Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

NEW QUESTION 1
Refer to the exhibit.

```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.
0"
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw-10.200.1.254
via port1"
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (policy 0)"
```

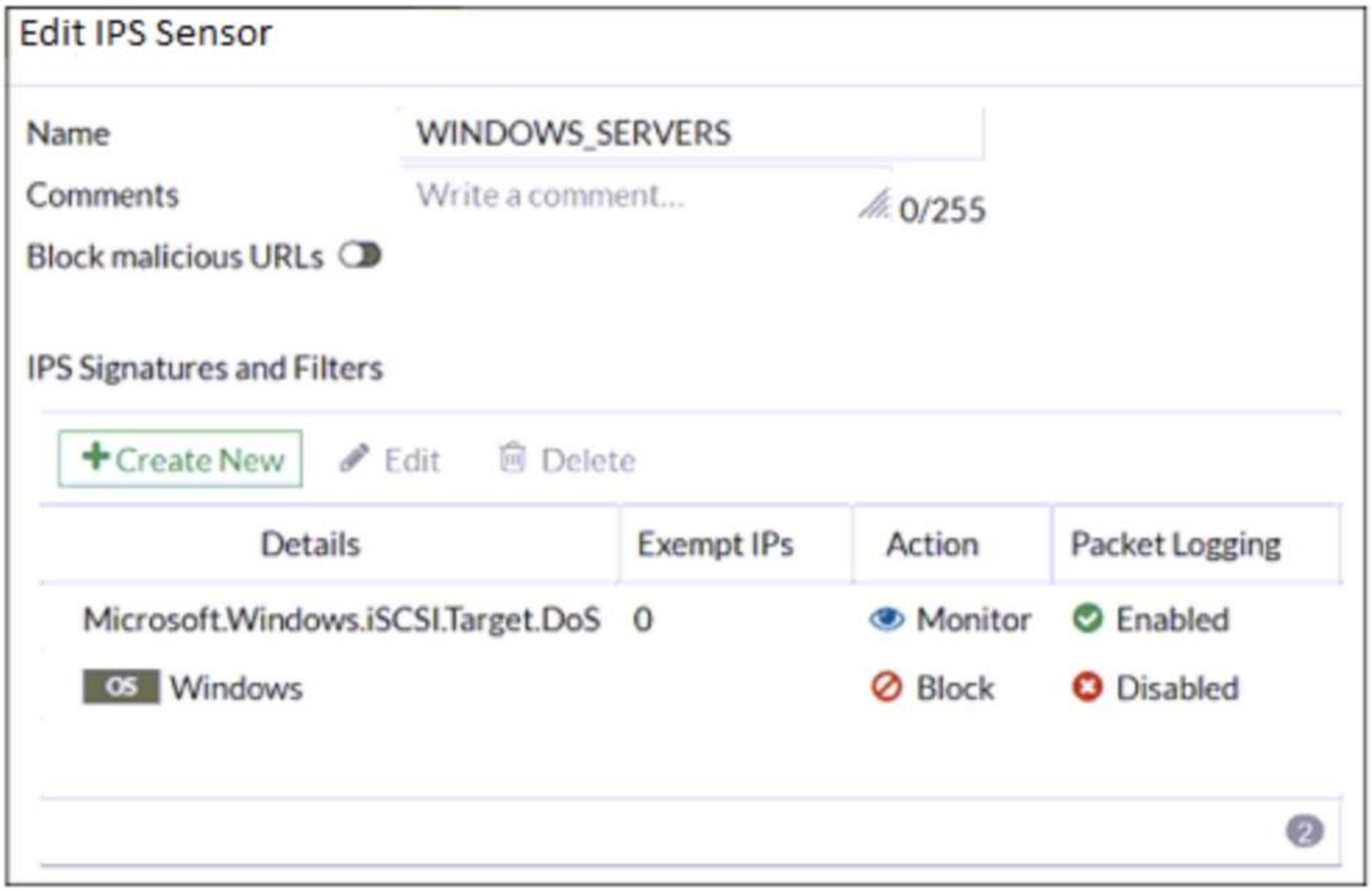
Why did FortiGate drop the packet?

A. It matched an explicitly configured firewall policy with the action DENY
B. It failed the RPF check.
C. The next-hop IP address is unreachable.
D. It matched the default implicit firewall policy

Answer: D

Explanation:
The debug trace output shows that the packet was "Denied by forward policy check (policy 0)." In FortiGate, policy ID 0 corresponds to the default implicit deny policy. This means that if a packet does not match any configured firewall policies, it is denied by the default implicit policy.
References:
FortiOS 7.4.1 Administration Guide: Firewall Policies

NEW QUESTION 2
Refer to the exhibit, which shows the IPS sensor configuration.



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 3
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 4
Which three methods are used by the collector agent for AD polling? (Choose three.)

A. WinSecLog
B. WMI
C. NetAPI
D. FSSO REST API
E. FortiGate polling

Answer: ABC

Explanation:
The Fortinet Single Sign-On (FSSO) Collector Agent supports three primary methods for Active Directory (AD) polling to collect user information:

WinSecLog: Monitors Windows Security Event Logs for login events.

WMI: Uses Windows Management Instrumentation to poll user login sessions.

NetAPI: Utilizes the Netlogon API to query domain controllers for user session data.
These methods allow the FortiGate to gather user logon information and enforce user-based policies effectively.
References:

FortiOS 7.4.1 Administration Guide: FSSO Configuration

NEW QUESTION 5
Which 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 6
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 7
Refer to the exhibit.

Review the intrusion prevention system (IPS) profile signature settings shown in the exhibit. What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

A. Traffic matching the signature will be allowed and logged.
B. The signature setting uses a custom rating threshold.
C. The signature setting includes a group of other signatures.
D. Traffic matching the signature will be silently dropped and logged.

Answer: A

Explanation:
The exhibit shows that the "FTP.Login.Failed" IPS signature is set with the action "Pass" and packet logging enabled. This means that any traffic matching this signature will be allowed through the FortiGate, and the traffic details will be logged for monitoring and analysis purposes.
References:
FortiOS 7.4.1 Administration Guide: IPS Signature Actions

NEW QUESTION 8
FortiGate is integrated with FortiAnalyzer and FortiManager.
When a firewall policy is created, which attribute is added to the policy to improve functionality and to support recording logs to FortiAnalyzer or FortiManager?

A. Log ID
B. Policy ID
C. (Sequence ID
D. Universally Unique Identifier

Answer: D

Explanation:
When a firewall policy is created in FortiGate integrated with FortiAnalyzer and FortiManager, a Universally Unique Identifier (UUID) is added to the policy to support logging and management.

NEW QUESTION 9
Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

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

Answer: AB

Explanation:

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

FortiOS 7.4.1 Administration Guide: HA Configuration Synchronization

NEW QUESTION 10
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 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 15
Which statement is a characteristic of automation stitches?

A. They can be run only on devices in the Security Fabric.
B. They can be created only on downstream devices in the fabric.
C. They can have one or more triggers.
D. They can run multiple actions at the same time.

Answer: C

Explanation:
Automation stitches on FortiGate can have one or more triggers, which are conditions or events that activate the automation stitch. The trigger defines when the automation stitch should execute the defined actions. Actions within a stitch can be executed sequentially or in parallel, depending on the configuration.
References:

FortiOS 7.4.1 Administration Guide: Automation Stitches

NEW QUESTION 18
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:

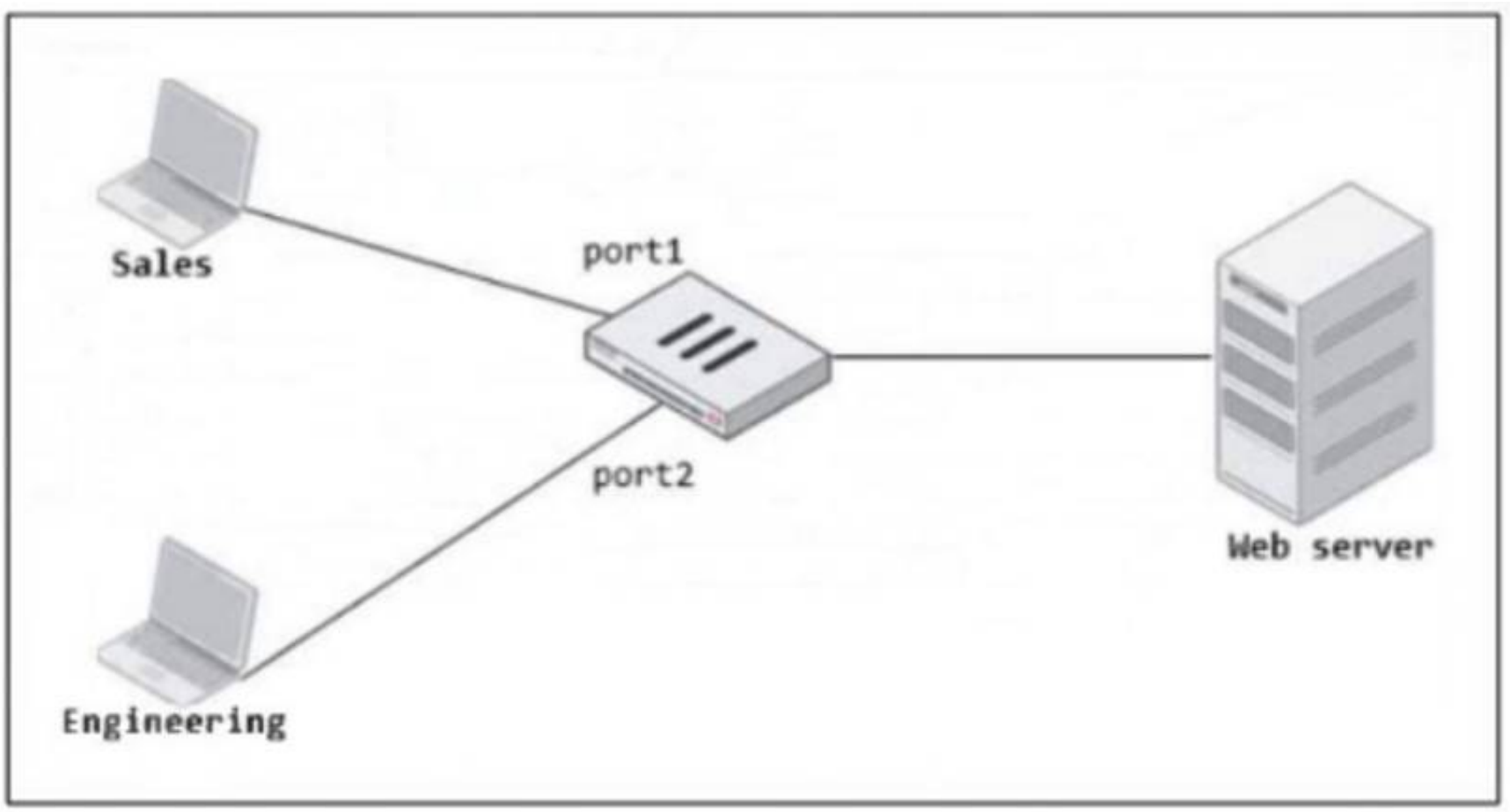
A. FortiGate will start sending all files to FortiSandbox for inspection: This is unrelated to memory usage and conserve mode.

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 20
Refer to the exhibit.



FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.
Which action must the administrator perform to consolidate the two policies into one?

A. Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy
B. Create an Interface Group that includes port1 and port2 to create a single firewall policy
C. Select port1 and port2 subnets in a single firewall policy.
D. Replace port1 and port2 with the any interface in a single firewall policy.

Answer: B

Explanation:
To consolidate the two separate firewall policies for Sales and Engineering departments accessing the same web server, you can create an Interface Group that includes both port1 (Sales) and port2 (Engineering). Once the Interface Group is created, you can use this group as a single incoming interface in a single firewall policy. This approach reduces the number of policies, making management more efficient.
References:

FortiOS 7.4.1 Administration Guide: Firewall Policy Configuration

NEW QUESTION 21
Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three.)

A. Manual with load balancing
B. Lowest Cost (SLA) with load balancing
C. Best Quality with load balancing
D. Lowest Quality (SLA) with load balancing
E. Lowest Cost (SLA) without load balancing

Answer: ABC

Explanation:
FortiGate's SD-WAN rule strategies for member selection include the following:

Manual with load balancing: This strategy allows an administrator to manually configure which SD- WAN member interfaces to use for specific traffic.

Lowest Cost (SLA) with load balancing: This strategy prioritizes the link with the lowest cost that meets the SLA requirements.

Best Quality with load balancing: This strategy selects the link with the best performance metrics, such as latency, jitter, or packet loss.

Options D and E are incorrect because "Lowest Quality" is not a valid strategy, and "Lowest Cost without load balancing" contradicts the requirement for load balancing in the strategy name.
References:

FortiOS 7.4.1 Administration Guide: SD-WAN Rule Strategies

NEW QUESTION 25
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 30
Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

A. Pre-shared key and certificate signature as authentication methods
B. Extended authentication (XAuth)to request the remote peer to provide a username and password
C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
D. No certificate is required on the remote peer when you set the certificate signature as the authentication method

Answer: AB

Explanation:
FortiGate supports both pre-shared key and certificate signature methods for IKEv1 authentication. These methods provide flexibility depending on the security requirements of the network. Additionally, FortiGate supports Extended Authentication (XAuth), which requests a username and password from the remote peer, enhancing security by adding an extra layer of authentication. The XAuth method does not necessarily make the authentication faster; it is an additional security measure.
References:

FortiOS 7.4.1 Administration Guide: IPsec VPN Configuration

NEW QUESTION 35
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?

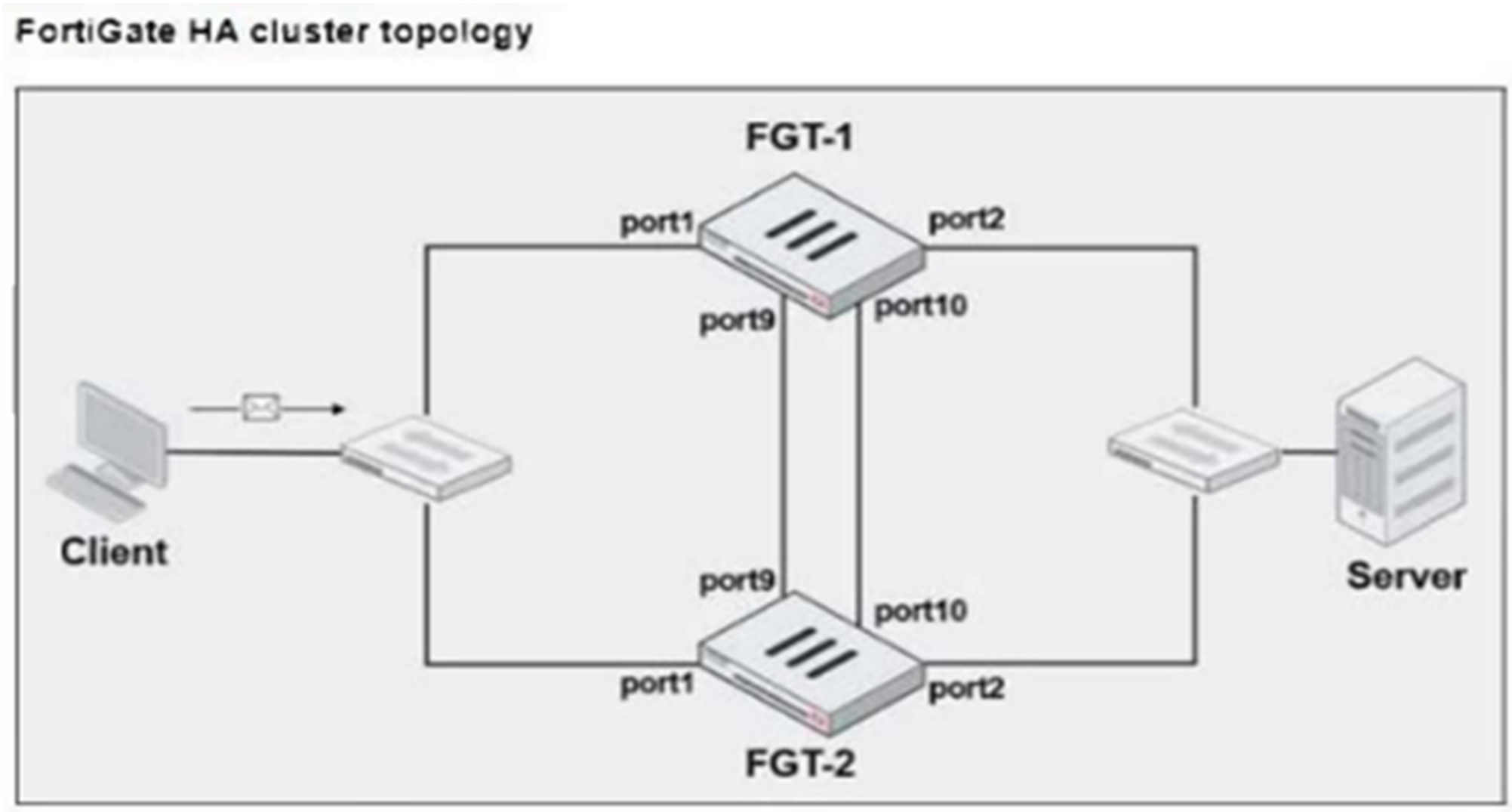
A. The Implicit group can include more than one deny firewall policy.
B. The firewall policies are listed by ID sequence view.
C. The firewall policies are listed by ingress and egress interfaces pairing view.
D. LAN to WA
E. WAN to LA
F. and Implicit are sequence grouping view lists.

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 36
Refer to the exhibits.



Current HA status

```
# get system ha status
...
Configuration Status:
    FGVM010000064692(updated 4 seconds ago): in-sync
    FGVM010000064692 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
    FGVM010000065036(updated 4 seconds ago): in-sync
    FGVM010000065036 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary     : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary   : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

New FortiGate HA configuration

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

FGT-2
#config system ha
     set group-id 3
     set group-name "Fortinet"
     set mode a-p
     set password *
     set hbdev "port9" 50 "port10" 50
     set session-pickup enable
     set override enable
     set priority 110
     set monitor port3
```

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

A. FGT-1 will remain the primary because FGT-2 has lower priority.
B. FGT-2 will take over as the primary because it has the override enable setting and higher priority than FGT-1.
C. FGT-1 will synchronize the override disable setting with FGT-2.
D. The HA cluster will become out of sync because the override setting must match on all HA members.

Answer: B

NEW QUESTION 38
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration

Based on the exhibit, which statement is true?

A. The underlay zone contains port1 and
B. The d-wan zone contains no member.
C. The d-wan zone cannot be deleted.
D. The virtual-wan-link zone contains no member.

Answer: C

Explanation:
In FortiGate's SD-WAN configuration, the d-wan zone is a system default SD-WAN zone that is automatically created and cannot be deleted. This zone is used to manage dynamic WAN links for SD-WAN
traffic balancing and routing. It ensures that multiple WAN interfaces can be grouped and managed
effectively for WAN link optimization.
Why the other options are less appropriate:
• A. The underlay zone contains port1 and: There is no mention in the exhibit about an "underlay zone" containing port1.
• B. The d-wan zone contains no member: This statement is irrelevant since the focus is on the zone's deletion, not its members.
• D. The virtual-wan-link zone contains no member: This is unrelated to the core fact that the d-wan zone cannot be deleted.
Reference:
FortiOS 7.4.1 Administration Guide: SD-WAN Zone Configuration

NEW QUESTION 40
Which of the following methods can be used to configure FortiGate to perform source NAT (SNAT) for outgoing traffic?

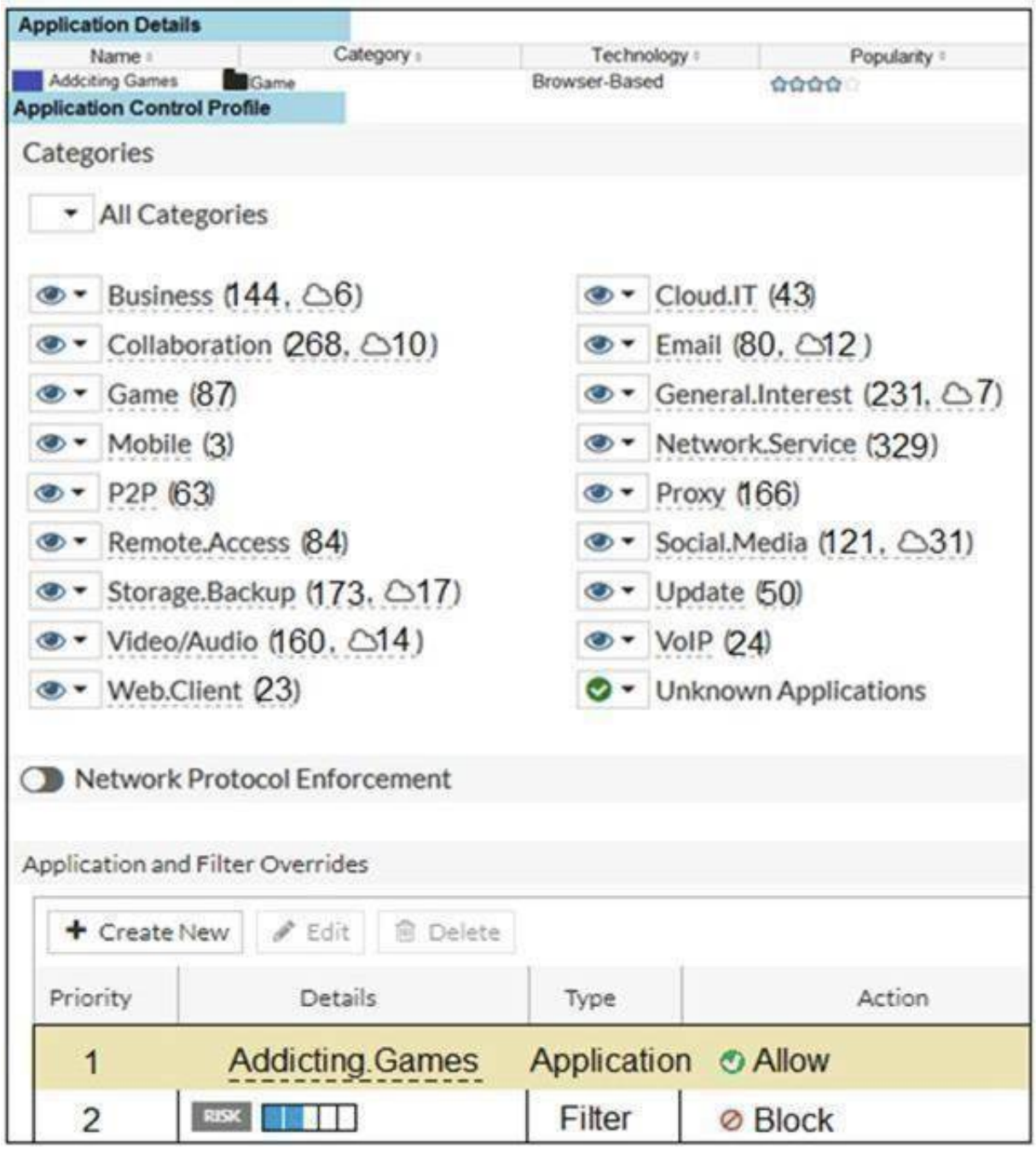
A. Configure a static route pointing to the external interface.
B. Enable the "Use Outgoing Interface Address" option in a firewall policy.
C. Create a virtual server with an external IP address.
D. Deploy an IPsec VPN tunnel with NAT enabled.

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 43
Refer to the exhibit.



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 44
Refer to the exhibit.

In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output 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 45
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 48
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FGT_AD-7.4 Practice Exam Features:

* FCP_FGT_AD-7.4 Questions and Answers Updated Frequently

* FCP_FGT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FGT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FGT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year