# Fortinet.FCP_FGT_AD-7.6.v2026-09-28.q63

| | |
|---|---|
| **Exam Code:** | FCP_FGT_AD-7.6 |
| **Exam Name:** | FCP - FortiGate 7.6 Administrator |
| **Certification Provider:** | Fortinet |
| **Free Question Number:** | 63 |
| **Version:** | v2026-09-28 |
| **# of views:** | 108 |
| **# of Questions views:** | 658 |
| https://www.freecram.net/torrent/Fortinet.FCP_FGT_AD-7.6.v2026-09-28.q63.html | |

**NEW QUESTION: 1**
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: (SHOW ANSWER)**
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: 2**
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: 3**
Refer to the exhibit.

**Firewall policies**

| ID | Name | From | To | Source | Destination | Schedule | Service | Action | IP Pool | NAT |
|---|---|---|---|---|---|---|---|---|---|---|
| **LAN to WAN 1** | | | | | | | | | | |
| 1 | Full_Access | LAN (port3) | WAN (port1)<br>WAN (port2) | all | all | always | ALL | ACCEPT | IP Pool | NAT |
| **WAN to LAN 3** | | | | | | | | | | |
| 2 | Deny | WAN (port1) | LAN (port3) | Deny_IP | all | always | ALL | DENY | | |
| 3 | Allow_access | WAN (port1) | LAN (port3) | all | Webserver | always | ALL | ACCEPT | | Disabled |
| 4 | Webserver | WAN (port1) | LAN (port3) | all | Webserver | always | ALL | ACCEPT | | Disabled |
| **Implicit 1** | | | | | | | | | | |
| 0 | Implicit Deny | any | any | all | all | always | ALL | DENY | | |

Which statement about this firewall policy list is true?
**A.** The firewall policies are listed by ID sequence view.
**B.** The firewall policies are listed by ingress and egress interfaces pairing view.
**C.** The Implicit group can include more than one deny firewall policy.
**D.** LAN to WAN, WAN to LAN, and Implicit are sequence grouping view lists.
**Answer: (SHOW ANSWER)**
The firewall policy list shown is displayed in the sequence grouping view, where policies are grouped based on their traffic direction - such as LAN to WAN, WAN to LAN, and Implicit. This view helps administrators quickly identify and manage policies according to their interface pairings and logical traffic flow, rather than by numerical ID order.

**NEW QUESTION: 4**
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: 5**
Refer to the exhibits.



**Firewall policy**




FORTINET
freecram.net




**HTTPS access**




freecram.net

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: 6**
Refer to the exhibit. Based on the routing table shown in the exhibit, which two statements are true? (Choose two.)

| Destination | Gateway IP | Interface | Status |
|---|---|---|---|
| 0.0.0.0/0 | 100.65.0.254 | port2 | Enabled |
| 10.10.10.0/24 | 100.66.0.254 | port3 | Enabled |
| 10.0.13.0/24 | 10.0.13.125 | port6 | Enabled |

**A.** A packet with the source IP address 10.100.110.10arriving on port3 is allowed if strict RPF is disabled.
**B.** A packet with the source IP address 10.100.110.10arriving on port2 is allowed if strict RPF is enabled.
**C.** A packet with the source IP address 10.0.13.10arriving on port2 is allowed if strict RPF is disabled.
**D.** A packet with the source IP address 10.10.10.10arriving on port2 is allowed if strict RPF is enabled.
**Answer: (SHOW ANSWER)**

With strict RPF enabled, the FortiGate checks that the return path to the source would use the same interface the packet arrived on defencedev.com
. For a source of 10.10.10.10, the routing table shows the return path is via the 10.10.10.0/24 route on port 3. If such a packet arrives on port 2, the return path doesn't match and strict RPF drops it.
When strict RPF is disabled, FortiGate uses loose RPF, which permits a packet as long as there is a route back to the source defencedev.com
. In this case the only route back to 10.100.110.10 is the default route via port 2, not the incoming port 3. Exam guidance takes a conservative view that, without a more specific route to the source (and with no RPF enabled on that interface), such a packet would not be accepted.

**NEW QUESTION: 7**
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: (SHOW ANSWER)**

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: 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.** Run SSL VPN on one interface using port 443 and enable HTTPS administrative access on a different interface, also using port 443.

**B.** Keep port 443 for both SSL VPN and HTTPS administrative access on the same interface without any problems.

**C.** Change the port number for either the SSL VPN service or the HTTPS administrative service if both are on the same interface.

**D.** Disable SSL VPN if HTTPS administrative access is using port 443 on any interface.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 9**

Refer to the exhibit. What can you conclude from the log shown in the exhibit?

```
date=2025-02-4 time=09:07:59 logid=0100022700 type=event subtype=system level=critical
vd= "root" logdesc= "IPS session scan paused" action= "drop" msg= "IPS session scan,
enter fail open mode"
```

**A.** The IPS scan is paused by the IPS diagnostic command with bypass mode option 5.

**B.** The IPS socket buffer is full and IPS engine needs more memory to create new sessions.

**C.** The IPS session scan is paused and reevaluating the packet because of a dirty flag.

**D.** The IPS socket buffer is full and IPS engine cannot decode a packet.

**Answer: (SHOW ANSWER)**

The log message IPS session scan paused, enter fail open mode indicates that the IPS socket buffer is full, meaning the IPS engine does not have enough memory to process new sessions.

As a result, FortiGate switches to fail-open mode, allowing traffic to pass (or temporarily dropping it) without full IPS scanning.

**NEW QUESTION: 10**

A FortiGate firewall policy is configured with active authentication, however, the user cannot authenticate when accessing a website.

Which protocol must FortiGate allow even though the user cannot authenticate?

Freecram.net

**A.** LDAP

**B.** TACASC+

**C.** Kerberos

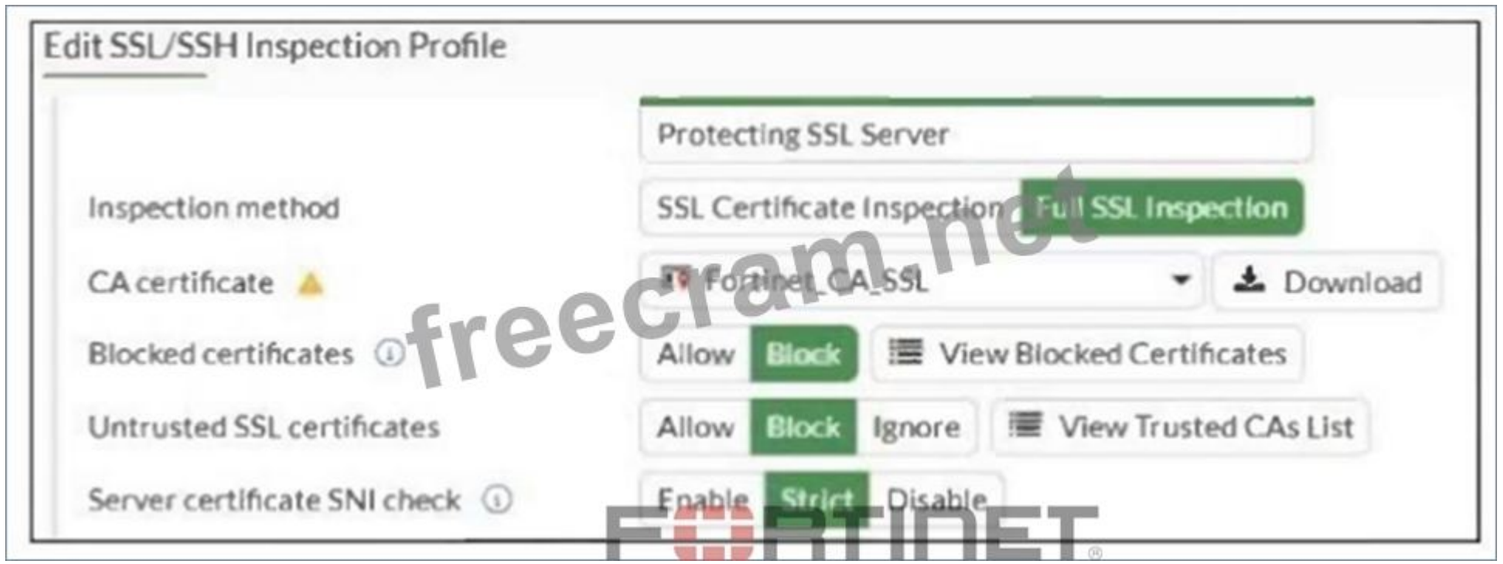
**D.** DNS

**Answer: (SHOW ANSWER)**

A firewall policy must allow a protocol in order to show the authentication dialog that is used in active authentication (such as HTTP/HTTPS/FTP/Telnet) and DNS.

**NEW QUESTION: 11**

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: 12**
Refer to the exhibit, which shows a partial configuration from the remote authentication server.




Why does the FortiGate administrator need this configuration?
**A.** To set up a RADIUS server Secret.
**B.** To authenticate Any FortiGate user groups.
**C.** To authenticate and match the Training OU on the RADIUS server.
**D.** To authenticate only the Training user group.
**Answer: (SHOW ANSWER)**
The Fortinet-Group-Name attribute is used to restrict authentication to users who belong specifically to the "Training" user group on the RADIUS server.

**NEW QUESTION: 13**
Refer to the exhibit. Why is the Antivirus scan switch grayed out when you are creating a new antivirus profile for FTP?




**A.** None of the inspected protocols are active in this profile.

**B.** FortiGate, with less than 2 GB RAM, does not support the Antivirus scan feature.

**C.** Antivirus scan is disabled under System -> Feature visibility.

**D.** The Feature Set for the profile is Flow-based but it must be Proxy-based.

**Answer: A (LEAVE A REPLY)**

Enable one or more protocols for inspection, then enable AntiVirus scan for the selected protocols with a specified action.
https://docs.fortinet.com/document/fortigate/7.6.4/administration-guide/922096/inspection-mode- feature-comparison

**NEW QUESTION: 14**

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: 15**

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

**A.** FortiGate buffers the whole file but transmits to the client at the same time.

**B.** Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.

**C.** If a virus is detected, the last packet is delivered to the client.

**D.** Flow-based inspection optimizes performance compared to proxy-based inspection.

**E.** The IPS engine handles the process as a standalone.

**Answer: (SHOW ANSWER)**

Flow-based antivirus buffers the entire file while simultaneously transmitting data to the client to minimize latency.

Flow-based inspection combines multiple scanning techniques from proxy-based modes for efficient detection.

Flow-based inspection provides better performance by processing traffic on the fly without full proxy overhead.

**NEW QUESTION: 16**

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**

Edit Application Sensor

Categories

Mixed · All Categories

| | |
|---|---|
| Business (157, 6) | Cloud/IT (72, 12) |
| Collaboration (266, 13) | Email (76, 11) |
| Game (83) | General Interest (254, 15) |
| Mobile (3) | Network Service (338) |
| Operational Technology | P2P (55) |
| Proxy (189) | Remote Access (96) |
| Social Media (113, 29) | Storage/Backup (150, 20) |
| Update (48) | Video/Audio (148, 17) |
| VoIP (23) | Web Client (24) |
| 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 Google | Filter | Monitor |

2

FORTINET
freecram.net

**Firewall policy**



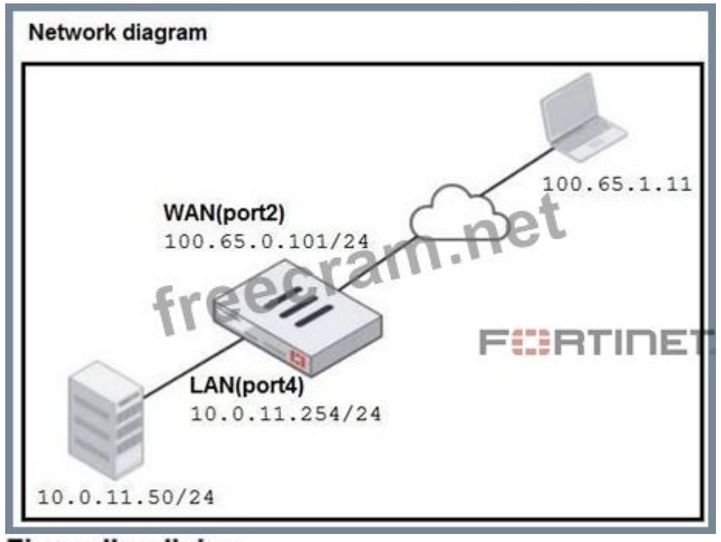

freecram.net
FORTINET

**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.

**Valid FCP_FGT_AD-7.6 Dumps** shared by EduDump.com for Helping Passing FCP_FGT_AD-7.6 Exam! EduDump.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the EduDump.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCP_FGT_AD-7.6 dumps with Test Engine here:
https://www.edudump.com/exams/Fortinet/FCP_FGT_AD-7.6/premium/ (**132** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

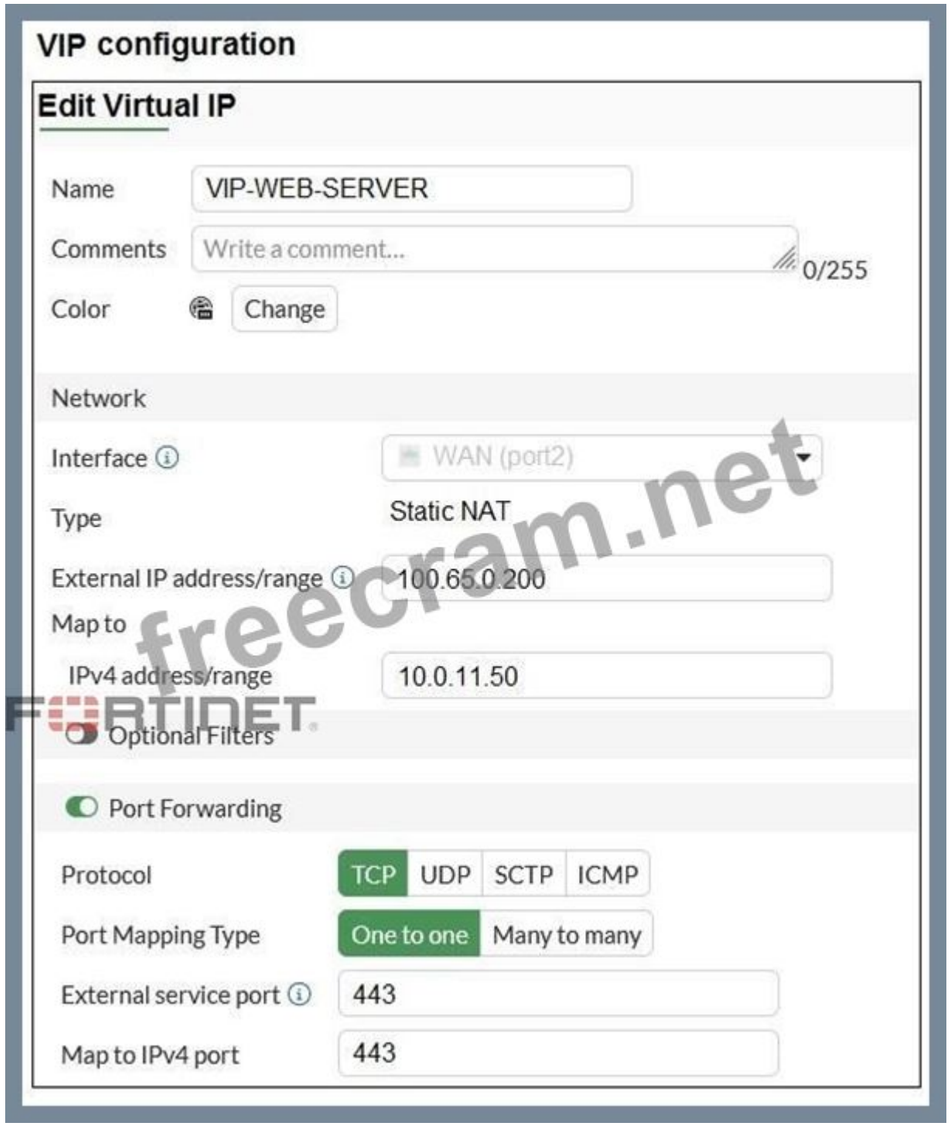
**NEW QUESTION: 17**
Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, and the firewall policies, VIP, and IP pool configurations on the FortiGate device.
The WAN (port2) interface has the IP address 100.65.0.101/24.
The LAN (port4) interface has the IP 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?




**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 |

freecram.net FORTINET




freecram.net

**NAT IP pool configuration**




freecram.net

**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: 18**
An administrator wants to form an HA cluster using the FGCP protocol.
Which two requirements must the administrator ensure both members fulfill? (Choose two.)
**A.** They must have the same HA group ID.
**B.** They must have the heartbeat interfaces in the same subnet.
**C.** They must have the same number of configured VDOMs.
**D.** They must have the same hard drive configuration.
**Answer: (SHOW ANSWER)**
They must have the same HA Group ID and same Hard Drive Configuration.

**NEW QUESTION: 19**
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)**

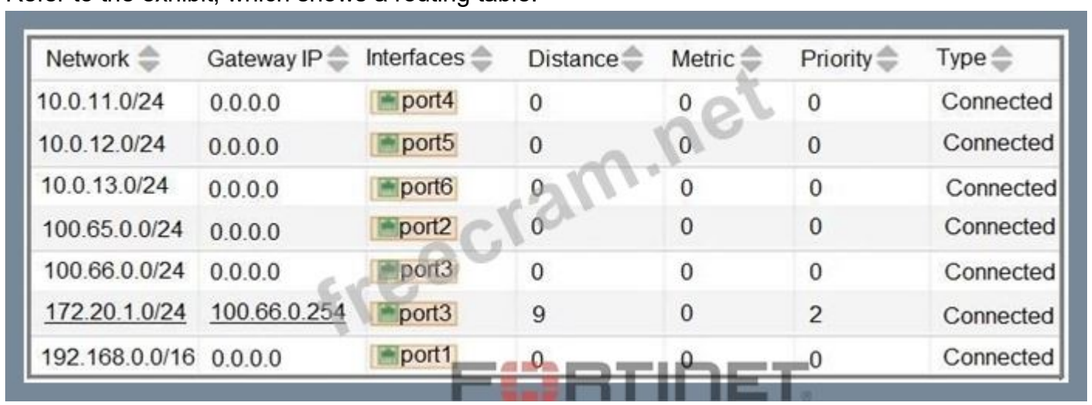
NTurbo creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface.

**NEW QUESTION: 20**
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: (SHOW ANSWER)**
Underlay is not a default zone. It is user defined and not active.

**NEW QUESTION: 21**
Refer to the exhibit, which shows a routing table.



| Network | Gateway IP | Interfaces | Distance | Metric | Priority | Type |
|---|---|---|---|---|---|---|
| 10.0.11.0/24 | 0.0.0.0 | port4 | 0 | 0 | 0 | Connected |
| 10.0.12.0/24 | 0.0.0.0 | port5 | 0 | 0 | 0 | Connected |
| 10.0.13.0/24 | 0.0.0.0 | port6 | 0 | 0 | 0 | Connected |
| 100.65.0.0/24 | 0.0.0.0 | port2 | 0 | 0 | 0 | Connected |
| 100.66.0.0/24 | 0.0.0.0 | port3 | 0 | 0 | 0 | Connected |
| 172.20.1.0/24 | 100.66.0.254 | port3 | 9 | 0 | 2 | Connected |
| 192.168.0.0/16 | 0.0.0.0 | port1 | 0 | 0 | 0 | Connected |

An administrator wants to create a new static route so the traffic to the subnet 172.20.1.0/24 is routed through port2 only.
What are the two criteria that the administrator can use to achieve this objective? (Choose two.)
**A.** The new static route must have the distance set to 9.
**B.** The existing static route through port3 must have the distance set to 11.
**C.** The new static route must have the priority set to 3.
**D.** The new static route must have the metric set to 1.
**Answer: (SHOW ANSWER)**
From the online study guide: "The lower the metric, the higher the preference" and "The lower the priority, the higher the preference" so it can't be C nor D.

**NEW QUESTION: 22**
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?

FORTINET

## Application sensor configuration

### Edit Application Sensor

Categories

All Categories

| | |
|---|---|
| Business (179, 6) | Cloud.IT (31) |
| Collaboration (293, 6) | Email (87, 12) |
| Game (124) | General.Interest (241, 9) |
| Mobile (3) | Network.Service (332) |
| P2P (85) | Proxy (106) |
| Remote.Access (91) | Social.Media (150, 31) |
| Storage.Backup (296, 16) | Update (48) |
| Video/Audio (206, 13) | VoIP (30) |
| Web.Client (18) | Unknown Applications |

Network Protocol Enforcement

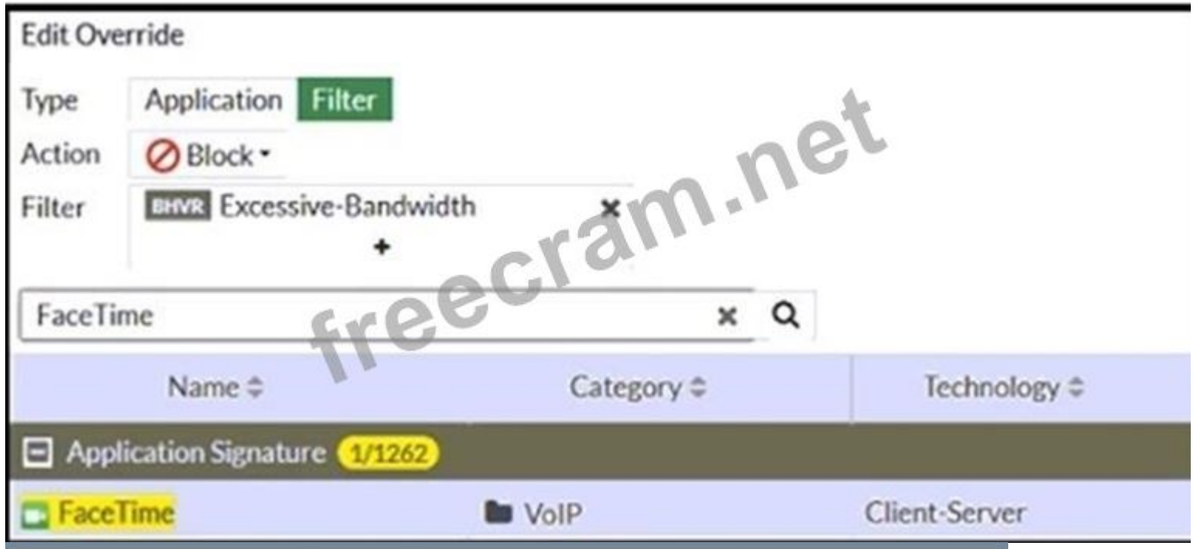
Application and Filter Overrides

+ Create New | Edit | Delete

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

freecram.net

**Application override configuration**




**Filter override configuration**




freecram.net

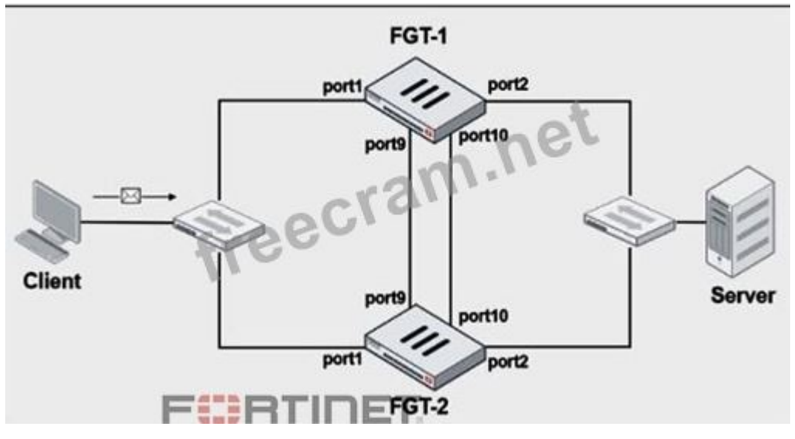
**A.** Apple Face Time will be allowed, based on the Video/Audio category configuration.
**B.** Apple Face Time will be blocked, based on the Excessive-Bandwidth filter configuration.
**C.** Apple Face Time will be allowed, based on the Apple filter configuration.
**D.** Apple Face Time will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.
**Answer: (SHOW ANSWER)**
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: 23**
Which two statements describe characteristics of automation stitches? (Choose two.)

**A.** Actions involve only devices included in the Security Fabric.
**B.** An automation stitch can have multiple triggers.
**C.** Multiple actions can run in parallel.
**D.** Triggers can involve external connectors.
**Answer: (SHOW ANSWER)**
Automation stitches can execute multiple actions concurrently (in parallel).
Triggers for automation stitches can come from external connectors beyond just Fortinet devices.

**NEW QUESTION: 24**
An administrator must enable a DHCP server on one of the directly connected networks on FortiGate. However, the administrator is unable to complete the process on the GUI to enable the service on the interface.
In this scenario, what prevents the administrator from enabling DHCP service?
**A.** The DHCP server setting is available only on the CLI.
**B.** Another interface is configured as the only DHCP server on FortiGate.
**C.** The FortiGate model does not support the DHCP server.
**D.** The role of the interface prevents setting a DHCP server.
**Answer: (SHOW ANSWER)**
An interface's role (for example, WAN or DMZ) determines whether DHCP server configuration is allowed. If the interface is set to a role such as WAN, FortiGate restricts enabling DHCP server service on that interface. To enable DHCP, the interface role must be changed to LAN or Internal, which supports DHCP server functionality.

**NEW QUESTION: 25**
Refer to the exhibits.
FortiGate HA cluster topology



freecram.net

**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.

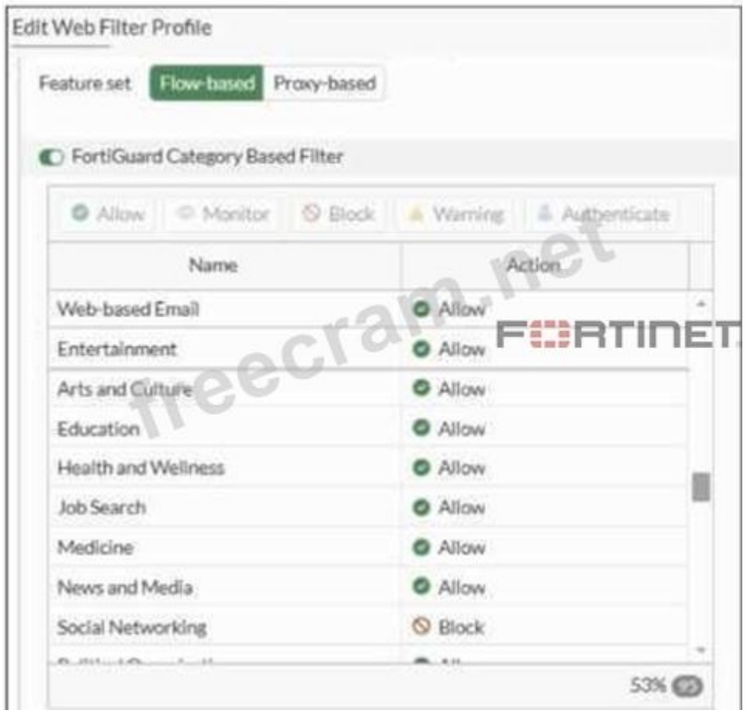
**Answer: (SHOW ANSWER)**

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: 26**
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?

**Web filter configuration**




**A.** Set the Social Networking action as warning in the FortiGuard Category Based Filter.
**B.** Change the Feature set of Web Filter Profile as Proxy-based.
**C.** Set the Action as Exempt for www.facebook.com
in the Static URL Filter.
**D.** Change the type as Simple in the Static URL Filter section.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 27**
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: (SHOW ANSWER)**
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: 28**
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.** SSL VPN dtls-hello-timeout
**B.** SSL VPN login-timeout
**C.** SSL VPN session-ttl
**D.** SSL VPN idle-timeout
**Answer: (SHOW ANSWER)**
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: 29**
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: (SHOW ANSWER)**
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: 30**
What is the primary FortiGate election process when the HA override setting is enabled?
**A.** Connected monitored ports > Priority > HA uptime > FortiGate serial number
**B.** Connected monitored ports > Priority > System uptime > FortiGate serial number
**C.** Connected monitored ports > HA uptime > Priority > FortiGate serial number
**D.** Connected monitored ports > System uptime > Priority > FortiGate serial number
**Answer: (SHOW ANSWER)**
If Override DISABLED then: ports > HA Uptime > Priority > SN.
If Overrrid ENABLED then: ports > Priority > HA Uptime > SN.

**NEW QUESTION: 31**
Refer to the exhibit. Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

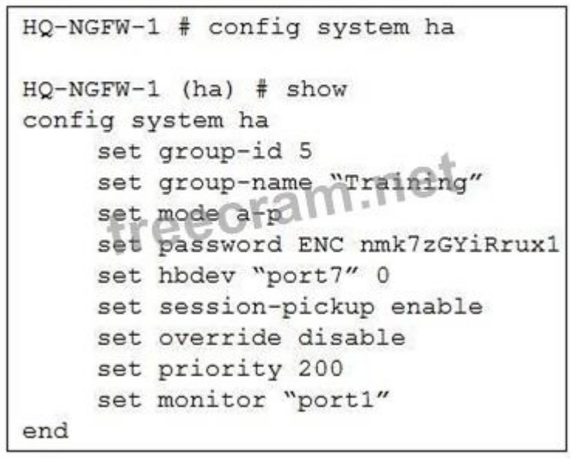



**A.** Administrators cannot change the configuration.
**B.** FortiGate skips quarantine actions.
**C.** Administrators must restart FortiGate to allow new session.
**D.** FortiGate drops new sessions requiring inspection.
**Answer: (SHOW ANSWER)**
System configuration cannot be changed because of the IPS Global configuration "fail-open enabled" FortiGate skips quarantine actions - again because of the IPS Global configuration "fail-open enabled"

**Valid FCP_FGT_AD-7.6 Dumps** shared by EduDump.com for Helping Passing FCP_FGT_AD-7.6 Exam! EduDump.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the EduDump.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCP_FGT_AD-7.6 dumps with Test Engine here:
https://www.edudump.com/exams/Fortinet/FCP_FGT_AD-7.6/premium/ (**132** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

**NEW QUESTION: 32**
Refer to the exhibits. An administrator configured both members of an HA cluster at the same time. After one week of monitoring, the administrator wants to verify the HA failover performance.
How can the administrator force a failover?

**HQ-NGFW-1 HA configuration**



HQ-NGFW-2 HA configuration

```
HQ-NGFW-2 (ha) # show
config system ha
      set group-id 5
      set group-name "Training"
      set mode a-p
      set password ENC n40G3dmn0K50s
      set hbdev "port7" 0
      set session-pickup enable
      set override disable
      set priority 100
      set monitor "port1"
end
```

**A.** The administrator must reset the HA uptime on HQ-NGFW-1.
**B.** The administrator must set the parameter override to enable on HQ-NGFW-2.
**C.** The administrator must increase the HA priority on HQ-NGFW-2.
**D.** The administrator must set the monitored port to down on HQ-NGFW-1.
**Answer: (SHOW ANSWER)**
Both FortiGates are in an active-passive (a-p) HA cluster with override disabled. This means failover is triggered only if the primary (HQ-NGFW-1) becomes unavailable or monitored interfaces fail. To test failover performance, the administrator can set the monitored interface (port1) down on HQ-NGFW-1, which will force a failover to HQ-NGFW-2.

**NEW QUESTION: 33**
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: (SHOW ANSWER)**
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: 34**
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 there is no inbound traffic.
Which DPD mode on FortiGate meets this requirement?
**A.** Enabled
**B.** On Idle

**C.** Disabled
**D.** On Demand
**Answer: (SHOW ANSWER)**
Disable: Disable Dead Peer Detection.
On-idle: Trigger Dead Peer Detection when no IPsec traffic is received.
On-demand: Trigger Dead Peer Detection when no IPsec traffic is received AND FortiGate has been sending IPsec traffic. On-demand is the default setting.

**NEW QUESTION: 35**
Which two statements are true about an HA cluster? (Choose two.)
**A.** An HA cluster cannot have both in-band and out-of-band management interfaces at the same time.
**B.** Link failover triggers a failover if the administrator sets the interface down on the primary device.
**C.** When sniffing the heartbeat interface, the administrator must see the IP address 169.254.0.2.
**D.** HA incremental synchronization includes FIB entries and IPsec SAs.
**Answer: (SHOW ANSWER)**
Incremental synchronization also synchronizes other dynamic configuration information such as the DHCP server address lease database, routing table updates, IPsec SAs, MAC address tables, and so on.
HA propagates more than just configuration details. Some runtime data, such as DHCP leases and FIB entries, are also synchronized.

**NEW QUESTION: 36**
A network administrator has configured an SSL/SSH inspection profile defined for full SSL inspection and set with a private CA certificate. The firewall policy that allows the traffic uses this profile for SSL inspection and performs web filtering. When visiting any HTTPS websites, the browser reports certificate warning errors.
What is the reason for the certificate warning errors?
**A.** The SSL cipher compliance option is not enabled on the SSL inspection profile. This setting is required when the SSL inspection profile is defined with a private CA certificate.
**B.** The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
**C.** The browser does not recognize the certificate in use as signed by a trusted CA.
**D.** With full SSL inspection it is not possible to avoid certificate warning errors at the browser level.
**Answer: (SHOW ANSWER)**
The certificate warning errors occur because the SSL inspection profile is configured to use a private CA certificate that is not recognized by the browser as being signed by a trusted CA. For the browser to trust the FortiGate's re-signed certificates, the CA certificate used by FortiGate for SSL inspection must be installed in the browser's trusted certificate store. Until the browser recognizes the certificate authority (CA) as trusted, it will continue to display warning errors when accessing HTTPS websites.

**NEW QUESTION: 37**
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: (SHOW ANSWER)**
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.

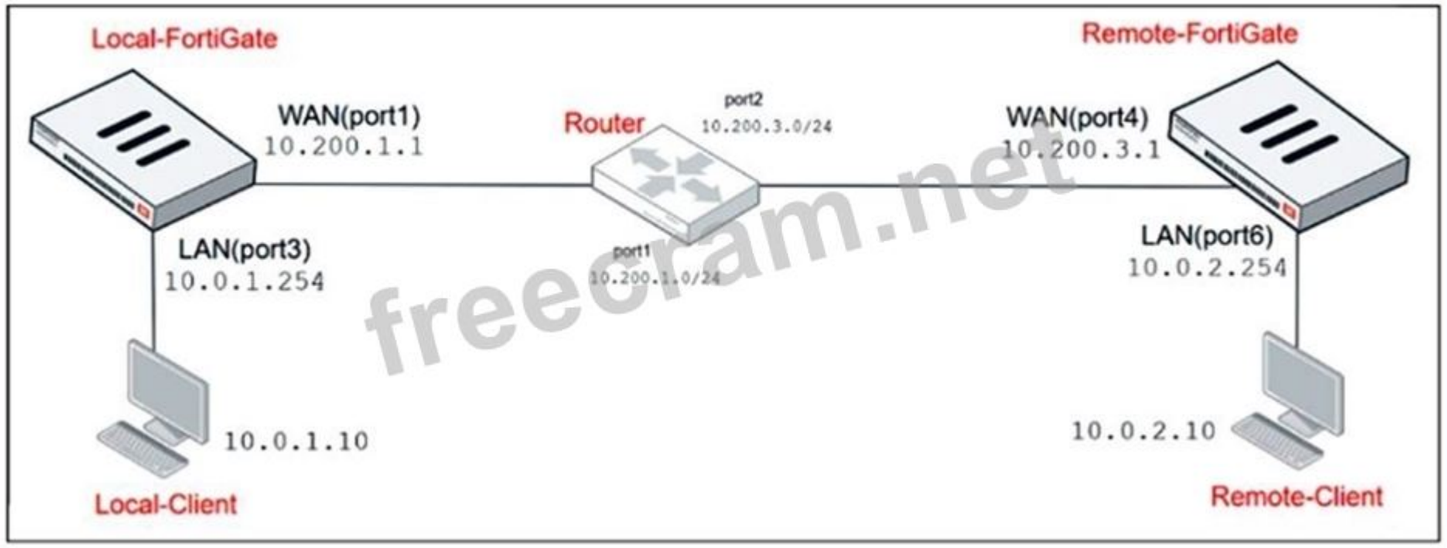
**NEW QUESTION: 38**
What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device?
(Choose two.)
**A.** Heartbeat interfaces have virtual IP addresses that are manually assigned.
**B.** Heartbeat IP addresses are used to distinguish between cluster members.
**C.** The heartbeat 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: (SHOW ANSWER)**
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: 39**
You have configured the FortiGate device for FSSO. A user is successful in log-in to windows, but their access to the internet is denied.
What should the administrator check first?
**A.** Whether the user is assigned to the correct AD group.
**B.** The FortiGate firewall policy settings for SSL decryption.
**C.** The FortiGate FSSO active users list for user's IP address.
**D.** The windows event viewer for failed login attempts.
**Answer: (SHOW ANSWER)**
Checking the active users list verifies if FortiGate correctly associates the user with their IP address, ensuring proper policy enforcement for internet access.

**NEW QUESTION: 40**
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?
Freecram.net
**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.

Refer to the exhibits.
**NEW QUESTION: 41**

**Network diagram**




**NAT IP pool configuration**

| Name | External IP Range | Type | ARP Reply |
|---|---|---|---|
| SNAT-Pool | 10.200.1.49 - 10.200.1.49 | Overload | Enabled |
| SNAT-Remote | 10.200.1.149 - 10.200.1.149 | Overload | Enabled |
| SNAT-Remote1 | 10.200.1.99 - 10.200.1.99 | Overload | Enabled |

**Firewall policy**

| ID | Name | Source | Destination | Schedule | Service | Action | IP Pool | NAT |
|---|---|---|---|---|---|---|---|---|
| LAN (port3) → WAN (port1) 3 | | | | | | | | |
| 2 | TCP traffic | all | REMOTE_FORTIGATE | always | ALL_TCP | ACCEPT | SNAT-Pool | NAT |
| 6 | PING traffic | all | all | always | PING | ACCEPT | SNAT-Remote1 | NAT |
| 7 | IGMP traffic | all | all | always | IGMP | ACCEPT | SNAT-Remote | NAT |

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

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.

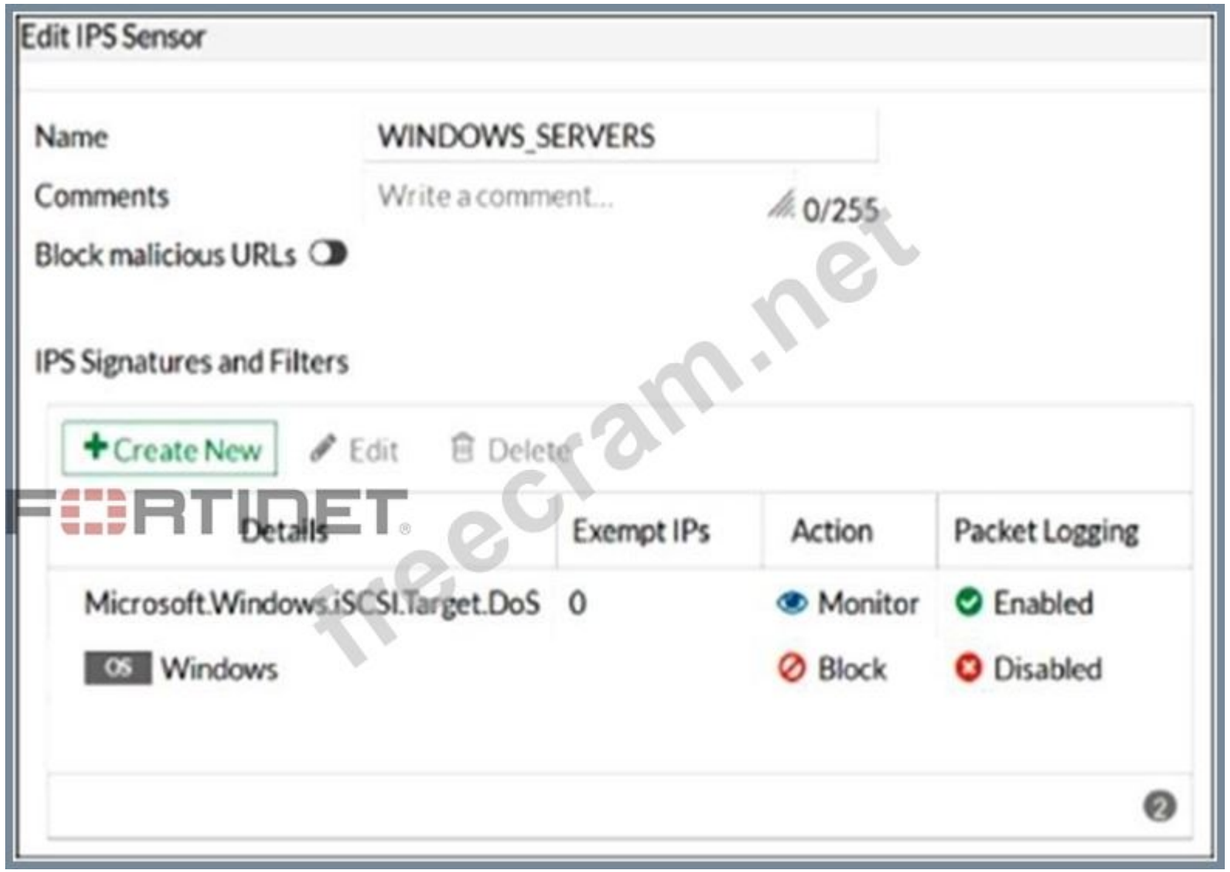
Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

**A.** 10.200.1.1

**B.** 10.200.1.149
**C.** 10.200.1.99
**D.** 10.200.1.49
**Answer: (SHOW ANSWER)**
All_TCP doesn't include ICMP. So you would match rule ID 2, in which uses IP Poop remote 1.

**NEW QUESTION: 42**
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: (SHOW ANSWER)**
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: 43**
Refer to the exhibit, which shows the IPS sensor configuration.




FORTINET
freecram.net

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: C,D (LEAVE A REPLY)**

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: 44**

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.

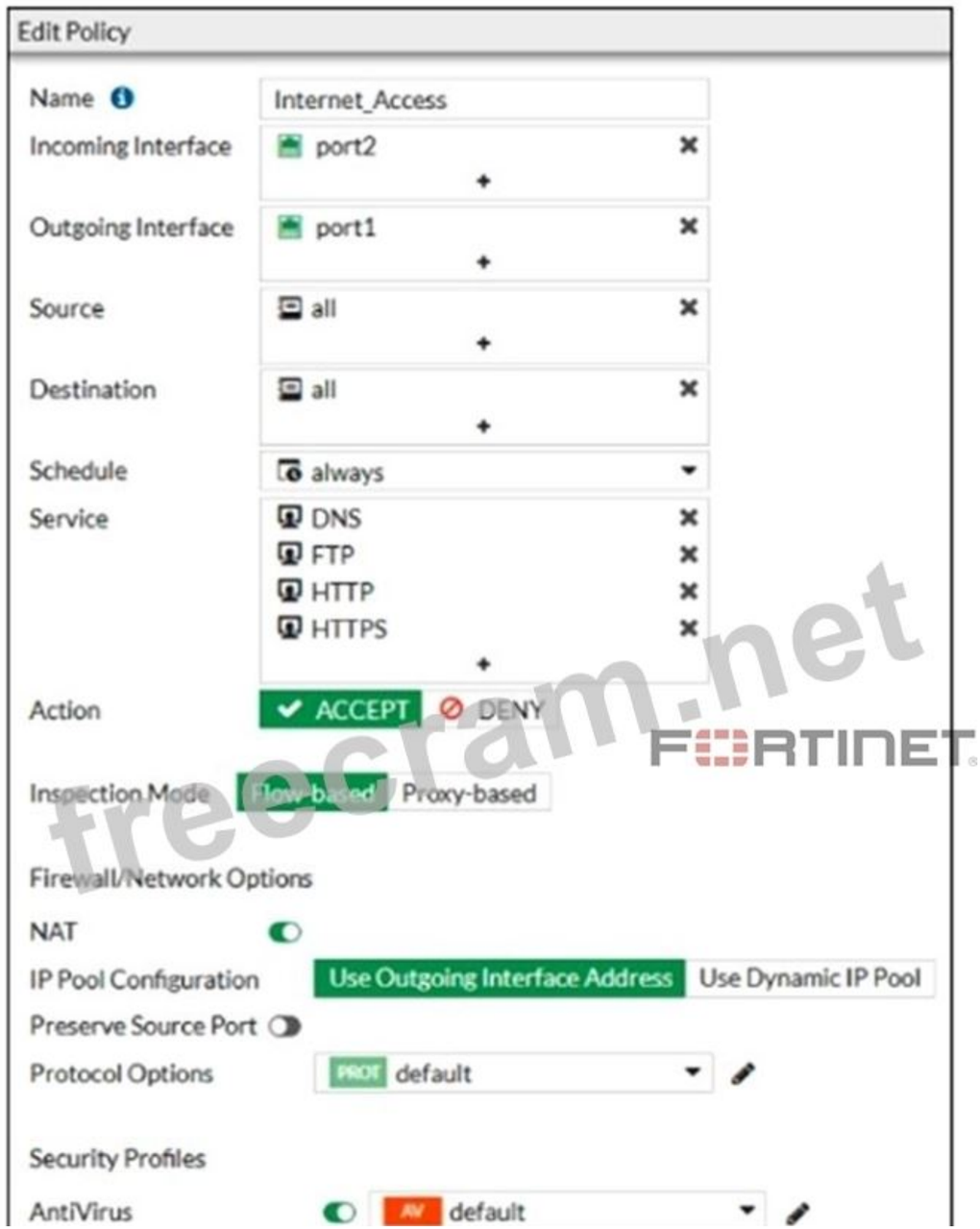
**D.** FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.

**Answer: (SHOW ANSWER)**

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: 45**
Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

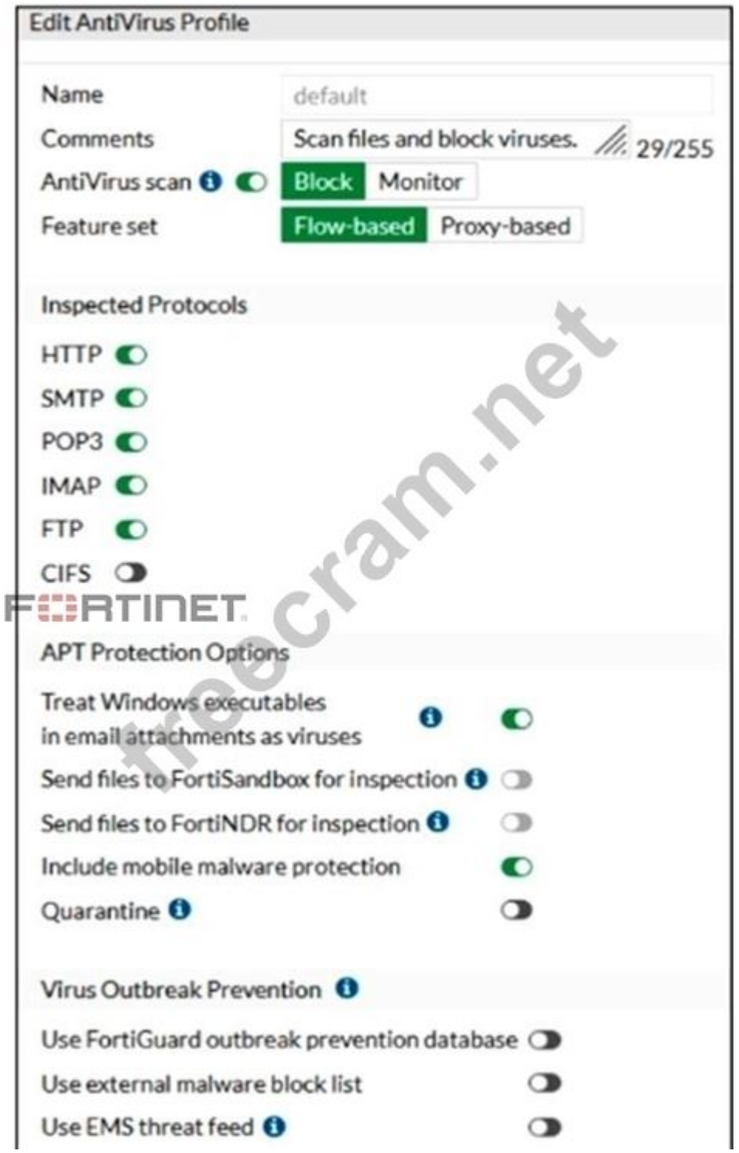
**Firewall policy configuration**




freecram.net




**Antivirus profile configuration**




FORTINET
freecram.net

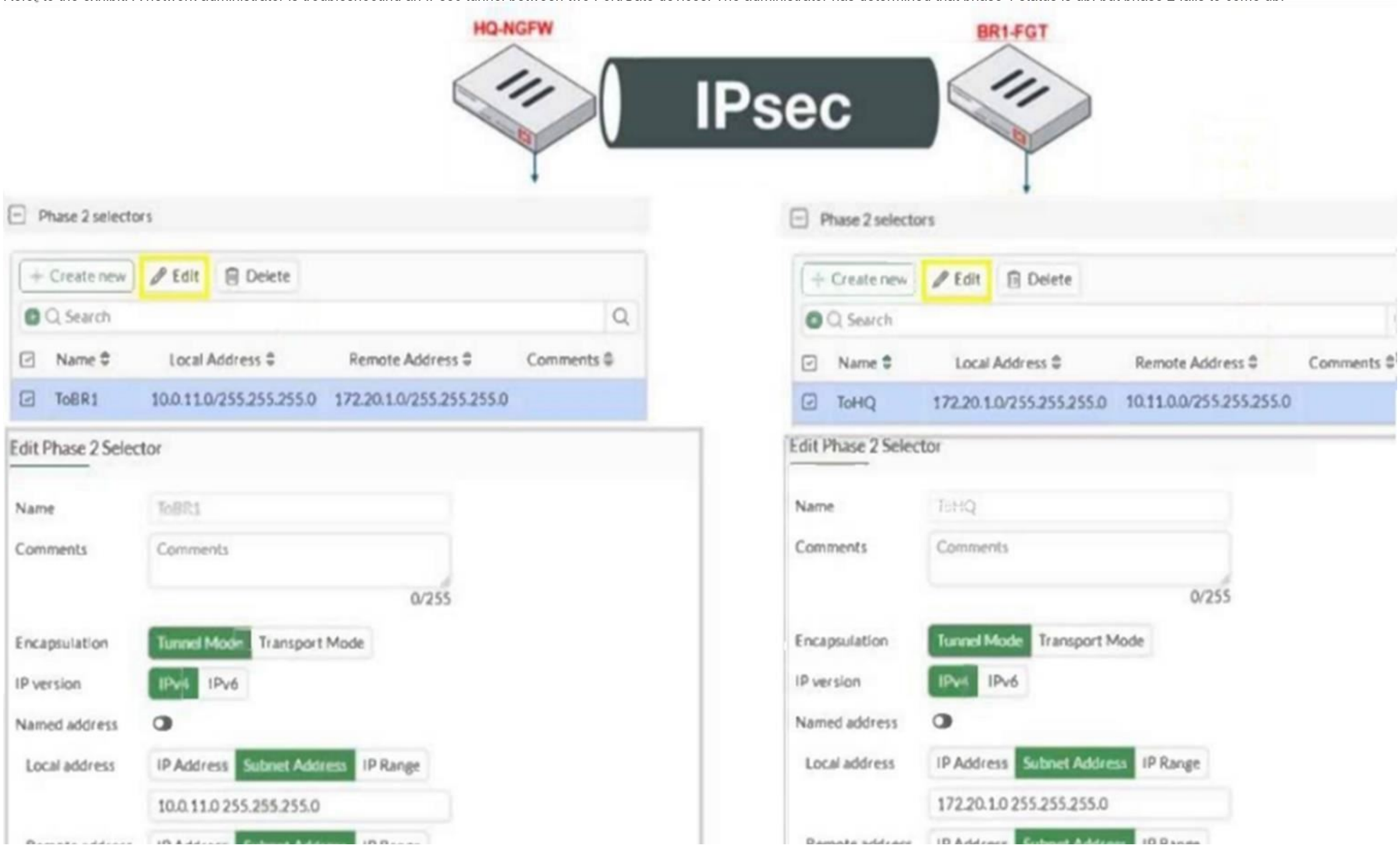
Why is the user unable to receive a block replacement message when downloading an infected file for the first time?
**A.** Flow-based inspection is used, which resets the last packet to the user.
**B.** The option to send files to FortiSandbox for inspection is enabled.
**C.** The firewall policy performs a full content inspection on the file.
**D.** The intrusion prevention security profile must be enabled when using flow-based inspection mode.
**Answer: (SHOW ANSWER)**
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: 46**
When configuring firewall policies which of the following is true regarding the policy ID?
**A.** It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.
**B.** A firewall policy ID identifies the order of policy execution in firewall policies.
**C.** You can create a policy in CLI with policy ID 0.
**D.** A policy ID cannot be edited once a policy is created.
**Answer: (SHOW ANSWER)**
Once a firewall policy is created, its policy ID is fixed and cannot be changed; this ID uniquely identifies the policy within the FortiGate configuration.

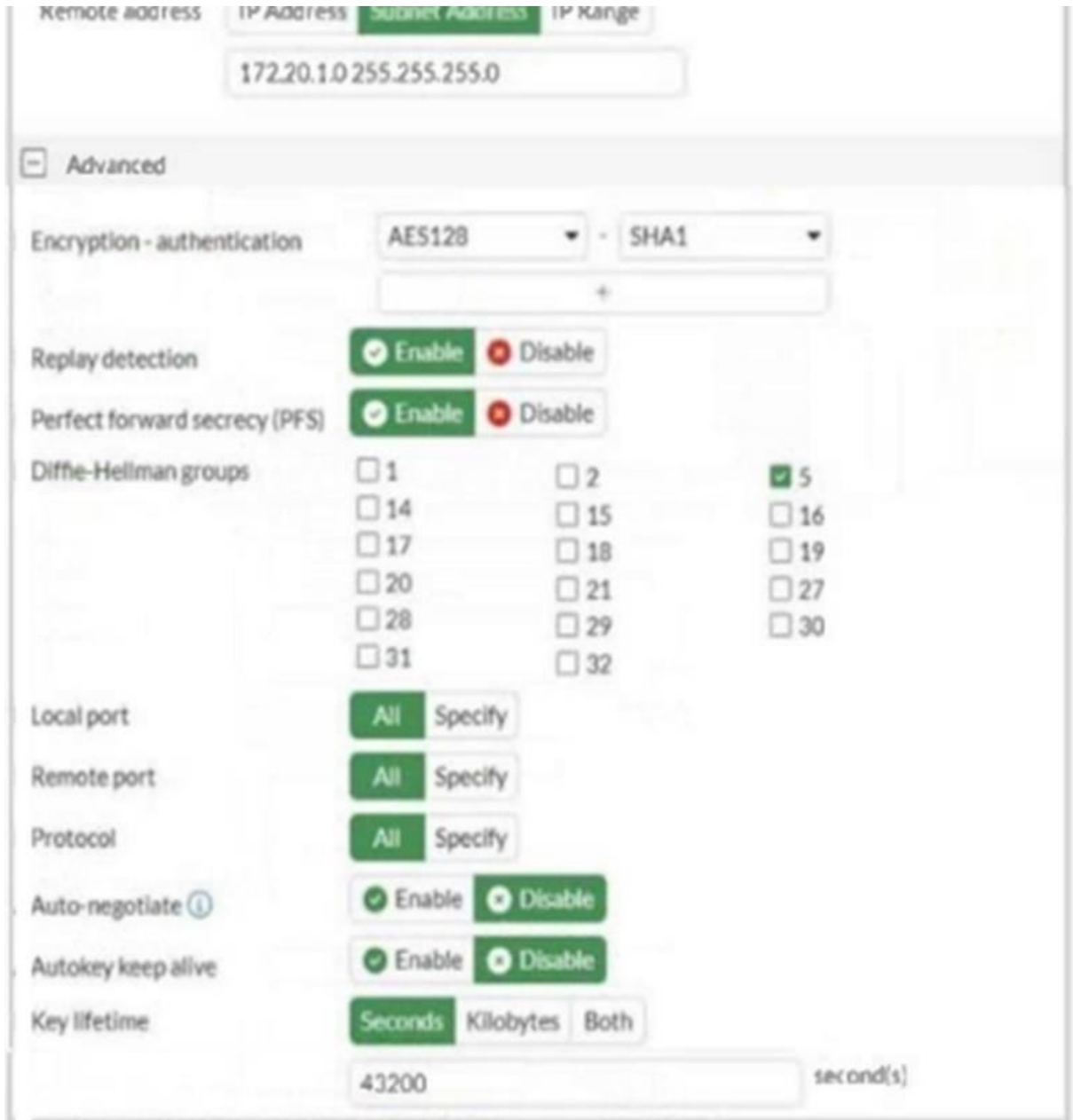
**Valid FCP_FGT_AD-7.6 Dumps** shared by EduDump.com for Helping Passing FCP_FGT_AD-7.6 Exam! EduDump.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the EduDump.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCP_FGT_AD-7.6 dumps with Test Engine here:
https://www.edudump.com/exams/Fortinet/FCP_FGT_AD-7.6/premium/ (**132** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

**NEW QUESTION: 47**
When configuring a FortiGate in a multi-WAN setup, why would an administrator enable session preservation on an interface?
**A.** To allow the FortiGate to dynamically change interfaces for all active sessions when a WAN link fails
**B.** To make sure all sessions without source NAT enabled always use the primary WAN link
**C.** To improve security by forcing users to authenticate again when the WAN link changes
**D.** To ensure that existing SSL VPN connections remain on the same interface even if route changes occur
**Answer: (SHOW ANSWER)**
Session preservation keeps active sessions, such as SSL VPNs, tied to the original interface to prevent disruption when WAN routes change.

**NEW QUESTION: 48**
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: (SHOW ANSWER)**
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: 49**
Refer to the exhibit. A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.









Based on the phase 2 configuration shown in the exhibit, which two configuration changes will bring phase 2 up? (Choose two.)

**A.** On BR1-FGT, set Seconds to 43200.

**B.** On HQ-NGFW, enable Diffie-Hellman Group 2.

**C.** On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0.

**D.** On HQ-NGFW. set Encryption to AES256.

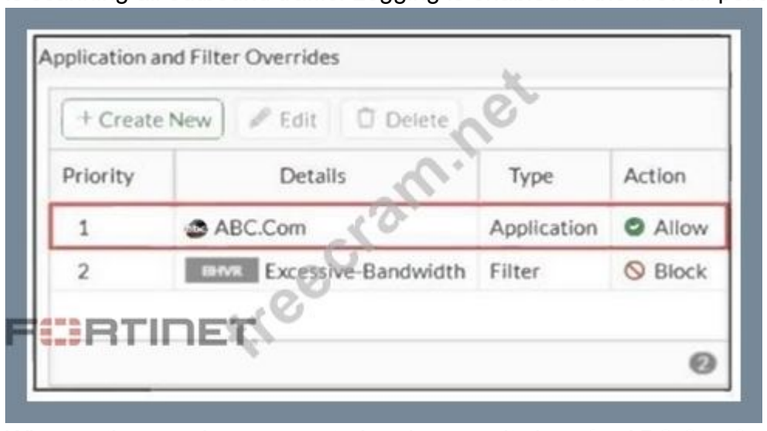
**Answer: (SHOW ANSWER)**

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: 50**
Which three methods are used by the collector agent for AD polling? (Choose three.)
**A.** WinSecLog
**B.** NetAPI
**C.** FortiGate polling
**D.** FSSO REST API
**E.** WMI
**Answer: (SHOW ANSWER)**
As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended: (WMI, WinSecLog, and NetAPI).

**NEW QUESTION: 51**
Refer to the exhibit. An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow. This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, the administrator accessed the ABC.Com web site several times.

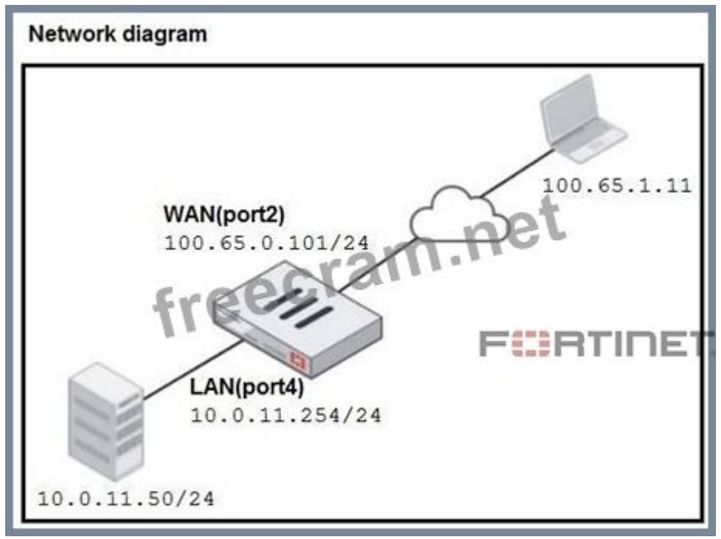



Why are there no logs generated under security logs for ABC.Com?
**A.** The ABC.Com Type is set as Application instead of Filter.
**B.** The ABC.Com is configured under application profile, which must be configured as a web filter profile.
**C.** The ABC.Com Action is set to Allow.
**D.** The ABC.Com is hitting the category Excessive-Bandwidth.
**Answer: (SHOW ANSWER)**
When the action is set to Allow in an application override, traffic matching this override is allowed without generating security logs because it bypasses deeper inspection and blocking.

**NEW QUESTION: 52**
Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)
**A.** The host field in the HTTP header.
**B.** The server name indication (SNI) extension in the client hello message.

**C.** The subject alternative name (SAN) field in the server certificate.
**D.** The subject field in the server certificate.
**E.** The serial number in the server certificate.
**Answer: (SHOW ANSWER)**
When using SSL certificate inspection, FortiGate is not decrypting the traffic. During the exchange of hello messages at the beginning of an SSL handshake, FortiGate parses the server name indication (SNI) from client Hello, which is an extension of the TLS protocol. The SNI tells FortiGate the hostname of the SSL server, which is validated against the DNS name before receipt of the server certificate. If there is no SNI exchanged, then FortiGate identifies the server by the value in the server by the value in the Subject field or SAN (Subject Alternative Name) field in the server certificate.

**NEW QUESTION: 53**
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?



freecram.net

**VIP object configuration**







**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: D (LEAVE A REPLY)**

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: 54**
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 EI 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: 55**
Refer to the exhibit. Which two statements about the FortiGuard connection are true? (Choose two.)

```
FortiGate # diagnose debug rating
Locale          : English

Service         : Web-filter
Status:         : Enable
License         : Contract
\
Num. of servers     : 1
Protocol            : https
Port                : 8888
Anycast             : Disable
Default servers     : Not included

-=- Server List (Wed Sep 20 09:22:42 2023) -=-

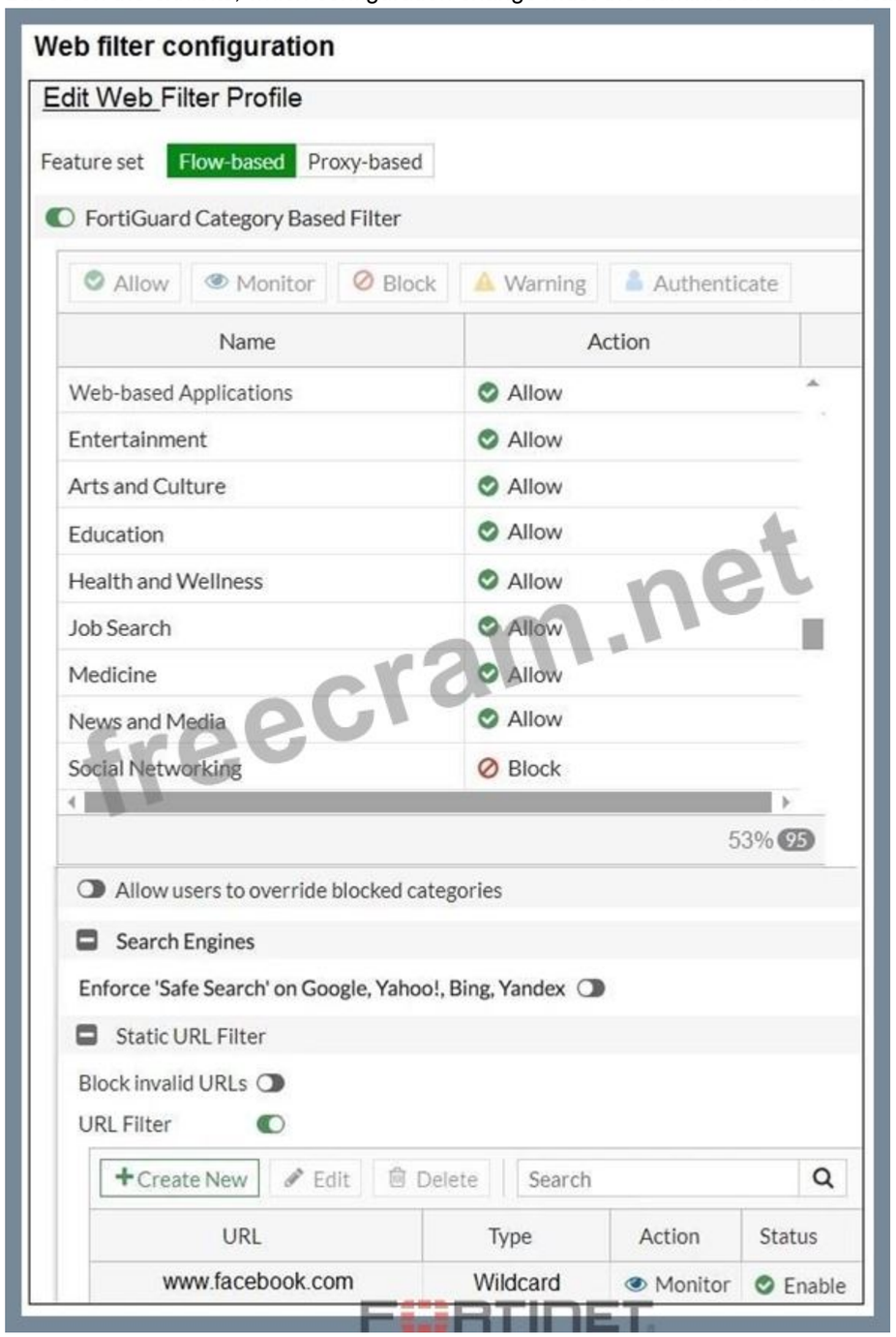
IP           Weight  RTT  Flags TZ  FortiGuard-requestsCurr Lost Total Lost Updated Time
10.0.1.241   -244    2    I     0                  122                0   Wed Sep 20 09:21:55 2023
```

**A.** FortiGate is using the default port for FortiGuard communication.
**B.** FortiGate identified the FortiGuard Server using DNS lookup.
**C.** The weight increases as the number of failed packets rises.
**D.** You can configure unreliable protocols to communicate with FortiGuard Server.
**Answer: (SHOW ANSWER)**
FortiGuard web filtering, DNS filtering, and antispam service.fortiguard.net uses a proprietary protocol over UDP port 53 or 8888 securewf.fortiguard.net uses HTTPS over ports 443, 53, or 8888.
The weight value reflects server reliability. It decreases with good performance and increases as packet loss or failures rise, meaning higher weight indicates more failures.

**NEW QUESTION: 56**
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.

freecram.net
FORTINET

Based on the exhibits, which configuration change must the administrator make to allow Facebook while blocking all other social networking sites?

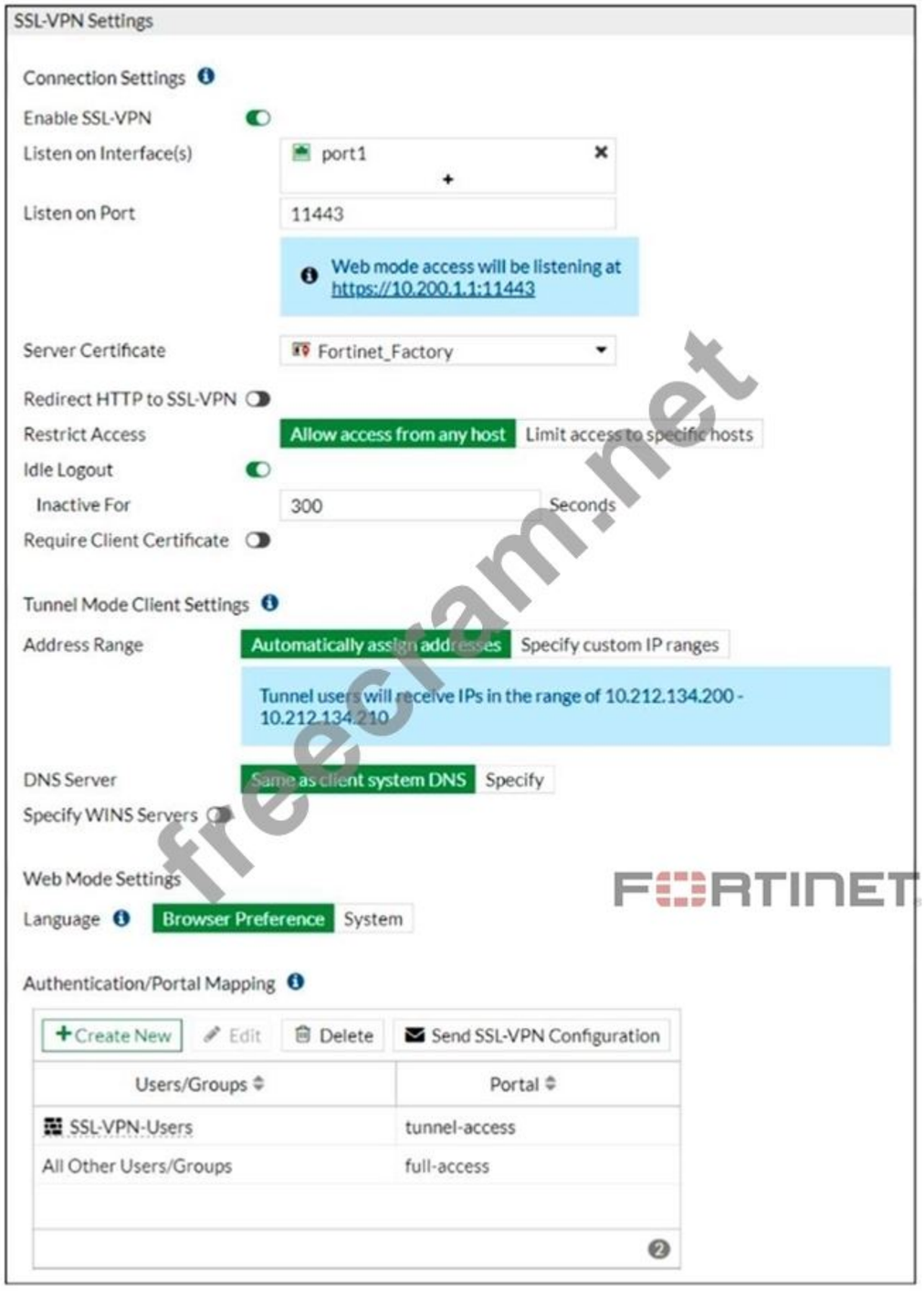





**A.** Change the type as Simple in the Static URL Filter section.
**B.** Set the Social Networking action as warning in the FortiGuard Category Based Filter.
**C.** Change the Feature set of Web Filter Profile as Proxy-based.
**D.** Set the Action as Exempt for www.facebook.com in the Static URL Filter.
**Answer: (SHOW ANSWER)**
The FortiGuard category filter is blocking Social Networking, which includes Facebook. Although a static URL filter entry for www.facebook.com exists, its action is set to Monitor, so it does not override the category block. To allow Facebook while blocking other social networking sites, the action for www.facebook.com in the Static URL Filter must be set to Exempt. This explicitly bypasses category filtering for that URL.

**NEW QUESTION: 57**
Refer to the exhibits.

**SSL-VPN settings**




freeexam.net
FORTINET



FORTINET
freecram.net

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: (SHOW ANSWER)**

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: 58**

An administrator manages a FortiGate model that supports NTurbo.
How does NTurbo acceleration enhance antivirus performance?

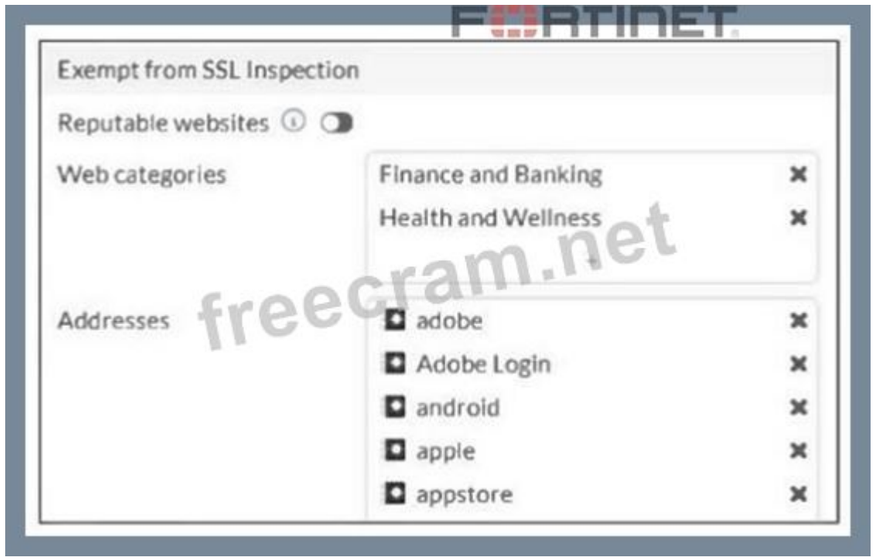
**A.** For proxy-based inspection, NTurbo offloads traffic to the content processor.
**B.** For flow-based inspection, NTurbo establishes a dedicated data path to redirect traffic between the IPS engine and FortiGate ingress and egress interfaces.
**C.** For proxy-based inspection, NTurbo buffers the whole file and then sends it to the antivirus engine.
**D.** For flow-based inspection, NTurbo creates two inspection sessions on the FortiGate device.

**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.

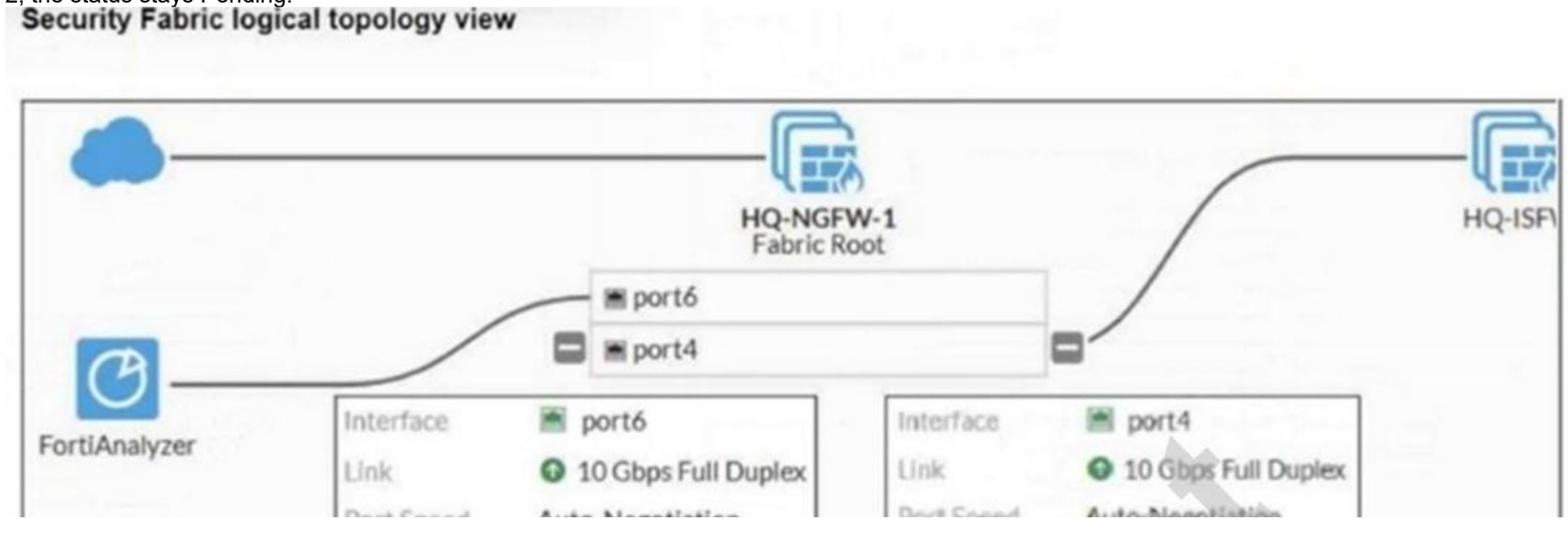
**NEW QUESTION: 59**

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



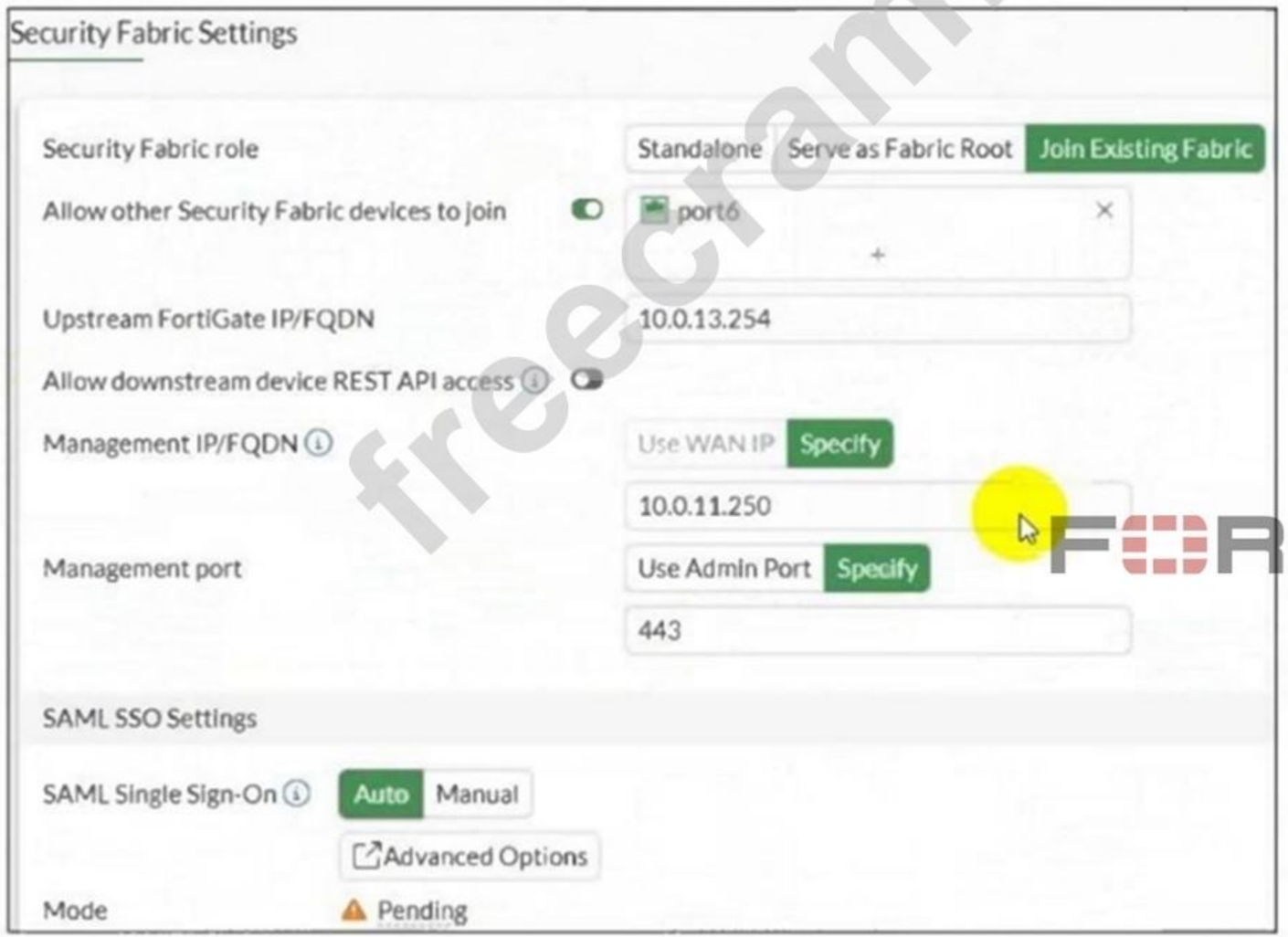

**A.** The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.
**B.** These websites are in an allowlist of reputable domain names maintained by FortiGuard.
**C.** The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
**D.** The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.
**Answer: A,D (LEAVE A REPLY)**
FortiGate's temporary SSL certificate may cause access denial to sites using HTTP Strict Transport Security (HSTS), so such sites are exempted from deep SSL inspection. Legal regulations require exemption of certain categories to protect user privacy and sensitive information, so these web categories are excluded from SSL inspection.

**NEW QUESTION: 60**
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.



| | | | | | |
|---|---|---|---|---|---|
| | 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: 61**
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.

**Valid FCP_FGT_AD-7.6 Dumps** shared by EduDump.com for Helping Passing FCP_FGT_AD-7.6 Exam! EduDump.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the EduDump.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCP_FGT_AD-7.6 dumps with Test Engine here:
https://www.edudump.com/exams/Fortinet/FCP_FGT_AD-7.6/premium/ (**132** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

**NEW QUESTION: 62**
Which three statements about SD-WAN performance SLAs are true? (Choose three.)
**A.** They rely on session loss and jitter.
**B.** They can be measured actively or passively.
**C.** They are applied in a SD-WAN rule lowest cost strategy.
**D.** They monitor the state of the FortiGate device.
**E.** All the SLAtargets can be configured.
**Answer: B,C,E (LEAVE A REPLY)**
FortiGate performance SLAs monitor the state of each member-whether it is alive or dead-and measures the member packet loss, latency, and jitter.
When you configure a performance SLA, you can decide whether you want to monitor the link health actively or passively. In active monitoring, the performance SLA checks the health of the member periodically-by default every 500ms- sending probes from the member to one or two servers that act as a beacon. In passive monitoring, the performance SLA determines the health of a member based on the traffic passing through the member.
The SLA target section is optional. It's where you define the performance requirements of alive members (latency, jitter, and packet loss thresholds). The performance SLA uses SLA targets with some SD-WAN rule strategies, like Lowest Cost (SLA), to decide if the link is eligible for traffic steering or not.

**NEW QUESTION: 63**
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: (SHOW ANSWER)**

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.

**Valid FCP_FGT_AD-7.6 Dumps** shared by EduDump.com for Helping Passing FCP_FGT_AD-7.6 Exam! EduDump.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the EduDump.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com FCP_FGT_AD-7.6 dumps with Test Engine here:

https://www.edudump.com/exams/Fortinet/FCP_FGT_AD-7.6/premium/ (**132** Q&As Dumps, **35%OFF Special Discount Code: freecram**)