Fortinet

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

NEW QUESTION 1
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 2
You have configured the below commands on a FortiGate.

```
config system settings
set strict-src-check enable
end

Config system interface
edit port1
set src-check disable
next
end
```

What would be the impact of this configuration on FortiGate?

A. FortiGate will enable strict RPF on ail its interfaces and port1 will be enable for asymmetric routing.
B. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
C. Port1 will be enabled with flexible RPF, and all other interfaces will be enabled for strict RPF
D. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.

Answer: B

Explanation:
The global setting enables strict source checking (RPF) on all interfaces by default. The per-interface setting disables the source check on port1, exempting it from strict RPF enforcement.

NEW QUESTION 3
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The NetSessionEnum function is used to track user logouts.
D. The collector agent must search Windows application event logs.

Answer: B

Explanation:
NetAPI polling mode involves frequent queries to domain controllers, which can cause increased bandwidth usage, especially in large networks with many login events.

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
```

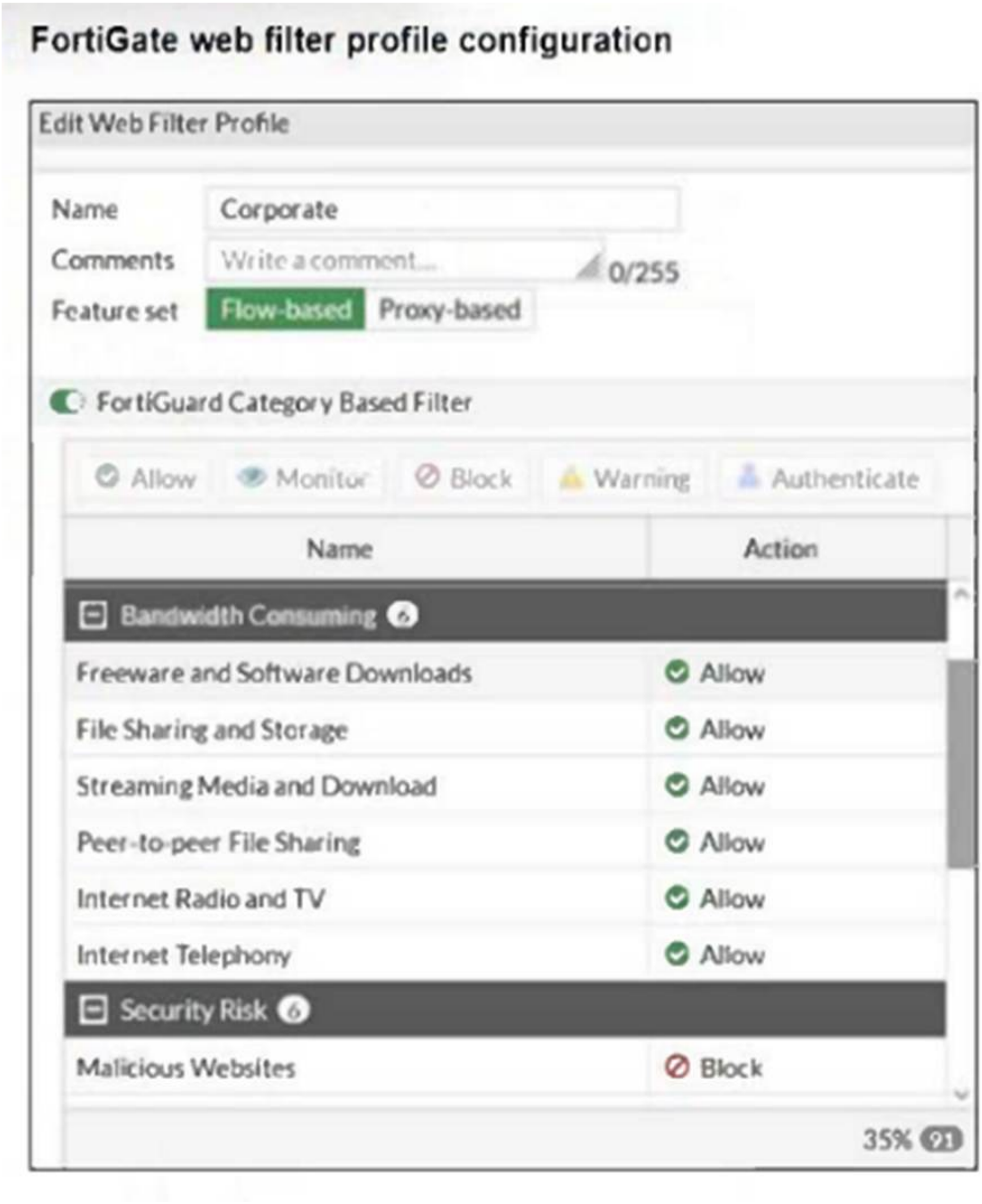
Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

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.



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 FortiGate firewall policy is configured with active authentication, however, the user cannot authenticate when accessing a website.
Which protocol must FortiGate allow even though the user cannot authenticate?

A. LDAP
B. TACASC+
C. Kerberos
D. DNS

Answer: D

Explanation:
DNS traffic must be allowed so the user can resolve domain names and reach the authentication server or web resources, even if authentication initially fails.

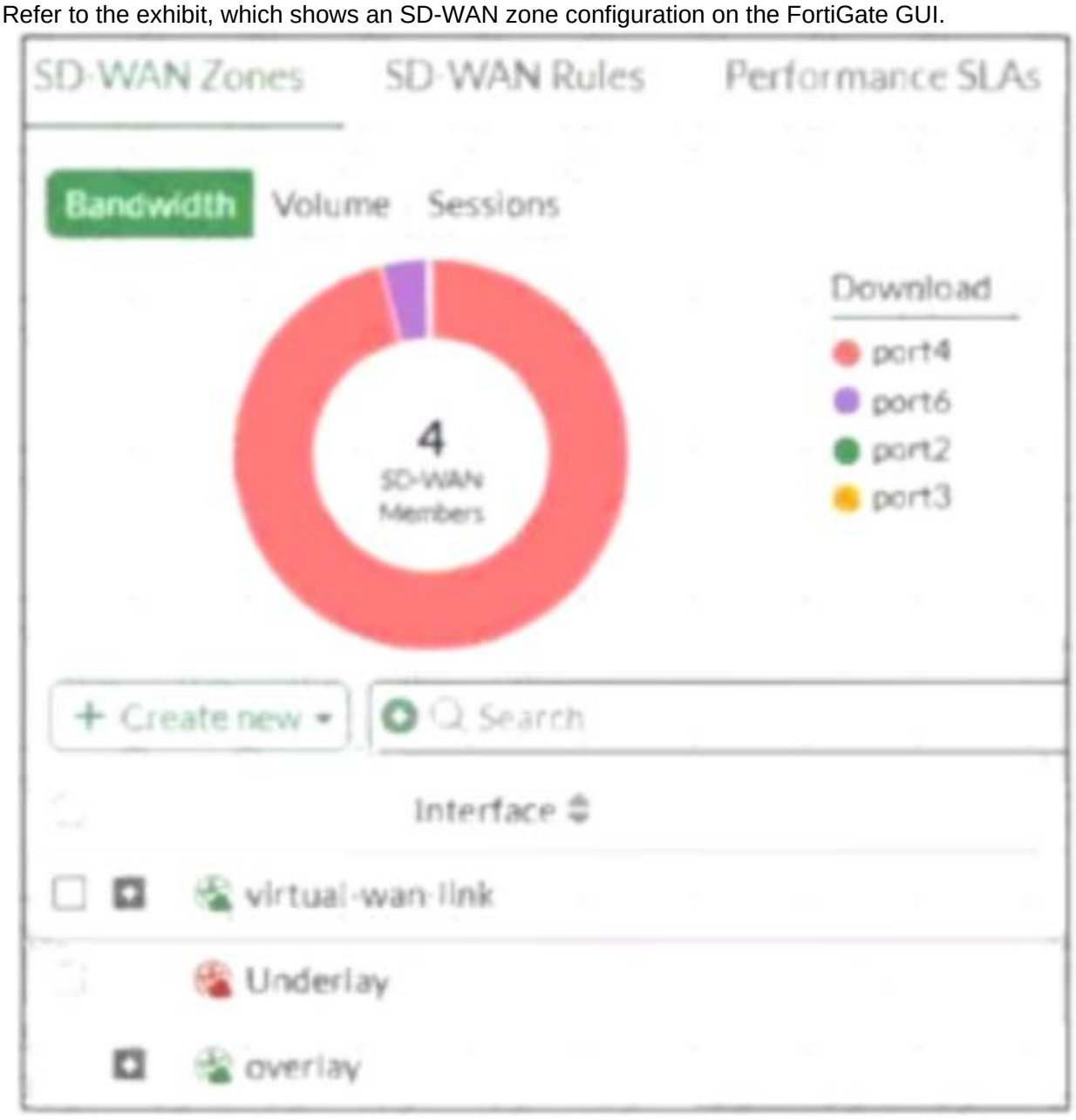
NEW QUESTION 8
You have configured an application control profile, set peer-to-peer traffic to Block under the Categories tab, and applied it to the firewall policy. However, your peer-to-peer traffic on known ports is passing through the FortiGate without being blocked.
What FortiGate settings should you check to resolve this issue?

A. FortiGuard category ratings
B. Application and Filter Overrides
C. Network Protocol Enforcement
D. Replacement Messages for UDP-based Applications

Answer: C

Explanation:
Network Protocol Enforcement settings control how FortiGate inspects and enforces protocols on traffic, including peer-to-peer applications on known ports. If not properly enabled, peer-to-peer traffic may bypass blocking despite the application control profile.

NEW QUESTION 9
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.

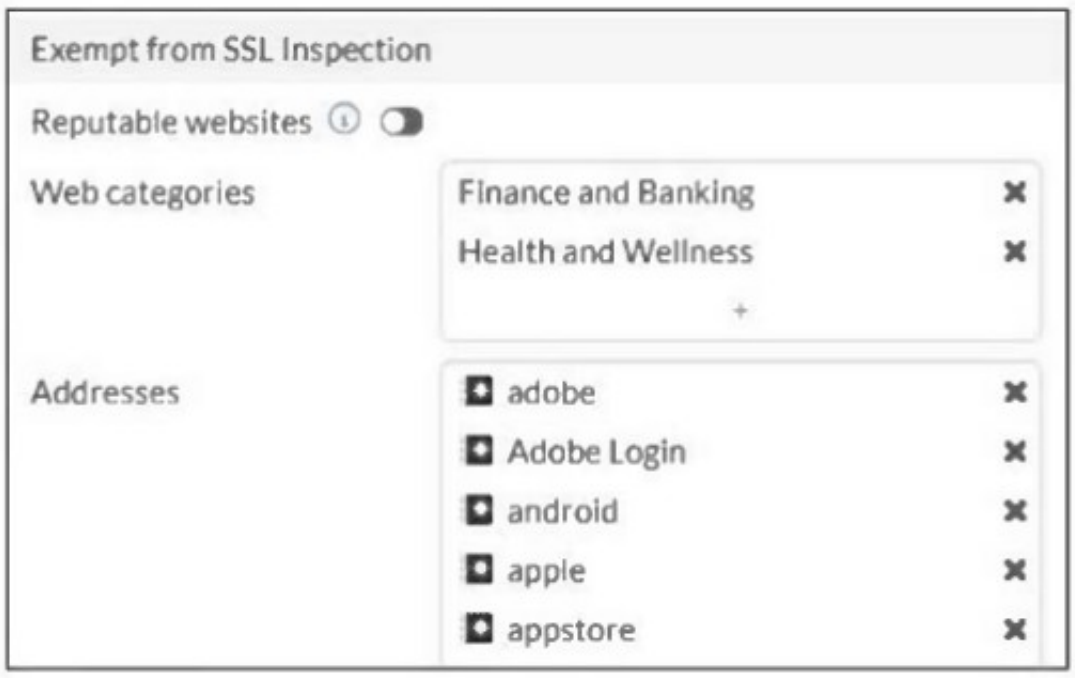
NEW QUESTION 10
An administrator wanted to configure an IPS sensor to block traffic that triggers a signature set number of times during a specific time period.
How can the administrator achieve the objective?

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.



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 15
What are three key routing principles in SD-WAN? (Choose three.)

A. By defaul
B. SD-WAN rules are skipped if the included SD-WAN members do not have a valid route to the destination.
C. SD-WAN rules have precedence over any other type of routes.
D. Regular policy routes have precedence over SD-WAN rules.
E. By defaul
F. SD-WAN rules are skipped if only one route to the destination is available.
G. By defaul
H. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Answer: ABE

Explanation:
SD-WAN rules are skipped if none of the SD-WAN members have a valid route to the destination. SD-WAN rules take precedence over other route types.
SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member by default.

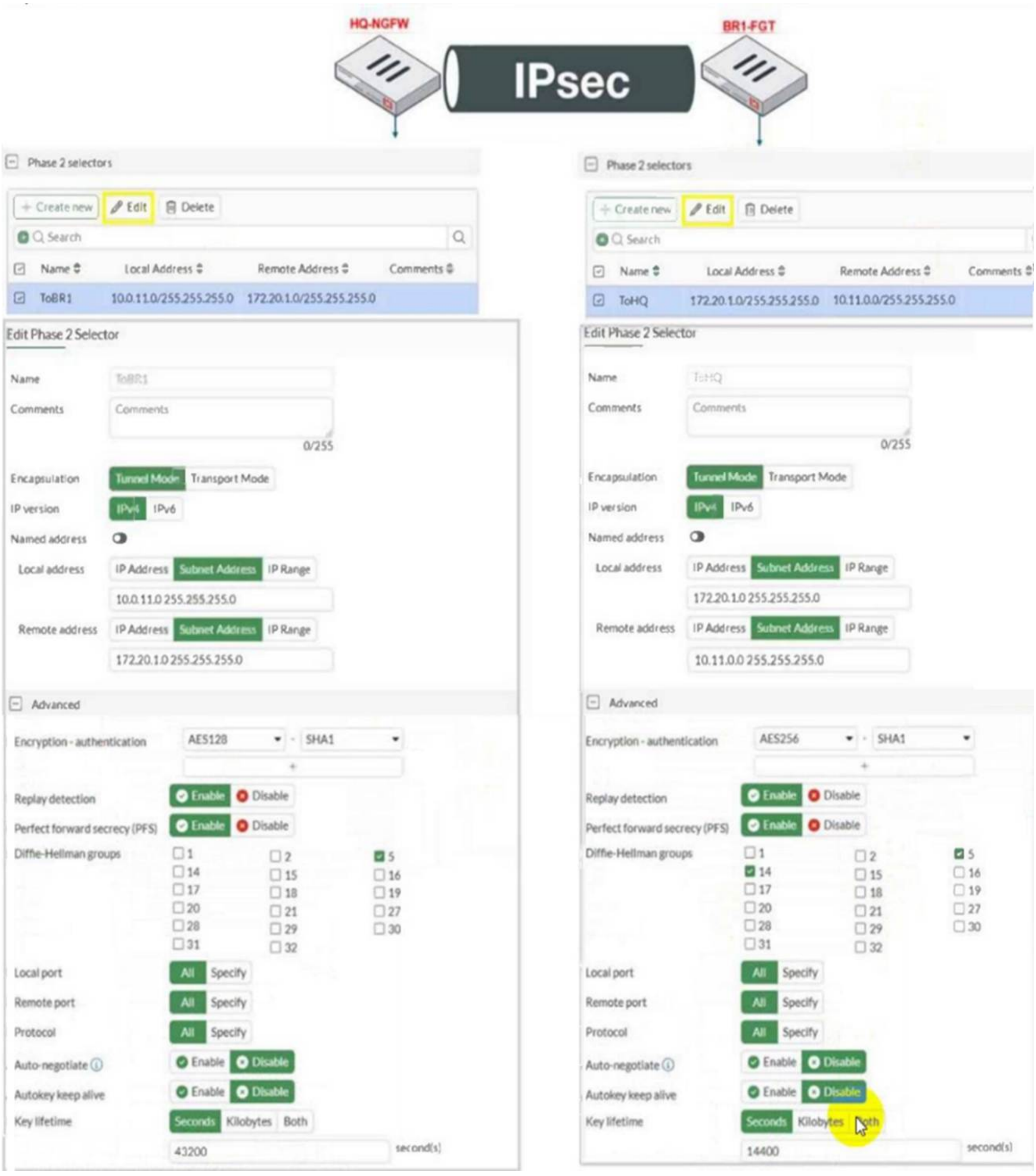
NEW QUESTION 16
A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode. Which step is NOT part of the expected process?

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
Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.
Based on the phase 2 configuration shown in the exhibit, which two configuration changes will bring phase 2 up? (Choose two.)

A. On BR1-FGT, set Seconds to 43200.
B. On HQ-NGFW, enable Diffie-Hellman Group 2.
C. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0
D. On HQ-NGF
E. set Encryption to AES256

Answer: AC

Explanation:
The key lifetime (Seconds) must match on both sides; BR1-FGT is set to 14400, so setting it to 43200 matches HQ-NGFW.
The remote address on BR1-FGT should match the HQ-NGFW??s local subnet (10.0.11.0/24), but it is currently set incorrectly as 172.20.1.0/24. Changing it to 10.0.11.0/255.255.255.0 will align the Phase 2 selectors.

NEW QUESTION 19
An administrator suspects that the Collector Agent is not forwarding login events to FortiGate. What is the most effective troubleshooting step?

A. Verify if DC agent is enabled on the FortiGate.
B. Restart the domain controller to refresh authentication services.
C. Verify if FortiGate is set to use LDAP authentication instead of FSSO.
D. Check if TCP port 8000 is open between the collector agent and FortiGate.

Answer: D

Explanation:
The Collector Agent communicates with FortiGate over TCP port 8000. Ensuring this port is open and reachable is essential for forwarding login events.

NEW QUESTION 23
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 27
Which three statements explain a flow-based antivirus profile? (Choose three.)

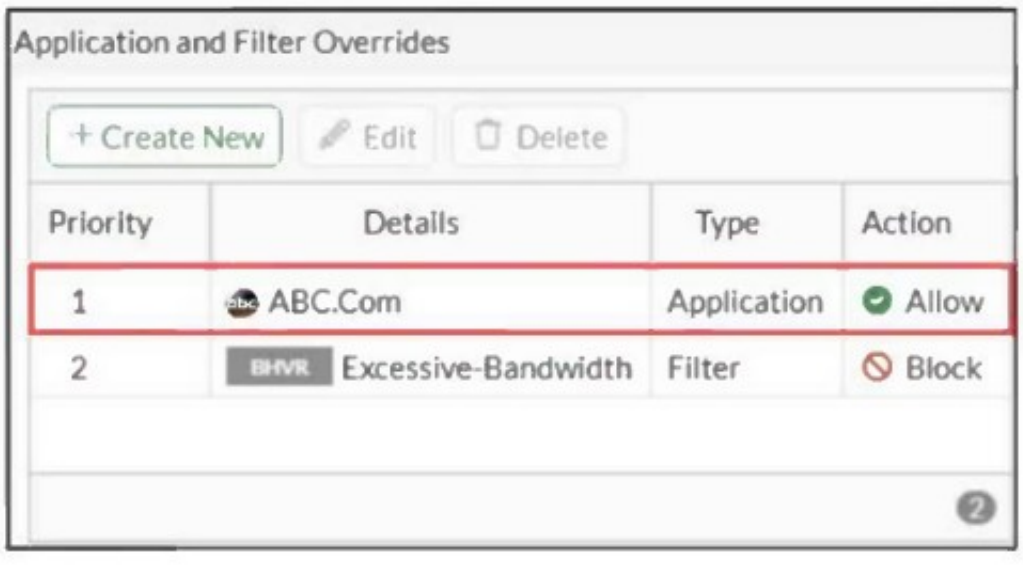
A. FortiGate buffers the whole file but transmits to the client at the same time.
B. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
C. If a virus is detected, the last packet is delivered to the client.
D. Flow-based inspection optimizes performance compared 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 32
Refer to the exhibit.



An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow. This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, the administrator accessed the ABC.Com web site several times.
Why are there no logs generated under security logs for ABC.Com?

A. The ABC.Com Type is set as Application instead of Filter.
B. The ABC.Com is configured under application profile, which must be configured as a web filter profile.
C. The ABC.Com Action is set to Allow.
D. The ABC.Com is hitting the category Excessive-Bandwidth.

Answer: A

Explanation:
When the action is set to Allow in an application override, traffic matching this override is allowed without generating security logs because it bypasses deeper inspection and blocking.

NEW QUESTION 33
.....

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-7.6 Practice Exam Features:

* FCP_FGT_AD-7.6 Questions and Answers Updated Frequently

* FCP_FGT_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FGT_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year