Fortinet

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

NEW QUESTION 1
What is the primary FortiGate election process when the HA override setting is enabled?

A. Connected monitored ports > Priority > HA uptime > FortiGate serial number
B. Connected monitored ports > Priority > System uptime > FortiGate serial number
C. Connected monitored ports > HA uptime > Priority > FortiGate serial number
D. Connected monitored ports > System uptime > Priority > FortiGate serial number

Answer: A

Explanation:
When HA override is enabled, FortiGate uses the following election order: number of connected monitored ports, then device priority, followed by HA uptime, and finally FortiGate serial number as a tiebreaker.

NEW QUESTION 2
You are analyzing connectivity problems caused by intermediate devices blocking traffic in SSL VPN environment.
In which two ways can you effectively resolve the problem? (Choose two.)

A. You can turn off IKE fragmentation to fix large certificate negotiation problems.
B. You should use IPsec to solve issues with fragment drops and large certificate exchanges.
C. You can use SSL VPN tunnel mode to prevent problems with blocked ESP and UDP ports (500 or 4500).
D. You can configure a hub-and-spoke topology with SSL VPN tunnels to bypass blocked UDP ports.

Answer: AC

Explanation:
Disabling IKE fragmentation helps resolve issues caused by intermediate devices blocking large fragmented packets during certificate negotiation.
Using SSL VPN tunnel mode encapsulates traffic over HTTPS, bypassing blocks on ESP and UDP ports commonly used by IPsec.

NEW QUESTION 3
You have configured the FortiGate device for FSSO. A user is successful in log-in to windows, but their access to the internet is denied.
What should the administrator check first?

A. Whether the user is assigned to the correct AD group.
B. The FortiGate firewall policy settings for SSL decryption.
C. The FortiGate FSSO active users list for user??s IP address.
D. The windows event viewer for failed login attempts.

Answer: C

Explanation:
Checking the active users list verifies if FortiGate correctly associates the user with their IP address, ensuring proper policy enforcement for internet access.

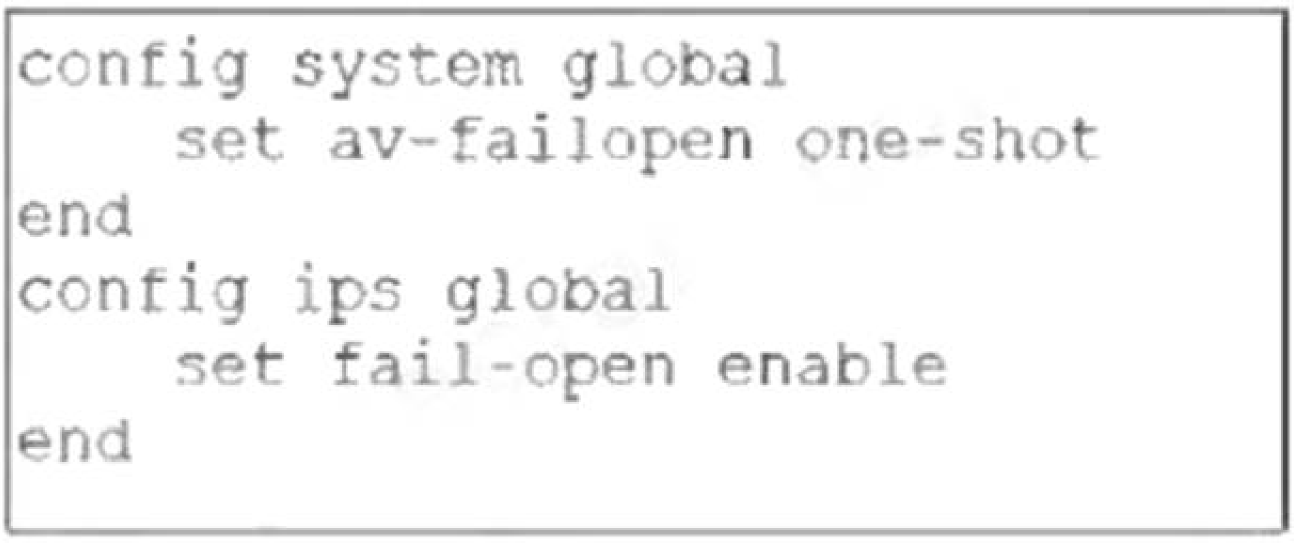
NEW QUESTION 4
A remote user reports slow SSL VPN performance and frequent disconnections. The user is located in an area with poor internet connectivity.
What setting should the administrator adjust to improve the user's experience?

A. Enable split tunneling to reduce VPN traffic.
B. Change the SSL VPN port to a non-standard port.
C. Increase the session timeout for inactive sessions.
D. Configure the DTLS timeout to accommodate high-latency connections.

Answer: D

Explanation:
Adjusting the DTLS timeout helps maintain SSL VPN stability and performance in environments with poor or high-latency internet connectivity by allowing more time for packet retransmissions before dropping the connection.

NEW QUESTION 5
Refer to the exhibit.



```
config system global
    set av-failopen one-shot
end
config ips global
    set fail-open enable
end
```

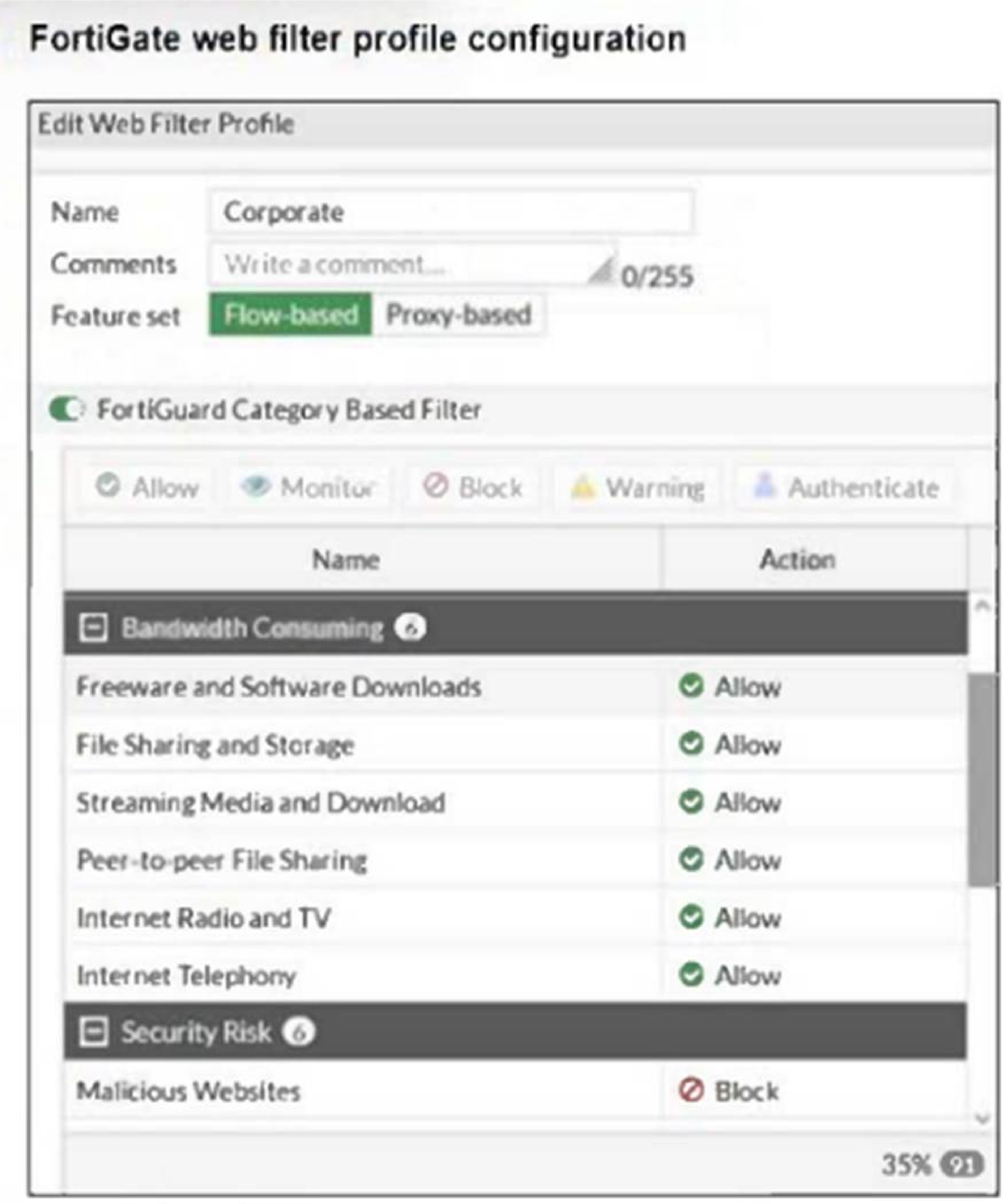
Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

A. Administrators cannot change the configuration.
B. FortiGate skips quarantine actions.
C. Administrators must restart FortiGate to allow new session.
D. FortiGate drops new sessions requiring inspection.

Answer: BD

Explanation:
In fail-open mode, FortiGate skips quarantine actions to maintain traffic flow despite IPS or antivirus failures. FortiGate drops new sessions that require inspection when in conserve mode and fail-open is enabled, to
protect the network from potentially harmful traffic.

NEW QUESTION 6
Refer to the exhibit.



FortiGate web filter profile configuration

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 theFortiGuard Category Based Filtersection of a corporate web filter profile.
An administrator must block access todownload.com, which belongs to theFreeware and Software Downloadscategory. The administrator must also allow other websites in the same category.
What are two solutions for satisfying the requirement? (Choose two.)

A. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.
B. Configure a web override rating for download.com and select Malicious Websites as the subcategory.
C. Configure a separate firewall policy with action Deny and an FQDN address object for*.download.com as destination address.
D. Set the Freeware and Software Downloads category Action to Warning.

Answer: AC

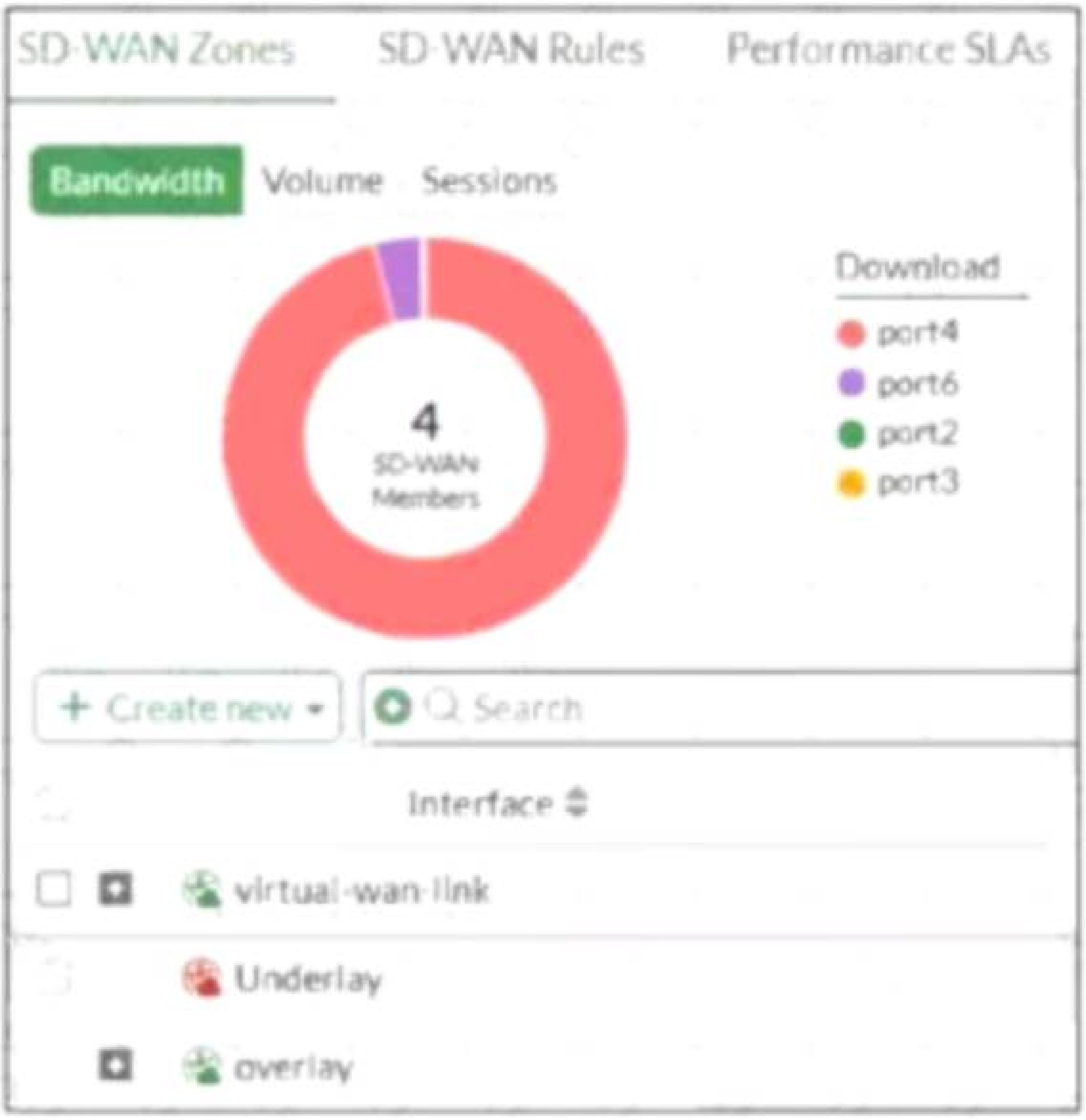
Explanation:
Creating a static URL filter to block download.com specifically allows blocking that site without affecting the entire category.
Using a separate firewall policy with a Deny action for an FQDN address object matching download.com can also block the site while allowing others in the same category.

NEW QUESTION 7
A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy.
When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded.
The administrator confirms that the traffic matches the configured firewall policy. What are two reasons for the failed virus detection by FortiGate? (Choose two.)

A. The selected SSL inspection profile has certificate inspection enabled.
B. The website is exempted from SSL inspection.
C. The El CAR test file exceeds the protocol options oversize limit.
D. The browser does not trust the FortiGate self-signed CA certificate.

Answer: BD

NEW QUESTION 8
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



Based on the exhibit, which statement is true?

A. The Underlay zone is the zone by default.
B. The Underlay zone contains no member.
C. port2 and port3 are not assigned to a zone.
D. The virtual-wan-link and overlay zones can be deleted.

Answer: A

Explanation:
The Underlay zone is the default SD-WAN zone, typically representing the physical interfaces in the SD- WAN configuration before overlay or virtual links are added.

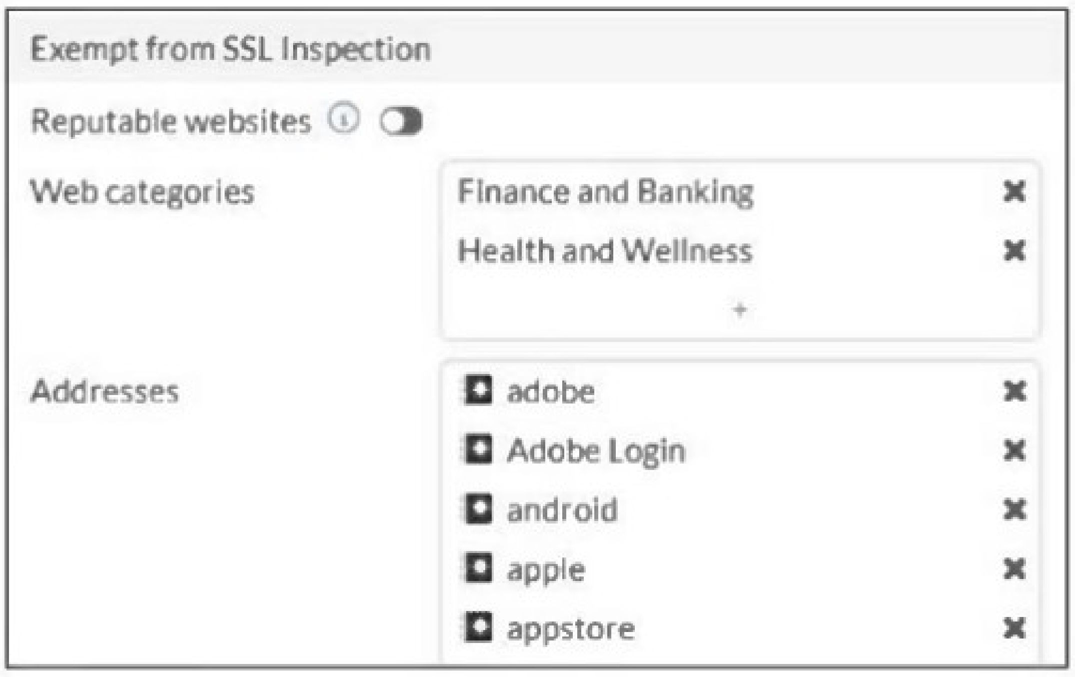
NEW QUESTION 9
An administrator wanted to configure an IPS sensor to block traffic that triggers a signature set number of times during a specific time period.
How can the administrator achieve the objective?

A. Use IPS group signatures, set rate-mode 60.
B. Use IPS packet logging option with periodical filter option.
C. Use IPS filter, rate-mode periodical option.
D. Use IPS filter, rate-mode periodical option.

Answer: C

Explanation:
The IPS filter with the rate-mode set to "periodical" allows the administrator to block traffic that triggers a signature a specified number of times within a defined time period, meeting the requirement.

NEW QUESTION 10
Refer to the exhibit.



Exempt from SSL Inspection

Reputable websites

Web categories: Finance and Banking; Health and Wellness

Addresses: adobe; Adobe Login; android; apple; appstore

The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit.
For which two reasons are these web categories exempted? (Choose two.)

A. The FortiGate temporary certificate denies the browser??s access to websites that use HTTP Strict Transport Security.
B. These websites are in an allowlist of reputable domain names maintained by FortiGuard.
C. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
D. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.

Answer: AD

Explanation:
FortiGate's temporary SSL certificate may cause access denial to sites using HTTP Strict Transport Security (HSTS), so such sites are exempted from deep SSL inspection.
Legal regulations require exemption of certain categories to protect user privacy and sensitive information, so these web categories are excluded from SSL inspection.

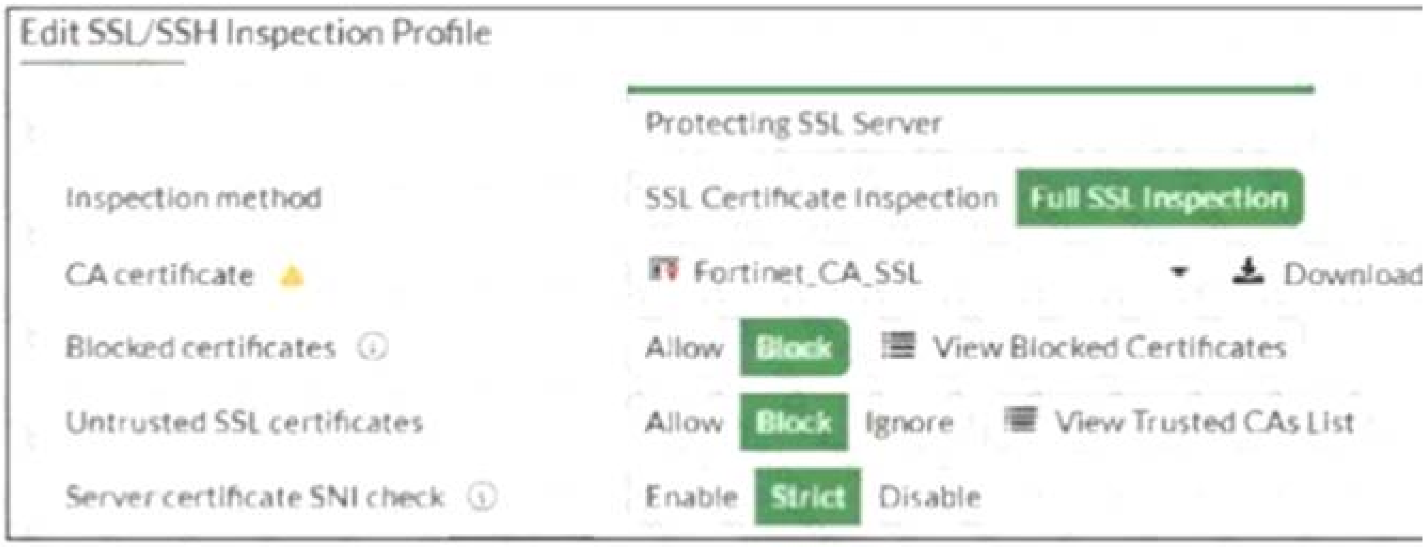
NEW QUESTION 10
An administrator wants to analyze and manage digital certificates to prevent browser warnings when users connect to the SSL VPN portal.
Which two statements describe how to correctly do this? (Choose two.)

A. The administrator can rely on the default FortiGate self-signed certificate to prevent all security warnings in the browser.
B. The administrator must disable HTTPS administrative access entirely to avoid certificate warnings.
C. The administrator can use a publicly trusted certificate from a known certificate authority (CA) to stop browser warnings.
D. The administrator can import the FortiGate self-signed certificate into each user??s browser as a trusted certificate.

Answer: CD

Explanation:
Using a publicly trusted certificate from a known CA prevents browser warnings without additional user action.
Importing the FortiGate self-signed certificate into users?? browsers as trusted eliminates warnings caused by untrusted certificates.

NEW QUESTION 12
Refer to the exhibit.



Edit SSL/SSH Inspection Profile

Protecting SSL Server

Inspection method: SSL Certificate Inspection [✓ Full SSL Inspection]

CA certificate: Fortinet_CA_SSL ▾ Download

Blocked certificates: Allow [✓ Block] View Blocked Certificates

Untrusted SSL certificates: Allow [✓ Block] Ignore View Trusted CAs List

Server certificate SNI check: Enable [✓ Strict] Disable

What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?

A. FortiGate will accept and use the CN in the server certificate for URL filtering if the SNI does not match the CN or SAN fields.
B. FortiGate will accept the connection with a warning if the SNI does not match the CN or SAN fields.
C. FortiGate will close the connection if the SNI does not match the CN or SAN fields.
D. FortiGate will close the connection if the SNI does not match the CN and SAN fields

Answer: D

Explanation:
With the Server certificate SNI check set to Strict, FortiGate enforces that the SNI must match either the Common Name (CN) or Subject Alternative Name (SAN) in the server certificate; otherwise, it closes the connection.

NEW QUESTION 16
A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode. Which step is NOT part of the expected process?

A. The DC agent sends login event data directly to FortiGate.
B. The user logs into the windows domain.
C. The collector agent forwards login event data to FortiGate.
D. FortiGate determines user identity based on the IP address in the FSSO list.

Answer: C

Explanation:
In DC Agent Mode, the DC agent sends login event data directly to FortiGate without involving a collector agent.

NEW QUESTION 18
An administrator notices that some users are unable to establish SSL VPN connections, while others can connect without any issues.
What should the administrator check first?

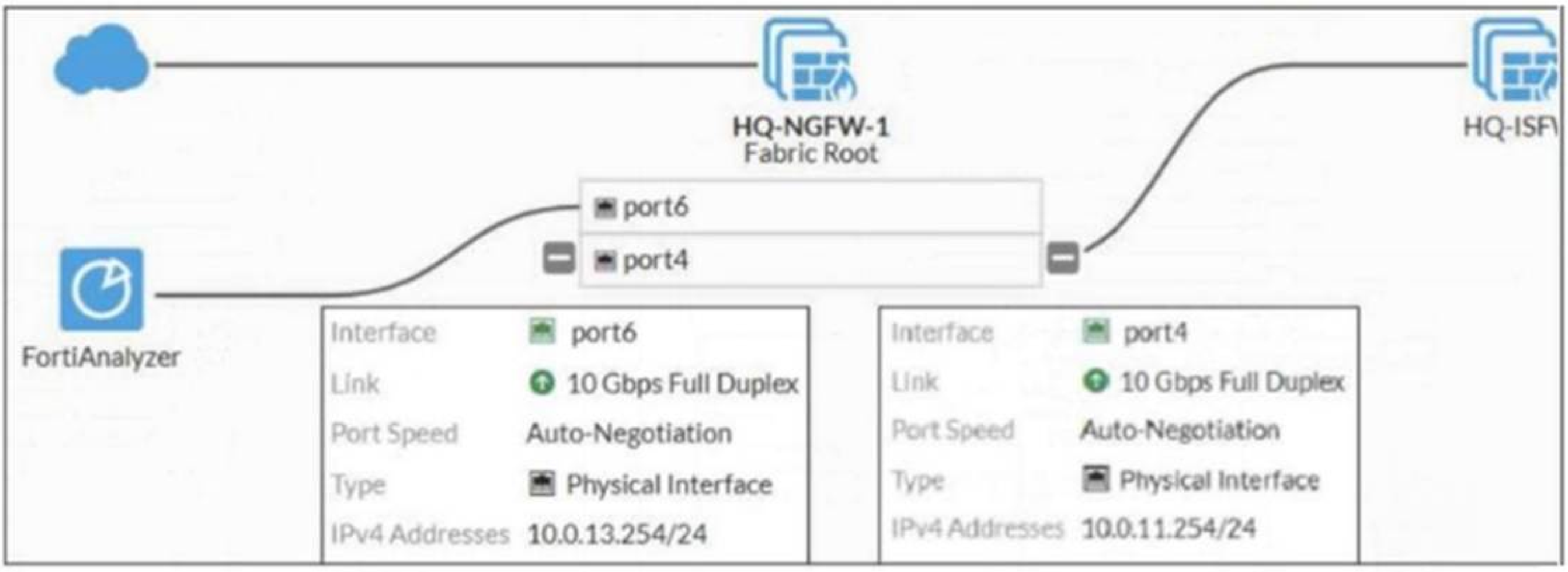
A. Ensure that the affected users are using the correct port number.
B. Ensure that user traffic is hitting the firewall policy.
C. Ensure that forced tunneling is enabled to reroute all traffic through the SSL VPN
D. Ensure that the HTTPS service is enabled on SSL VPN tunnel interface

Answer: B

Explanation:
If user traffic is not matching the appropriate firewall policy that permits SSL VPN, users will be unable to establish connections, making this the first aspect to verify.

NEW QUESTION 20
Refer to the exhibits.

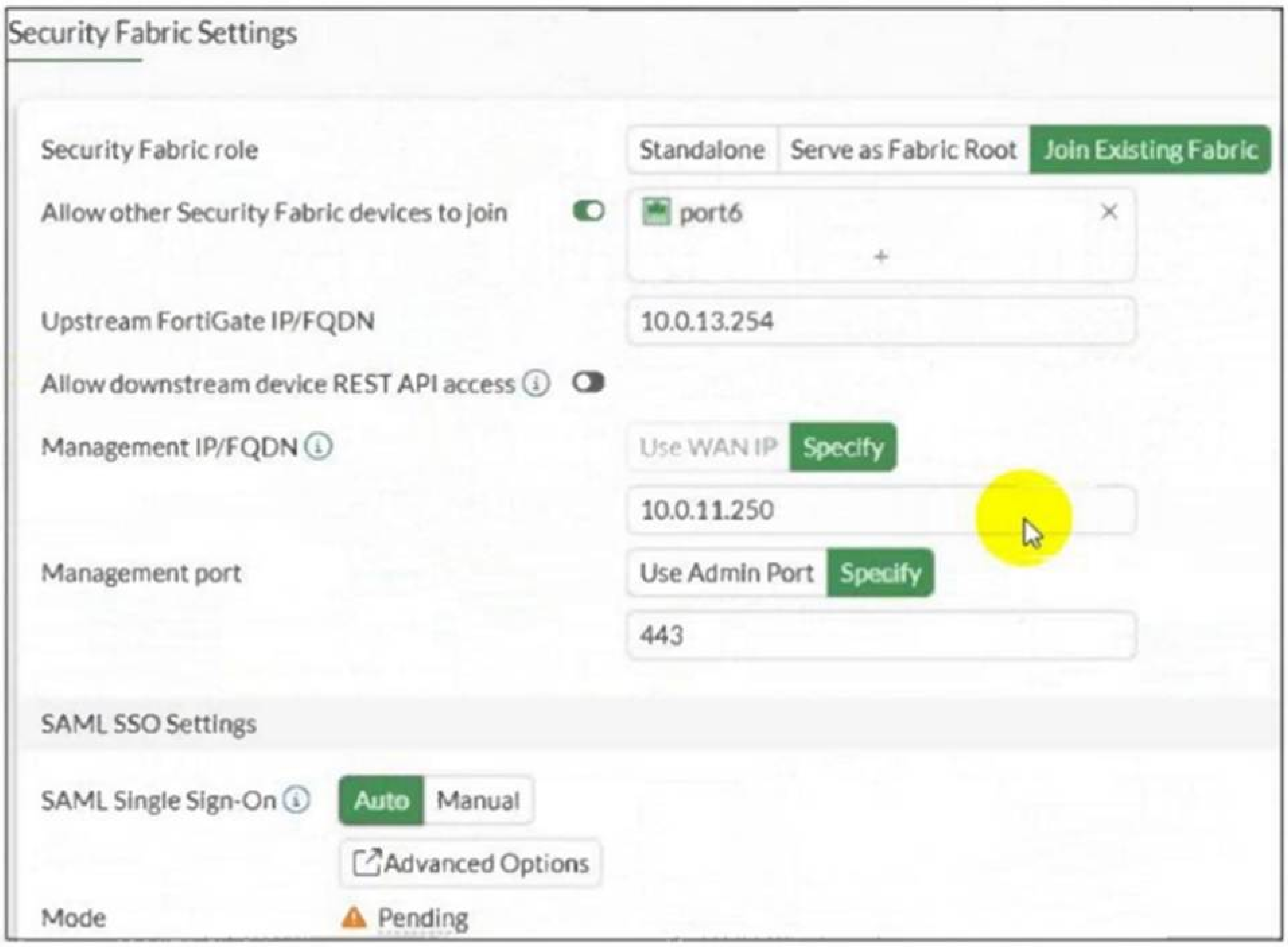
Security Fabric logical topology view



Interface	port6
Link	10 Gbps Full Duplex
Port Speed	Auto-Negotiation
Type	Physical Interface
IPv4 Addresses	10.0.13.254/24

Interface	port4
Link	10 Gbps Full Duplex
Port Speed	Auto-Negotiation
Type	Physical Interface
IPv4 Addresses	10.0.11.254/24

Security Fabric settings on HQ-ISFW-2



Security Fabric Settings

Security Fabric role: Standalone | Serve as Fabric Root | **Join Existing Fabric**

Allow other Security Fabric devices to join: ● port6 ×

Upstream FortiGate IP/FQDN: 10.0.13.254

Allow downstream device REST API access ⓘ: ○

Management IP/FQDN ⓘ: Use WAN IP | **Specify**

10.0.11.250

Management port: Use Admin Port | **Specify**

443

SAML SSO Settings

SAML Single Sign-On ⓘ: **Auto** | Manual

Advanced Options

Mode: Pending

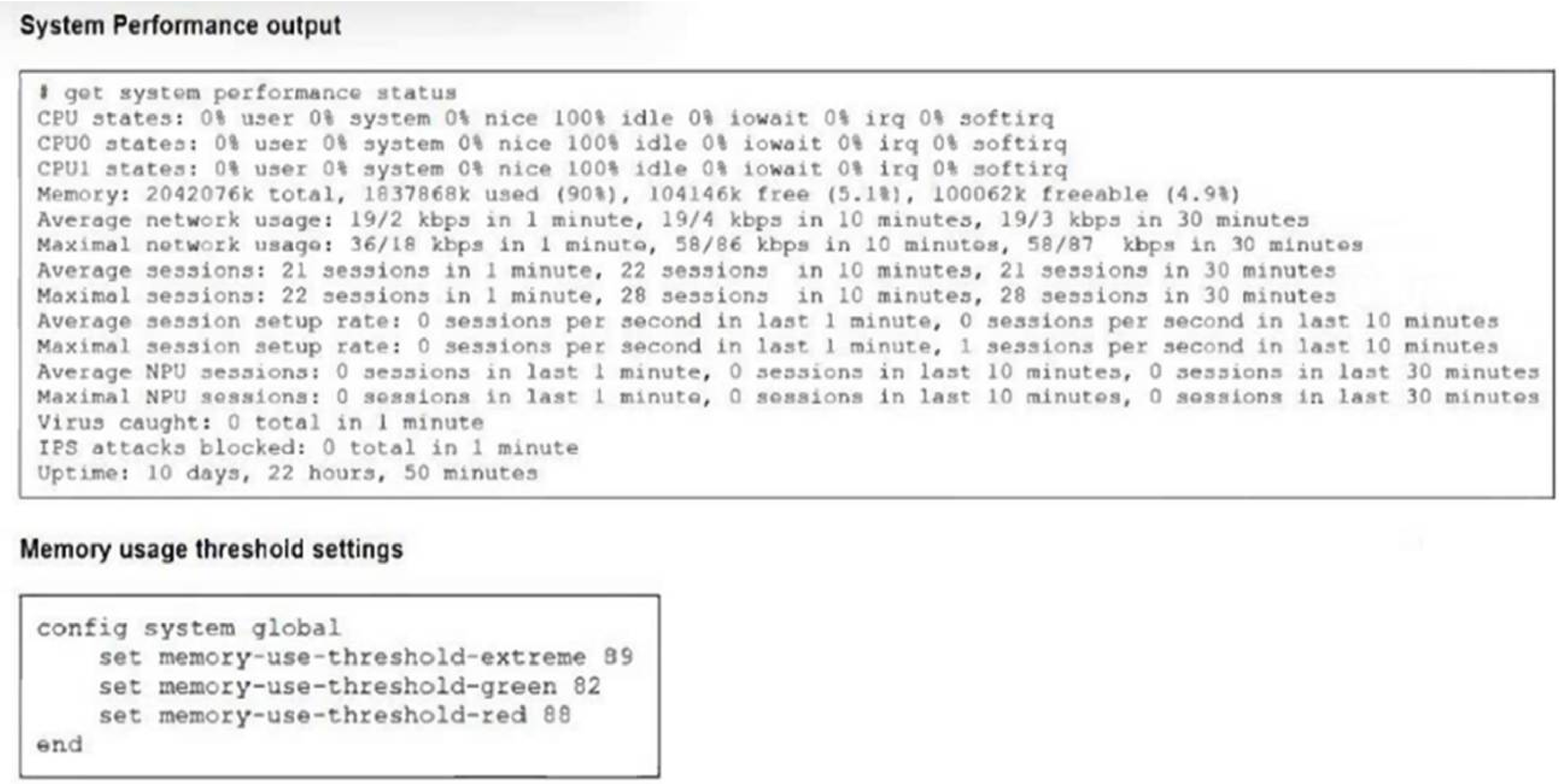
An administrator wants to add HQ-ISFW-2 in the Security Fabric. HQ-ISFW-2 is in the same subnet as HQ- ISFW. After configuring the Security Fabric settings on HQ-ISFW-2, the status staysPending.
What can be the two possible reasons? (Choose two.)

A. Upstream FortiGate IP must be set to 10.0.11.254.
B. SAML Single Sign-On must be set to Manual.
C. HQ-ISFW-2 must be authorized on HQ-ISFW.
D. Management IP must be set to 10.0.13.254.

Answer: AC

Explanation:
The Upstream FortiGate IP should match the IP address of the Fabric Root interface, which is 10.0.11.254, not 10.0.13.254.
The new device (HQ-ISFW-2) must be authorized on the Fabric Root (HQ-ISFW) before it can join the Security Fabric, otherwise the status remains pending.

NEW QUESTION 22
Refer to the exhibits.



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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

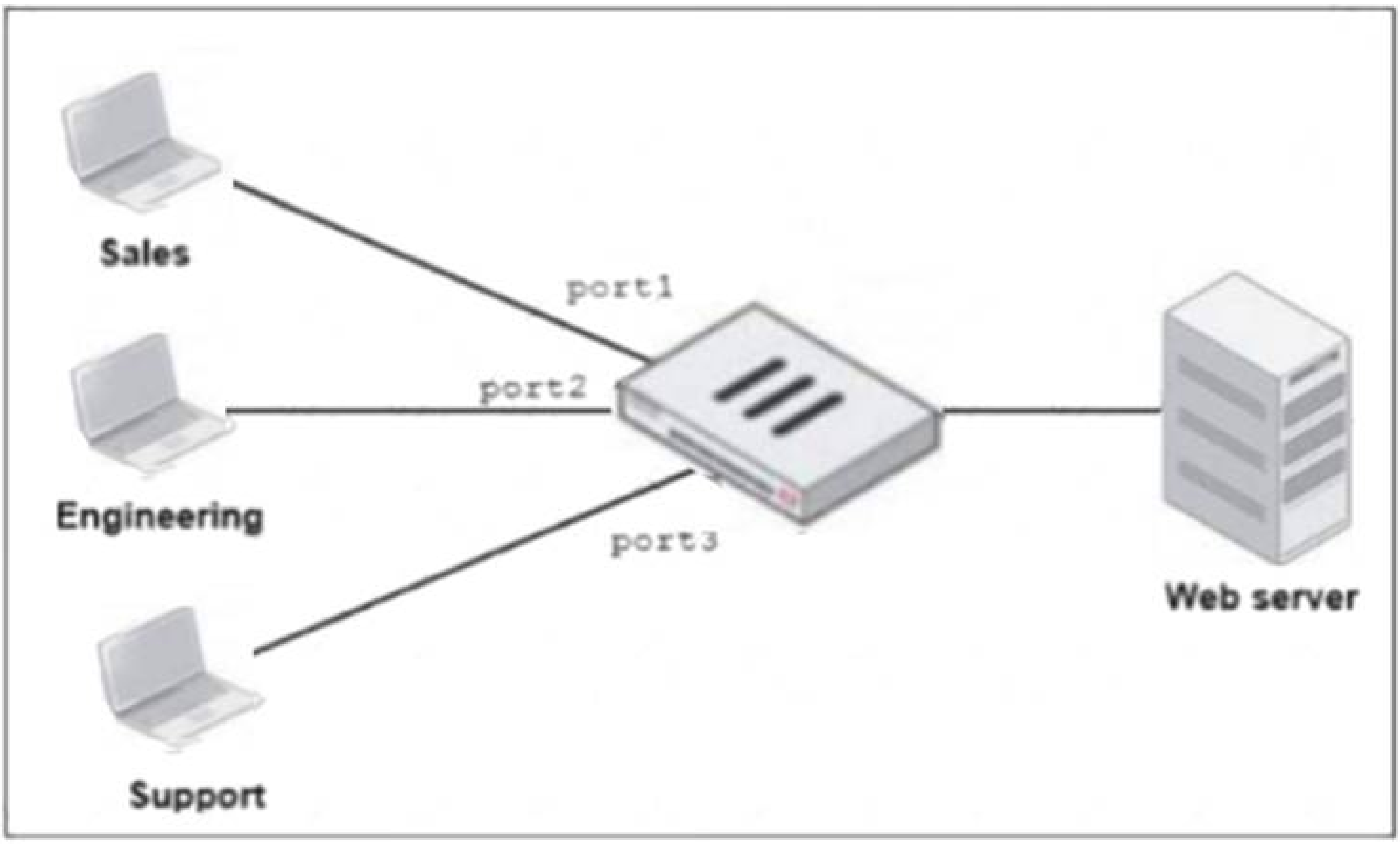
The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.
Based on the system performance output, what are the two possible outcomes? (Choose two.)

A. FortiGate has entered conserve mode.
B. Administrators can access FortiGate only through the console port.
C. Administrators can change the configuration.
D. FortiGate drops new sessions.

Answer: CD

Explanation:
Since memory usage is at 90%, exceeding the red threshold (88%), FortiGate enters a state where configuration changes are still allowed.
In this state, FortiGate drops new sessions to preserve resources and maintain stability.

NEW QUESTION 26
Refer to the exhibit.



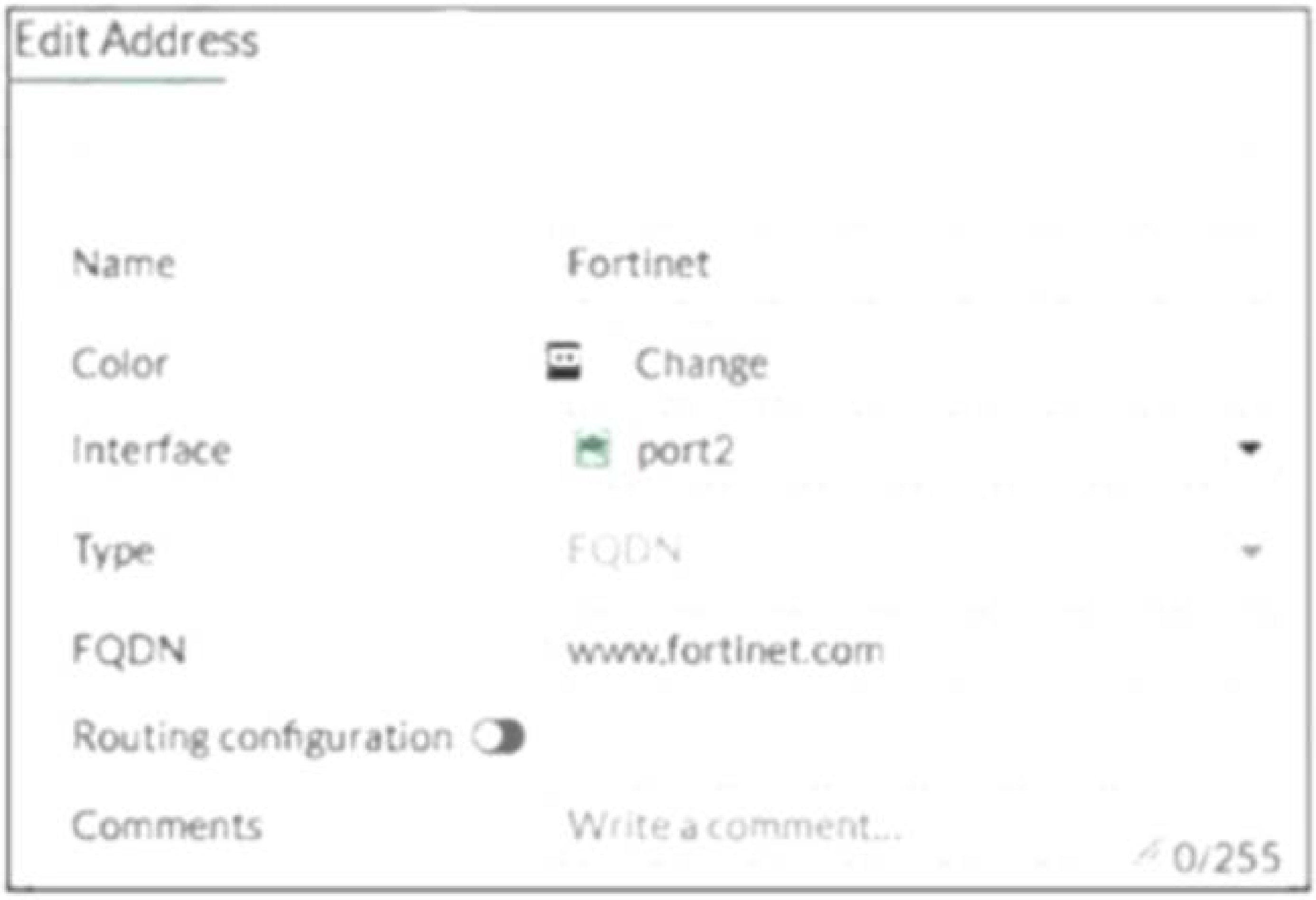
FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.
Which action must the administrator perform to consolidate the two policies into one?

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

Answer: D

Explanation:
Enabling Multiple Interface Policies allows you to select multiple interfaces (like port1 and port2) in a single firewall policy, consolidating access rules for both Sales and Engineering to the web server.

NEW QUESTION 29
Refer to the exhibit.



Edit Address

Name Fortinet

Color Change

Interface port2

Type FQDN

FQDN www.fortinet.com

Routing configuration ○

Comments Write a comment... 0/255

An administrator has created a new firewall address to use as the destination for a static route.
Why is the administrator not able to select the new address in theDestinationfield of the new static route?

A. In the new static route, the administrator must select Named Address.
B. In the new firewall address, the FQDN address must first beresolved.
C. In the new static route, the administrator must first set the interface to port2.
D. In the new firewall address, Routing configuration must be enabled.

Answer: D

Explanation:
To use an FQDN-based address object as a destination in a static route, the "Routing configuration" option must be enabled in the firewall address settings. Without this, the address cannot be selected for routing.

NEW QUESTION 34
Which three statements explain a flow-based antivirus profile? (Choose three.)

A. FortiGate buffers the whole file but transmits to the client at the same time.
B. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
C. If a virus is detected, the last packet is delivered to the client.
D. Flow-based inspection optimizes performance compared to proxy-based inspection.
E. The IPS engine handles the process as a standalone.

Answer: ABD

Explanation:
Flow-based antivirus buffers the entire file while simultaneously transmitting data to the client to minimize latency.
Flow-based inspection combines multiple scanning techniques from proxy-based modes for efficient detection. Flow-based inspection provides better performance by processing traffic on the fly without full proxy overhead.

NEW QUESTION 38
......