to the desired configuration.

References

- FortiOS 7.4.1 Administration Guide - Configuring IPsec VPN, page 1320.
- FortiOS 7.4.1 Administration Guide - Redundant VPN Configuration, page 1335.

NEW QUESTION 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.

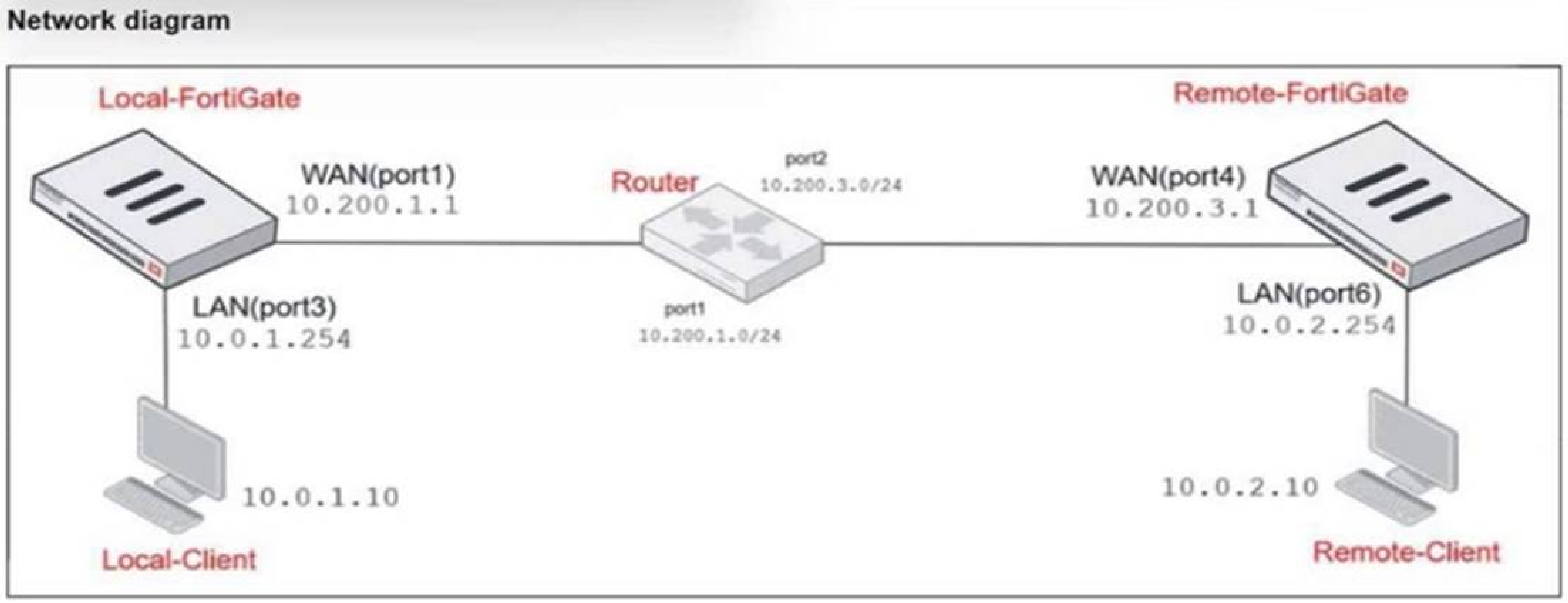
Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of 10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2.

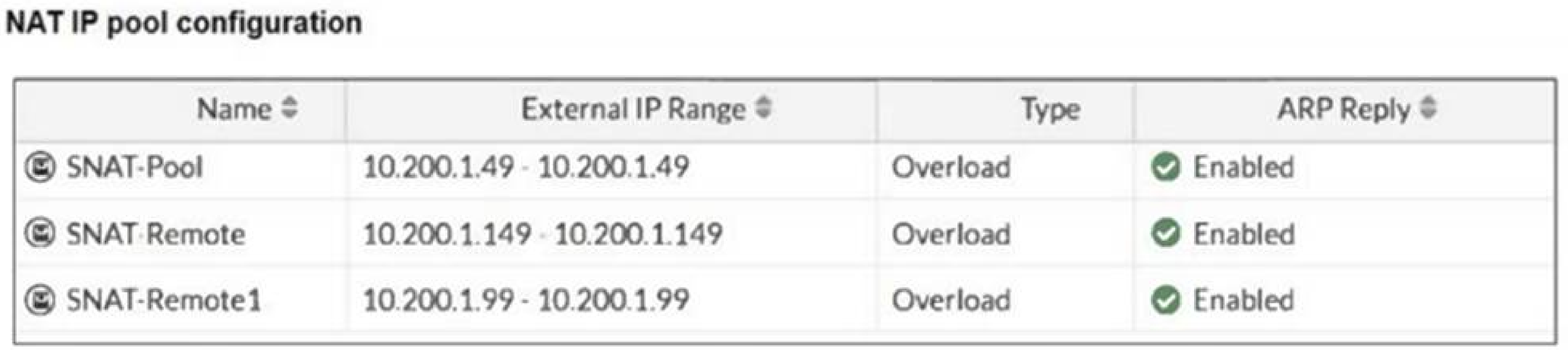
Regarding the statement that the port2 interface is marked as inactive, there is no indication in the routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.

References:

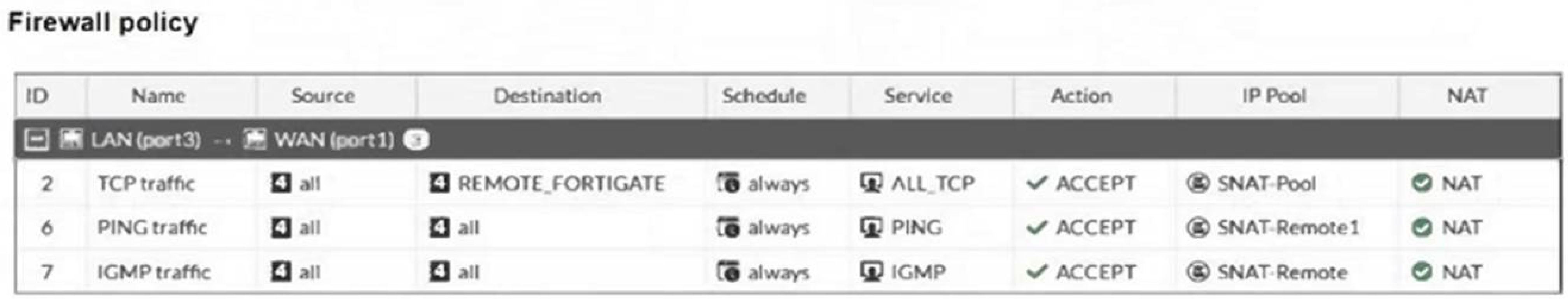
- FortiOS 7.4.1 Administration Guide: Default route configuration
- FortiOS 7.4.1 Administration Guide: Routing table

NEW QUESTION 10
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

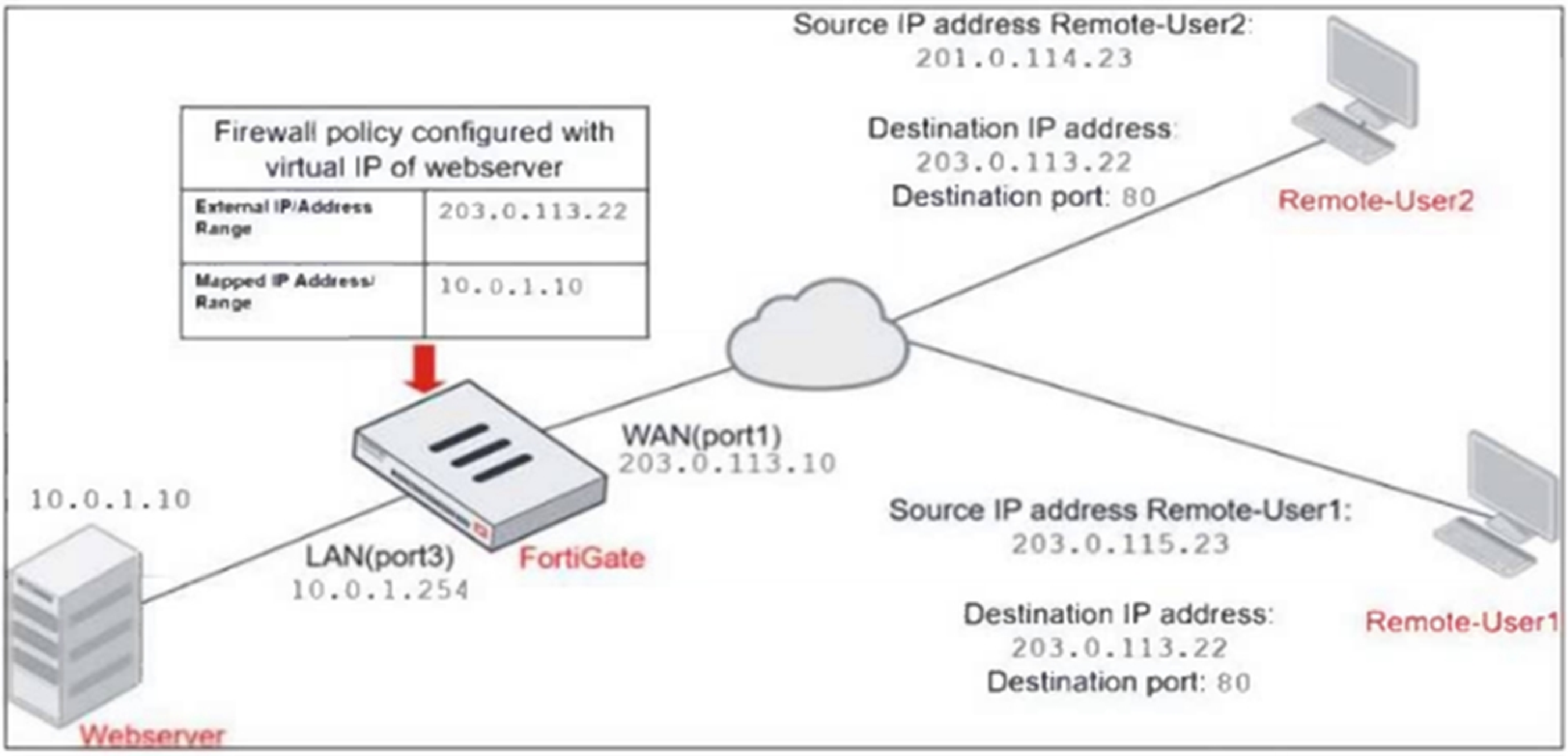
Answer: C

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 12
Refer to the exhibits.

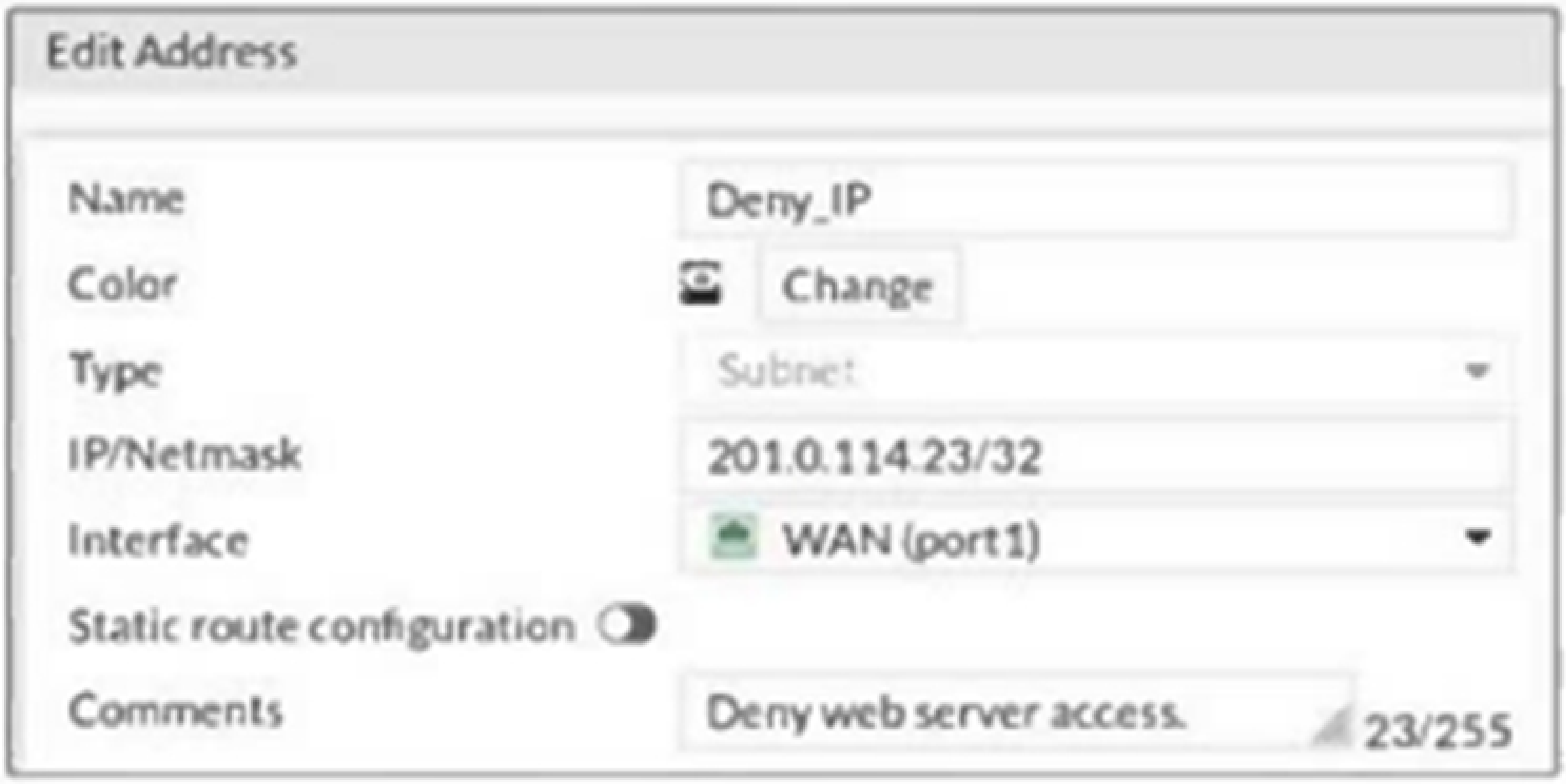
Network diagram



Firewall policy configured with virtual IP of webserver

External IP/Address Range	203.0.113.22
Mapped IP Address/ Range	10.0.1.10

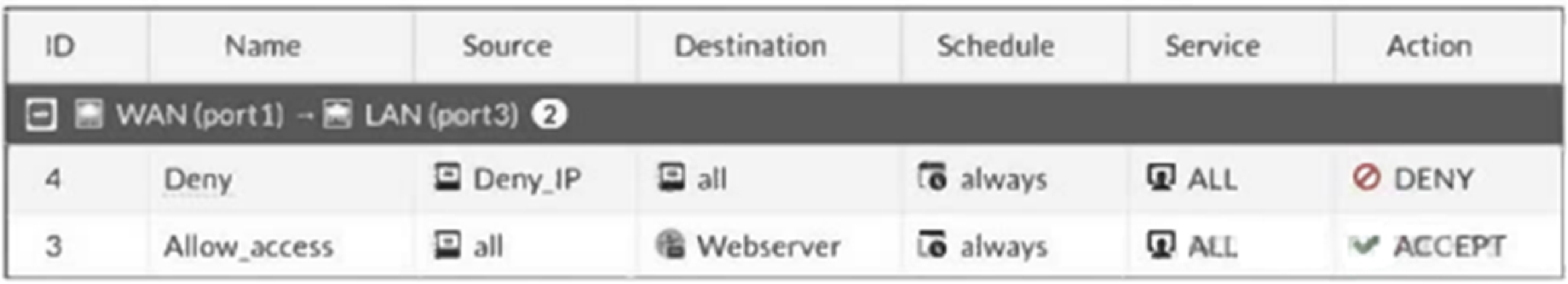
Firewall address object



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

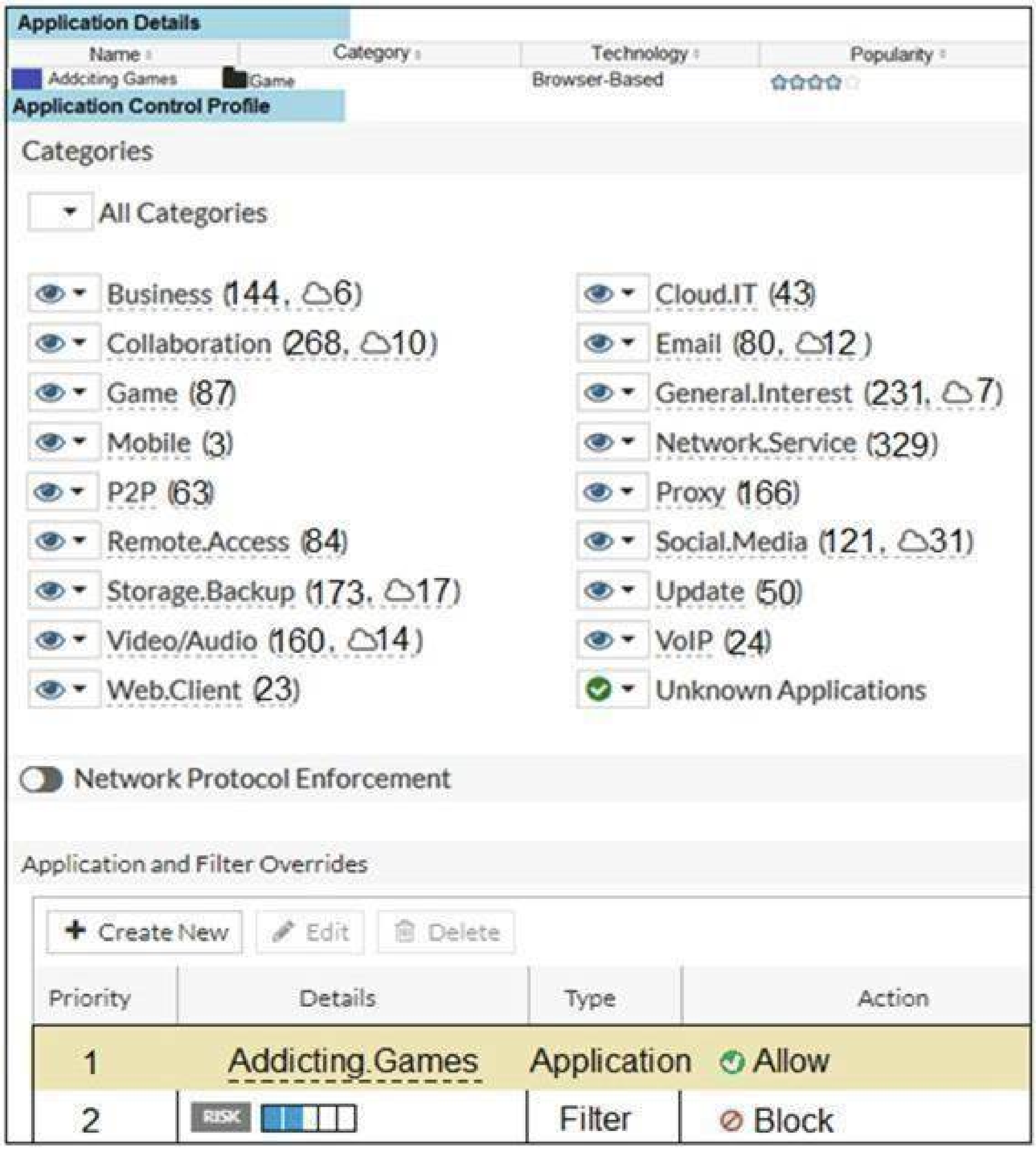
NEW QUESTION 15
Which of the following methods can be used to configure FortiGate to perform source NAT (SNAT) for outgoing traffic?

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 16
Refer to the exhibit.



Application Details

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

Application Control Profile

Categories

All Categories

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

Network Protocol Enforcement

Application and Filter Overrides

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

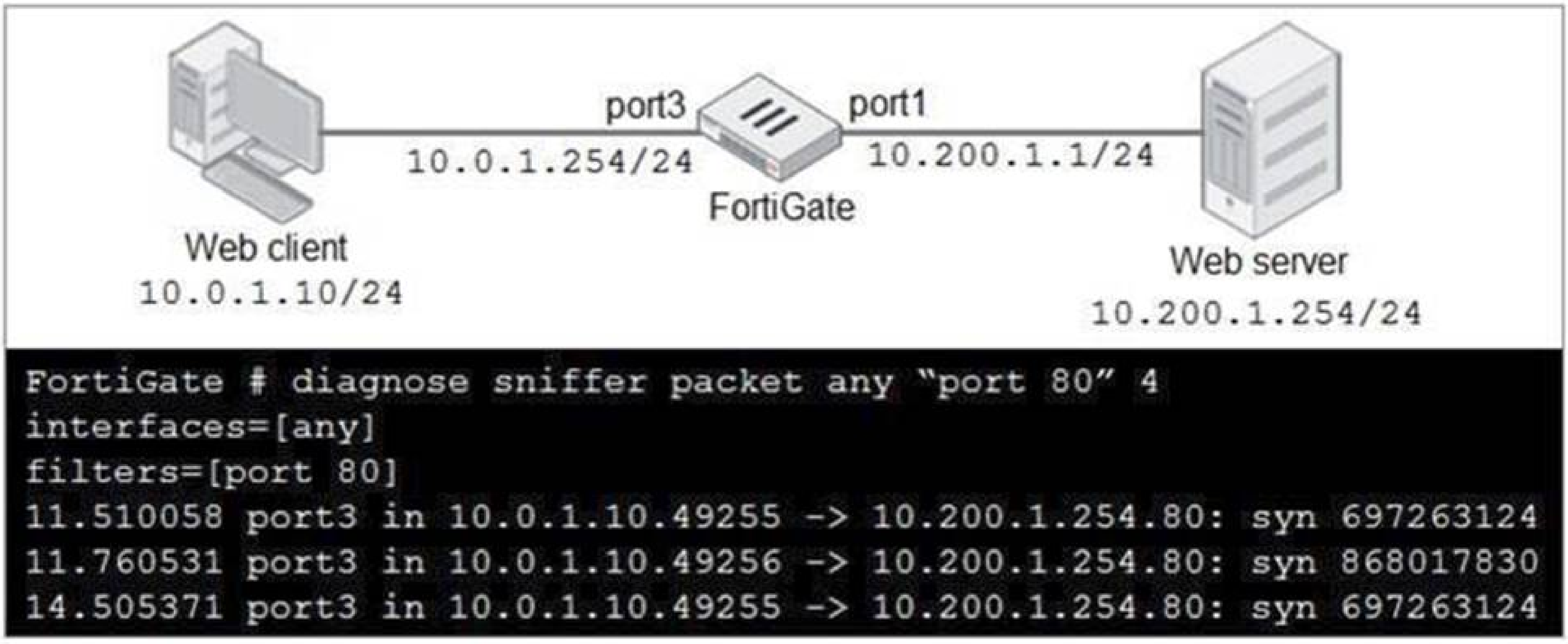
A user located behind the FortiGate device is trying to go to http://www.addictinggames.com (Addicting.Games). The exhibit shows the application detains and application control profile.
Based on this configuration, which statement is true?

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 19
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
```

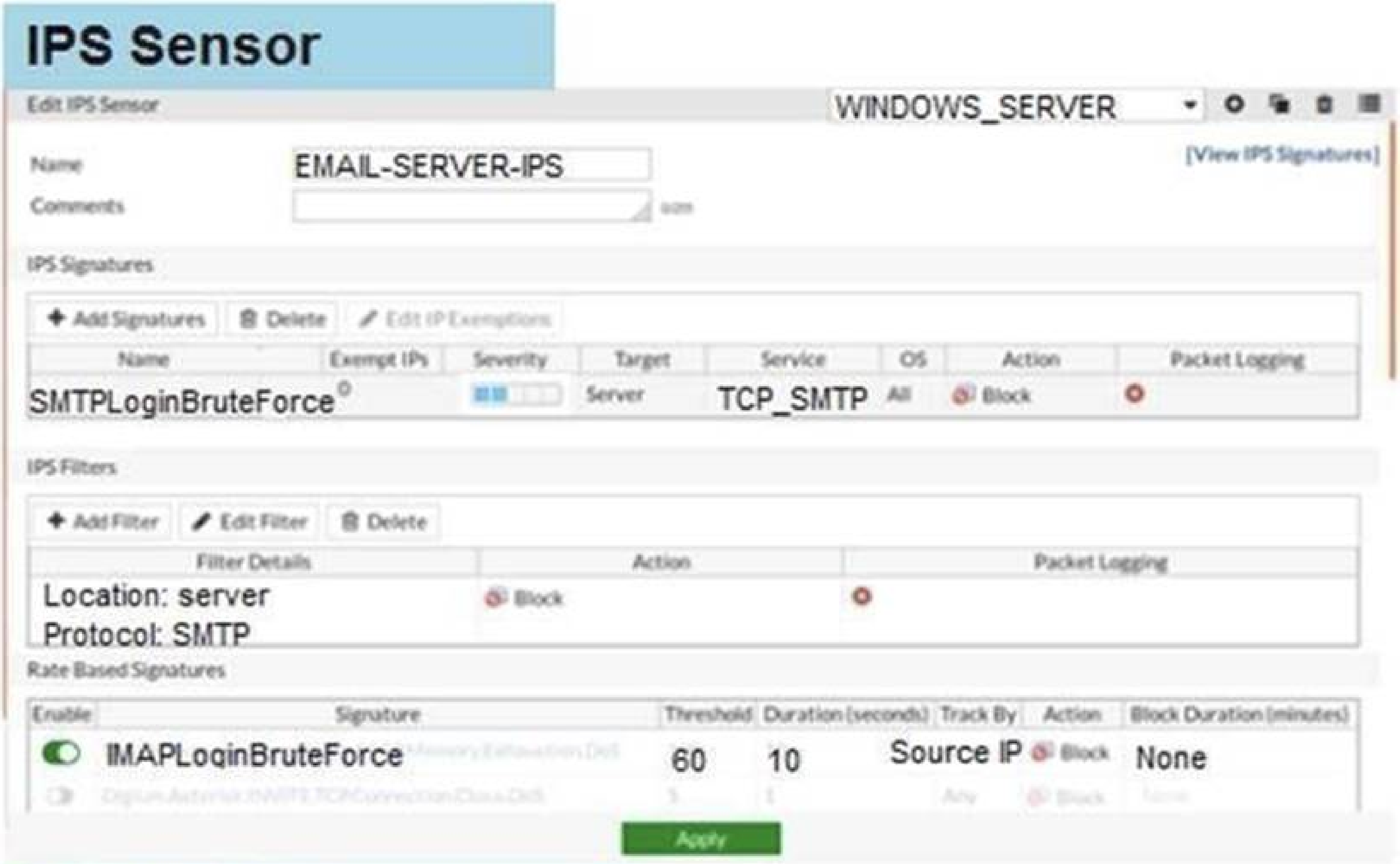
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

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 20
Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



IPS Sensor

Edit IPS Sensor — WINDOWS_SERVER

Name: EMAIL-SERVER-IPS

Comments: 0/255

IPS Signatures

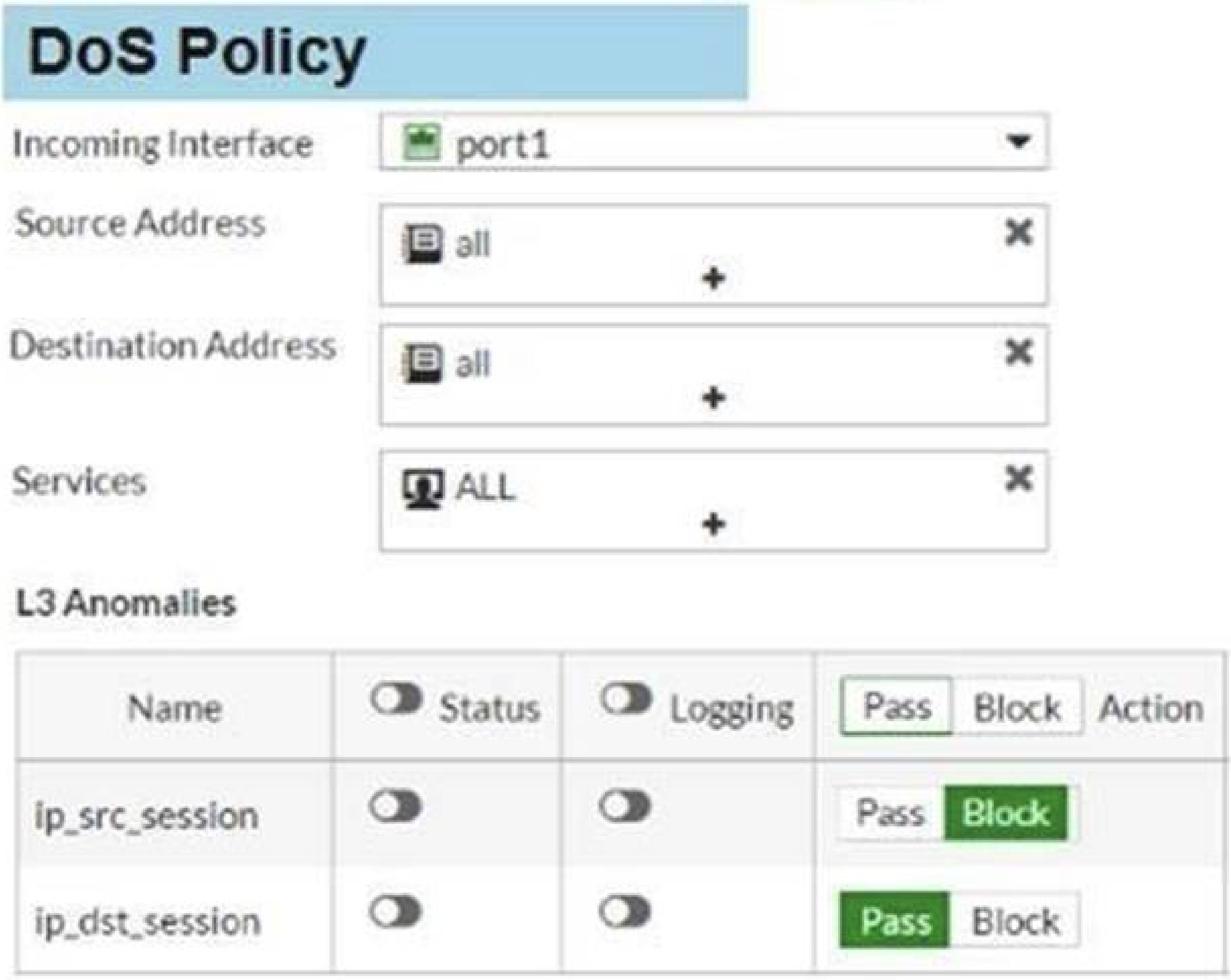
Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce	0	■■□□□	Server	TCP_SMTP	All	Block	●

IPS Filters

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	●

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
●	IMAPLoginBruteForce	60	10	Source IP	Block	None



DoS Policy

Incoming Interface: port1

Source Address: all

Destination Address: all

Services: ALL

L3 Anomalies

Name	Status	Logging	Action
ip_src_session	○	○	Pass [✓ Block]
ip_dst_session	○	○	[✓ Pass] Block

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

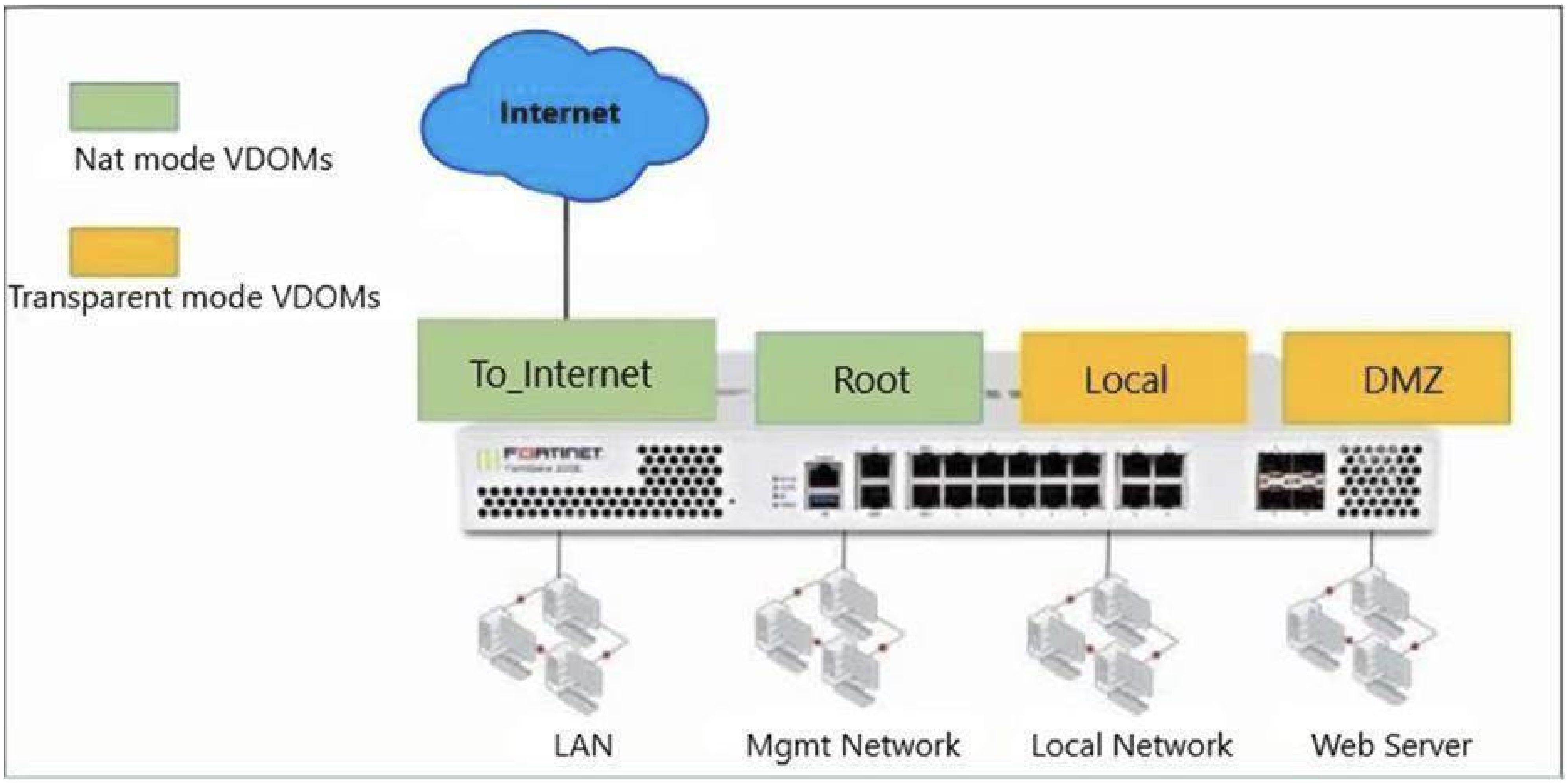
A. SMTP.Login.Brute.Force
B. IMAP.Login.brute.Force
C. ip_src_session
D. Location: server Protocol: SMTP

Answer: B

Explanation:
When FortiGate evaluates potential attacks, the IPS sensor follows a specific processing order based on the configuration of filters, signatures, and anomaly thresholds. In this case:
- The IPS sensor is configured with IMAP.Login.brute.Force, which comes first in the order of evaluation.
- FortiGate prioritizes based on signature definitions in the sensor, and since IMAP.Login.brute.Force appears higher in the configuration, it will be evaluated before the other signatures and anomalies.

Why the other options are less appropriate:
- A. SMTP.Login.Brute.Force: This would be evaluated after IMAP.Login.brute.Force, based on the sensor configuration hierarchy.
- C. ip_src_session: This is part of the DoS policy and does not come into play until after IPS signatures are evaluated.
- D. Location: server Protocol: SMTP: This appears to be part of the broader IPS sensor rule, but it is not the first item in the evaluation chain.

NEW QUESTION 22
Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
B. A default static route is not required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

Explanation:
In this scenario, multiple Virtual Domains (VDOMs) are used, and each VDOM operates either in NAT mode or transparent mode:
- Root VDOM (management) and To_Internet VDOM are in NAT mode.
- DMZ VDOM and Local VDOM are in transparent mode.

To allow traffic between different VDOMs (e.g., Local and Root), inter-VDOM links must be configured.
Since Local VDOM is in transparent mode, it functions at Layer 2, meaning it requires an inter-VDOM link to pass traffic through the Root VDOM, which operates in NAT mode at Layer 3.
Why the other options are less appropriate:
- B. A default static route is not required on the To_Internet VDOM:

A default route is required on the To_Internet VDOM to send traffic from LAN users to the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs:

Both Local and DMZ are in transparent mode and operate at Layer 2, so direct communication would require inter-VDOM links if passing through another VDOM.
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs:

Even if the Root VDOM is only used for management, it still requires inter-VDOM links to communicate with other VDOMs (like To_Internet) in the Security Fabric.

NEW QUESTION 27
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 30

......