Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

https://www.2passeasy.com/dumps/NSE4_FGT-7.2/

NEW QUESTION 1
To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

A. FortiManager
B. Root FortiGate
C. FortiAnalyzer
D. Downstream FortiGate

Answer: B

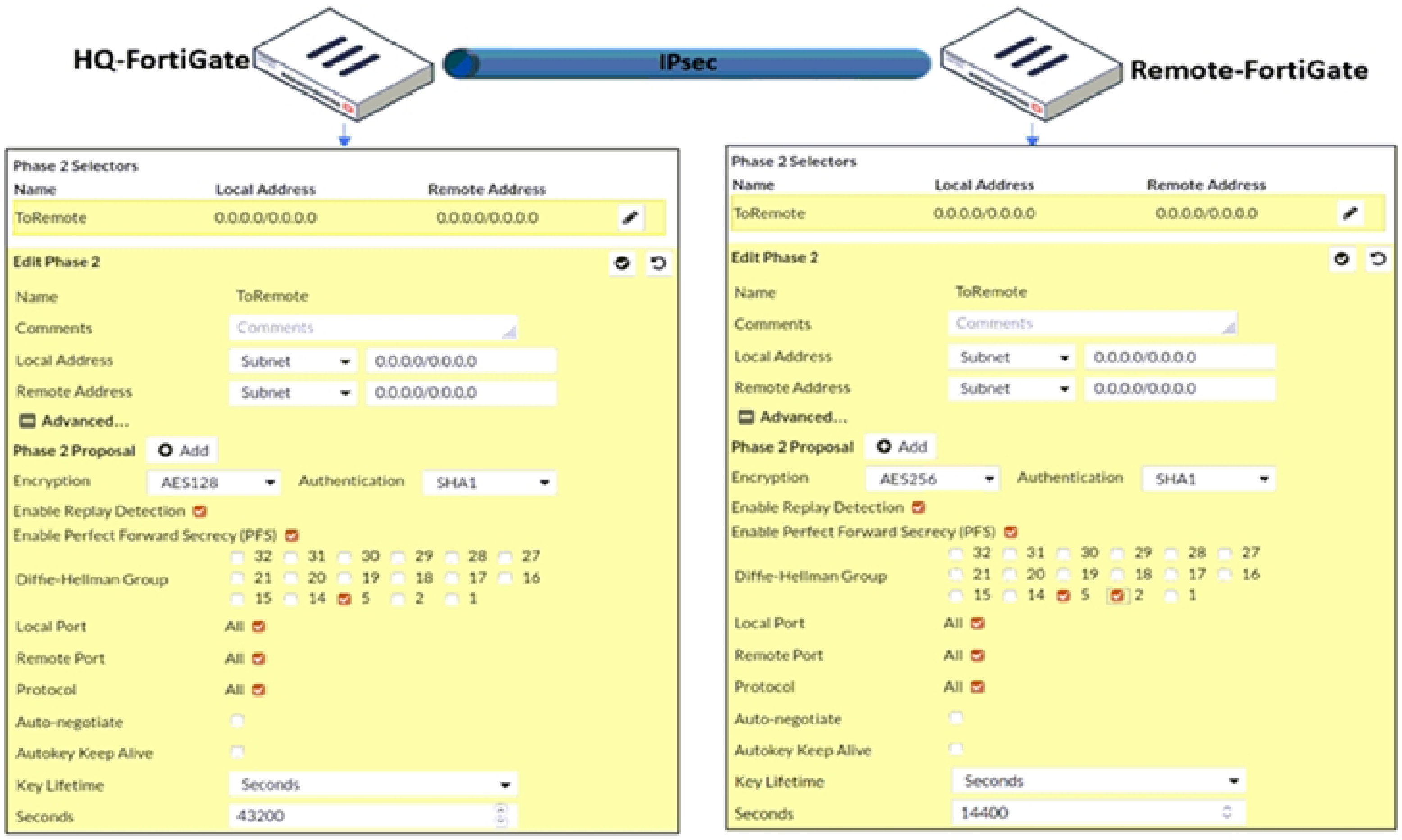
NEW QUESTION 2
Which two statements explain antivirus scanning modes? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Answer: BC

Explanation:
An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM--something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.
FortiGate Security 7.2 Study Guide (p.350 & 352): "In flow-based inspection mode, the IPS engine reads the payload of each packet, caches a local copy, and forwards the packet to the receiver at the same time. Because the file is ransmitted simultaneously, flow-based mode consumes more CPU cycles than proxy-based." "Each protocol’s proxy picks up a connection and buffers the entire file first (or waits until the oversize limit is reached) before scanning. The client must wait for the scanning to finish."

NEW QUESTION 3
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.



HQ-FortiGate:

Phase 2 Selectors		
Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2
Name: ToRemote
Comments: Comments
Local Address: Subnet 0.0.0.0/0.0.0.0
Remote Address: Subnet 0.0.0.0/0.0.0.0
Advanced...
Phase 2 Proposal: Add
Encryption: AES128 Authentication: SHA1
Enable Replay Detection ☑
Enable Perfect Forward Secrecy (PFS) ☑
Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 □ 2 □ 1
Local Port: All ☑
Remote Port: All ☑
Protocol: All ☑
Auto-negotiate □
Autokey Keep Alive □
Key Lifetime: Seconds
Seconds: 43200

Remote-FortiGate:

Phase 2 Selectors		
Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2
Name: ToRemote
Comments: Comments
Local Address: Subnet 0.0.0.0/0.0.0.0
Remote Address: Subnet 0.0.0.0/0.0.0.0
Advanced...
Phase 2 Proposal: Add
Encryption: AES256 Authentication: SHA1
Enable Replay Detection ☑
Enable Perfect Forward Secrecy (PFS) ☑
Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 ☑ 2 □ 1
Local Port: All ☑
Remote Port: All ☑
Protocol: All ☑
Auto-negotiate □
Autokey Keep Alive □
Key Lifetime: Seconds
Seconds: 14400

Based on the phase 2 configuration shown in the exhibit, which configuration change will bring phase 2 up?

A. On Remote-FortiGate, set Seconds to 43200.
B. On HQ-FortiGate, set Encryption to AES256.
C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
D. On HQ-FortiGate, enable Auto-negotiate.

Answer: B

NEW QUESTION 4
Which two statements describe how the RPF check is used? (Choose two.)

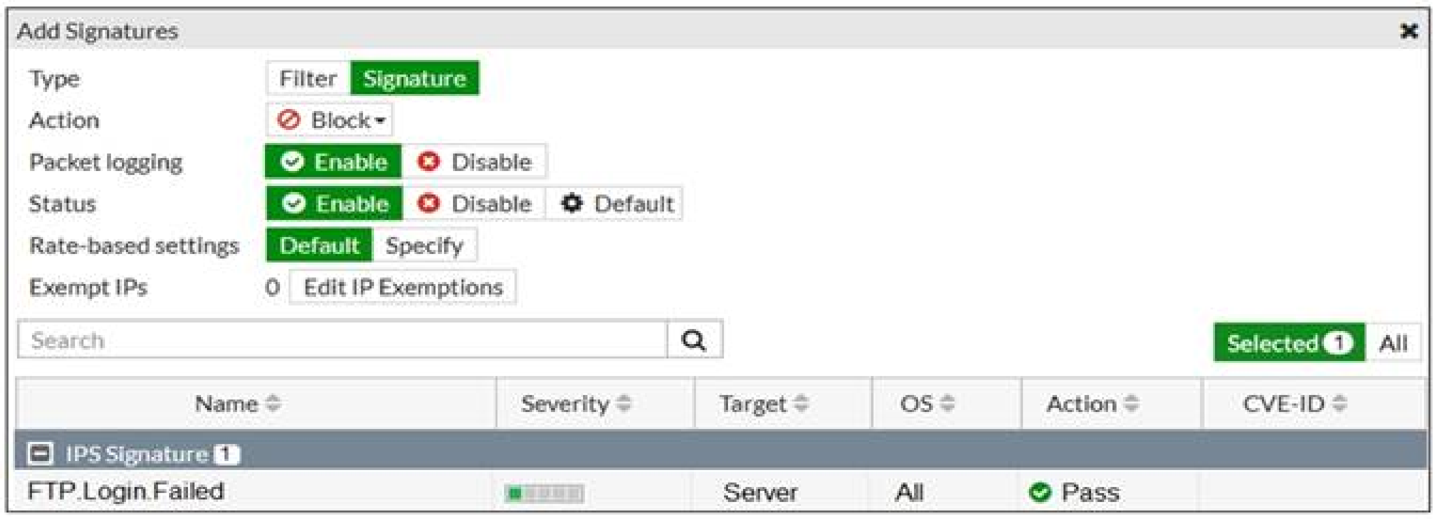
A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
B. The RPF check is run on the first sent and reply packet of any new session.

C. The RPF check is run on the first sent packet of any new session.
D. The RPF check is run on the first reply packet of any new session.

Answer: AC

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.41): "The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table." "FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session."
* A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks1
* C. The RPF check is run on the first sent packet of any new session.
This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the session initiation. This reduces the processing overhead and improves performance2

NEW QUESTION 5
Refer to the exhibit.



Add Signatures ✖

Type	Filter [✓ Signature]
Action	⊘ Block ▾
Packet logging	[✓ Enable] ⊗ Disable
Status	[✓ Enable] ⊗ Disable ⚙ Default
Rate-based settings	[✓ Default] Specify
Exempt IPs	0 Edit IP Exemptions

Search 🔍 [✓ Selected 1] All

Name	Severity	Target	OS	Action	CVE-ID
⊟ IPS Signature 1					
FTP.Login.Failed	▮▯▯▯▯	Server	All	✓ Pass	

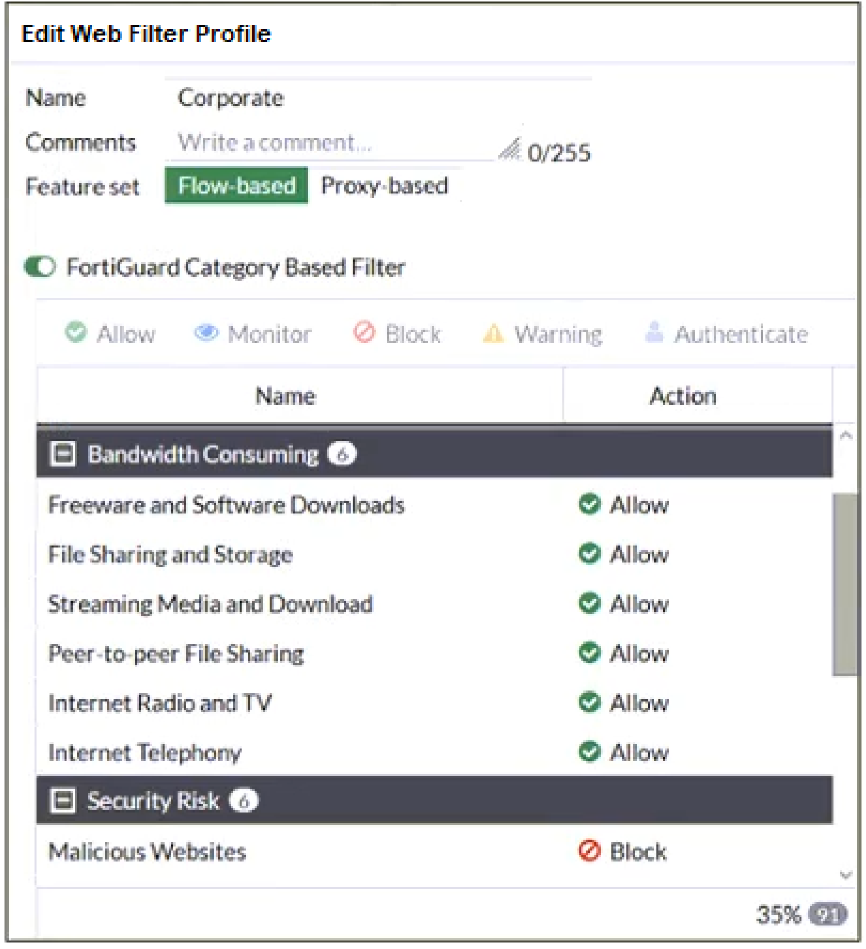
Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

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

Answer: D

Explanation:
Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be 'Pass' for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be 'Default'.
Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

NEW QUESTION 6
Refer to the exhibit.
The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.
An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.



Edit Web Filter Profile

Name	Corporate
Comments	Write a comment... 0/255
Feature set	[✓ Flow-based] Proxy-based

● FortiGuard Category Based Filter

✓ Allow 👁 Monitor ⊘ Block ⚠ Warning 👤 Authenticate

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

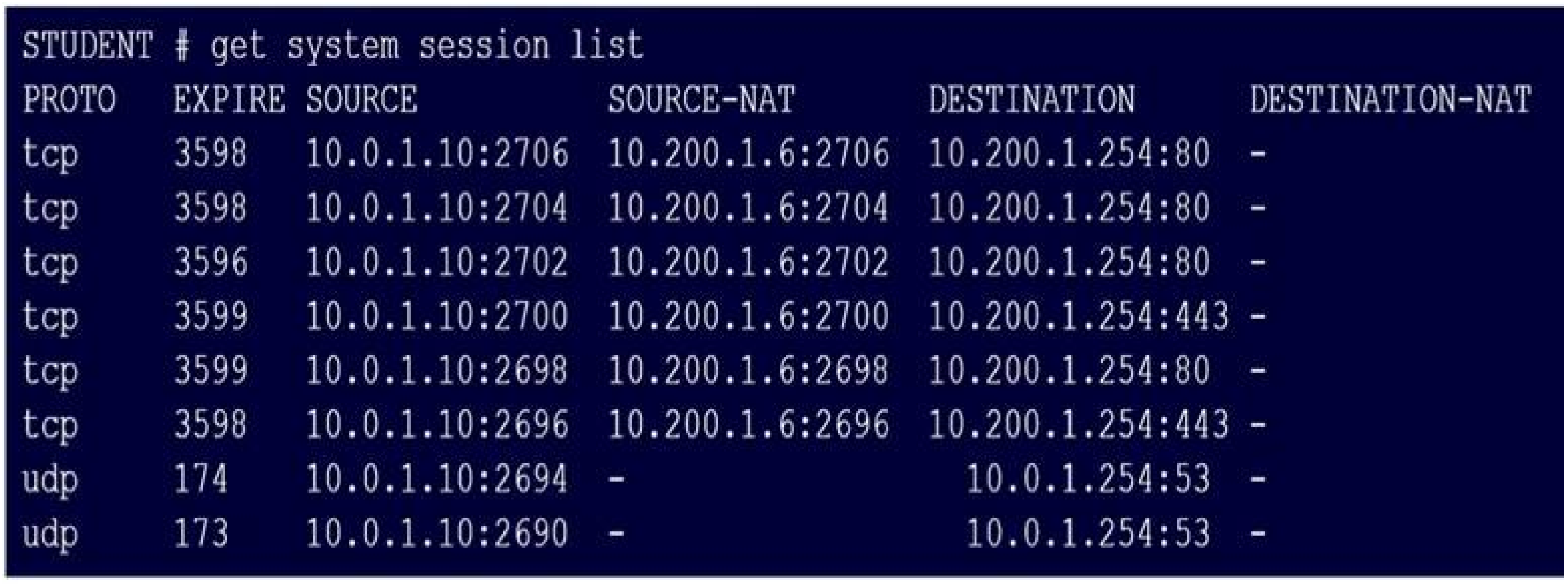
What are two solutions for satisfying the requirement? (Choose two.)

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

Answer: BD

Explanation:
FortiGate Security 7.2 Study Guide (p.268-269): "If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. You can block a website that belongs to an allowed category." "Static URL filtering is another web filter feature. Configured URLs in the URL filter are checked against the visited websites. If a match is found, the configured action is taken. URL filtering has the same patterns as static domain filtering: simple, regular expressions, and wildcard."
* B. Configure a web override rating for download.com and select Malicious Websites as the subcategory. This is true because a web override rating is a feature that allows the administrator to change the FortiGuard category of a specific website or domain, and apply a different action to it based on the web filter profile. By configuring a web override rating for download.com and selecting Malicious Websites as the subcategory, the administrator can block access to download.com, which belongs to the Freeware and Software Downloads category by default, without affecting other websites in the same category. The Malicious Websites category has the action Block in the web filter profile shown in the exhibit.
* D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.
This is true because a static URL filter entry is a feature that allows the administrator to define custom rules for filtering specific URLs or domains, and apply an action to them based on the web filter profile. By configuring a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively, the administrator can block access to download.com and any subdomains or paths under it, without affecting other websites in the Freeware and Software Downloads category. The static URL filter entries have higher priority than the FortiGuard category based filter entries in the web filter profile.

NEW QUESTION 7
Refer to the exhibit.



```
STUDENT # get system session list
PROTO   EXPIRE SOURCE           SOURCE-NAT         DESTINATION        DESTINATION-NAT
tcp     3598   10.0.1.10:2706   10.200.1.6:2706    10.200.1.254:80    -
tcp     3598   10.0.1.10:2704   10.200.1.6:2704    10.200.1.254:80    -
tcp     3596   10.0.1.10:2702   10.200.1.6:2702    10.200.1.254:80    -
tcp     3599   10.0.1.10:2700   10.200.1.6:2700    10.200.1.254:443   -
tcp     3599   10.0.1.10:2698   10.200.1.6:2698    10.200.1.254:80    -
tcp     3598   10.0.1.10:2696   10.200.1.6:2696    10.200.1.254:443   -
udp     174    10.0.1.10:2694   -                    10.0.1.254:53    -
udp     173    10.0.1.10:2690   -                    10.0.1.254:53    -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

A. Destination NAT is disabled in the firewall policy.
B. One-to-one NAT IP pool is used in the firewall policy.
C. Overload NAT IP pool is used in the firewall policy.
D. Port block allocation IP pool is used in the firewall policy.

Answer: B

Explanation:
FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

NEW QUESTION 8
An employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

A. idle-timeout
B. login-timeout
C. udp-idle-timer
D. session-ttl

Answer: B

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.222):
"When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under config vpn ssl settings have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN connections."

NEW QUESTION 9
If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source filed of a firewall policy?

A. IP address
B. Once Internet Service is selected, no other object can be added

C. User or User Group
D. FQDN address

Answer: B

NEW QUESTION 10
Examine this PAC file configuration.
Which of the following statements are true? (Choose two.)

A. Browsers can be configured to retrieve this PAC file from the FortiGate.
B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 10
Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
B. The client FortiGate requires a manually added route to remote subnets.
C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
D. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.9/administration-guide/508779/fortigate-as-ssl-vpn-client
To establish an SSL VPN connection between two FortiGate devices, the following two settings are required:
The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate will use a CA (Certificate Authority) certificate to verify the client FortiGate certificate, ensuring that the client device is trusted and allowed to establish an SSL VPN connection.
The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: The client FortiGate must have an SSL VPN tunnel interface type configured in order to establish an SSL VPN connection. This interface type will be used to connect to the server FortiGate over the SSL VPN.

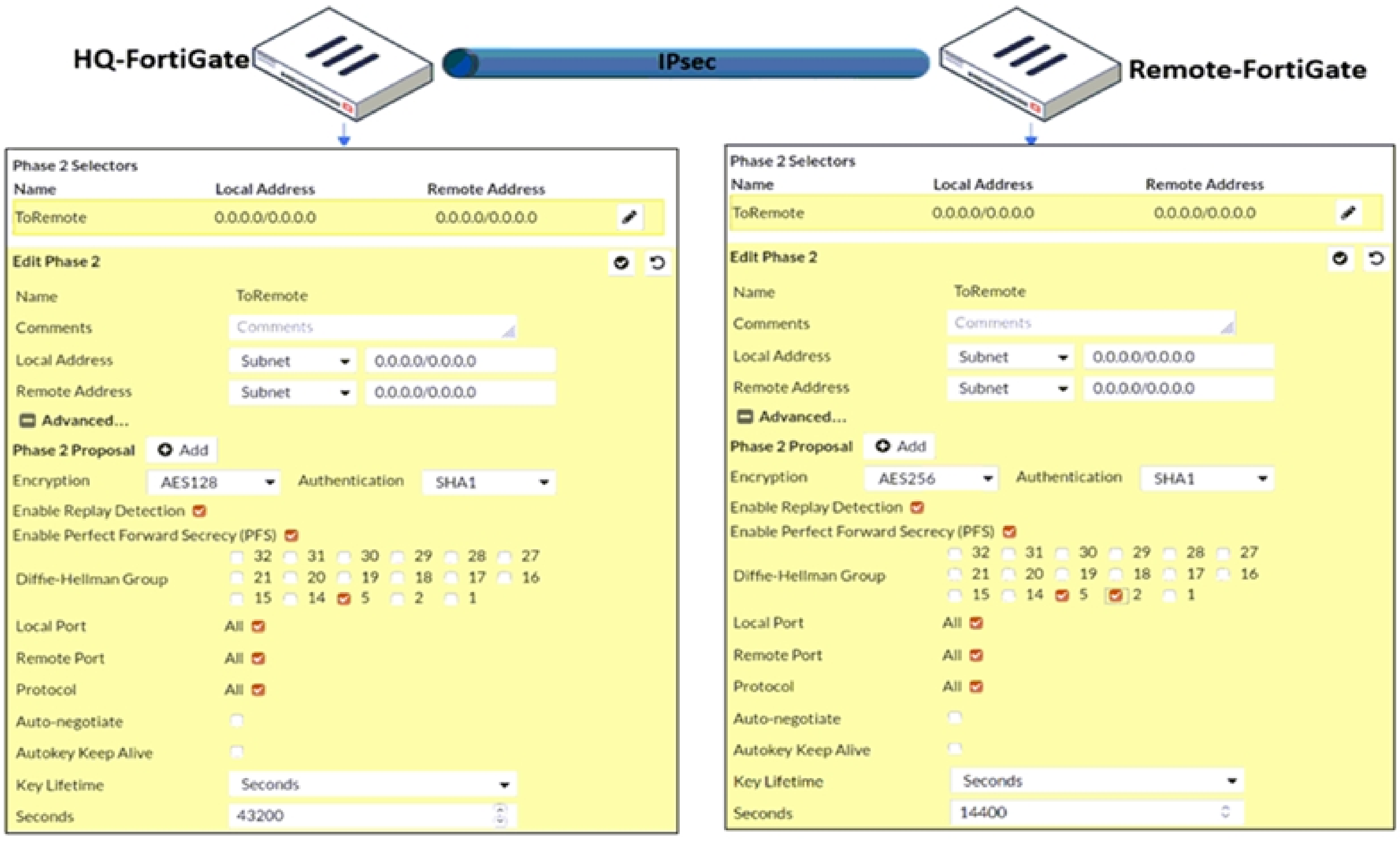
NEW QUESTION 15
An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSL/TLS connection.
Which FortiGate configuration can achieve this goal?

A. SSL VPN bookmark
B. SSL VPN tunnel
C. Zero trust network access
D. SSL VPN quick connection

Answer: B

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.198): "Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as fortissl to the user's PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated. The main advantage of tunnel mode over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel."
An SSL VPN tunnel allows remote users to establish a secure and encrypted Virtual Private Network (VPN) connection to the private network using the SSL/TLS protocol1. An SSL VPN tunnel can provide access to network resources such as FTP servers, as well as external applications running on the user's PC1.
An SSL VPN bookmark is a web link that provides access to network resources through the SSL VPN web portal1. It does not support external applications running on the user's PC.
Zero trust network access (ZTNA) is a security model that provides role-based application access to remote users without exposing the private network to the internet2. It does not use SSL/TLS protocol, but rather a proprietary ZTNA protocol.
SSL VPN quick connection is a feature that allows users to connect to an SSL VPN tunnel without installing FortiClient or any other software on their PC3. It requires a web browser that supports Java or ActiveX. It does not support external applications running on the user's PC.

NEW QUESTION 16
Refer to the exhibit.



HQ-FortiGate

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name	ToRemote
Comments	Comments
Local Address	Subnet 0.0.0.0/0.0.0.0
Remote Address	Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal Add

Encryption	AES128
Authentication	SHA1
Enable Replay Detection	☑
Enable Perfect Forward Secrecy (PFS)	☑
Diffie-Hellman Group	☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☐ 14 ☑ 5 ☐ 2 ☐ 1
Local Port	All ☑
Remote Port	All ☑
Protocol	All ☑
Auto-negotiate	☐
Autokey Keep Alive	☐
Key Lifetime	Seconds
Seconds	43200

Remote-FortiGate

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name	ToRemote
Comments	Comments
Local Address	Subnet 0.0.0.0/0.0.0.0
Remote Address	Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal Add

Encryption	AES256
Authentication	SHA1
Enable Replay Detection	☑
Enable Perfect Forward Secrecy (PFS)	☑
Diffie-Hellman Group	☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☐ 14 ☑ 5 ☑ 2 ☐ 1
Local Port	All ☑
Remote Port	All ☑
Protocol	All ☑
Auto-negotiate	☐
Autokey Keep Alive	☐
Key Lifetime	Seconds
Seconds	14400

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, what configuration change will bring phase 2 up?

A. On HQ-FortiGate, enable Auto-negotiate.
B. On Remote-FortiGate, set Seconds to 43200.
C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
D. On HQ-FortiGate, set Encryption to AES256.

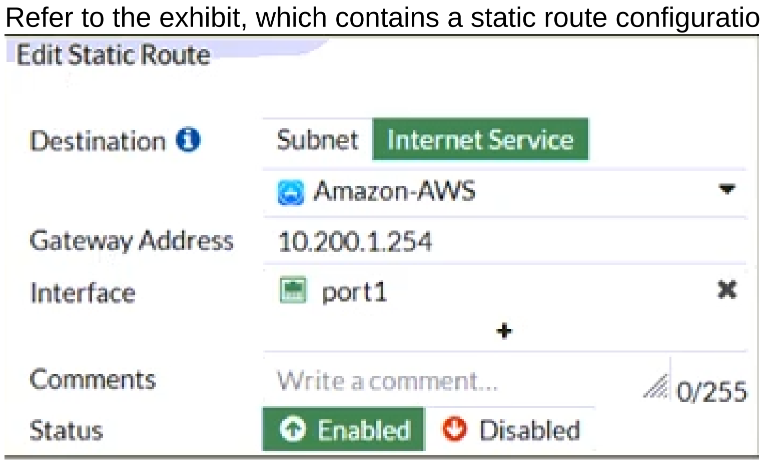
Answer: D

NEW QUESTION 18
An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

A. Add the support of NTLM authentication.
B. Add user accounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

Answer: D

NEW QUESTION 19
Refer to the exhibit, which contains a static route configuration. An administrator created a static route for Amazon Web Services.



Edit Static Route

Destination	Subnet [✓ Internet Service] Amazon-AWS
Gateway Address	10.200.1.254
Interface	port1
Comments	Write a comment... 0/255
Status	[✓ Enabled] Disabled

Which CLI command must the administrator use to view the route?

A. get router info routing-table database
B. diagnose firewall route list
C. get internet-service route list
D. get router info routing-table all

Answer: B

Explanation:
ISDB static route will not create entry directly in routing-table. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/1
and here
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640
FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take

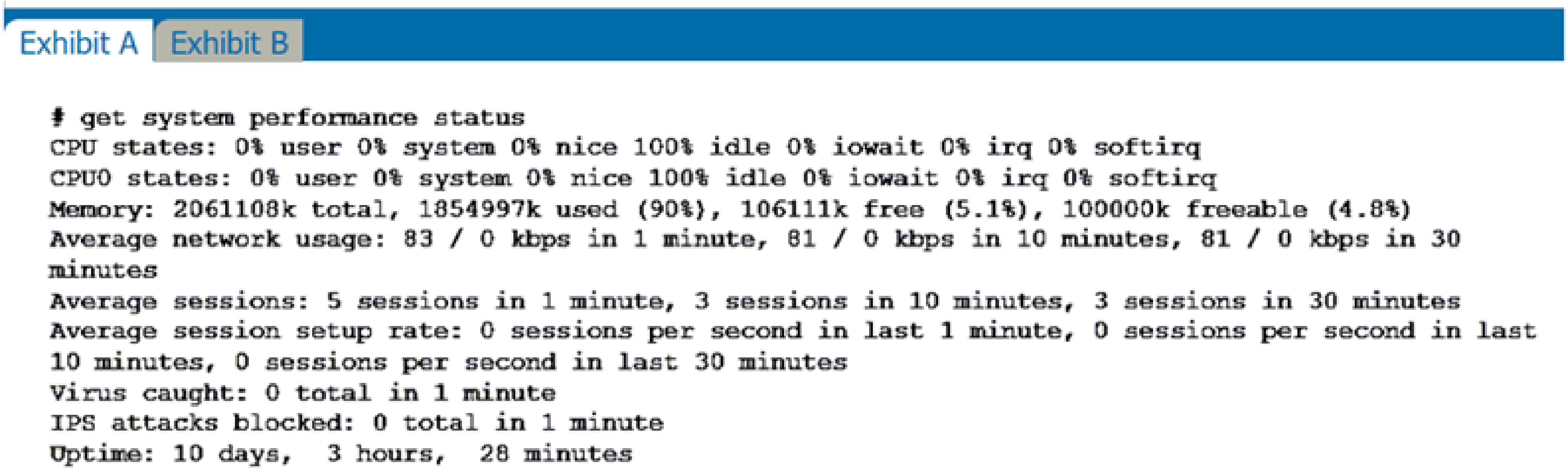
precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

NEW QUESTION 22
Which three statements explain a flow-based antivirus profile? (Choose three.)

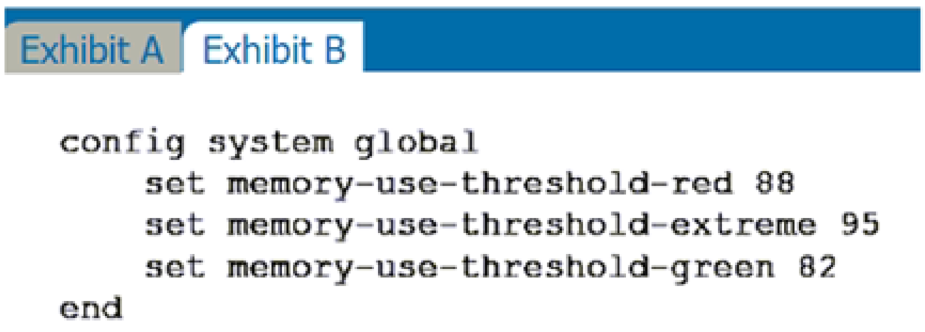
A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
B. If a virus is detected, the last packet is delivered to the client.
C. The IPS engine handles the process as a standalone.
D. FortiGate buffers the whole file but transmits to the client at the same time.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

Answer: ADE

NEW QUESTION 27
Refer to the exhibits.



```
# 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
```



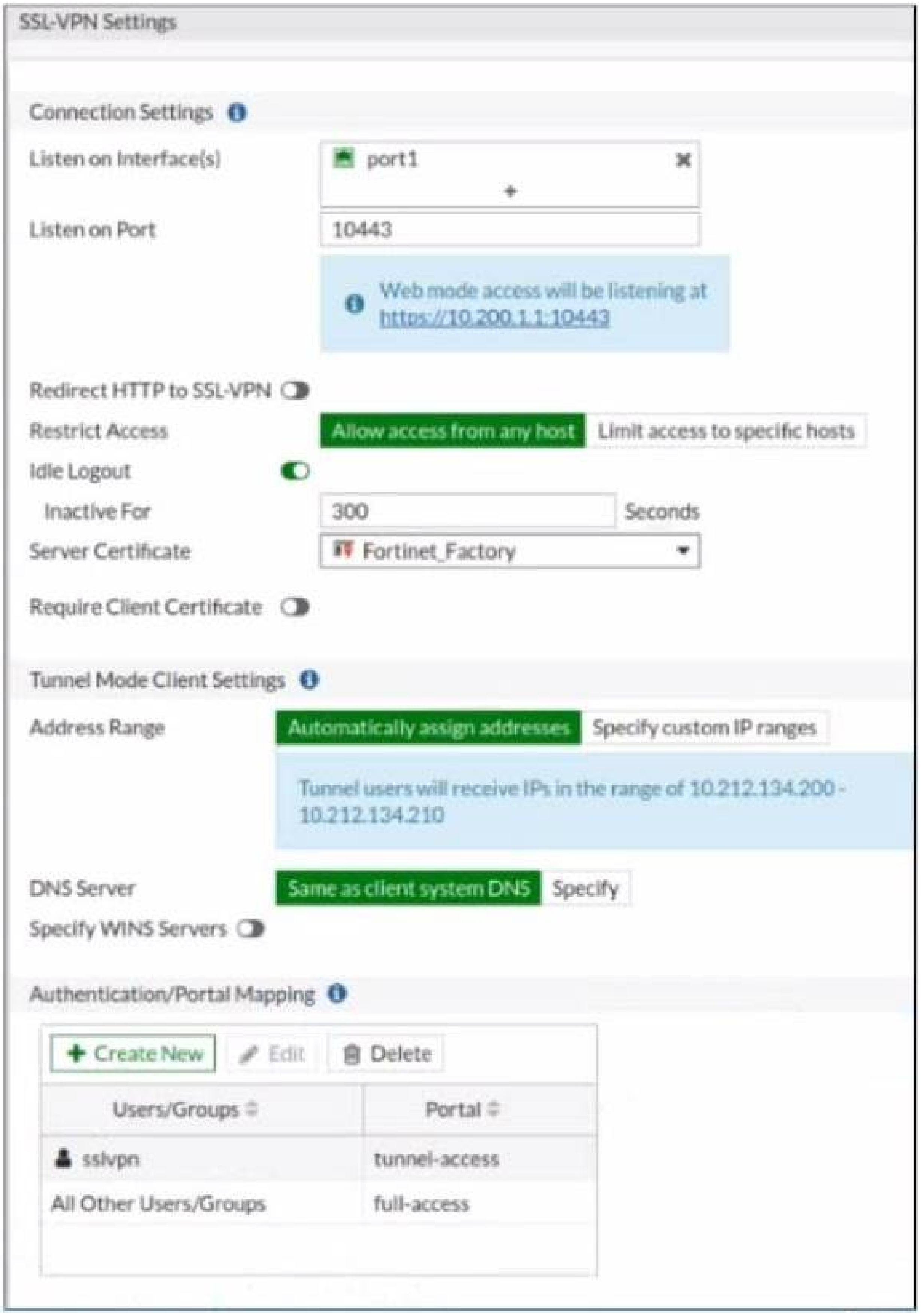
```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

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

Answer: BD

NEW QUESTION 32
Refer to the exhibits.



SSL-VPN Settings

Connection Settings

Listen on Interface(s): port1

Listen on Port: 10443

Web mode access will be listening at https://10.200.1.1:10443

Redirect HTTP to SSL-VPN: ○

Restrict Access: Allow access from any host | Limit access to specific hosts

Idle Logout: ●

Inactive For: 300 Seconds

Server Certificate: Fortinet_Factory

Require Client Certificate: ○

Tunnel Mode Client Settings

Address Range: Automatically assign addresses | Specify custom IP ranges

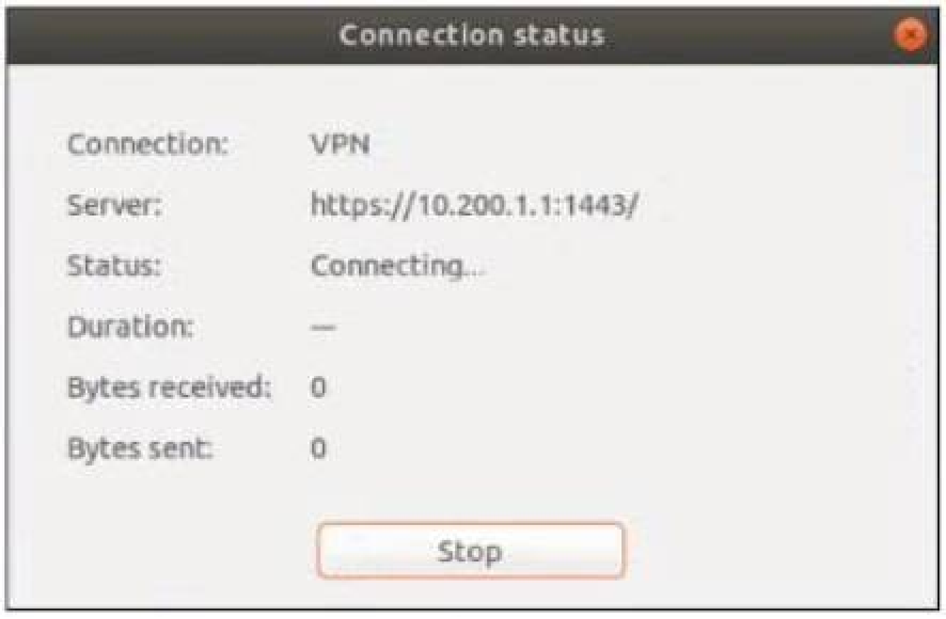
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server: Same as client system DNS | Specify

Specify WINS Servers: ○

Authentication/Portal Mapping

Users/Groups	Portal
sslvpn	tunnel-access
All Other Users/Groups	full-access



Connection status

Connection: VPN

Server: https://10.200.1.1:1443/

Status: Connecting...

Duration: —

Bytes received: 0

Bytes sent: 0

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.
B. Change the Server IP address.
C. Change the idle-timeout.
D. Change the SSL VPN portal to the tunnel.

Answer: A

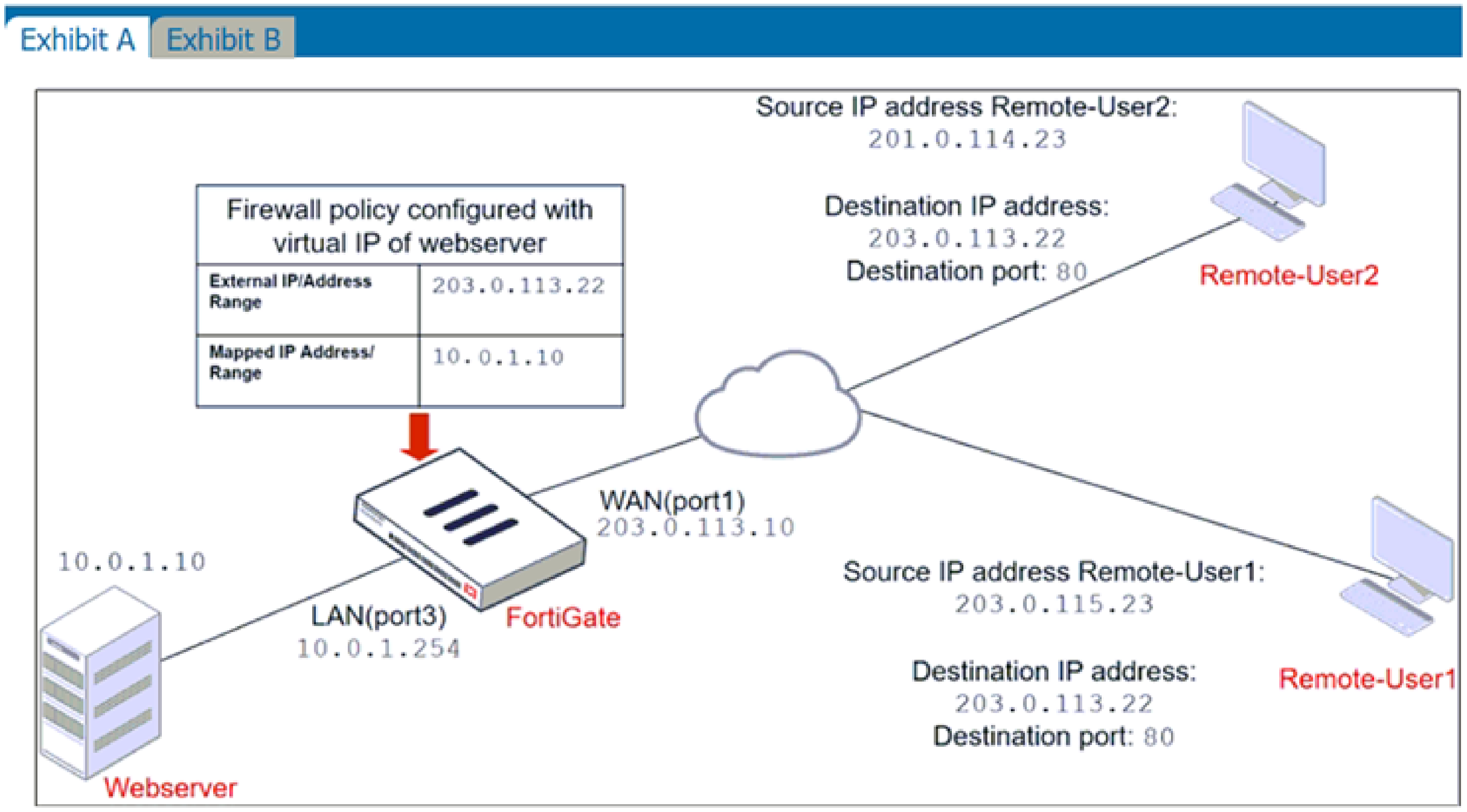
NEW QUESTION 36
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

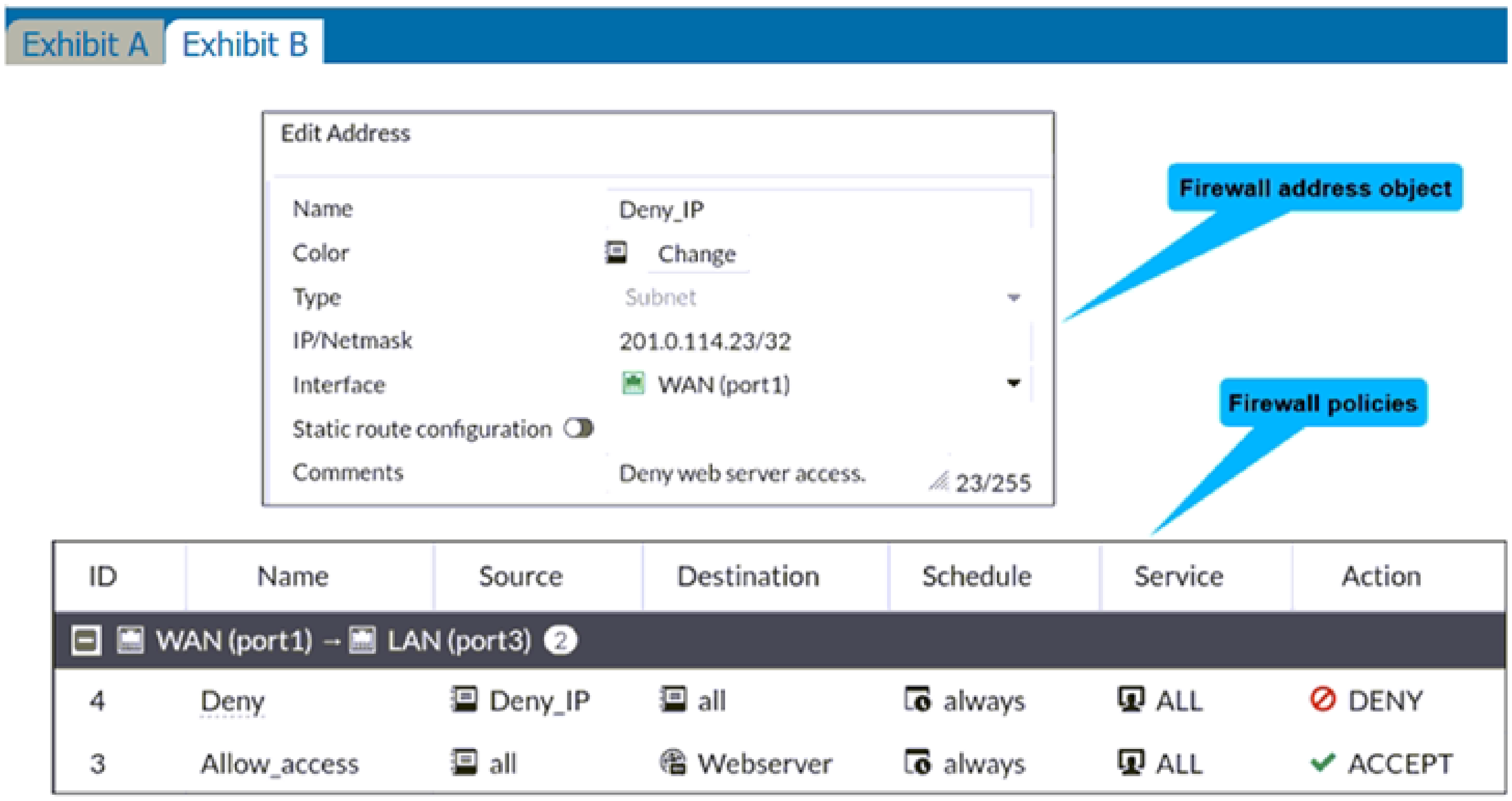
A. Warning
B. Exempt

C. Allow
D. Learn

Answer: AC

NEW QUESTION 41
Refer to the exhibits.
The exhibits show a network diagram and firewall configurations.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.





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

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

In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

A. Disable match-vip in the Deny policy.
B. Set the Destination address as Deny_IP in the Allow-access policy.
C. Enable match vip in the Deny policy.
D. Set the Destination address as Web_server in the Deny policy.

Answer: BC

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta The exhibits show a network diagram and firewall configurations for a FortiGate unit that has two policies:
Allow_access and Deny. The Allow_access policy allows traffic from the WAN (port1) interface to the LAN (port3) interface with the destination address of VIP and the service of HTTPS. The VIP object maps the external IP address 10.200.1.10 and port 10443 to the internal IP address 10.0.1.10 and port 443 of the Webserver. The Deny policy denies traffic from the WAN (port1) interface to the LAN (port3) interface with the source address of Deny_IP and the destination address of All.
In this scenario, the administrator wants to deny Webserver access for Remote-User2, who has the IP address 10.200.3.2 , which is included in the Deny_IP address object. Remote-User1, who has the IP address 10.200.3.1, must be able to access the Webserver.
To achieve this goal, the administrator can make two changes to deny Webserver access for Remote-User2:

- Set the Destination address as Webserver in the Deny policy. This will make the Deny policy more specific and match only the traffic that is destined for the Webserver's internal IP address, instead of any destination address.
- Enable match-vip in the Deny policy. This will make the Deny policy apply to traffic that matches a VIP object, instead of ignoring it1. This way, the Deny policy will block Remote-User2's traffic that uses the VIP object's external IP address and port.

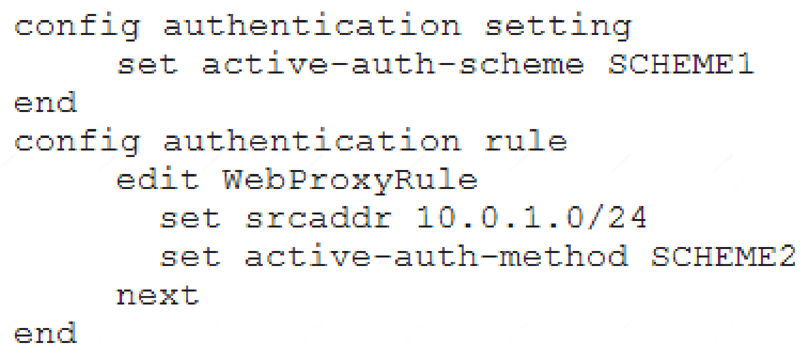
NEW QUESTION 46
Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
B. To finish any inspection operations
C. To remove the NAT operation
D. To generate logs

Answer: A

Explanation:
TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

NEW QUESTION 48
Examine this FortiGate configuration:



```
config authentication setting
     set active-auth-scheme SCHEME1
end
config authentication rule
     edit WebProxyRule
       set srcaddr 10.0.1.0/24
       set active-auth-method SCHEME2
     next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

A. It always authorizes the traffic without requiring authentication.
B. It drops the traffic.
C. It authenticates the traffic using the authentication scheme SCHEME2.
D. It authenticates the traffic using the authentication scheme SCHEME1.

Answer: D

Explanation:
"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

NEW QUESTION 49
In which two ways can RPF checking be disabled? (Choose two)

A. Enable anti-replay in firewall policy.
B. Disable the RPF check at the FortiGate interface level for the source check
C. Enable asymmetric routing.
D. Disable strict-arc-check under system settings.

Answer: CD

NEW QUESTION 51
Refer to the exhibits.
Exhibit A shows the application sensor configuration. Exhibit B shows the Excessive-Bandwidth and Apple filter details.

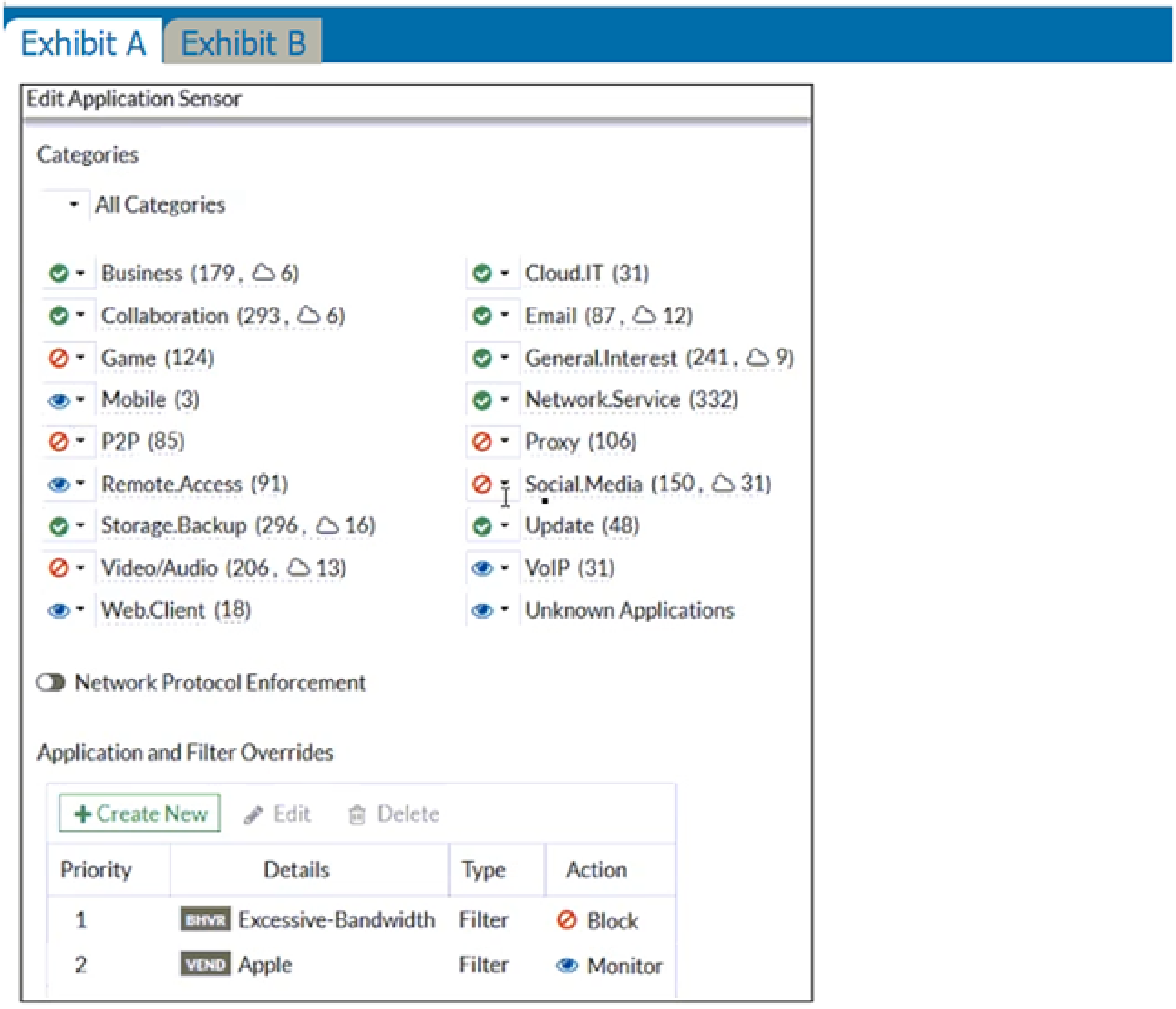


Exhibit A | Exhibit B

Edit Application Sensor

Categories

All Categories

- ✓ Business (179, ☁ 6)
- ✓ Collaboration (293, ☁ 6)
- ⊘ Game (124)
- 👁 Mobile (3)
- ⊘ P2P (85)
- 👁 Remote.Access (91)
- ✓ Storage.Backup (296, ☁ 16)
- ⊘ Video/Audio (206, ☁ 13)
- 👁 Web.Client (18)
- ✓ Cloud.IT (31)
- ✓ Email (87, ☁ 12)
- ✓ General.Interest (241, ☁ 9)
- ✓ Network.Service (332)
- ⊘ Proxy (106)
- ⊘ Social.Media (150, ☁ 31)
- ✓ Update (48)
- 👁 VoIP (31)
- 👁 Unknown Applications

○ Network Protocol Enforcement

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	⊘ Block
2	VEND Apple	Filter	👁 Monitor

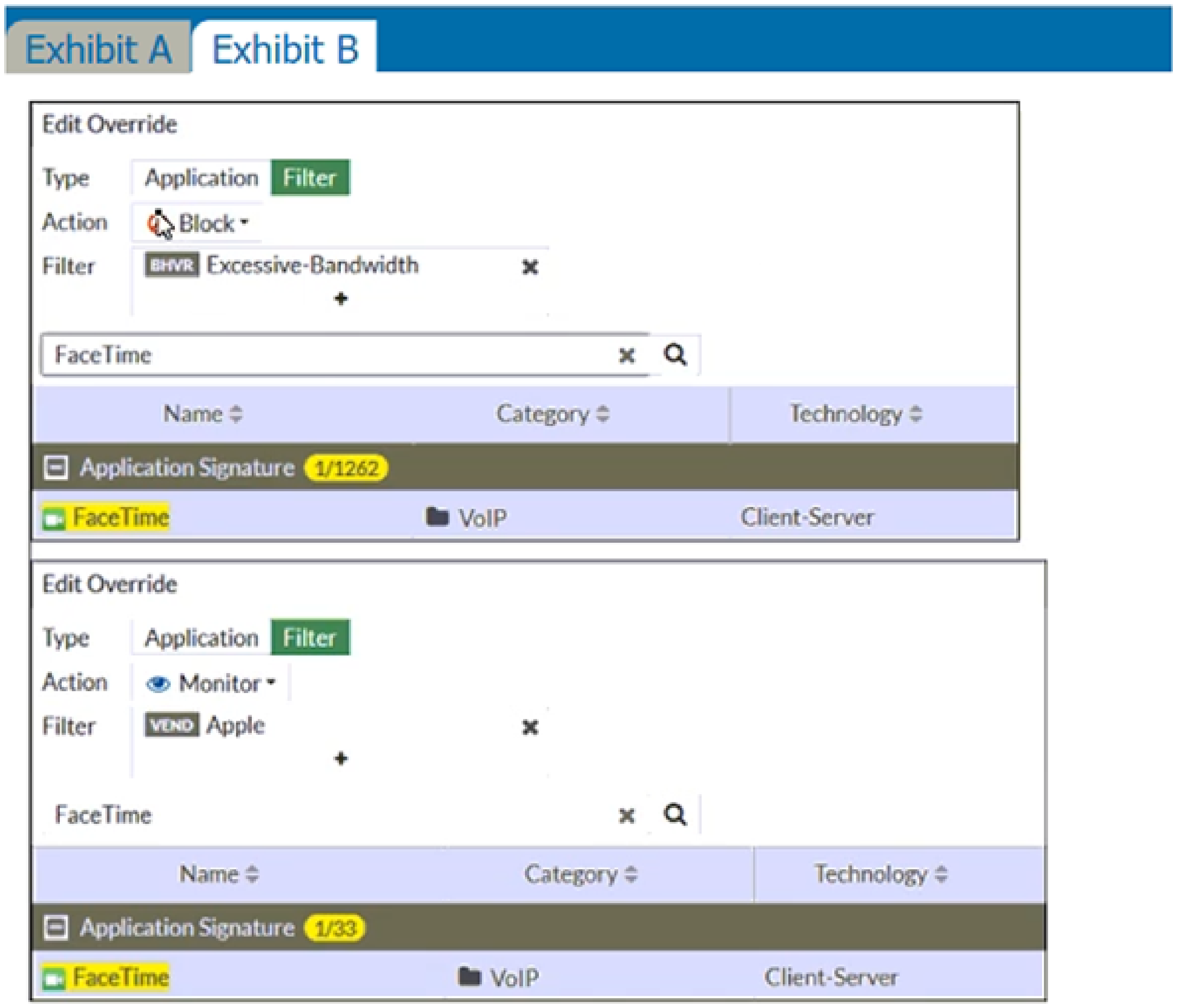


Exhibit A | Exhibit B

Edit Override

Type: Application | Filter

Action: ⊘ Block

Filter: BHVR Excessive-Bandwidth ✕

FaceTime

Name	Category	Technology
Application Signature 1/1262		
FaceTime	VoIP	Client-Server

Edit Override

Type: Application | Filter

Action: 👁 Monitor

Filter: VEND Apple ✕

FaceTime

Name	Category	Technology
Application Signature 1/33		
FaceTime	VoIP	Client-Server

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

A. Apple FaceTime will be allowed, based on the Categories configuration.
B. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.
C. Apple FaceTime will be allowed, based on the Apple filter configuration.
D. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

Answer: B

Explanation:
FortiGate Security 7.2 Study Guide (p.310): "Then, FortiGate scans packets for matches, in this order, for the application control profile: 1. Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies. 2. Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories."

NEW QUESTION 55
Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

A. Web filter in flow-based inspection
B. Antivirus in flow-based inspection
C. DNS filter
D. Web application firewall
E. Application control

Answer: ABE

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow

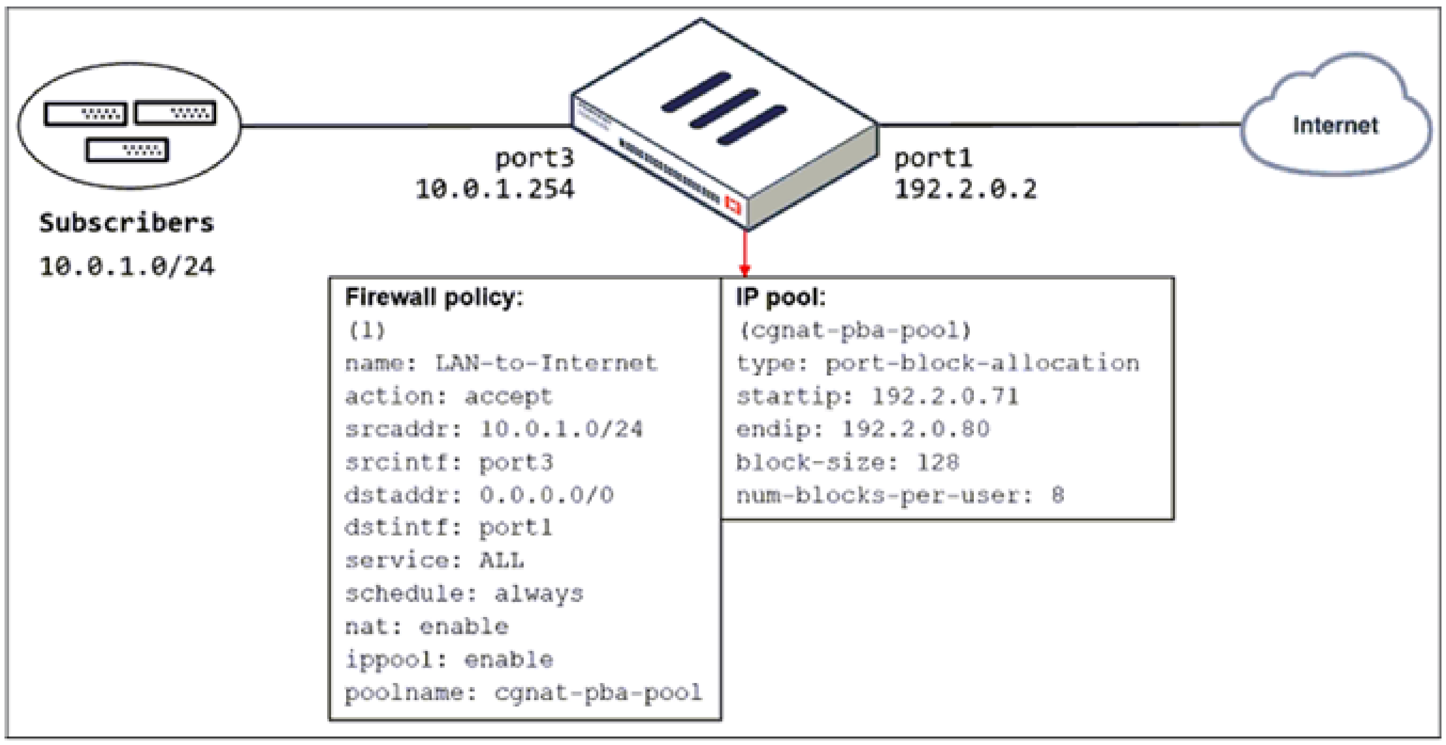
NEW QUESTION 57
What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scanning of application traffic to the DNS protocol only.
B. It limits the scanning of application traffic to use parent signatures only.
C. It limits the scanning of application traffic to the browser-based technology category only.
D. It limits the scanning of application traffic to the application category only.

Answer: C

Explanation:
FortiGate Security 7.2 Study Guide (p.317): "You can configure the URL Category within the same security policy; however, adding a URL filter causes application control to scan applications in only the browser-based technology category, for example, Facebook Messenger on the Facebook website."

NEW QUESTION 58
Refer to the exhibit.
The exhibit shows a diagram of a FortiGate device connected to the network and the firewall policy and IP pool configuration on the FortiGate device.



Firewall policy:

```
(1)
name: LAN-to-Internet
action: accept
srcaddr: 10.0.1.0/24
srcintf: port3
dstaddr: 0.0.0.0/0
dstintf: port1
service: ALL
schedule: always
nat: enable
ippool: enable
poolname: cgnat-pba-pool
```

IP pool:

```
(cgnat-pba-pool)
type: port-block-allocation
startip: 192.2.0.71
endip: 192.2.0.80
block-size: 128
num-blocks-per-user: 8
```

Which two actions does FortiGate take on internet traffic sourced from the subscribers? (Choose two.)

A. FortiGate allocates port blocks per user, based on the configured range of internal IP addresses.
B. FortiGate allocates port blocks on a first-come, first-served basis.
C. FortiGate generates a system event log for every port block allocation made per user.
D. FortiGate allocates 128 port blocks per user.

Answer: BC

Explanation:
FortiGate Security 7.2 Study Guide (p.109): "FortiGate allocates port blocks on a first-come, first-served basis." "For logging purposes, when FortiGate allocates a port block to a host, it generates a system event log to inform the administrator."

NEW QUESTION 60
A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. 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 the file can be
downloaded.
What is the reason for the failed virus detection by FortiGate?

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

Answer: AC

Explanation:
SSL Inspection Profile, on the Inspection method there are 2 options to choose from, SSL Certificate Inspection or Full SSL Inspection. FG SEC 7.2 Studi Guide: Full SSL Inspection level is the only choice that allows antivirus to be effective.

NEW QUESTION 63
Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

A. DNS
B. ping
C. udp-echo
D. TWAMP

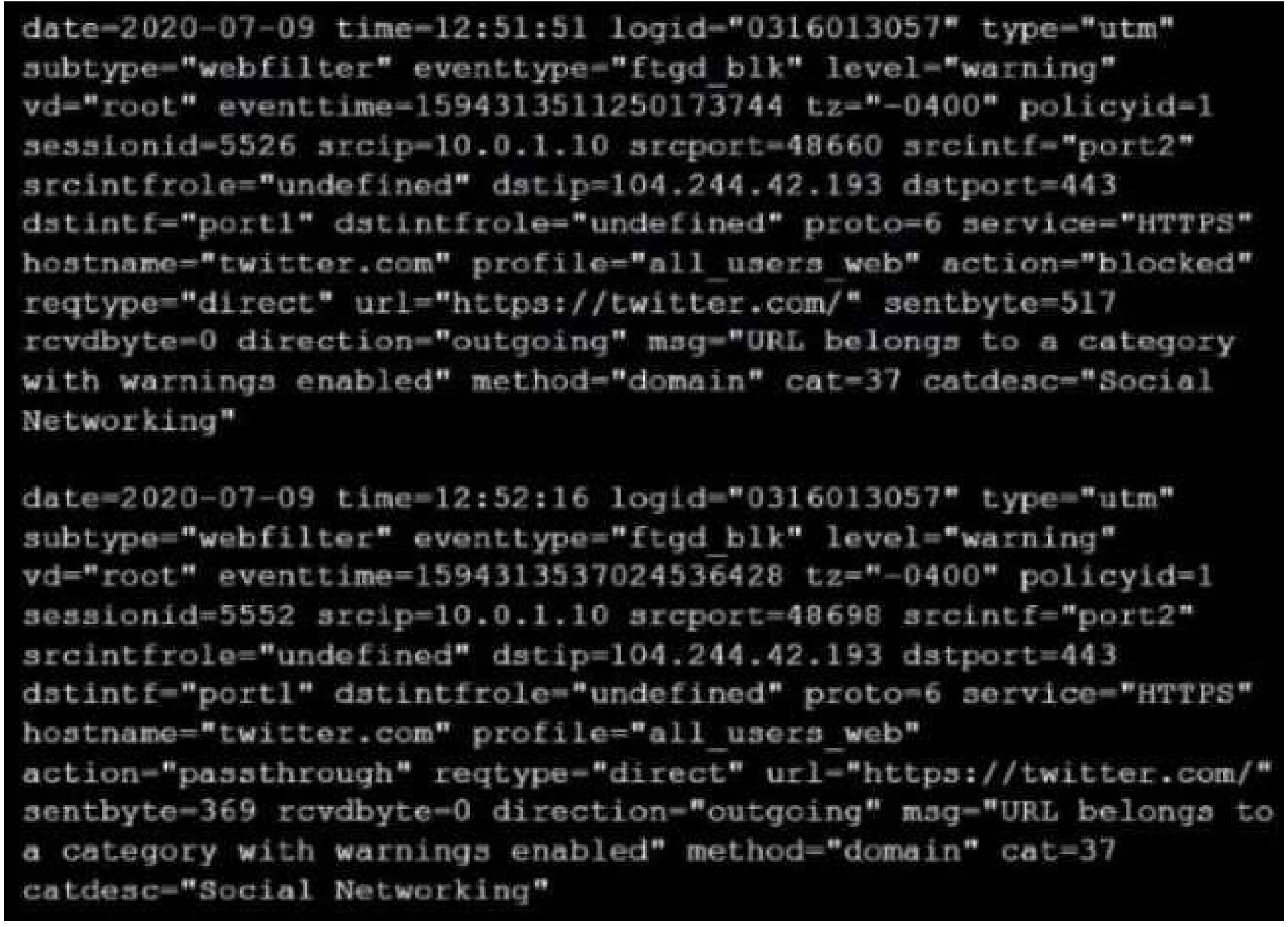
Answer: CD

NEW QUESTION 66
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

A. diagnose wad session list
B. diagnose wad session list | grep hook-pre&&hook-out
C. diagnose wad session list | grep hook=pre&&hook=out
D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 67
Refer to the web filter raw logs.



```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web" action="blocked"
reqtype="direct" url="https://twitter.com/" sentbyte=517
rcvdbyte=0 direction="outgoing" msg="URL belongs to a category
with warnings enabled" method="domain" cat=37 catdesc="Social
Networking"

date=2020-07-09 time=12:52:16 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313537024536428 tz="-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web"
action="passthrough" reqtype="direct" url="https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction="outgoing" msg="URL belongs to
a category with warnings enabled" method="domain" cat=37
catdesc="Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

A. Social networking web filter category is configured with the action set to authenticate.
B. The action on firewall policy ID 1 is set to warning.
C. Access to the social networking web filter category was explicitly blocked to all users.
D. The name of the firewall policy is all_users_web.

Answer: A

NEW QUESTION 70
On FortiGate, which type of logs record information about traffic directly to and from the FortiGate management IP addresses?

A. System event logs
B. Forward traffic logs
C. Local traffic logs
D. Security logs

Answer: C

NEW QUESTION 74
Which timeout setting can be responsible for deleting SSL VPN associated sessions?

A. SSL VPN idle-timeout

B. SSL VPN http-request-body-timeout
C. SSL VPN login-timeout
D. SSL VPN dtls-hello-timeout

Answer: A

NEW QUESTION 76
An administrator configures outgoing interface any in a firewall policy. What is the result of the policy list view?

A. Search option is disabled.
B. Policy lookup is disabled.
C. By Sequence view is disabled.
D. Interface Pair view is disabled.

Answer: D

Explanation:
"If you use multiple source or destination interfaces, or the any interface in a firewall policy, you cannot separate policies into sections by interface pairs—some would be triplets or more. So instead, policies are then always displayed in a single list (By Sequence)."

NEW QUESTION 79
When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

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

Answer: B

Explanation:
FortiGate Security 7.2 Study Guide (p.67): "When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer."

NEW QUESTION 82
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. In advanced mode, security profiles can be applied only to user groups, not individual users.
C. Advanced mode uses the Windows convention—NetBios: Domain\Username.
D. Advanced mode supports nested or inherited groups.

Answer: AD

Explanation:
* A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
This is true because advanced mode allows FortiGate to query the LDAP server directly for user information and group membership, without relying on the collector agent. This enables FortiGate to apply security policies based on LDAP group filters, which can be configured on FortiGate1
* D. Advanced mode supports nested or inherited groups.
This is true because advanced mode can handle complex group structures, such as nested groups or inherited groups, where a user belongs to a group that is a member of another group. This allows FortiGate to apply security policies based on the effective group membership of a user, not just the direct group membership1
FortiGate Infrastructure 7.2 Study Guide (p.146): "Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups." "In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent."

NEW QUESTION 86
FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.
Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

A. www.example.com:443
B. www.example.com
C. example.com
D. www.example.com/index.html

Answer: BC

Explanation:
When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names - no URLs or wildcard characters are allowed.
OK: google.com or www.google.com
NO OK: www.google.com/index.html or google.* FortiGate_Security_6.4 page 384
When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names-- "no URLs or wildcard characters are allowed".

NEW QUESTION 91

An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.
Which DPD mode on FortiGate will meet the above requirement?

A. Disabled
B. On Demand
C. Enabled
D. On Idle

Answer: D

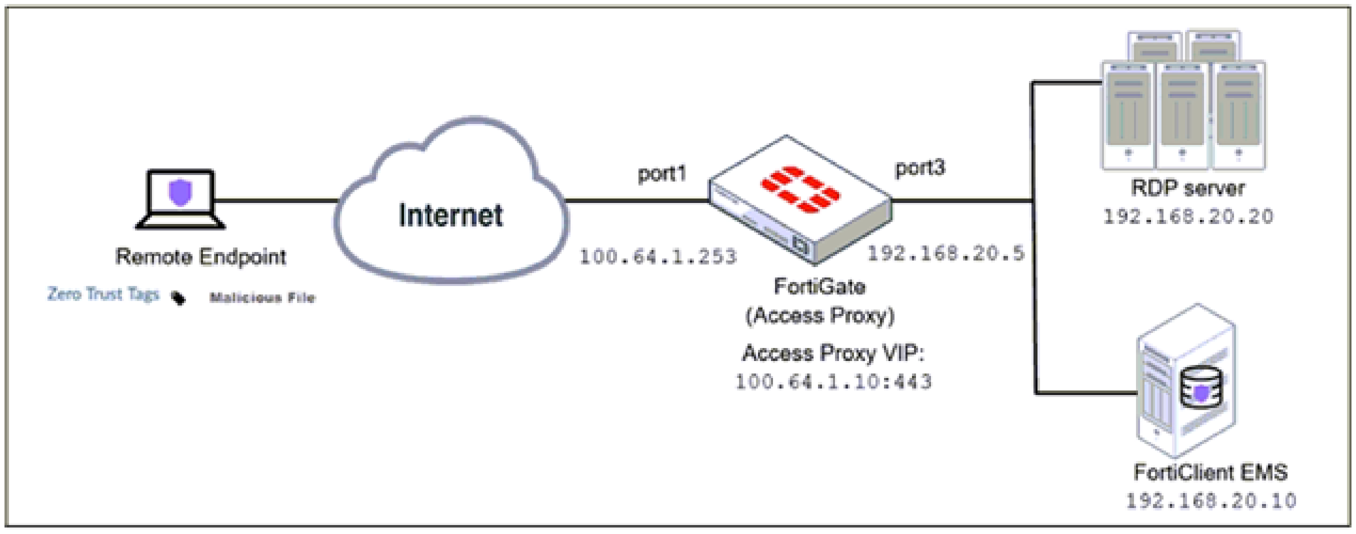
NEW QUESTION 94
By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

A. set fortiguard-anycast disable
B. set webfilter-force-off disable
C. set webfilter-cache disable
D. set protocol tcp

Answer: A

Explanation:
y default, "fortiguard-anycast" is enabled, and this setting only works with "set protocol https". To use udp (ie. "set protocol udp"), "fortiguard-anycast" must be disabled.

NEW QUESTION 95
Refer to the exhibit.



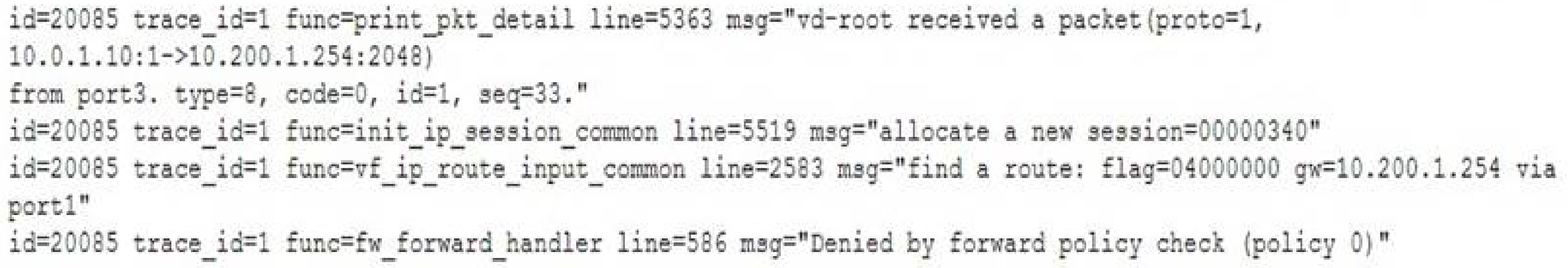
Based on the ZTNA tag, the security posture of the remote endpoint has changed. What will happen to endpoint active ZTNA sessions?

A. They will be re-evaluated to match the endpoint policy.
B. They will be re-evaluated to match the firewall policy.
C. They will be re-evaluated to match the ZTNA policy.
D. They will be re-evaluated to match the security policy.

Answer: C

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-zt FortiGate Infrastructure 7.2 Study Guide (p.182): "Endpoint posture changes trigger active ZTNA proxy
sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy."

NEW QUESTION 97
Examine this output from a debug flow:



```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

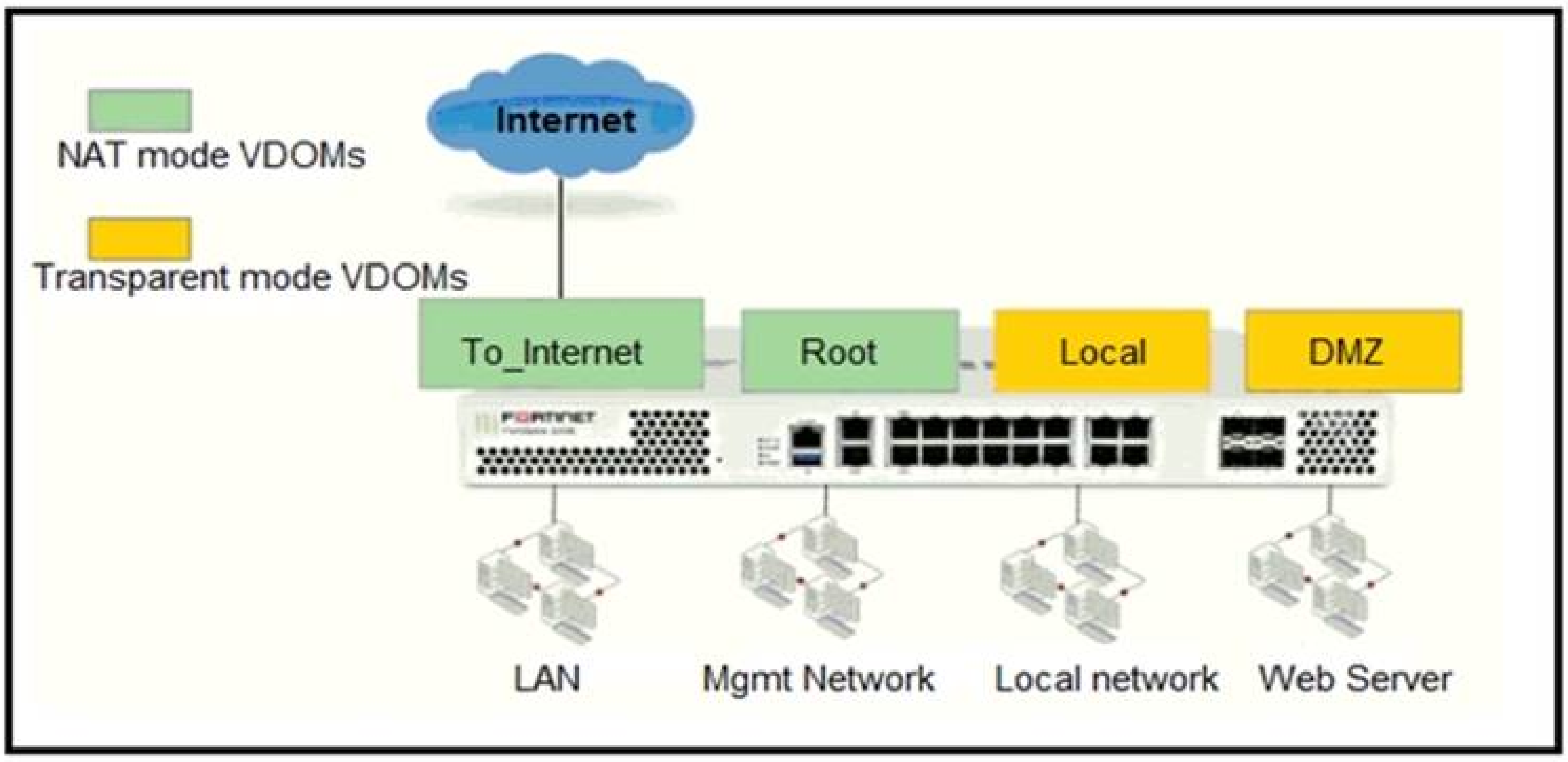
A. The next-hop IP address is unreachable.
B. It failed the RPF check .
C. It matched an explicitly configured firewall policy with the action DENY.
D. It matched the default implicit firewall policy.

Answer: D

Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=13900 https://www.fortinetguru.com/2016/03/what-is-policy-id-0-and-why-lot-of-denied-traffic-on-this-policy/

NEW QUESTION 98
Refer to the exhibit.

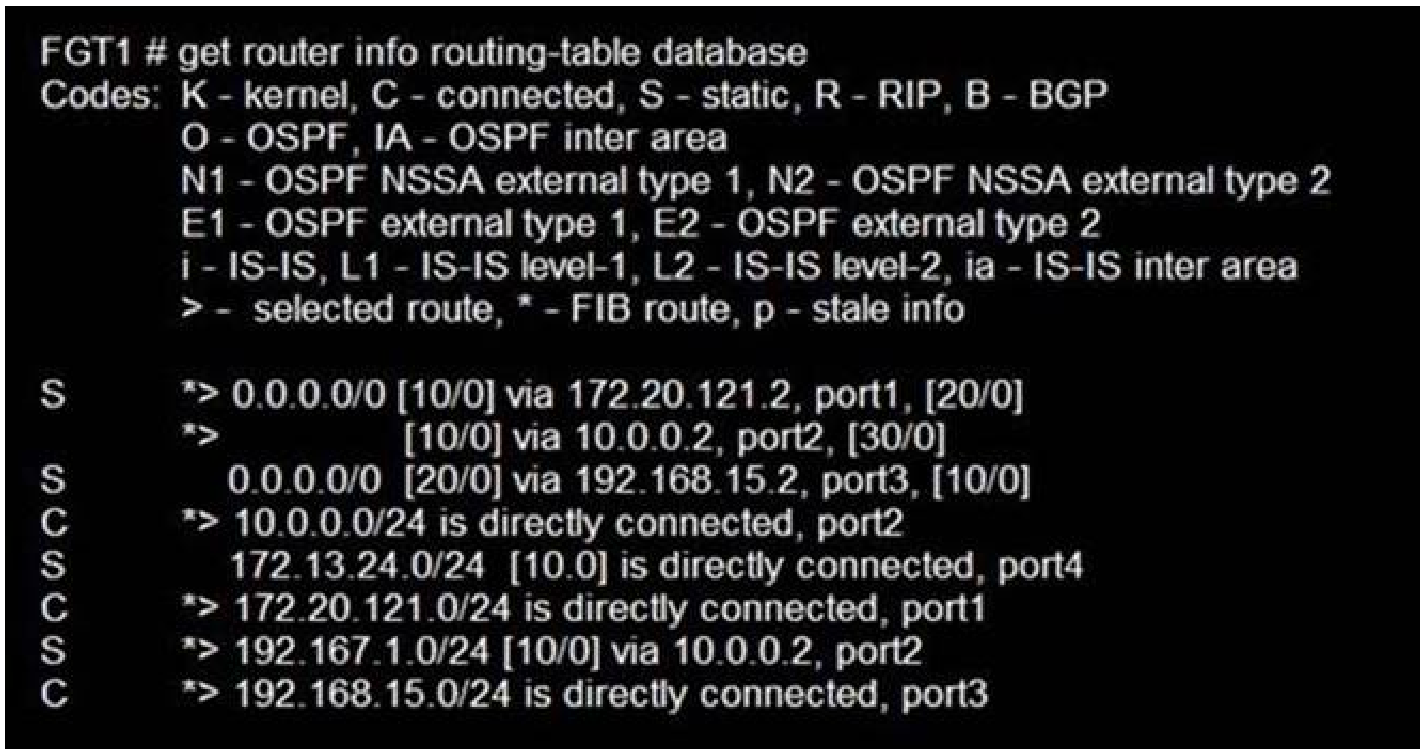


The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected 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 static route is 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

NEW QUESTION 103
Refer to the exhibit.



```
FGT1 # 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
        > -  selected route, * - FIB route, p - stale info

S       *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
        *>              [10/0] via 10.0.0.2, port2, [30/0]
S          0.0.0.0/0  [20/0] via 192.168.15.2, port3, [10/0]
C       *> 10.0.0.0/24 is directly connected, port2
S          172.13.24.0/24  [10.0] is directly connected, port4
C       *> 172.20.121.0/24 is directly connected, port1
S       *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C       *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

A. The port3 default route has the lowest metric.
B. The port1 and port2 default routes are active in the routing table.
C. The ports default route has the highest distance.
D. There will be eight routes active in the routing table.

Answer: BC

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-identify-Inactive-Routes-in-the-Routing/ta-p

NEW QUESTION 104
An administrator needs to increase network bandwidth and provide redundancy.
What interface type must the administrator select to bind multiple FortiGate interfaces?

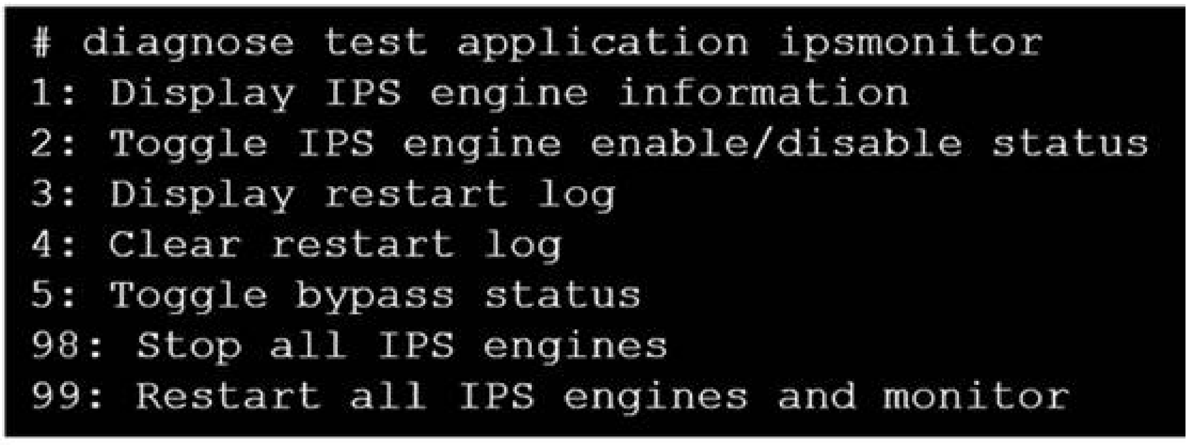
A. VLAN interface
B. Software Switch interface

C. Aggregate interface
D. Redundant interface

Answer: C

Explanation:
An aggregate interface is a logical interface that combines two or more physical interfaces into one virtual interface1. An aggregate interface can increase network bandwidth and provide redundancy by distributing traffic across multiple physical interfaces using a load balancing algorithm1. An aggregate interface can also support link aggregation control protocol (LACP) to negotiate the link aggregation settings with the connected device1.

NEW QUESTION 108
Refer to the exhibit.



```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.
Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.
B. The IPS engine was unable to prevent an intrusion attack .
C. The IPS engine was blocking all traffic.
D. The IPS engine will continue to run in a normal state.

Answer: A

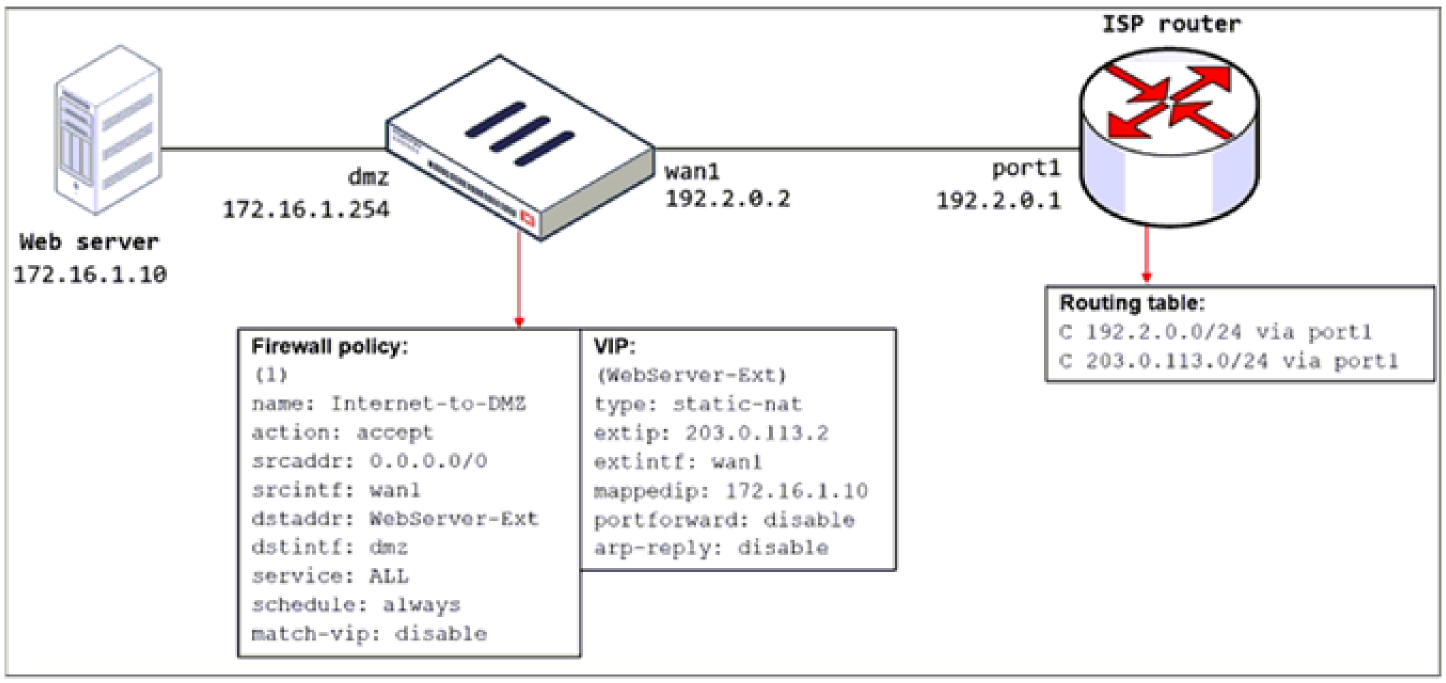
Explanation:
fortinet-fortigate-security-study-guide-for-fortios-72 page 417 If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

NEW QUESTION 110
In an explicit proxy setup, where is the authentication method and database configured?

A. Proxy Policy
B. Authentication Rule
C. Firewall Policy
D. Authentication scheme

Answer: D

NEW QUESTION 112
Refer to the exhibit.
The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.
When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



Firewall policy:

```
(1)
name: Internet-to-DMZ
action: accept
srcaddr: 0.0.0.0/0
srcintf: wan1
dstaddr: WebServer-Ext
dstintf: dmz
service: ALL
schedule: always
match-vip: disable
```

VIP:

```
(WebServer-Ext)
type: static-nat
extip: 203.0.113.2
extintf: wan1
mappedip: 172.16.1.10
portforward: disable
arp-reply: disable
```

Routing table:

```
C 192.2.0.0/24 via port1
C 203.0.113.0/24 via port1
```

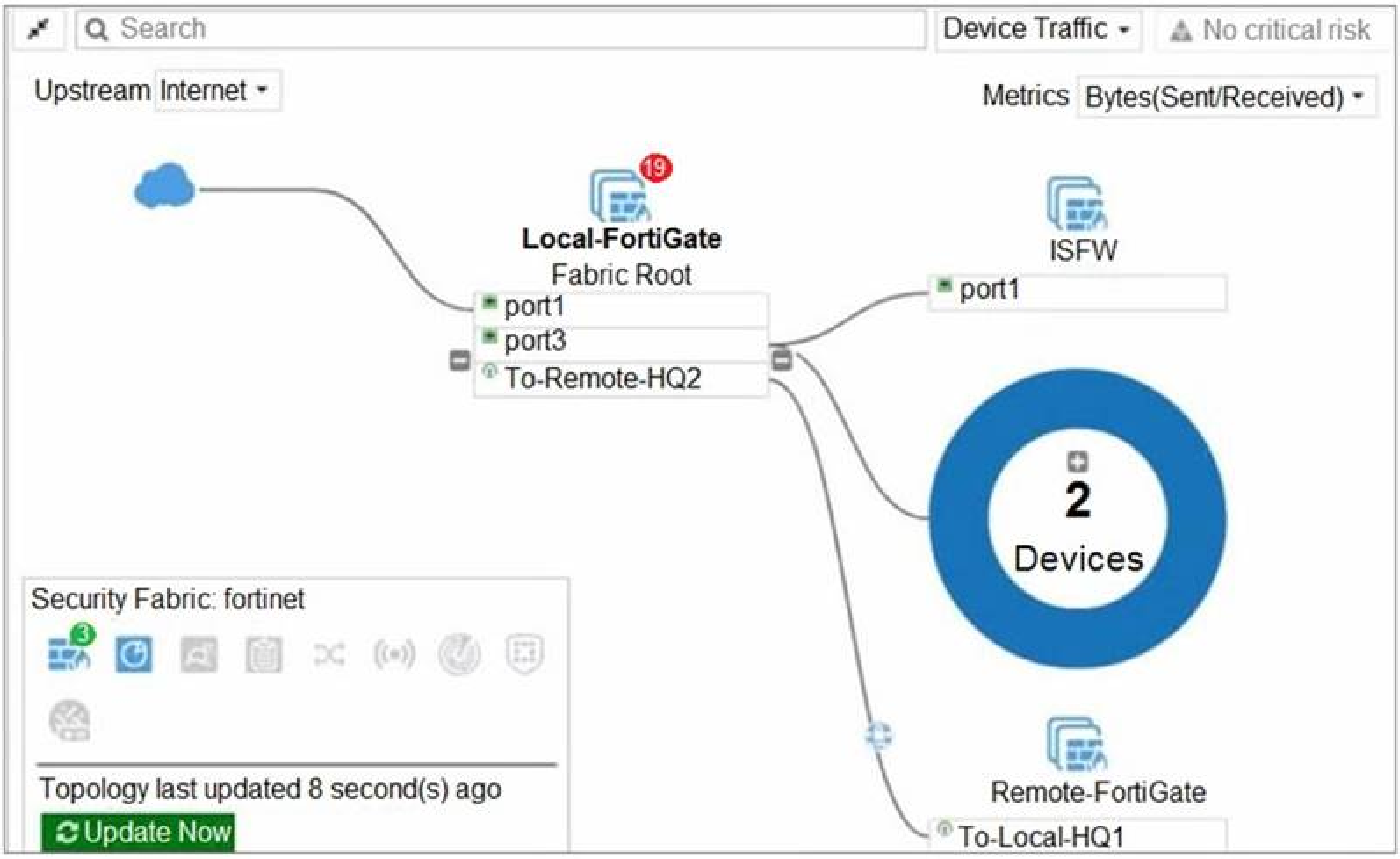
Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

A. Configure a loopback interface with address 203.0.113.2/32.
B. In the VIP configuration, enable arp-reply.
C. Enable port forwarding on the server to map the external service port to the internal service port.
D. In the firewall policy configuration, enable match-vip.

Answer: B

Explanation:
FortiGate Security 7.2 Study Guide (p.115): "Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled."

NEW QUESTION 114
Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. There are five devices that are part of the security fabric.
B. Device detection is disabled on all FortiGate devices.
C. This security fabric topology is a logical topology view.
D. There are 19 security recommendations for the security fabric.

Answer: CD

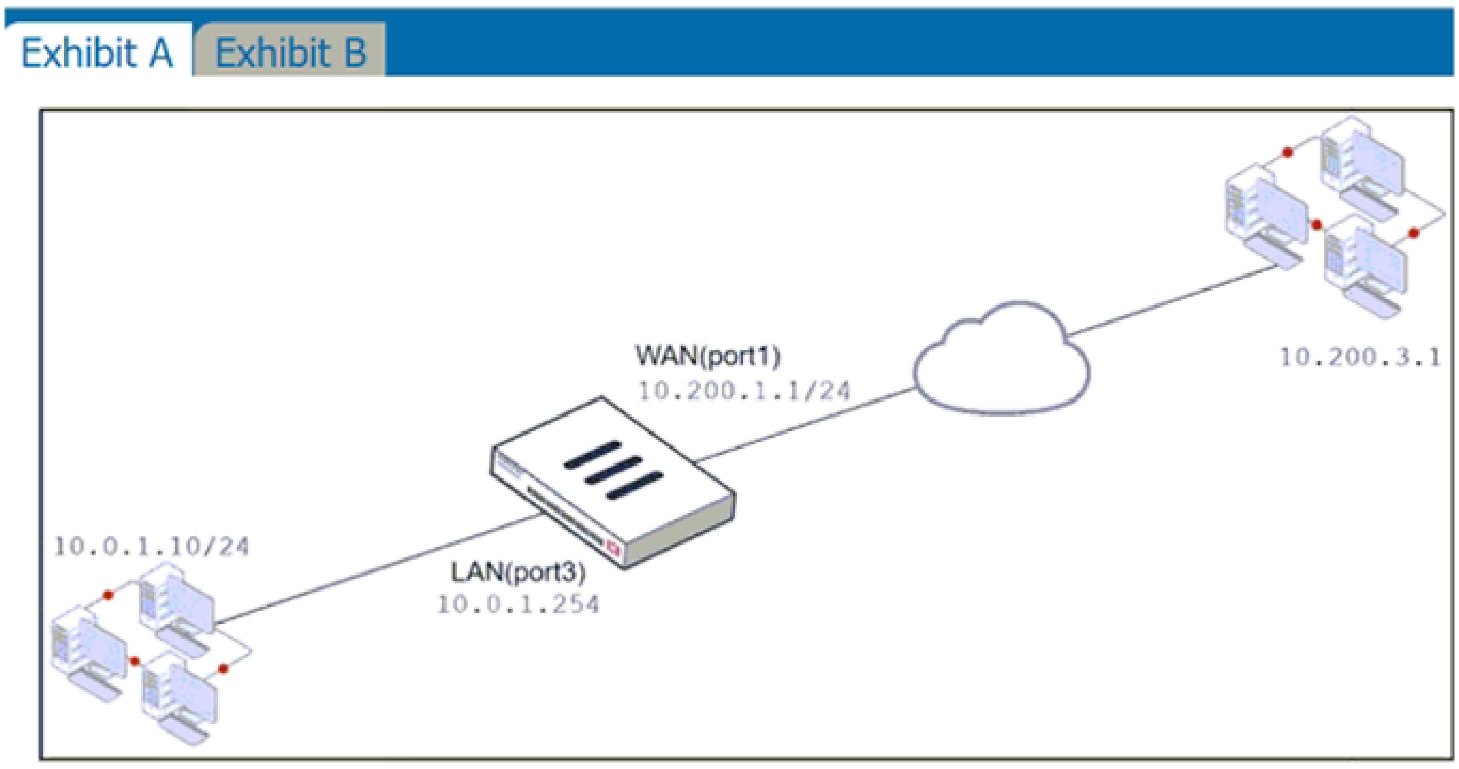
Explanation:
References: https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results
https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology

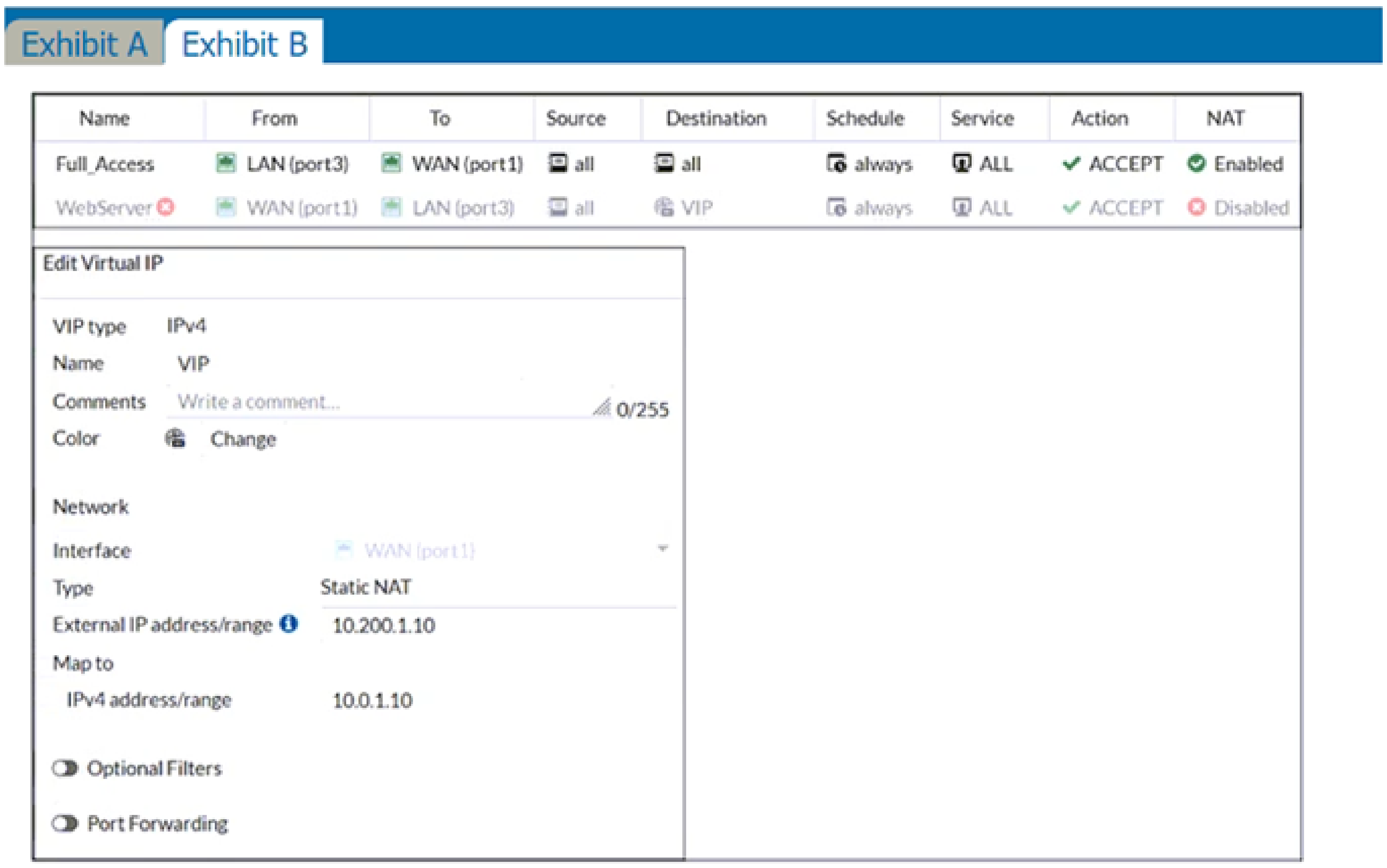
NEW QUESTION 117
Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

A. Subject Key Identifier value
B. SMMIE Capabilities value
C. Subject value
D. Subject Alternative Name value

Answer: A

NEW QUESTION 120
Refer to the exhibits.
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.
The WAN (port1) interface has the IP address 10.200.1.1/24.
The LAN (port3) interface has the IP address 10.0.1.254/24.
The administrator disabled the WebServer firewall policy.





Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	✓ ACCEPT	Enabled
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	✓ ACCEPT	Disabled

Edit Virtual IP

VIP type IPv4
Name VIP
Comments Write a comment... 0/255
Color Change

Network

Interface WAN (port1)
Type Static NAT
External IP address/range 10.200.1.10
Map to
IPv4 address/range 10.0.1.10

Optional Filters

Port Forwarding

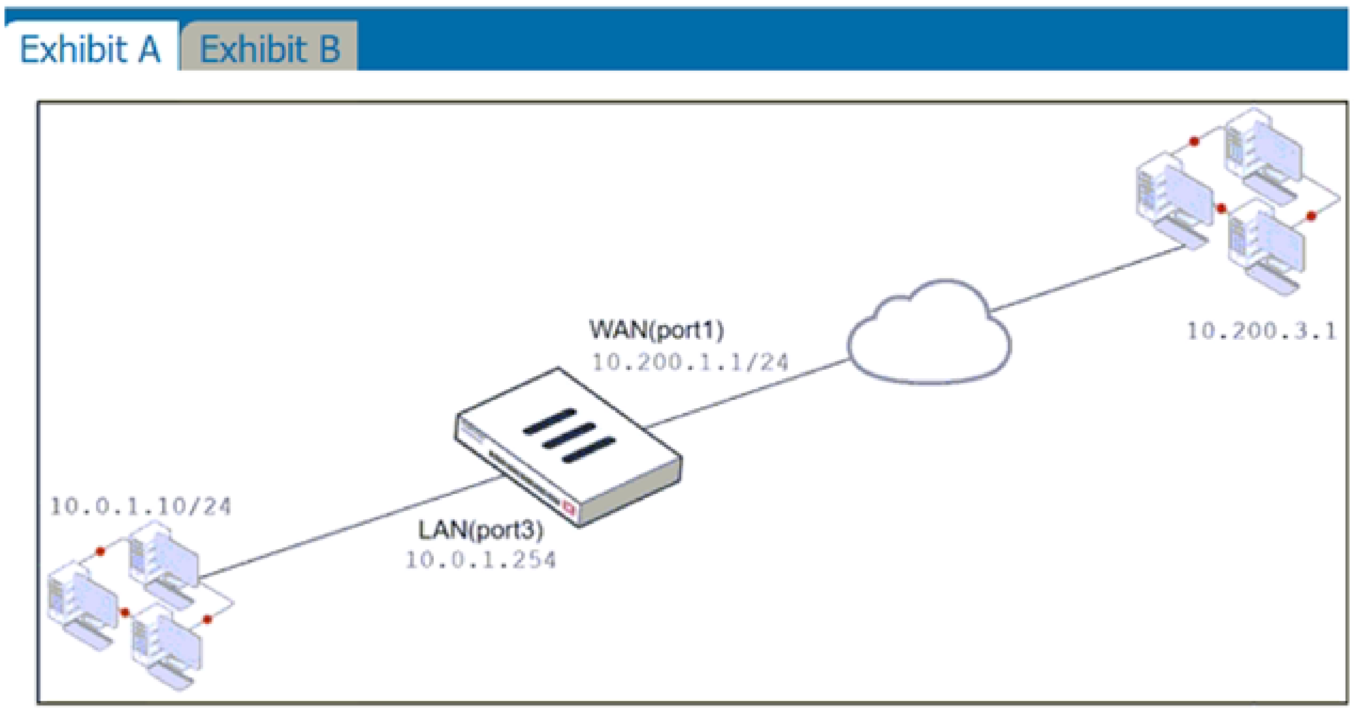
Which IP address will be used to source NAT the traffic, if a user with address 10.0.1.10 connects over SSH to the host with address 10.200.3.1?

A. 10.200.1.10
B. 10.0.1.254
C. 10.200.1.1
D. 10.200.3.1

Answer: C

Explanation:
Traffic is coming from LAN to WAN, matches policy Full_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

NEW QUESTION 125
Refer to the exhibit.



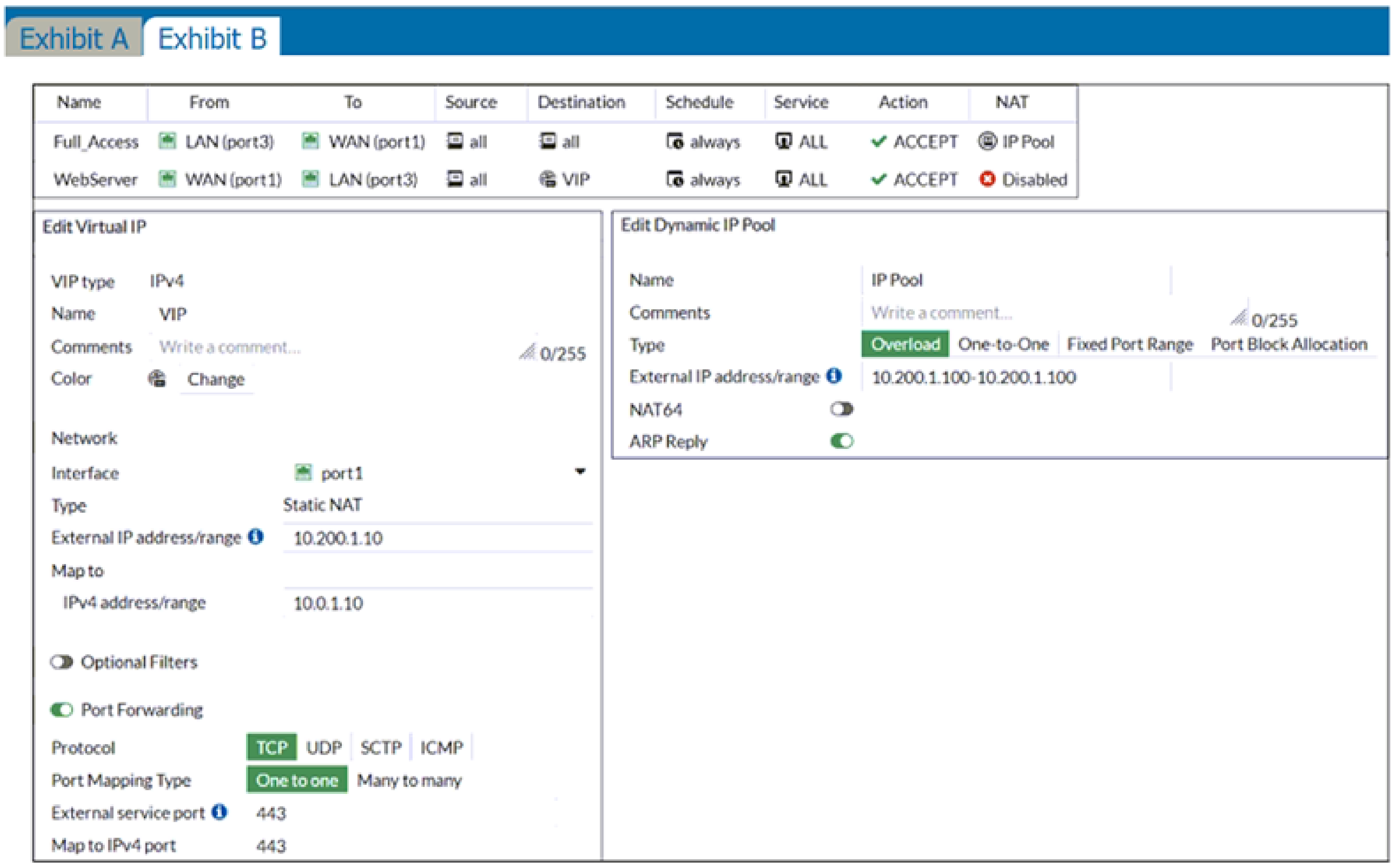


Exhibit A Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	✓ ACCEPT	IP Pool
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	✓ ACCEPT	Disabled

Edit Virtual IP

VIP type IPv4
Name VIP
Comments Write a comment... 0/255
Color Change

Network
Interface port1
Type Static NAT
External IP address/range 10.200.1.10
Map to
IPv4 address/range 10.0.1.10

Optional Filters
Port Forwarding
Protocol TCP UDP SCTP ICMP
Port Mapping Type One to one Many to many
External service port 443
Map to IPv4 port 443

Edit Dynamic IP Pool

Name IP Pool
Comments Write a comment... 0/255
Type Overload One-to-One Fixed Port Range Port Block Allocation
External IP address/range 10.200.1.100-10.200.1.100
NAT64
ARP Reply

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration. The WAN (port1) interface has the IP address 10.200. 1. 1/24.
The LAN (port3) interface has the IP address 10 .0.1.254. /24. The first firewall policy has NAT enabled using IP Pool.
The second firewall policy is configured with a VIP as the destination address.
Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0. 1. 10?

A. 10.200. 1. 1
B. 10.200.3. 1
C. 10.200. 1. 100
D. 10.200. 1. 10

Answer: C

Explanation:
Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

NEW QUESTION 129
An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
B. Create a new service object for HTTP service and set the session TTL to never
C. Set the TTL value to never under config system-ttl
D. Set the session TTL on the HTTP policy to maximum

Answer: BC

NEW QUESTION 132
If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

A. A CRL
B. A person
C. A subordinate CA
D. A root CA

Answer: D

NEW QUESTION 133
......