Fortinet.NSE4_FGT_AD-7.6.v2026-05-23.q69

Exam Code:	NSE4_FGT_AD-7.6
Exam Name:	Fortinet NSE 4 - FortiOS 7.6 Administrator
Certification Provider:	Fortinet
Free Question Number:	69
Version:	v2026-05-23
# of views:	152
# of Questions views:	690
https://www.freepdfdumps.com/Fortinet.NSE4_FGT_AD-7.6.v2026-05-23.q69.html	

NEW QUESTION: 1
Refer to the exhibits. The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.

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
```


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.

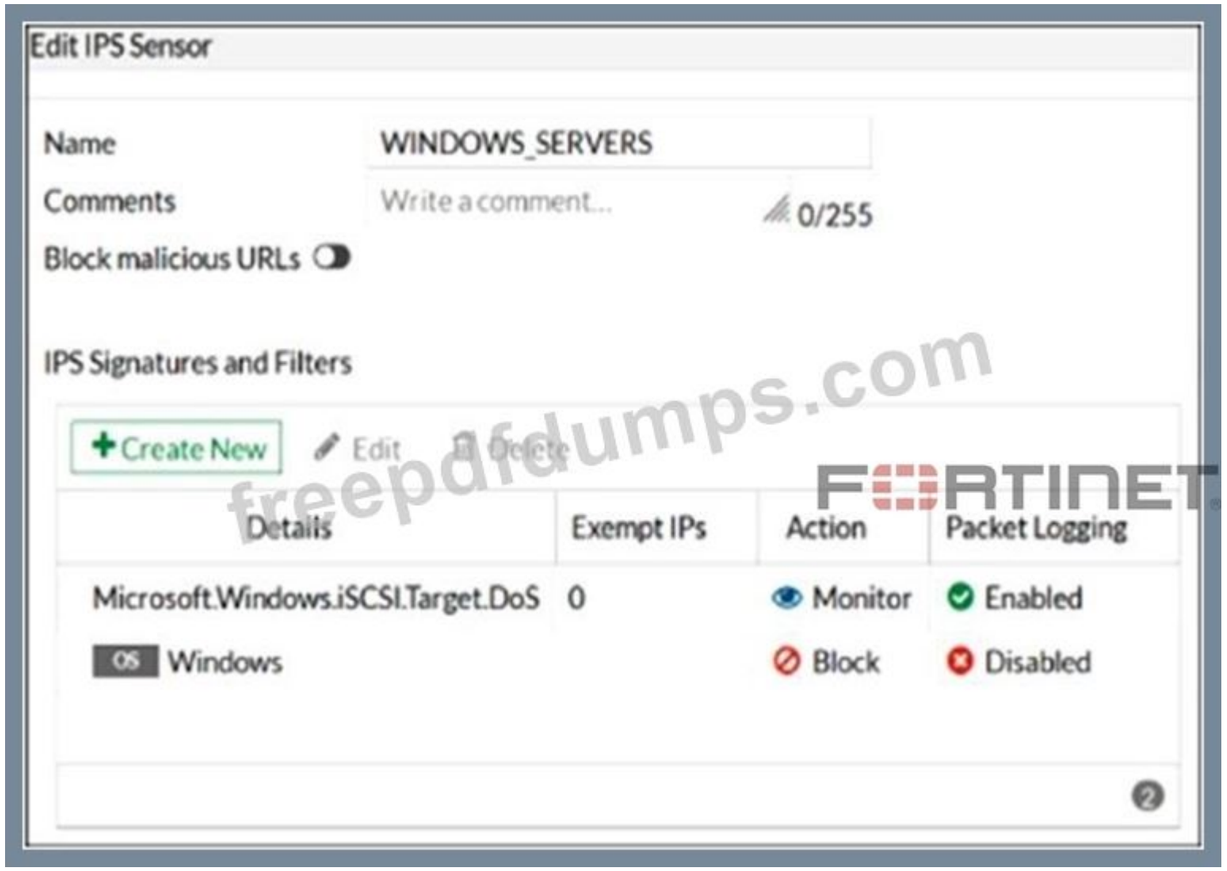
D. FortiGate drops new sessions.

Answer: (SHOW ANSWER)

FG enters conserve mode at 88% by default, at which point you can't make configuration changes. Also, without additional config, FG will drop sessions that require inspection. At 95%, all new sessions are dropped.

NEW QUESTION: 2

Refer to the exhibit, which shows the IPS sensor configuration.



If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will reset all connections that match these signatures.

B. The sensor will gather a packet log for all matched traffic.

C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.

D. The sensor will block all attacks aimed at Windows servers.

Answer: (SHOW ANSWER)

The sensor will allow attackers matching the Microsoft.Windows.iSCSITarget.DoS signature.

The action for this specific signature is set to Monitor, which means FortiGate will only detect and log the activity but will not block or reset the session.

The sensor will block all attacks aimed at Windows servers.

The general Windows filter is configured with the Block action, so any traffic matching Windows- related attack signatures will be blocked.

NEW QUESTION: 3

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

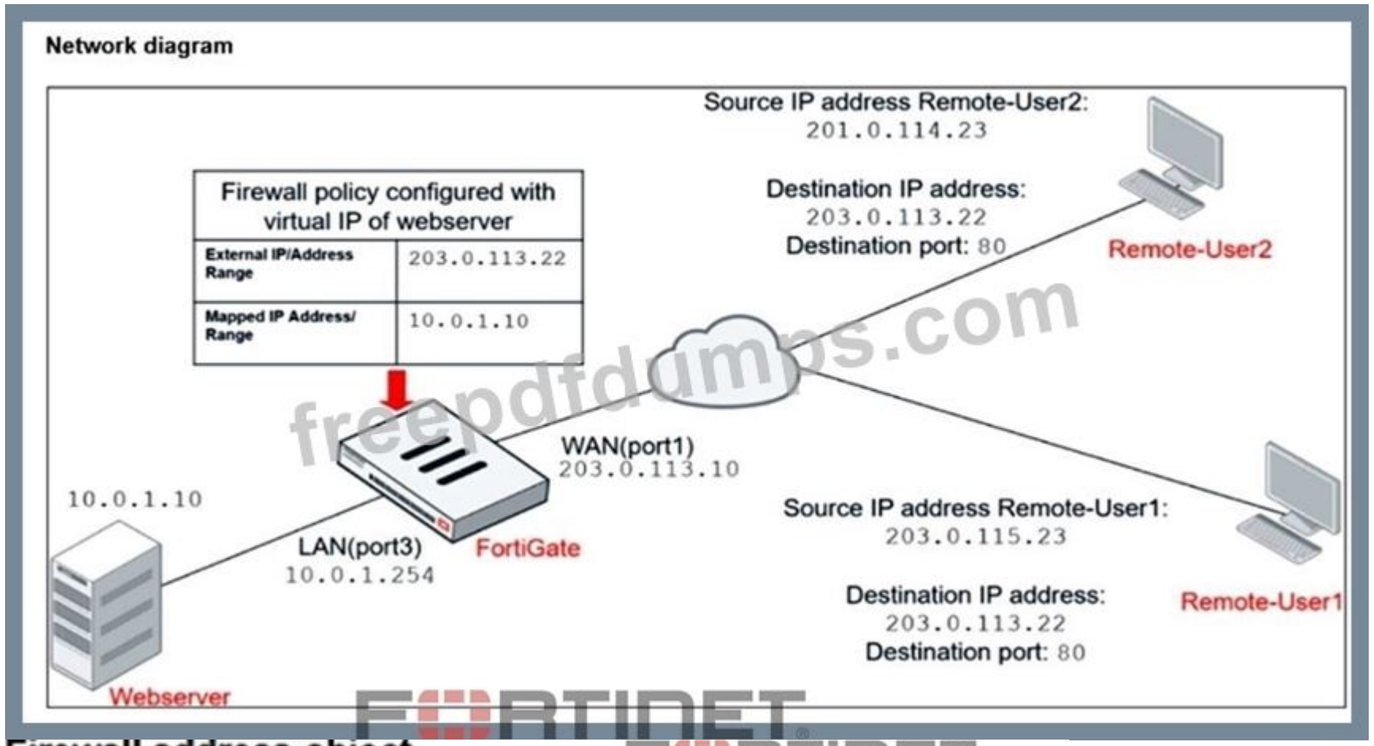
ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Critical-DIA	LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 ✓ port2
2	Non-Critical-DIA	LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2 ✓
3	Default-Internet	LOCAL_SUBNET	REMOTE_SUBNET	Latency	port1 port2
Implicit 1					
	sd-wan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

A. All traffic from a source IP to a destination IP is sent to the same interface.
B. Traffic is sent to the link with the lowest latency.
C. Traffic is distributed based on the number of sessions through each interface.
D. All traffic from a source IP is sent to the same interface
Answer: A (LEAVE A REPLY)
For traffic that does not match any of the defined SD-WAN rules, the default implicit SD-WAN rule is applied. By default, the FortiGate uses a "source-destination IP-based" algorithm, which means all traffic from a specific source IP to a specific destination IP is sent through the same interface.
This ensures that a consistent path is used for traffic between the same source and destination IP addresses.

NEW QUESTION: 4
You have created a web filter profile named restrict_media-profile with a daily category usage quota. When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down.
What could be the reason?
A. The firewall policy is in no-inspection mode instead of deep-inspection.
B. The inspection mode in the firewall policy is not matching with web filter profile feature set.
C. The web filter profile is already referenced in another firewall policy.
D. The naming convention used in the web filter profile is restricting it in the firewall policy.
Answer: (SHOW ANSWER)
Web filter profiles with category usage quotas require the firewall policy to be in proxy-based (deep) inspection mode; if the inspection mode does not match this requirement, the profile will not appear in the drop-down list.

NEW QUESTION: 5

Refer to the exhibits.



Firewall address object

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.
The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.
Which two configuration changes can the administrator make to the policy to deny Webserver access for Remote-User2? (Choose two.)
A. Set the Destination address as Webserver in the Deny policy.
B. Disable match-vipin the Deny policy.
C. Set the Destination address as Deny_IP in the Allow_access policy.
D. Enable match-vipin the Deny policy.
Answer: A,D (LEAVE A REPLY)
In this scenario, the FortiGate uses a Virtual IP (VIP) to map the external IP 203.0.113.22 to the internal web server 10.0.1.10. When using VIPs, firewall policies must be configured carefully to match the translated destination address.
The external users (Remote-User1 and Remote-User2) connect to 203.0.113.22, which is the VIP for the web server.
By default, firewall policies match pre-NAT addresses (the original destination before VIP translation).
To make the deny policy recognize traffic destined for the VIP-mapped address, the match-vip option must be enabled.
The destination in the Deny policy should explicitly be the Webserver (the VIP object), so FortiGate correctly identifies the target.

NEW QUESTION: 6
A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view.
Why is the policy order different in these two views?
A. Policies in Interface Pair View are prioritized by security levels, while By Sequence View strictly follows the administrator's manual ordering.
B. By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.
C. The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.
D. Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.
Answer: D (LEAVE A REPLY)
Interface Pair View organizes policies grouped by source and destination interfaces, whereas By Sequence View displays policies in the exact order they are processed by the firewall.

NEW QUESTION: 7
Refer to the exhibit showing a debug flow output.

Debug Flow output

vd-root:0 received a packet(proto=1, 10.0.11.50:3–>100.65.0.254:2048) tun_id=0.0.0.0 from port4, type=8, code=0, id=3, seq=5.
allocate a new session-00000721
in-[port4], out-[]
len=0
result:skb_flags-02000000, vid-0, ret no-match, act-accept, flag-00000000
find a route: flag=00000000 gw-0.0.0.0 via port2
in[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
gnum-100004, use addr/intf hash, len=3
checked gnum-100004 policy-2, ret-matched. act-accept
ret-matched
gnum-4e20, check-ffffffffa002c9c7
checked gnum-4e20 policy-6, ret-no-match, act-accept
gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000
policy-2 is matched, act-drop
after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-2
Denied by forward policy check (policy 2)

Which two conclusions can you make from the debug flow output? (Choose two.)

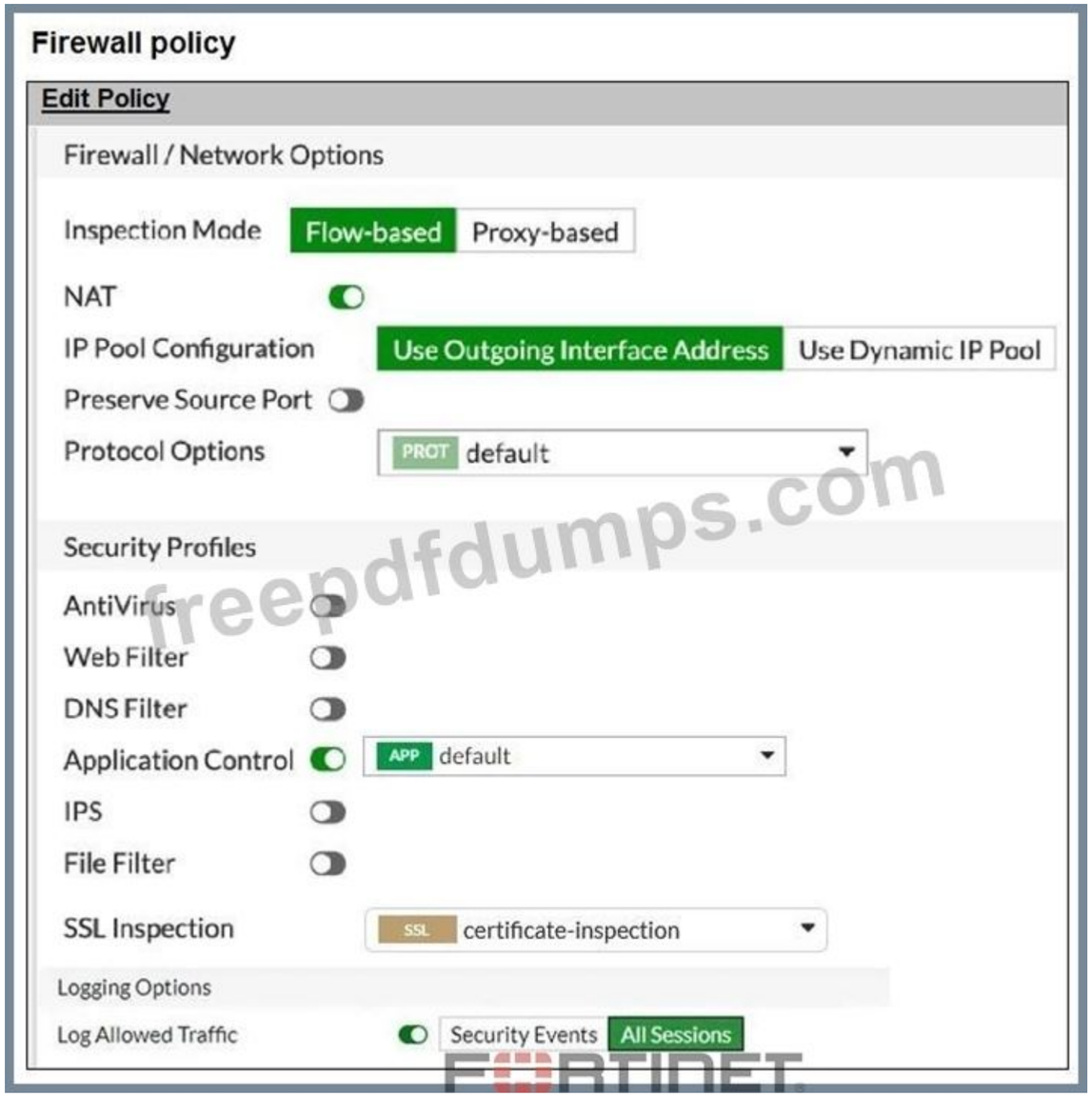
A. The default gateway is configured on port2.

B. The RPF check fails.
C. The debug flow is for UDP traffic.
D. The matching firewall policy denies the traffic.
Answer: A,D (LEAVE A REPLY)
The default gateway is configured on port2 → The debug output shows find a route:
flag=00000000 gw-0.0.0.0 via port2, which indicates that the default route (0.0.0.0/0) points out port2.
The matching firewall policy denies the traffic → The log line Denied by forward policy check (policy 2) confirms that policy 2 matched and explicitly dropped the traffic.

NEW QUESTION: 8
An administrator needs to analyze and resolve port conflicts between SSL VPN and HTTPS administrative access on the same interface.
In which two ways can this be done? (Choose two.)
A. Disable SSL VPN if HTTPS administrative access is using port 443 on any interface.
B. Keep port 443 for both SSL VPN and HTTPS administrative access on the same interface without any problems.
C. Run SSL VPN on one interface using port 443 and enable HTTPS administrative access on a different interface, also using port 443.
D. Change the port number for either the SSL VPN service or the HTTPS administrative service if both are on the same interface.
Answer: (SHOW ANSWER)
You can keep port 443 for SSL VPN on one interface and also use port 443 for HTTPS admin access on a different interface. Since the services are bound to different interfaces, no conflict occurs.
If both SSL VPN and HTTPS admin access are required on the same interface, you must change the port number for one of the services to avoid a port conflict.

NEW QUESTION: 9
Refer to the exhibits. You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.
You cannot access any of the Google applications, but you are able to access www.fortinet.com.
What would you do to resolve this issue?

Application sensor



A. Change the Inspection mode to Proxy-based.
B. Set SSL inspection to deep-content-inspection.
C. Move up Google in the Application and Filter Overrides section to set its priority to 1.
D. Add *Google*.com to the URL category in the security profile.
Answer: (SHOW ANSWER)
In the Application and Filter Overrides, the Excessive-Bandwidth filter (set to Block) is priority 1, and Google (set to Monitor) is priority 2. Since overrides are evaluated by priority, Google traffic is being blocked by the higher-priority rule. Moving Google to the top (priority 1) ensures it is matched first, allowing access while still monitoring it.

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 filteroption.
C. Use IPS filter, rate-mode periodicaloption.
D. Use IPS signatures, rate-mode periodicaloption.
Answer: D (LEAVE A REPLY)
You can also add rate-based signatures to block specific traffic when the threshold is exceeded.
On the CLI, If you set the command rate-mode to periodical, FortiGate triggers the action when the threshold is reached during the configured Duration time period.

NEW QUESTION: 11
Refer to the exhibit. As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit.
What could be the possible reason of the diagnose output shown in the exhibit?

```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
            pid = 2044, engine count = 0 (+1)
            0 - pid:2074:2074 cfg:1 master:0 run:1
```


A. There is a no firewall policy configured with an IPS security profile.
B. FortiGate entered into IPS fail open state.
C. Administrator entered the command diagnose test application ipsmonitor 5.
D. Administrator entered the command diagnose test application ipsmonitor 99.
Answer: (SHOW ANSWER)
The output shows the IPS engine count as 0, indicating no active IPS engines are running. This typically means no firewall policy is referencing the IPS security profile, so the IPS profile is not being applied or triggered.

NEW QUESTION: 12
An administrator has configured the following settings:

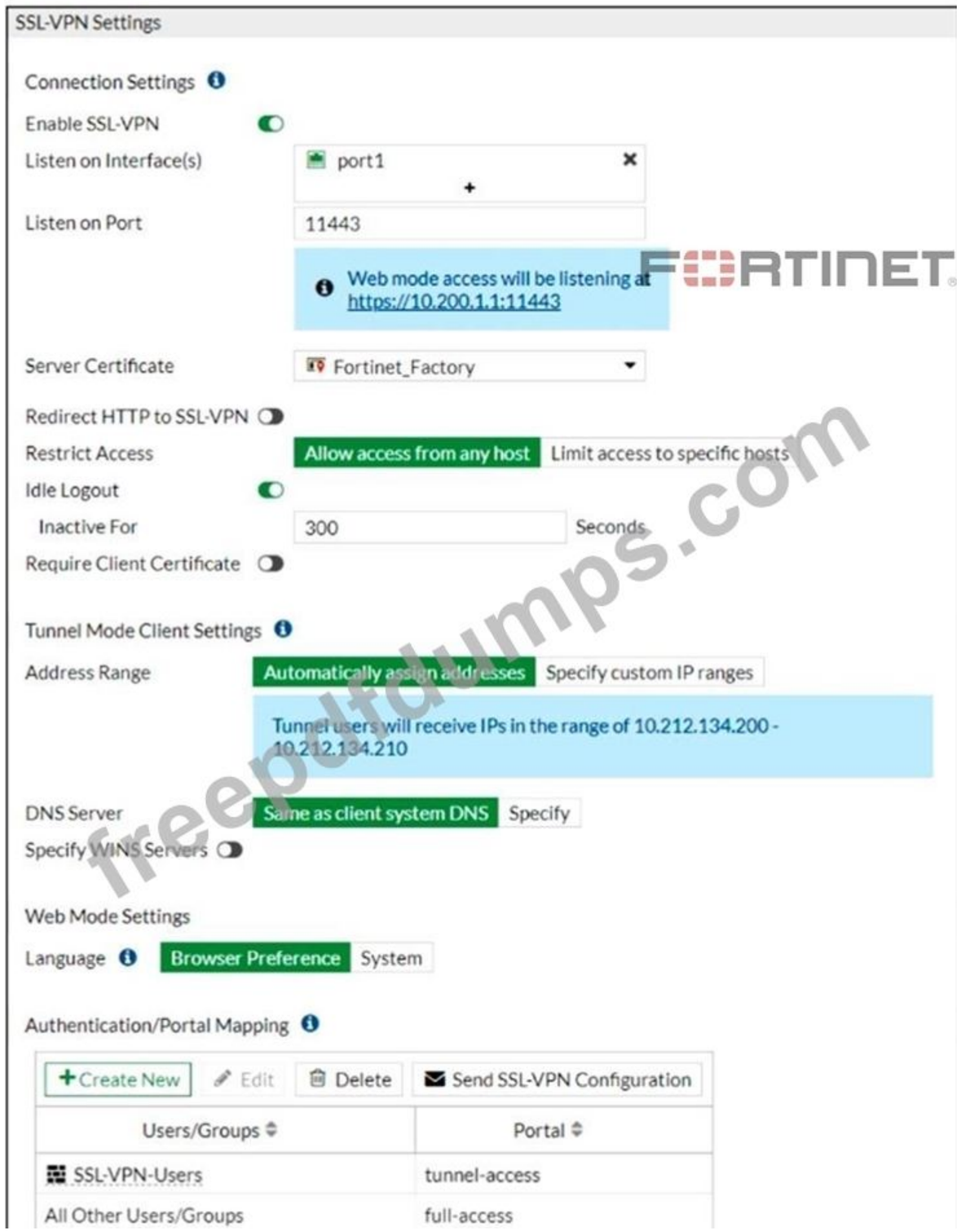
```
config system settings
set ses-denied-traffic enable
end

config system global
set block-session-timer 30
end
```


What are the two results of this configuration? (Choose two.)
A. Denied users are blocked for 30 minutes.
B. A session for denied traffic is created.
C. Session helpers are disabled for denied traffic.
D. The number of logs generated by denied traffic is reduced.
Answer: (SHOW ANSWER)
During the session, if a security profile detects a violation, FortiGate records the attack log immediately. To reduce the number of log messages generated and improve performance, you can enable a session table entry of dropped traffic. This creates the denied session in the session table and, if the session is denied, all packets of that session are also denied. This ensures that FortiGate does not have to perform a policy lookup for each new packet matching the denied session, which reduces CPU usage and log generation.

The CLI command is ses-denied-traffic. You can also set the duration for block sessions. This determines how long a session will be kept in the session table by setting block-session-timer in the CLI. By default, it is set to 30 seconds.

NEW QUESTION: 13
Refer to the exhibits.

SSL-VPN settings



The SSL VPN connection fails when a user attempts to connect to it.
What should the user do to successfully connect to the SSL VPN?
A. Change the SSL VPN port on the client.
B. Change the SSL VPN portal to the tunnel.
C. Change the server IP address.
D. Change the idle-timeout.
Answer: A (LEAVE A REPLY)
In the FortiGate SSL-VPN settings, the VPN is configured to listen on port 11443, as shown in the
"Listen on Port" field. However, the VPN client is attempting to connect to https://10.200.1.1:443/, which uses the default HTTPS port (443) instead of the configured port.
To successfully connect, the user must change the SSL VPN port on the client to 11443 so that it matches the listening port defined on the FortiGate device.

NEW QUESTION: 14
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: (SHOW ANSWER)
The key part of the question is some users can connect and some cannot, which strongly suggests a client-side connection issue rather than a firewall-policy issue (policy only applies after the tunnel is established).

For SSL-VPN, the first thing to check when users fail to connect is whether they are using the correct connection settings (especially the port).

NEW QUESTION: 15
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: A,B (LEAVE A REPLY)
Certificate inspection is not deep ssl inspection hence no inspection of the packet would happen since it is encrypted.
If the https site is in exampted list then yes it is a valid reason.

NEW QUESTION: 16
A FortiGate administrator is required to reduce the attack surface on the SSL VPN portal.
Which SSL timer can you use to mitigate a denial of service (DoS) attack?
A. SSL VPN http-request-header-timeout
B. SSL VPN dtls-hello-timeout
C. SSL VPN login-timeout
D. SSL VPN idle-timeout
Answer: (SHOW ANSWER)
config vpn ssl settings
set http-request-header-timeout <1-60>
end
Timers can also help to mitigate DoS attacks with SSL VPN caused by partial HTTP requests.

NEW QUESTION: 17
Refer to the exhibit.

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt.

What is the most likely reason for this situation?

A. The Service DNS is required in the firewall policy.

B. The user is using an incorrect user name.

C. No matching user account exists for this user.

D. The Remote-users group is not added to the Destination.

Answer: A (LEAVE A REPLY)

DNS traffic can be allowed if user has not authenticated yet.

Hostname resolution is often required by the application layer protocol (HTTP/HTTPS/FTP/Telnet) that is used to authenticate.

DNS service must be explicity listed as a service in the policy.

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.

Edit Phase 2 Selector

Name: ToBR1

Comments: Comments 0/255

Encapsulation: Tunnel Mode | Transport Mode

IP version: IPv4 | IPv6

Named address:

Local address: IP Address | Subnet Address | IP Range

10.0.11.0 255.255.255.0

Remote address: IP Address | Subnet Address | IP Range

172.20.1.0 255.255.255.0

Advanced

Encryption - authentication: AES128 - SHA1

Replay detection: Enable | Disable

Perfect forward secrecy (PFS): Enable | Disable

Diffie-Hellman groups:

☐ 1	☐ 2	☑ 5
☐ 14	☐ 15	☐ 16
☐ 17	☐ 18	☐ 19
☐ 20	☐ 21	☐ 27
☐ 28	☐ 29	☐ 30
☐ 31	☐ 32	

Local port: All | Specify

Edit Phase 2 Selector

Name: ToHQ

Comments: Comments 0/255

Encapsulation: Tunnel Mode | Transport Mode

IP version: IPv4 | IPv6

Named address:

Local address: IP Address | Subnet Address | IP Range

172.20.1.0 255.255.255.0

Remote address: IP Address | Subnet Address | IP Range

10.11.0.0 255.255.255.0

Advanced

Encryption - authentication: AES256 - SHA1

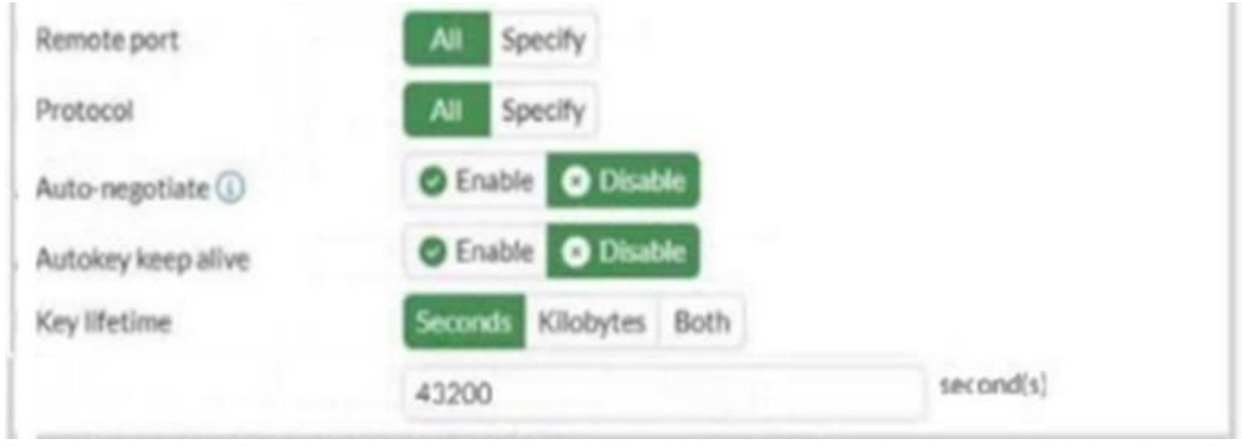
Replay detection: Enable | Disable

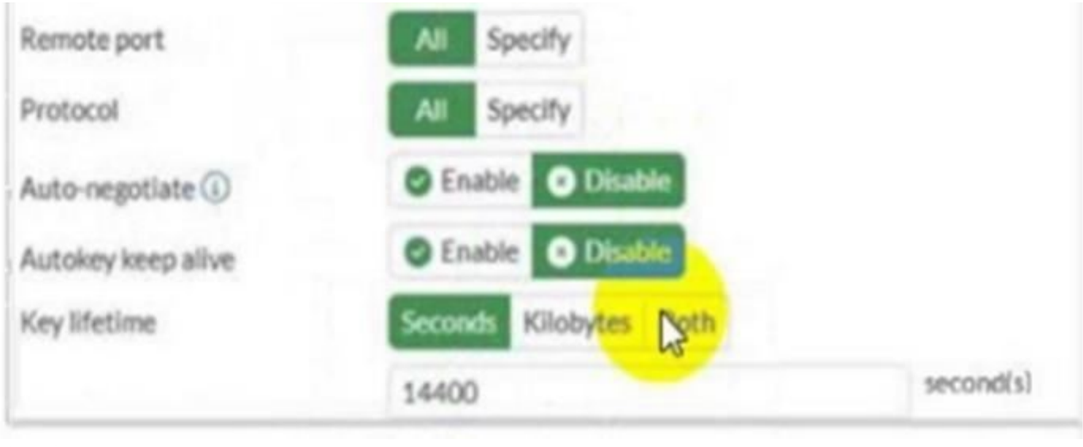
Perfect forward secrecy (PFS): Enable | Disable

Diffie-Hellman groups:

☐ 1	☐ 2	☑ 5
☑ 14	☐ 15	☐ 16
☐ 17	☐ 18	☐ 19
☐ 20	☐ 21	☐ 27
☐ 28	☐ 29	☐ 30
☐ 31	☐ 32	

Local port: All | Specify





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-NGFW, set Encryption to AES256.

Answer: C,D (LEAVE A REPLY)

Check the IP address

The remote subnet selectors don't match. Set BR1-FGT's Remote Address to 10.0.11.0/255.255.255.0 (C).

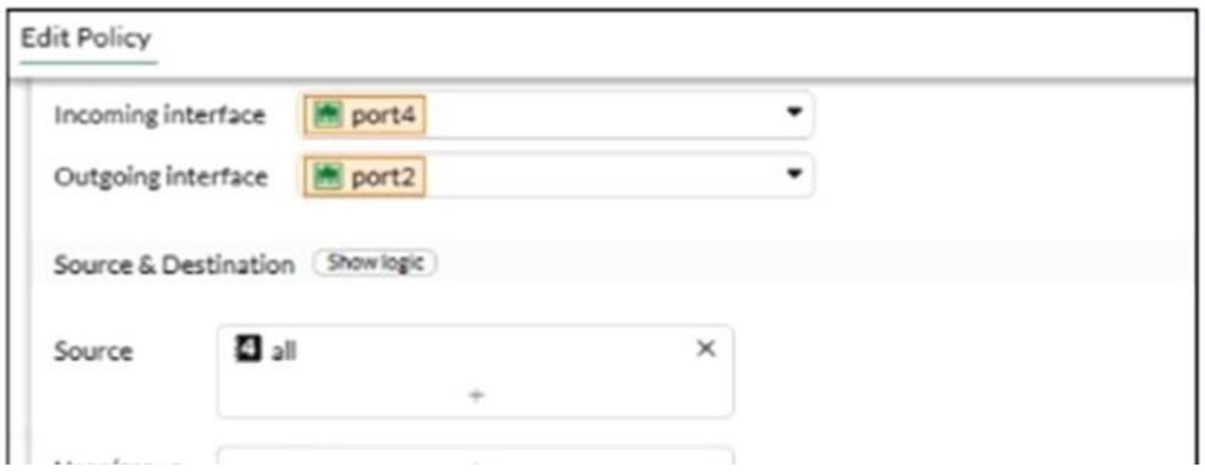
The phase-2 proposal algorithms don't match. Change HQ-NGFW Encryption from AES128 to AES256 to match BR1-FGT (D).

NEW QUESTION: 19

Refer to the exhibits.

Antivirus profile

Firewall policy



You are asked to implement an antivirus profile for files downloaded through FTP, HTTP, and HTTPS.
While testing, you are successful with HTTP and FTP protocols, but FortiGate does not block the file download over HTTPS.
What could be the cause?
A. The feature set in the antivirus profile is not set to Flow-based.
B. Web filter is not enabled on the firewall policy to complement the antivirus profile.
C. The action on the firewall policy is not set to deny.
D. The SSL inspection mode in the firewall policy is not deep content inspection.
Answer: (SHOW ANSWER)
The SSL inspection mode in the firewall policy is set to certificate-inspection, which only examines SSL certificates without decrypting HTTPS traffic. Because of this, FortiGate cannot inspect or block files downloaded over HTTPS, as the content remains encrypted. To enable antivirus scanning on HTTPS traffic, the SSL inspection mode must be set to deep-inspection, allowing the FortiGate to decrypt, inspect, and re-encrypt the traffic.

NEW QUESTION: 20
A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.
What is the reason for the certificate warning errors?
A. The browser does not trust the certificate used by FortiGate for SSL inspection.
B. The option invalid SSL certificates is set to allow on the SSL/SSH inspection profile
C. The matching firewall policy is set to proxy inspection mode.
D. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
Answer: A (LEAVE A REPLY)
The browser presents a certificate warning when you attempt to access an HTTPS site that uses an untrusted certificate. Untrusted certificates include self-signed SSL certificates, unless the certificate is imported into the browser-trusted certificate store. FortiGate has its own configuration setting on the SSL/SSH Inspection profile, which includes options to Allow, Block, or Ignoreuntrusted SSL certificates.

NEW QUESTION: 21
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: (SHOW ANSWER)
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: 22
FortiGate is integrated with FortiAnalyzer and FortiManager.
When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?
A. Policy ID
B. Log ID
C. Universally Unique Identifier
D. Sequence ID
Answer: C (LEAVE A REPLY)
When creating firewall objects or policies, a UUID attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer.

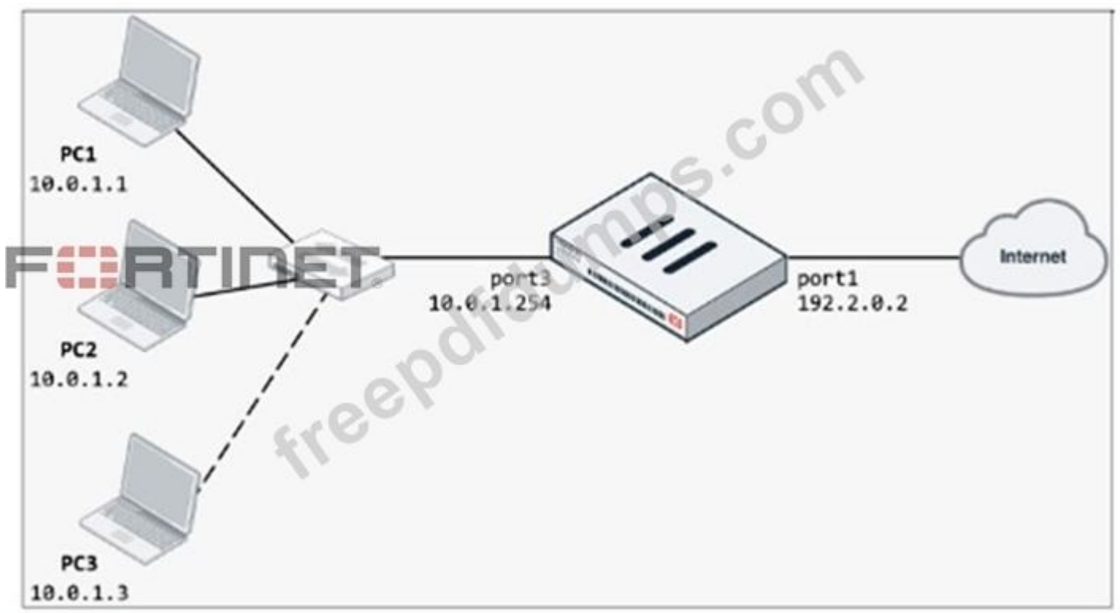
NEW QUESTION: 23
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

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: B (LEAVE A REPLY)

Underlay is not a default zone. It is user defined and not active.

NEW QUESTION: 24
Refer to the exhibits.

Network diagram



The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device.

Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.

Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

A. In the IP pool configuration, set typeto overload.

B. In the firewall policy configuration, add 10.0.1.3as an address object in the source field.

C. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.

D. In the IP pool configuration, set endipto 192.2.0.12.

Answer: A,D (LEAVE A REPLY)

With IP pool type set to One-to-One, only as many internal hosts as there are public IPs in the pool (192.2.0.10-192.2.0.11) can use NAT. Changing the type to overload allows all internal hosts (including PC3) to share the available public IPs, so PC3 can reach the internet.

Alternatively, keeping One-to-One but extending the pool to 192.2.0.10-192.2.0.12 adds another public IP, allowing a third internal host (PC3) to be mapped and gain internet access.

NEW QUESTION: 25

Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true?

(Choose two.)

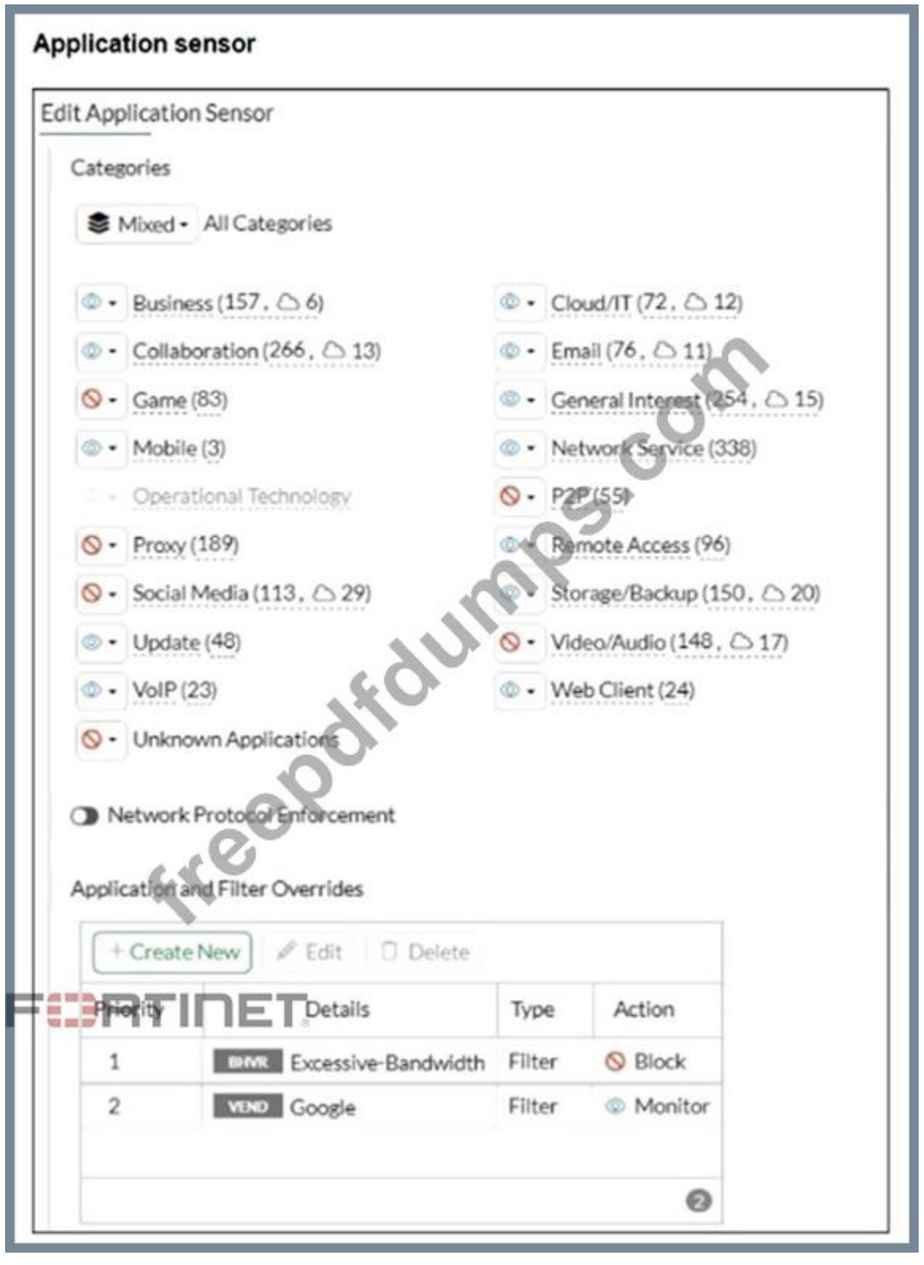
A. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.

B. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP.
C. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.
D. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance- mode.
Answer: C,D (LEAVE A REPLY)
SD-WAN is enabled: v4-ecmp-mode is hide and you control the ECMP algorithm with the load- balance-mode setting.
SD-WAN is disabled: ECMP algorithm is set on the CLI: config system settings.
https://docs.fortinet.com/document/fortigate/7.4.6/administration-guide/25967/equal-cost-multi- path

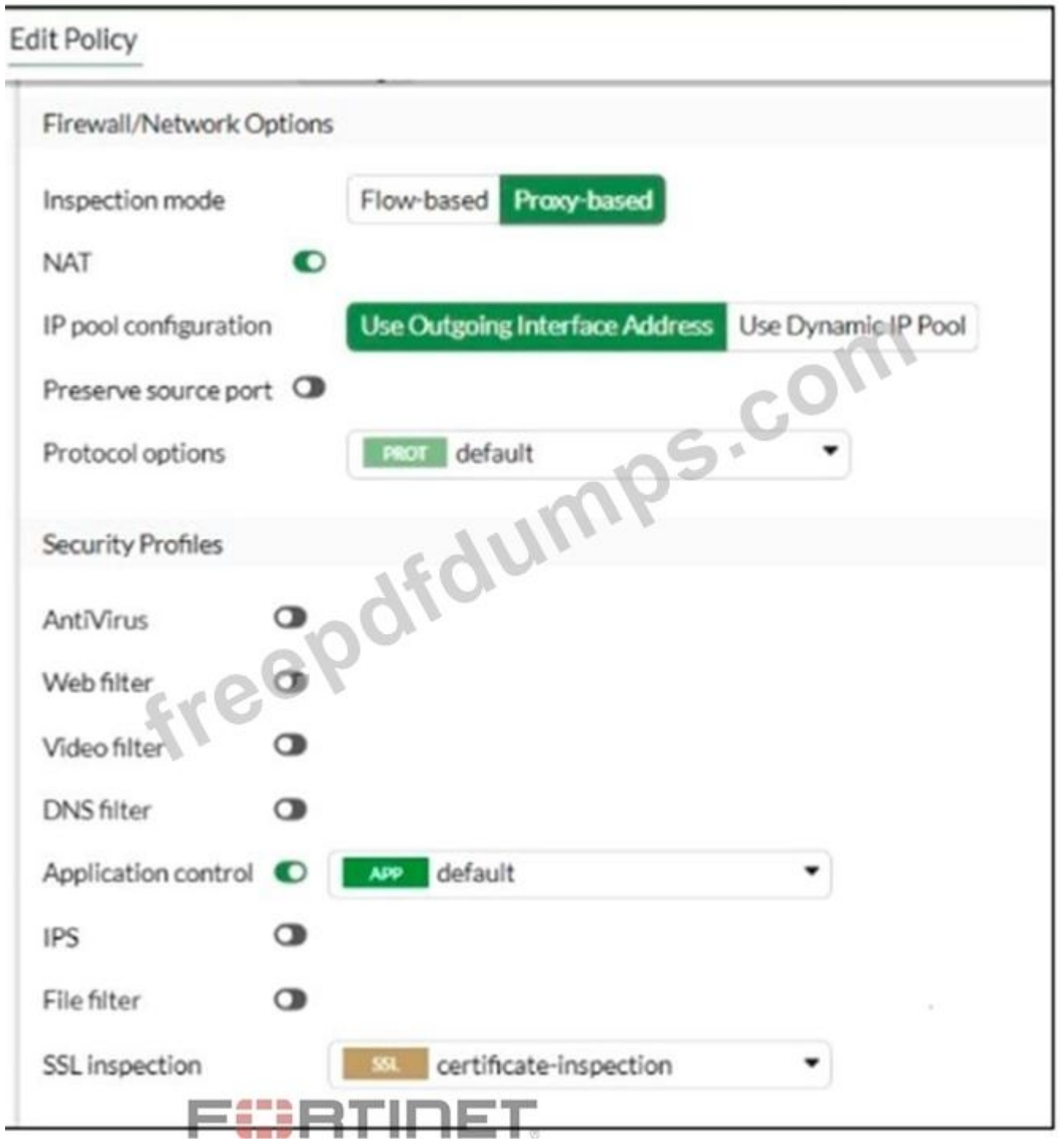
NEW QUESTION: 26
A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode.
Which step is NOT part of the expected process?
A. The DC agent sends login event data directly to FortiGate.
B. The user logs into the windows domain.
C. The collector agent forwards login event data to FortiGate.
D. FortiGate determines user identity based on the IP address in the FSSO list.
Answer: (SHOW ANSWER)
In DC Agent mode, the DC agent installed on the Domain Controller captures the logon events (e.g., Event ID 4624) in real-time. It then pushes this information to the Collector Agent. The Collector Agent, which runs as a service on a dedicated machine, is responsible for consolidating this information and then forwarding it to the FortiGate firewall. The FortiGate receives this data and uses the user's IP address to apply appropriate security policies.

NEW QUESTION: 27
Refer to the exhibits. You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.
You cannot access any of the Google applications, but you are able to access www.fortinet.com.
Which two actions would you take to resolve the issue? (Choose two.)

Application sensor



Firewall policy



A. Move up Google in the Application and Filter Overrides section to set its priority to 1.
B. Set the action for Google in the Application and Filter Overrides section to Allow.
C. Add *Google*.com to the URL category in the security profile.
D. Change the Inspection mode to Flow-based.
E. Set SSL inspection to deep-content inspection.
Answer: (SHOW ANSWER)
Move up Google in the Application and Filter Overrides section to set its priority to 1.
The "Excessive-Bandwidth" filter has a higher priority (1) and is configured to Block. Because Google applications generate significant bandwidth, they match this rule first and get blocked.
Moving the "Google" filter to priority 1 ensures that the monitor action for Google is applied before the block rule.

Set SSL inspection to deep-content inspection.
Google applications use HTTPS encryption, so the FortiGate cannot identify or control them unless SSL traffic is decrypted. Changing from certificate-inspection (which only inspects certificates) to deep-inspection allows FortiGate to fully analyze encrypted application traffic and properly apply the Application Control rules.

NEW QUESTION: 28
An administrator has configured a dialup IPsec VPN on FortiGate with add-route enabled.
However, the static route is not showing in the routing table.
Which two statements about this scenario are correct? (Choose two.)
A. The administrator must enable a dynamic routing protocol on the dialup interface.
B. The administrator must use a policy route instead of a static route for add-route to work properly.
C. The administrator must ensure phase 2 is successfully established.
D. The administrator must define the remote network correctly in the phase 2 selectors.
Answer: (SHOW ANSWER)
The administrator must ensure phase 2 is successfully established → The static route for the dialup VPN is only added after Phase 2 negotiation completes successfully.
The administrator must define the remote network correctly in the phase 2 selectors → The add- route feature installs a route based on the Phase 2 selectors; if they are incorrect, no route will appear in the routing table.

NEW QUESTION: 29
Refer to the exhibit to view the firewall policy.

Firewall policy configuration

Why would the firewall policy not block a well-known virus, for example eicar?

A. The firewall policy does not apply deep content inspection.

B. Web filter is not enabled on the firewall policy to complement the antivirus profile.

C. The firewall policy is not configured in proxy-based inspection mode.

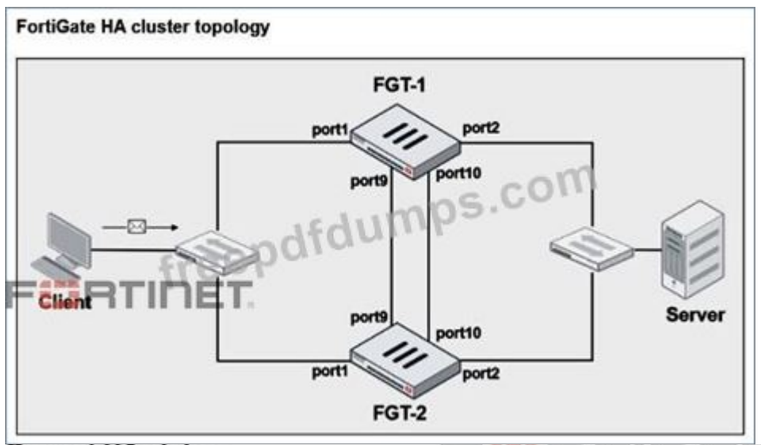
D. The action on the firewall policy is not set to deny.

Answer: (SHOW ANSWER)

The firewall policy uses certificate-inspection under SSL inspection and flow-based inspection mode. Certificate inspection does not decrypt HTTPS traffic; it only checks the certificate fields. Because of this, FortiGate cannot perform deep content inspection, which is required for antivirus to detect and block threats such as the EICAR test virus within encrypted HTTPS sessions.

NEW QUESTION: 30

Refer to the exhibits.



Current HA status

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

New FortiGate HA configuration

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

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


FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.

What would be the expected outcome in the HA cluster?

A. FGT-2 will take over as the primary because it has the override enablesetting and higher priority than FGT-1.

B. FGT-1 will synchronize the override disablesetting with FGT-2.

C. The HA cluster will become out of sync because the overridesetting must match on all HA members.

D. FGT-1 will remain the primary because FGT-2 has lower priority.

Answer: (SHOW ANSWER)

With override enabled, the primary unit with the highest device priority will always become the primary unit. Whenever an event occurs that may affect primary unit selection, the cluster negotiates. For example, when override is enabled a cluster renegotiates when you change the device priority of any cluster unit or when you add a new unit to a cluster.

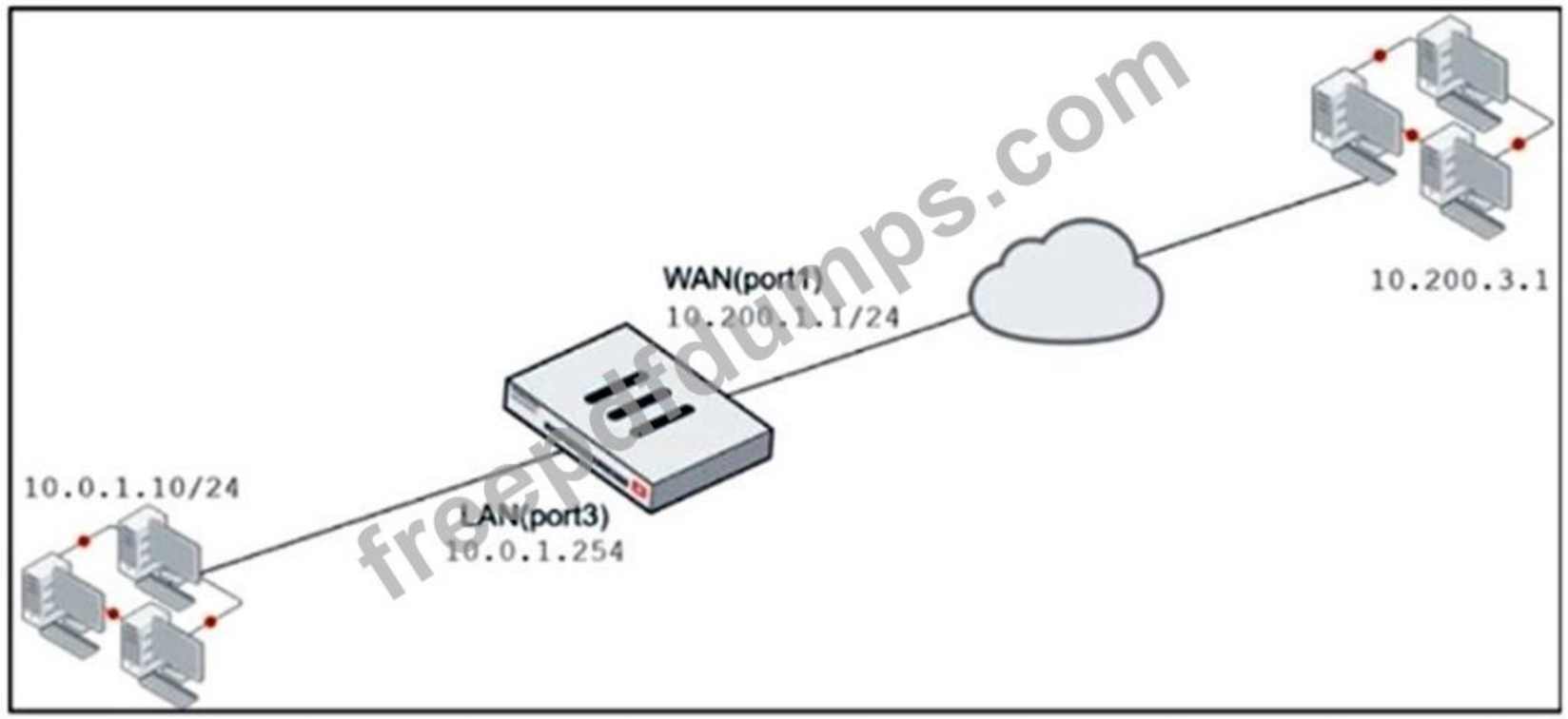
Override and primary unit selection

Enabling override changes the order of primary unit selection. As shown below, if override is enabled, primary unit selection considers device priority before age and serial number. This means that if you set the device priority higher on one cluster unit, with override enabled this cluster unit becomes the primary unit even if its age and serial number are lower than other cluster units..

NEW QUESTION: 31

Refer to the exhibits.

Network diagram



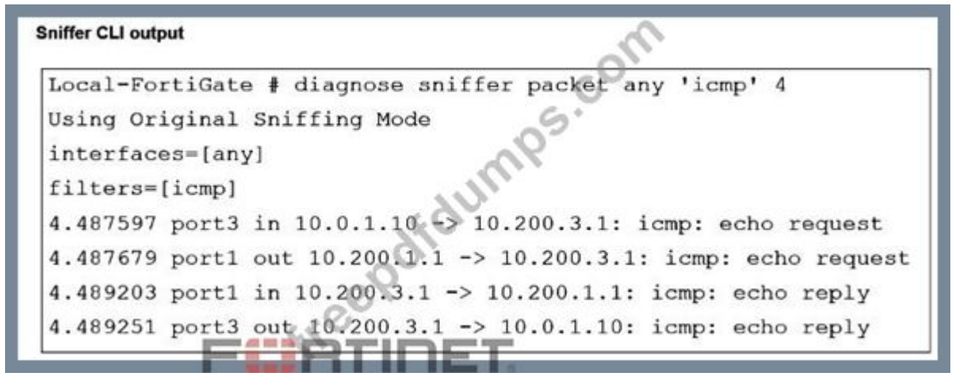
VIP object configuration

Edit Virtual IP

Name	Webserver
Comments	Write a comment... 0/255
Color	Change
Network	
Interface	WAN (port1)
Type	Static NAT
External IP address/range	10.200.1.200
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	80
Map to IPv4 port	80

Firewall policy

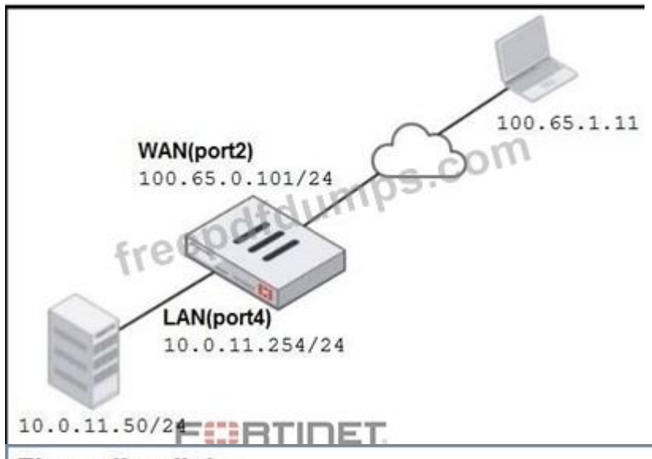
ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port3) → WAN (port1) 1								
2	Internet_Access	all	all	always	ALL	ACCEPT		NAT
WAN (port1) → LAN (port3) 1								
3	Allow_access	all	Webserver	always	HTTP HTTPS	ACCEPT		Disabled



The exhibits show a diagram of a FortiGate device connected to the network, VIP configuration, firewall policy, and the sniffer CLI output on the FortiGate device.
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 webserver host (10.0.1.10) must use its VIP external IP address as the source NAT (SNAT) when it pings remote server (10.200.3.1).
Which two statements are valid to achieve this goal? (Choose two.)
A. Enable NAT on the Allow_access firewall policy.
B. Disable NAT on the Internet_Access firewall policy.
C. Disable port forwarding on the VIP object.
D. Create a new firewall policy before Internet_Access for the webserver and apply the IP pool.
Answer: (SHOW ANSWER)
The current VIP is configured with port forwarding, so it only applies to TCP/80 traffic. To use the VIP's external address (10.200.1.200) as the source for any outbound sessions (such as ICMP ping), the VIP must be a full static 1-to-1 NAT, which requires disabling port forwarding.
You then need a dedicated firewall policy for the webserver that is placed before the generic Internet_Access policy and that uses an IP pool with 10.200.1.200. Traffic from 10.0.1.10 will match this policy first and be SNATed to 10.200.1.200, so the remote server 10.200.3.1 sees the VIP external IP as the source.

NEW QUESTION: 32
Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, and the firewall policies, VIP, and IP pool configurations on the FortiGate device.
The WAN (port2) interface has the IP address 100.65.0.101/24.
The LAN (port4) interface has the IP address 10.0.11.254/24.
The first firewall policy has NAT enabled using the IP pool. The second firewall policy is configured with a VIP as the destination address.
Which IP address will be used to source NAT (SNAT) the internet traffic coming from a workstation with the IP address 10.0.11.50?

Network diagram



Firewall policies

	Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
☐	Internet(1)	LAN(port4)	WAN(port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
☐	WebServer(2)	WAN(port2)	LAN(port4)	all	VIP	always	ALL	ACCEPT		Disabled


VIP configuration
Edit Virtual IP
Name
VIP-WEB-SERVER
Comments
Write a comment...
0/255
Color
Change
Network
Interface
WAN (port2)
Type
Static NAT
External IP address/range
100.65.0.200
Map to
IPv4 address/range
10.0.11.50
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
NAT IP pool configuration
Edit Dynamic IP Pool
Name
IP Pool
Comments
Write a comment...
0/255
Type
Overload
External IP Range
100.65.0.102–100.65.0.102
NAT64
ARP Reply

A. 100.65.0.101

B. 100.65.0.200
C. 100.65.0.102
D. 10.0.11.254
Answer: (SHOW ANSWER)
Traffic from the workstation 10.0.11.50 going to the internet matches the Internet(1) policy (LAN
→ WAN) which has NAT enabled and is configured to use the IP Pool. The IP pool specifies the external address 100.65.0.102.
FortiGate will perform source NAT (SNAT) on the outbound traffic, translating the source IP of the workstation to 100.65.0.102.

NEW QUESTION: 33
You are onboarding an agentless, secure web gateway (SWG) endpoint for secure internet access (SIA). What will happen to the user's nonweb traffic?
A. All the nonweb traffic will bypass FortiSASE.
B. FortiSASE will use SWG to redirect nonweb traffic to FortiExtender.
C. FortiSASE will use Firewall-as-a-Service (FWaaS) to redirect nonweb traffic.
D. The endpoint will use split tunneling to redirect nonweb traffic to FortiSASE.
Answer: A (LEAVE A REPLY)
With an agentless SWG for Secure Internet Access (SIA), only web traffic is redirected and inspected. Nonweb traffic bypasses FortiSASE and is sent directly to its original destination.

NEW QUESTION: 34
Refer to the exhibit. How can the administrator view the log messages shown in the exhibit?
(Choose two.)

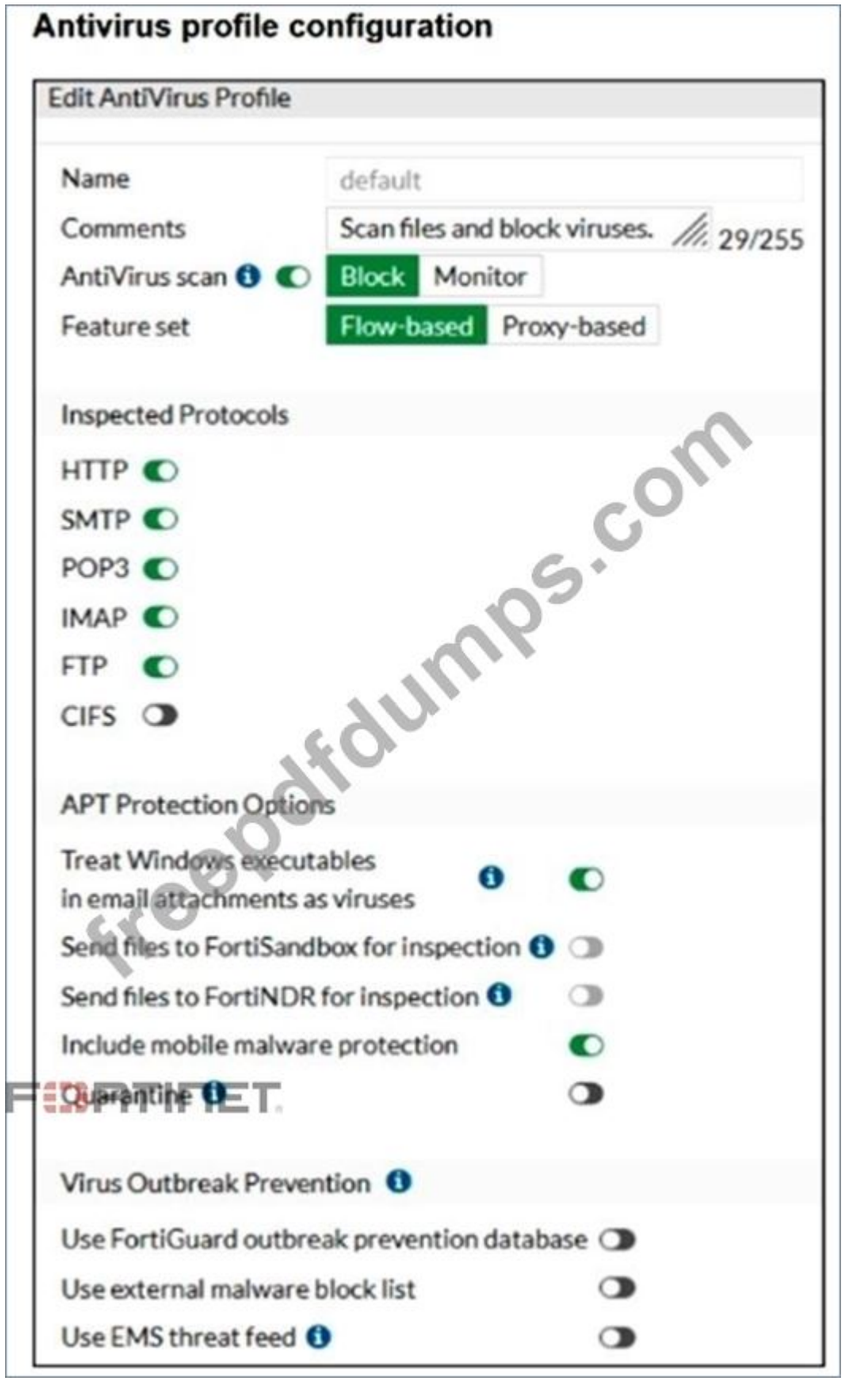
```
date=2025-09-03 time=09:09:57 id=754589591143238860 8 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluuid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

A. Through Security event log page
B. Through FortiGate CLI command diagnose log test
C. By right clicking the Implicit deny policy
D. Filtering by Policy UUID and Application Name in the log entry
Answer: A,D (LEAVE A REPLY)
The log shown is a UTM application control log, which can be viewed through the Security Event log page. The administrator can also filter logs by the Policy UUID and Application Name to find specific entries like the one in the exhibit.

NEW QUESTION: 35
Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

Firewall policy configuration

Antivirus profile configuration



Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

A. Flow-based inspection is used, which resets the last packet to the user.

B. The option to send files to FortiSandbox for inspection is enabled.

C. The firewall policy performs a full content inspection on the file.

D. The intrusion prevention security profile must be enabled when using flow-based inspection mode.

Answer: A (LEAVE A REPLY)
In Flow Based scanning, if a virus is detected, the final packet is dropped making the file unusable tot the end user. FG caches the URL of the file. If the user attempts to download again, rather than scanning the file again, the IPS engine then sends a block message to the user.

NEW QUESTION: 36
Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)
A. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
B. Pre-shared key and certificate signature as authentication methods
C. No certificate is required on the remote peer when you set the certificate signature as the authentication method
D. Extended authentication (XAuth) to request the remote peer to provide a username and password
Answer: B,D (LEAVE A REPLY)
Authentication-wise, both versions support PSK and certificate signature. Although only IKEv1 supports XAuth, IKEv2 supports EAP, which is equivalent to XAuth.

NEW QUESTION: 37
Which two settings are required for SSL VPN to function between two FortiGate devices?
(Choose two.)
A. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.
B. The client FortiGate requires a manually added route to remote subnets.
C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
D. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.
Answer: A,D (LEAVE A REPLY)
The FortiGate can be configured as an SSL VPN client, using an SSL-VPN Tunnel interface type.
The FortiGate devices must have the proper CA certificate installed to verify the certificate chain to the root CA that signed the certificate.

NEW QUESTION: 38
Refer to the exhibits. 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 stays Pending.

Link	10 Gbps Full Duplex	Link	10 Gbps Full Duplex
Port Speed	Auto-Negotiation	Port Speed	Auto-Negotiation
Type	Physical Interface	Type	Physical Interface
IPv4 Addresses	10.0.13.254/24	IPv4 Addresses	10.0.11.254/24

Security Fabric settings on HQ-ISFW-2

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.

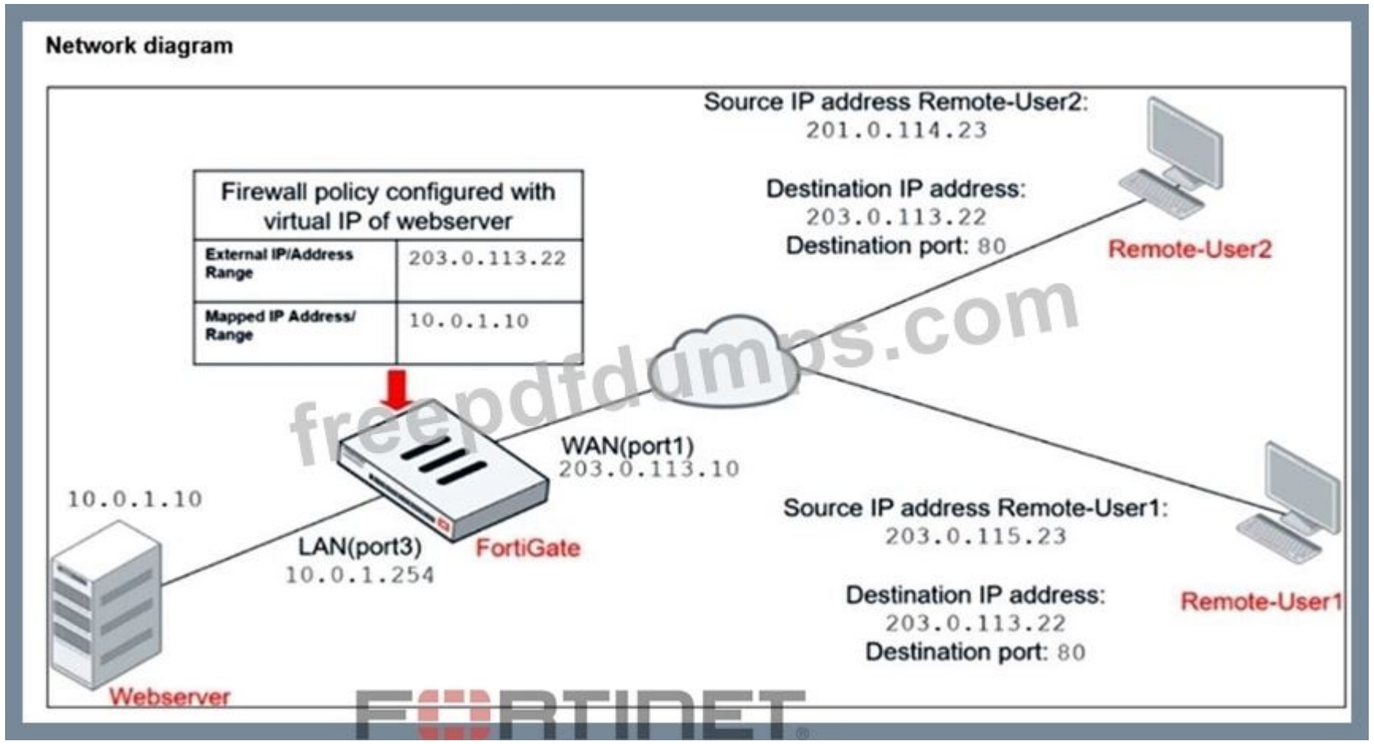
Answer: A,C (LEAVE A REPLY)

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: 39

Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.



Firewall address object

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.
The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.
Which additional configuration can the administrator add to a deny firewall policy, beyond the default behavior, to block Remote-User2 from accessing the Webserver?

A. Disable match-vip in the Allow_access policy
B. Configure a One-to-One IP Pool object in a new policy.
C. Set the Destination address as Webserver in the Deny policy.
D. Set the Destination address as Deny_IP in the Allow_access policy.

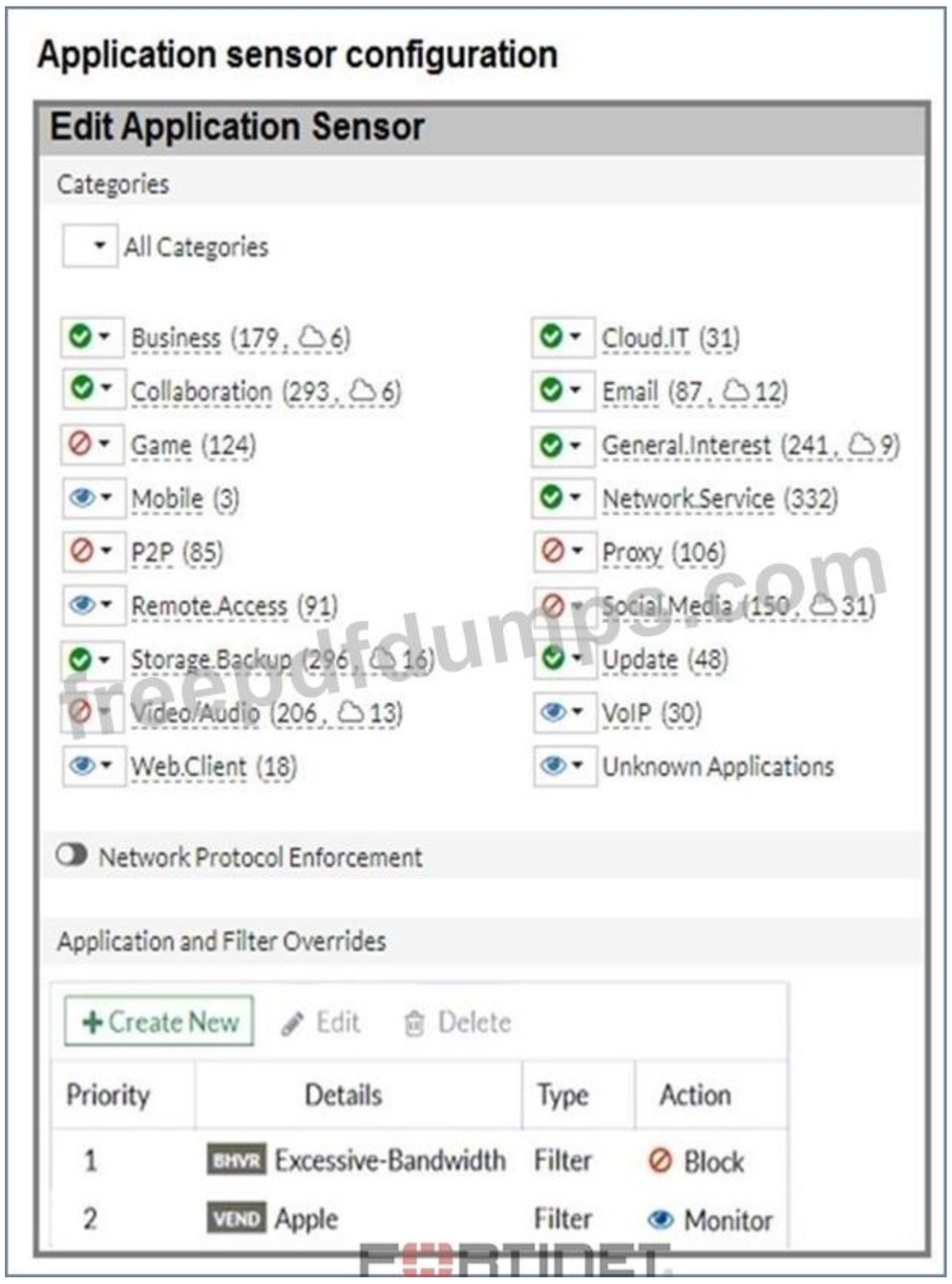
Answer: C (LEAVE A REPLY)

To block Remote-User2's access to the Webserver, the deny policy must explicitly specify the Webserver as the destination address; otherwise, it denies traffic to all destinations, which is not the desired behavior.

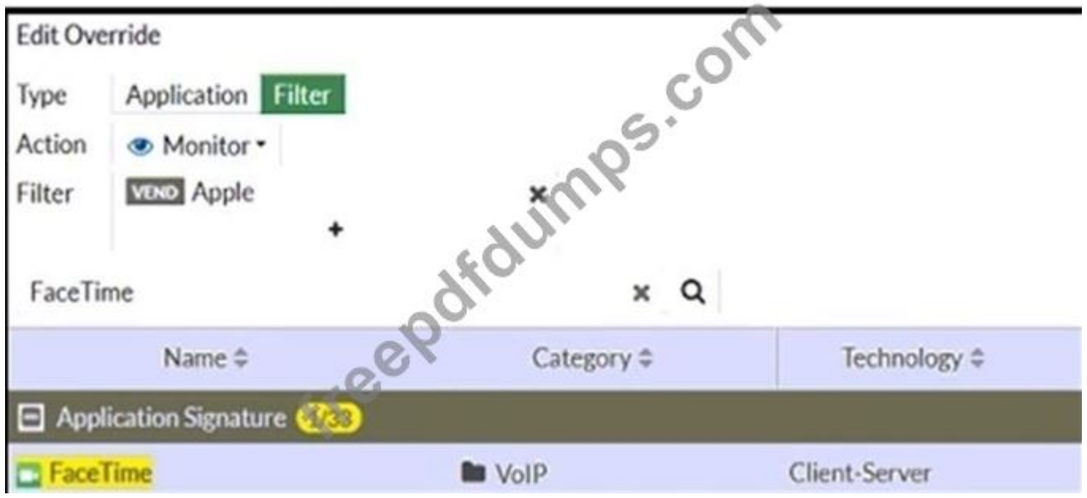
NEW QUESTION: 40

Refer to the exhibits. The exhibits show the application sensor configuration and the Excessive- Bandwidth and Apple filter details.
Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

Application sensor configuration



Filter override configuration



A. Apple Face Time will be allowed, based on the Video/Audio category configuration.
B. Apple Face Time will be blocked, based on the Excessive-Bandwidth filter configuration.
C. Apple Face Time will be allowed, based on the Apple filter configuration.
D. Apple Face Time will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.
Answer: C (LEAVE A REPLY)
Apple FaceTime normally falls under Video/Audio and could be blocked by the Excessive- Bandwidth filter. However, in this configuration, an override is applied under the Apple vendor filter with Monitor action. Overrides take precedence over general filter actions. Therefore, FaceTime will not be blocked; instead, it will be monitored, and since only a few calls are made (not excessive bandwidth usage), it will be allowed based on the Apple filter configuration.

NEW QUESTION: 41

Which inspection mode does FortiGate use for application profiles if it is configured as a profile- based next-generation firewall (NGFW)?

A. Certificate inspection

B. Flow-based inspection

C. Proxy-based inspection

D. Full content inspection

Answer: B (LEAVE A REPLY)

You can configure application control in proxy-based and flow-based firewall policies. However, because application control uses the IPS engine, which uses flow-based inspection, the INSPECTION is always flow-based.

NEW QUESTION: 42

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 (LEAVE A REPLY)

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: 43

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: (SHOW ANSWER)

Network Protocol Enforcement:

- Ensures that traffic on a specific port matches the expected protocol.
- Enabling it forces FortiGate to examine payloads even on known ports.

NEW QUESTION: 44

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad.

Which IPsec Wizard template must the administrator apply?

A. Hub-and-Spoke
B. Site to Site
C. Remote Access
D. Dial up User
Answer: C (LEAVE A REPLY)
The Remote Access IPsec Wizard template is used for individual users connecting from remote locations, such as traveling employees. This template configures FortiGate to act as an IPsec VPN server, allowing remote clients (like FortiClient) to securely connect and access internal network resources while abroad.

NEW QUESTION: 45
Which two statements about the Security Fabric rating are true? (Choose two.)
A. A license is required to obtain an executive summary in the Security Rating section.
B. The root FortiGate provides executive summaries of all the FortiGate devices in the Security Fabric.
C. The Security Posture category provides PCI compliance results.
D. Security Rating Insights are available only in the Security Rating page.
Answer: B,C (LEAVE A REPLY)
The Security Rating section provides an executive summary of all the security rating checks. By default, it is available with a base set of free checks, otherwise a licensed set is available with a subscription service that requires a FortiGuard Security Rating Service subscription.

NEW QUESTION: 46
Refer to the exhibit. Which two ways can you view the log messages shown in the exhibit?
(Choose two.)

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluuid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

A. By right clicking the implicit deny policy
B. By filtering the policy universally unique identifier (UUID) and application name in the log entry
C. Using the FortiGate CLI command diagnose log test
D. In the Forward Traffic section
Answer: B,D (LEAVE A REPLY)
You can view log messages by filtering based on the policy UUID and application name in the log entry, and also in the Forward Traffic section, which displays logs related to allowed and denied traffic.

NEW QUESTION: 47
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 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 sent and reply packet of any new session.
Answer: A,C (LEAVE A REPLY)
The RPF (Reverse Path Forwarding) check is used to prevent IP spoofing attacks by verifying that the source IP address of a received packet is reachable through the same interface it arrived on. If not, the packet is dropped, ensuring traffic legitimacy.
The RPF check runs on the first sent packet of any new session to validate that the route to the source IP is consistent with the interface it's received on. This helps FortiGate detect spoofed or asymmetric routing scenarios early in the session establishment.

NEW QUESTION: 48
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 forced tunneling is enabled to reroute all traffic through the SSL VPN
C. Ensure that user traffic is hitting the firewall policy.
D. Ensure that the HTTPS service is enabled on SSL VPN tunnel interface
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
What are three key routing principles in SD-WAN? (Choose three.)
A. By default. SD-WAN rules are skipped if the included SD-WAN members do not have a valid route to the destination.
B. SD-WAN rules have precedence over any other type of routes.
C. Regular policy routes have precedence over SD-WAN rules.
D. By default. SD-WAN rules are skipped if only one route to the destination is available.
E. By default. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.
Answer: A,C,E (LEAVE A REPLY)
SD-WAN rules are matched only if the best route to the destination points to SD-WAN SD-WAN member is selected only if it has a route to the destination
https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan-sd-branch-architecture-for- mssps/768108/sd-wan-routing-logic SDWAN rules are 'policy routes', but regular policy routes have precedence over SD-WAN rules.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Explaining-the-SD-WAN-rule-matching- process/ta-p/284325

NEW QUESTION: 50
Refer to the exhibits. An administrator configured the Web Filter Profile to block access to all social networking sites except Facebook. However, when users try to access Facebook.com, they are redirected to a FortiGuard web filtering block page.
Based on the exhibits, which configuration change must the administrator make to allow Facebook while blocking all other social networking sites?

A. Set the Action as Exempt for www.facebook.com in the Static URL Filter.

B. Change the type as Simple in the Static URL Filter section.

C. Set the Social Networking action as warning in the FortiGuard Category Based Filter.

D. Change the Feature set of Web Filter Profile as Proxy-based.

Answer: (SHOW ANSWER)

NEW QUESTION: 51

An administrator manages a FortiGate model that supports NTurbo.

How does NTurbo enhance performance for flow-based inspection?

A. NTurbo buffers the whole file and then sends it to the antivirus engine.

B. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.

C. NTurbo creates two inspection sessions on the FortiGate device.

D. NTurbo offloads traffic to the content processor.

Answer: (SHOW ANSWER)

NTurbo creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface.

NEW QUESTION: 52

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

A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.

B. Advanced mode supports nested or inherited groups.

C. In advanced mode, security profiles can be applied only to user groups, not individual users.

D. Advanced mode uses the Windows convention -NetBios: Domain\Username.

Answer: A,B (LEAVE A REPLY)
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: 53
Refer to the exhibit showing a FortiGuard connection debug output.

FortiGuard connection debug output

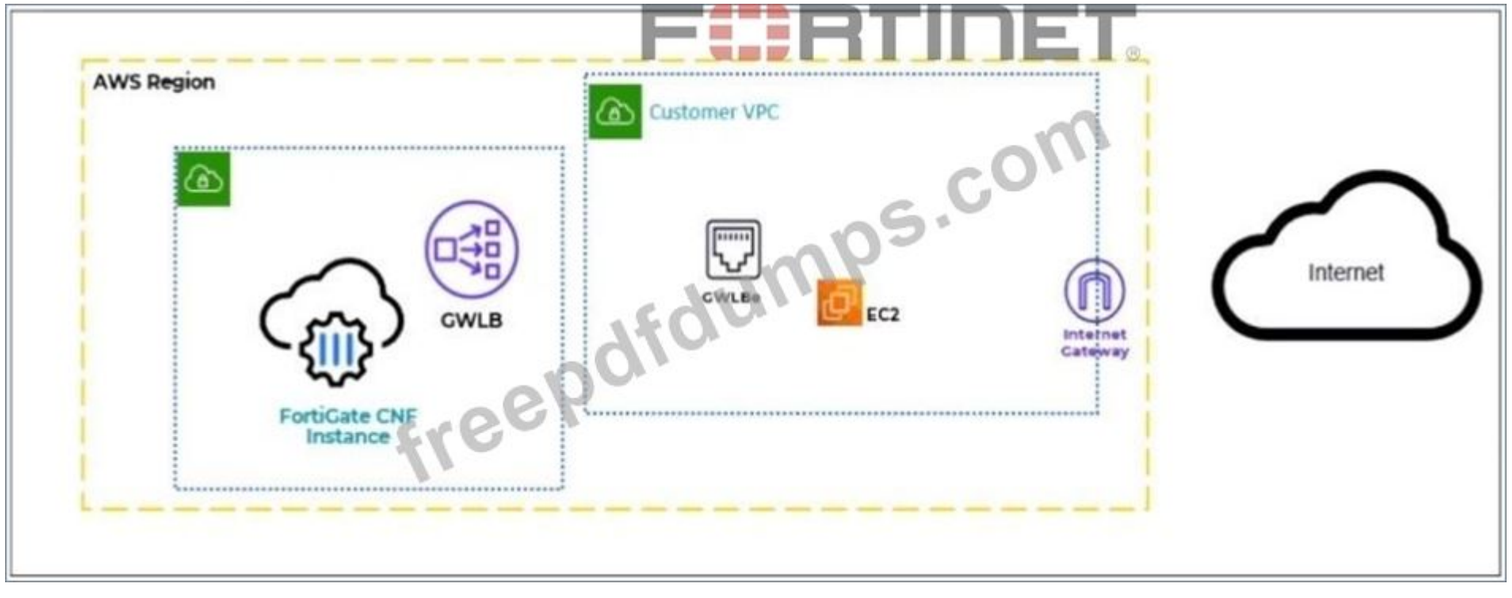
```
FortiGate # diagnose debug rating
Locale        : english

Service       : Web-filter
Status        : Enable
License       : Contract

Service       : Antispam
Status        : Disable

Service       : Virus Outbreak Prevention
Status        : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Thu Jun  9 11:26:56 2022) -=-

IP              Weight  RTT Flags TZ  FortiGuard-requests  Curr Lost Total Lost Updated Time
173.243.141.16      -8   18    DI  0                     4          0          0 Thu Jun  9 11:26:24 2022
12.34.97.18         20   30        1                     1          0          0 Thu Jun  9 11:26:24 2022
210.7.96.18        160  305        9                     0          0          0 Thu Jun  9 11:26:24 2022
```


Based on the output, which two facts does the administrator know about the FortiGuard connection? (Choose two.)
A. One server was contacted to retrieve the contract information.

B. FortiGate is using default FortiGuard communication settings.
C. There is at least one server that lost packets consecutively.
D. A local FortiManager is one of the servers FortiGate communicates with.
Answer: A,B (LEAVE A REPLY)
The output shows that one server was contacted to retrieve FortiGuard contract information, as indicated under "Service : Web-filter" with "License : Contract" and "Num. of servers : 1." The entry "Default servers : Included" confirms that FortiGate is using the default FortiGuard communication settings, meaning it communicates directly with Fortinet's public FortiGuard servers instead of a custom or local override.

NEW QUESTION: 54
When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate.
Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)
A. Allow
B. Trust & Allow
C. Allow & Warning
D. Block
E. Block & Warning
Answer: (SHOW ANSWER)
When a certificate fails for any of the reasons above, you can configure any of the following actions:
* Keep Untrusted & Allow: FortiGate allows the website and lets the browser decide the action to take.
FortiGate takes the certificate as untrusted.
* Block: FortiGate blocks the content of the site.
* Trust & Allow: FortiGate allows the website and takes the certificate as trusted.

NEW QUESTION: 55
Refer to the exhibit.
A partial cloud topology is shown.



You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS for FortiGate CNF policy enforcement for EC2 instance traffic.
Which path does the EC2 traffic take from the EC2 instance to the internet?

A. EC2 instance -> internet gateway (IGW) -> gateway load balancer (GWLB) -> FortiGate CNF -> internet

B. EC2 instance -> GWLBe -> FortiGate CNF -> GWLBe -> IGW -> internet

C. EC2 instance -> GWBL endpoint (GWLBe) -> FortiGate CNF -> IGW -> internet

D. EC2 instance -> FortiGate CNF -> GWLB -> GWLBe -> IGW -> internet

Answer: (SHOW ANSWER)

In an AWS Cloud-Native Firewall deployment, EC2 traffic is routed through the Gateway Load Balancer endpoint (GWLBe), which forwards the traffic to the FortiGate CNF for inspection. After processing, the FortiGate CNF sends the traffic out to the Internet Gateway (IGW) to reach the internet.

NEW QUESTION: 56

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

A. Lowest Cost (SLA) without load balancing

B. Manual with load balancing

C. Lowest Quality (SLA) with load balancing

D. Lowest Cost (SLA) with load balancing

E. Best Quality with load balancing

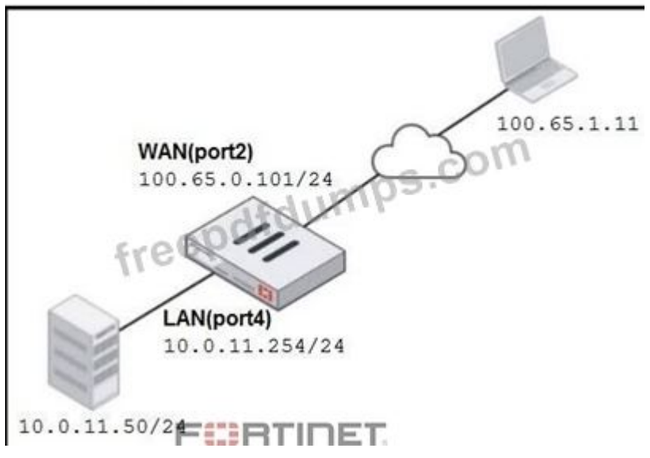
Answer: A,B,D (LEAVE A REPLY)

When you select Best Quality the "Load Balancing" toggle disappears from the UI. When you select Lowest Cost (SLA) you can choose to enable or disable load balancing.

NEW QUESTION: 57

Refer to the exhibits. A diagram of a FortiGate device connected to the network VIP object and firewall policy configurations are shown.
The WAN (port2) interface has the IP address 100.65.0.101/24.
The LAN (port4) interface has the IP address 10.0.11.254/24.
If the host 100.65.1.111sends a TCP SYN packet on port 443 to 100.65.0.200, what will the source address, destination address, and destination port of the packet be at the time FortiGate forwards the packet to the destination?

Network diagram



VIP object configuration

Firewall policies

	Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
☐	Internet(1)	LAN(port4)	WAN(port2)	all	all	always	ALL	ACCEPT		NAT
☐	Web_Server_Access(2)	WAN(port2)	LAN(port4)	all	VIP-WEB-SERVER	always	HTTPS	ACCEPT		Disabled

A. 10.0.11.254, 10.0.15.50, and 4443, respectively
B. 100.65.1.111, 10.0.11.50and 443, respectively
C. 10.0.11.254, 100.65.0.200, and 443, respectively
D. 100.65.1.111, 10.0.11.50, and 4443, respectively

Answer: (SHOW ANSWER)
The VIP object maps the external IP 100.65.0.200:443 to the internal server 10.0.11.50:4443.
Since NAT is disabled on the firewall policy, the source IP is preserved.
So, when host 100.65.1.111 connects to 100.65.0.200:443:
- The source remains 100.65.1.111.
- The destination IP is translated to 10.0.11.50.
- The destination port is translated to 4443.

NEW QUESTION: 58
What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device?
(Choose two.)
A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
B. Heartbeat IP addresses are used to distinguish between cluster members.
C. The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.
D. A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.
Answer: B,D (LEAVE A REPLY)
The FGCP uses link-local IPv4 addresses (see RFC 3927) in the 169.254.0.x range for the virtual HA heartbeat interface (port_ha) and for the inter-VDOM link interfaces between the vsys_ha and management VDOM. When members join an HA cluster, each member's heartbeat interface (port_ha) is assigned an IP address from the range of 169.254.0.1 to 169.254.0.63/26. HA inter- VDOM link interfaces (havdlink0 and havdlink1) are assigned IP address from the range of 169.254.0.65 to 169.254.0.66/26.
The IP address that is assigned to a virtual heartbeat interface depends on the serial number priority of the member. Higher serial numbers have a higher priority, and therefore a lower serialno_prio number.

NEW QUESTION: 59
Refer to the exhibit. 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: (SHOW ANSWER)
SNI-server-cert-check
Enable: Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.
Strict: Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.
Disable: Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.

NEW QUESTION: 60
What are two features of FortiGate FSSO agentless polling mode? (Choose two.)
A. FortiGate directs the collector agent to use a remote LDAP server.
B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
C. FortiGate does not support workstation check.
D. FortiGate uses the AD server as the collector agent.
Answer: B,C (LEAVE A REPLY)
FortiGate FSSO agentless polling mode uses the SMB protocol to directly read event viewer logs from domain controllers (DCs), eliminating the need for external collector agents.
Workstation checks are not supported in this mode, as FortiGate polls only DC logs and lacks the additional verification features of agent-based modes.

NEW QUESTION: 61
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

All traffic must be routed through the primary tunnel when both tunnels are up. The secondary tunnel must be used only if the primary tunnel goes down. In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.
Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)
A. In the phase1-interface, enable npu-offload to detect a dead tunnel.
B. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
C. Enable Dead Peer Detection.
D. Use the VPN wizard to create an IPsec template for a redundant IPsec VPN tunnel.
Answer: B,C (LEAVE A REPLY)
First, create one phase 1 for each path-one phase 1 for the primary VPN and one for the backup VPN. You should also enable DPD on both ends.
Second, create at least one phase 2 definition for each phase 1.
Third, you must add at least one static route for each VPN. Routes for the primary VPN must have a lower distance (or lower priority) than the backup. This causes FortiGate to use the primary VPN while it's available.
If the primary VPN fails, then FortiGate automatically uses the backup route. Alternatively, you could use a dynamic routing protocol, such as OSPF or BGP.

NEW QUESTION: 62
Refer to the exhibit.

You are configuring FortiAnalyzer on FortiGate.
Which step must you take to connect FortiAnalyzer to FortiGate?

A. Verify the FortiAnalyzer serial number.
B. Enable disk logging on FortiGate.
C. Authorize FortiGate on FortiAnalyzer.
D. Configure UDP port 514 on FortiGate.
Answer: C (LEAVE A REPLY)
Before FortiGate can send logs to FortiAnalyzer, the FortiGate device must be authorized on the FortiAnalyzer. This establishes trust and allows log forwarding from FortiGate to FortiAnalyzer.

NEW QUESTION: 63
Which two statements are correct when FortiGate enters conserve mode? (Choose two.)
A. FortiGate continues to run critical security actions, such as quarantine.
B. FortiGate refuses to accept configuration changes.
C. FortiGate halts complete system operation and requires a reboot to regain available resources.
D. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.
Answer: B,D (LEAVE A REPLY)
It does not accept config changes, because it might increase memory usage even further. It explicitly does NOT run any quarantine actions. You can configure IPS fail-open to control how IPS behaves when the IPS socket buffer is full.

NEW QUESTION: 64
Refer to the exhibit. The administrator configured SD-WAN rules and set the FortiGate traffic log page to display SD-WAN-specific columns: SD-WAN Quality and SD- WAN Rule Name.
FortiGate allows the traffic according to policy ID 1 placed at the top. This is the policy that allows SD-WAN traffic. Despite these settings, the traffic logs do not show the name of the SD-WAN rule used to steer those traffic flows.
What could be the reason?
SD-WAN traffic log

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
YouTube	Accept (8.08 kB / 27...	1(DIA)	port2		
YouTube	Accept (UTM Allowed)	1(DIA)	port2		
Facebook	Accept (UTM Allowed)	1(DIA)	port1		
Facebook	Accept (UTM Allowed)	1(DIA)	port1		
Facebook	Accept (3.33 kB / 10...	1(DIA)	port1		
YouTube	Accept (44.63 kB/ 3...	1(DIA)	port2		
CNN	Accept (UTM Allowed)	1(DIA)	port1		
CNN	Accept (UTM Allowed)	1(DIA)	port2		
CNN	Accept (UTM Allowed)	1(DIA)	port2		

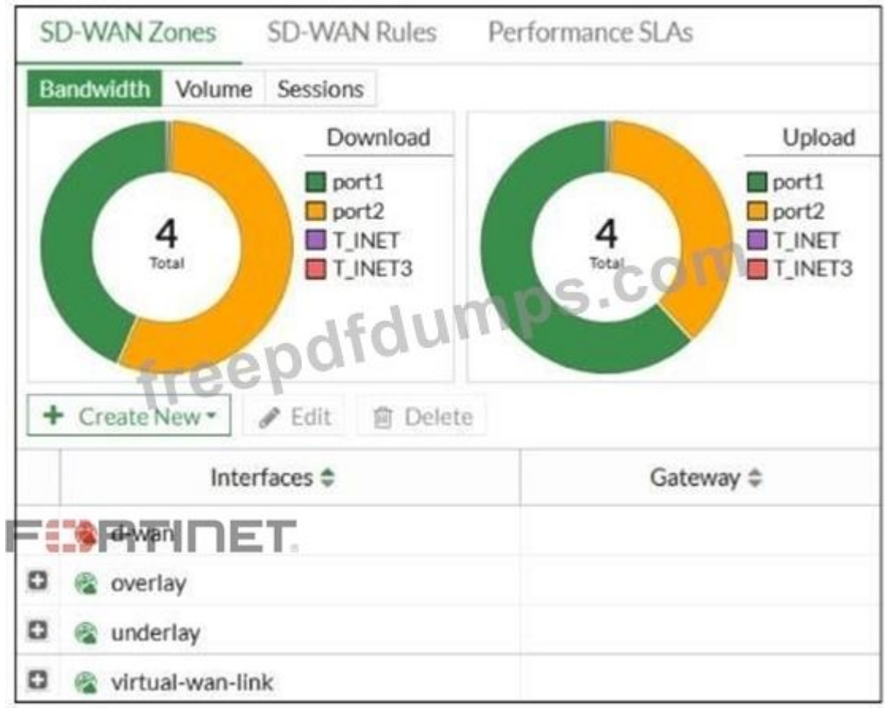
A. SD-WAN rule names do not appear immediately. The administrator must refresh the page.
B. There is no application control profile applied to the firewall policy.
C. FortiGate load balanced the traffic according to the implicit SD-WAN rule.
D. Destinations in the SD-WAN rules are configured for each application, but feature visibility is not enabled.
Answer: (SHOW ANSWER)

Note that the ImplicitSD-WAN rule name does not appear in the SD-WAN Rule Name column. When the traffic is steered according to this rule, the field remains empty.

NEW QUESTION: 65

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

FortiGate SD-WAN zone configuration



Based on the exhibit, which statement is true?

A. The underlay zone contains port1 and port2.

B. The d-wan zone contains no member.

C. The d-wan zone cannot be deleted.

D. The virtual-wan-link zone contains no member.

Answer: (SHOW ANSWER)

The "d-wan" zone in FortiGate SD-WAN configuration is the default SD-WAN zone created when SD- WAN is enabled. This zone contains all the interfaces assigned to SD-WAN and is essential for the functionality of the SD-WAN feature. The "d-wan" zone cannot be deleted because it is required for SD-WAN operations. Option A is incorrect because the underlay zone does not contain port1.

NEW QUESTION: 66

There are multiple dialup IPsec VPNs configured in aggressive mode on the HQ FortiGate. The requirement is to connect dial-up users to their respective department VPN tunnels. Which phase 1 setting you can configure to match the user to the tunnel?

A. Dead Peer Detection

B. Peer ID

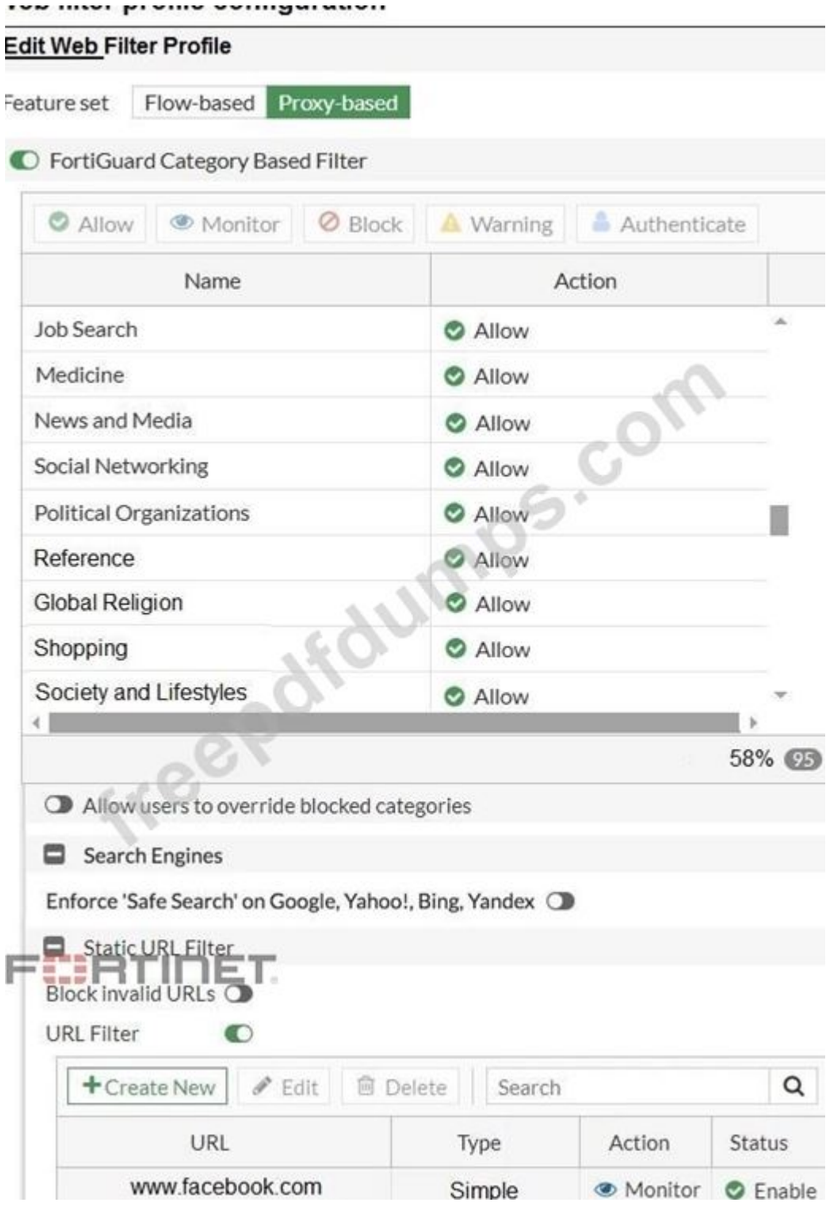
C. Local Gateway

D. IKE Mode Config

Answer: (SHOW ANSWER)
Peer ID is used in aggressive mode dialup IPsec VPNs to identify and match incoming VPN connections to their correct phase 1 configuration/tunnel. This allows each department or user to have a unique identifier, ensuring users are connected to the correct VPN tunnel. This is the recommended approach for environments with multiple dial-up users or tunnels.

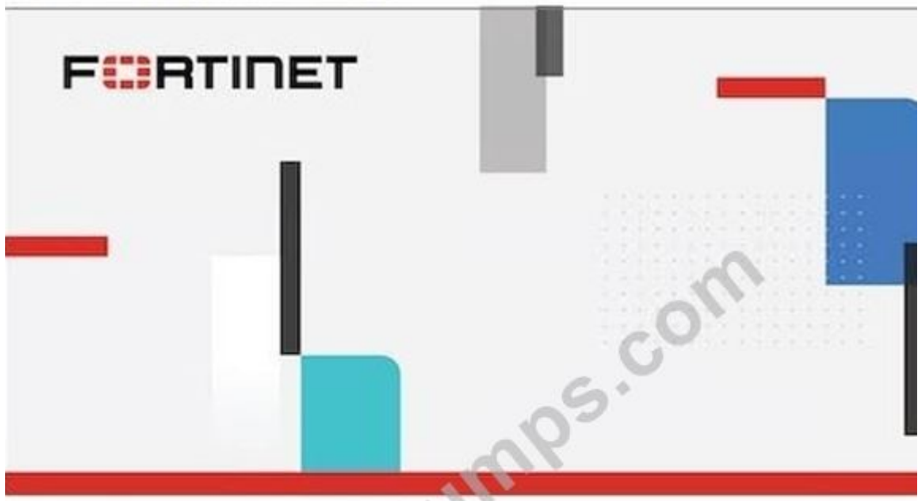
NEW QUESTION: 67
What are two features of the NGFW profile-based mode? (Choose two.)
A. NGFW profile-based mode can only be applied globally and not on individual VDOMs.
B. NGFW profile-based mode must require the use of central source NAT policy.
C. NGFW profile-based mode policies support both flow inspection and proxy inspection.
D. NGFW profile-based mode supports applying applications and web filtering profiles in a firewall policy.
Answer: C,D (LEAVE A REPLY)
NGFW (Next Generation Firewall) profile-based mode in FortiGate allows policies to use both flow- based and proxy-based inspection modes, providing flexibility depending on security and performance requirements. Additionally, profile-based mode supports applying applications and web filtering profiles directly in a firewall policy, allowing granular control over the traffic.

NEW QUESTION: 68
Refer to the exhibits. A web filter profile configuration and firewall policy configuration are shown.
You are trying to access www.facebook.com, but you are redirected to a FortiGuard web filtering block page.
Based on the exhibits, what is the possible cause of the issue?


Edit Web Filter Profile
Feature set
Flow-based
Proxy-based
FortiGuard Category Based Filter
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Job Search
Allow
Medicine
Allow
News and Media
Allow
Social Networking
Allow
Political Organizations
Allow
Reference
Allow
Global Religion
Allow
Shopping
Allow
Society and Lifestyles
Allow
58%
95
Allow users to override blocked categories
Search Engines
Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex
Static URL Filter
Block invalid URLs
URL Filter
Create New
Edit
Delete
Search
URL
Type
Action
Status
www.facebook.com
Simple
Monitor
Enable

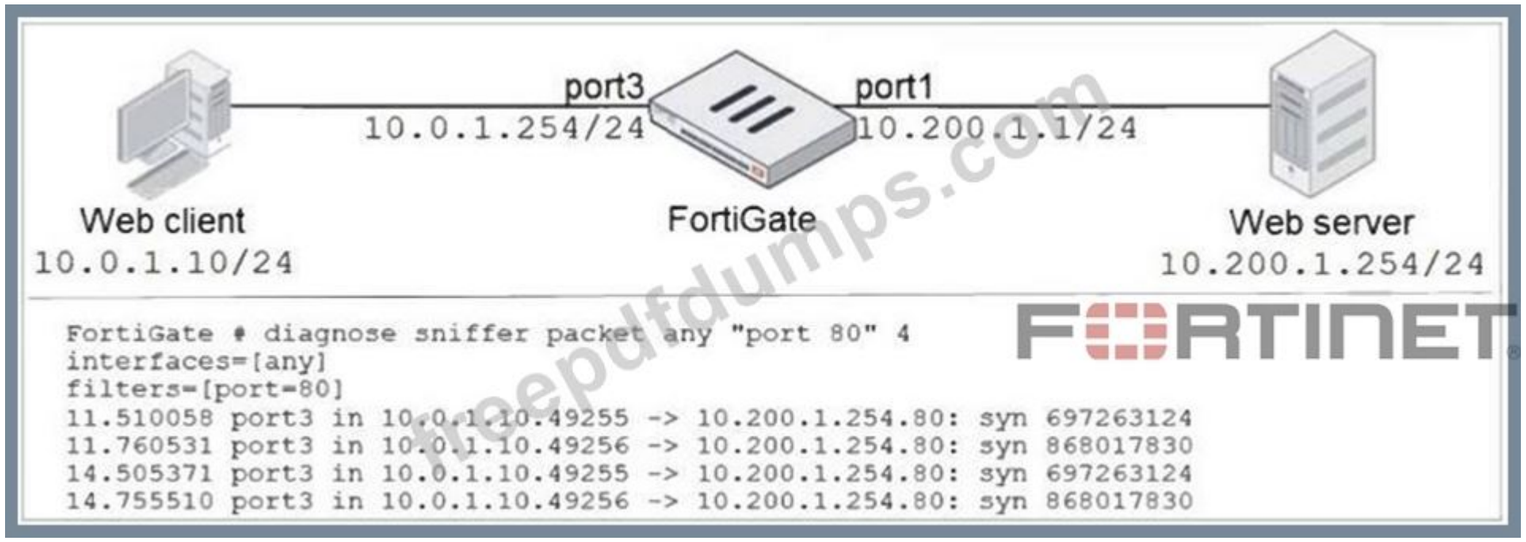
Firewall policy configuration

FortiGuard block page



A. The web filter profile feature set is configured incorrectly.
B. The web rating override configuration is incorrect.
C. The firewall policy inspection mode is incorrect.
D. For www.facebook.com, the URL filter action is incorrect.
Answer: B (LEAVE A REPLY)
The web filter profile shows a URL filter override for www.facebook.com with action Monitor, which should allow access. However, the block page shows FortiGuard categorizing www.facebook.com as Malicious Websites and blocking it. This indicates that the web rating override configuration is incorrect (the override is not applied properly), so FortiGuard's default category action takes precedence and blocks the site.

NEW QUESTION: 69
Refer to the exhibit. In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit. What should the administrator do next, to troubleshoot the problem?



A. Execute a debug flow.

B. Capture the traffic using an external sniffer connected to port1.

C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".

D. Run a sniffer on the web server.

Answer: (SHOW ANSWER)

If FortiGate is dropping packets, can a packet capture (sniffer) be used to identify the reason? To find the cause, you should use the debug (packet) flow.