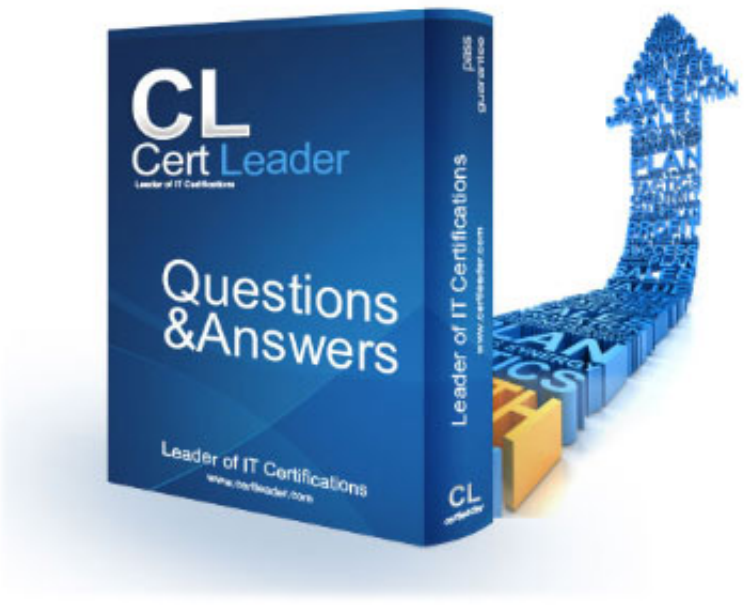
# NSE4_FGT-7.0 Dumps

# Fortinet NSE 4 - FortiOS 7.0

**https://www.certleader.com/NSE4_FGT-7.0-dumps.html**



**NEW QUESTION 1**
If Internet Service is already selected as Destination in a firewall policy, which other configuration object can be selected for the Destination field of a firewall policy?

A. IP address
B. No other object can be added
C. FQDN address
D. User or User Group

**Answer:** B

**Explanation:**
FortiGate Security 7.2 Study Guide (p.59): "When configuring your firewall policy, you can use Internet Service as the destination in a firewall policy, which contains all the IP addresses, ports, and protocols used by that service. For the same reason, you cannot mix regular address objects with ISDB objects, and you cannot select services on a firewall policy. The ISDB objects already have services information, which is hardcoded."
This is true because Internet Service is a special type of destination object that can only be used alone in a firewall policy. Internet Service is a feature that allows FortiGate to identify and filter traffic based on the internet service or application that it belongs to, such as Facebook, YouTube, Skype, etc. Internet Service uses a database of IP addresses and ports that are associated with each internet service or application, and updates it regularly from FortiGuard. When Internet Service is selected as the destination in a firewall policy, FortiGate will match the traffic to the corresponding internet service or application, and apply the appropriate action and security profiles to it. However, Internet Service cannot be combined with any other destination object, such as IP address, FQDN address, user or user group, etc., as this would create a conflict or ambiguity in the firewall policy. Therefore, no other object can be added if Internet Service is already selected as the destination in a firewall policy

**NEW QUESTION 2**
Refer to the exhibits.
Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.

Exhibit A | Exhibit B

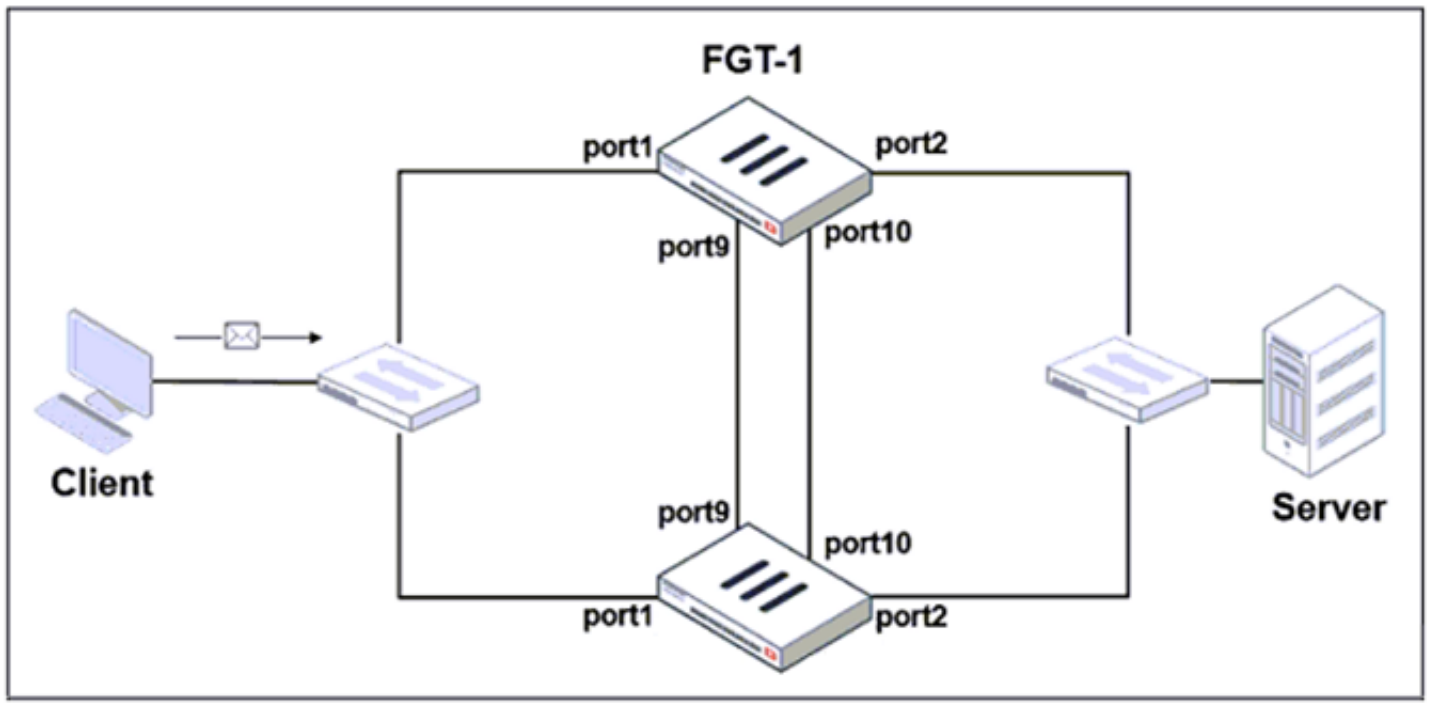



Exhibit A | Exhibit B

```
        set group-id 3
        set group-name "NSE"
        set mode a-a
        set password *
        set hbdev "port9" 50 "port10" 50
        set session-pickup enable
        set override disable
        set monitor port3
    end

    # get system ha status
    ...
    Primary      : FGT-2, FGVM010000065036, HA cluster index = 1
    Secondary    : FGT-1, FGVM010000064692, HA cluster index = 0
    number of vcluster: 1
    vcluster 1: work 169.254.0.2
    Primary: FGVM010000065036, HA operating index = 1
    Secondary: FGVM010000064692, HA operating index = 0
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

A. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.
B. The traffic sourced from the client and destined to the server is sent to FGT-1.
C. The cluster can load balance ICMP connections to the secondary.
D. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

**Answer:** AD

**Explanation:**
FortiGate Infrastructure 7.2 Study Guide (p.317 & p.320): "To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses." "The primary forwards the SYN packet to the selected secondary. (...) This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic."

**NEW QUESTION 3**
Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale       : english

Service      : Web-Filter
Status       : Enable
License      : Contract

Num. of servers : 3
Protocol        : https
Port            : 443
Anycast         : Disable
Default servers : Included
-=- Server List (Mon July 5 12:00:25 2021) -=-

IP               Weight    RTT  Flags  TZ  FortiGuard-requests Curr Lost Total Lost  Updated Time
173.243.138.210      10     350  DI   -8              29          0          0         Mon Jul 5 09:23:33 2021
12.34.97.18          20     30        -5              25          0          0         Mon Jul 5 09:23:33 2021
210.7.96.18          160    605        9              25          0          0         Mon Jul 5 09:23:33 2021
```

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

A. A local FortiManager is one of the servers FortiGate communicates with.
B. One server was contacted to retrieve the contract information.
C. There is at least one server that lost packets consecutively.
D. FortiGate is using default FortiGuard communication settings.

**Answer:** BD

**Explanation:**
FortiGate Security 7.2 Study Guide (p.287-288): "Flags: D (IP returned from DNS), I (Contract server contacted), T (being timed), F (failed)" "By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. Other ports and protocols are available by disabling the FortiGuard anycast setting on the CLI."

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

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

**Answer:** AC

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

**NEW QUESTION 5**
Refer to the exhibit.

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

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

**Answer:** D

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

**NEW QUESTION 6**
An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.12" 5
```

Which three pieces of Information will be Included in me sniffer output? {Choose three.)

A. Interface name
B. Packet payload
C. Ethernet header
D. IP header
E. Application header

**Answer:** ABD

**NEW QUESTION 7**
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

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

**Answer:** D

**Explanation:**
FortiGate_Infrastructure_7.0 page 270: "NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows."

**NEW QUESTION 8**
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time
B. FortiGuaid update servers
C. Operating mode
D. NGFW mode

**Answer:** CD

**Explanation:**
C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.
D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

**NEW QUESTION 9**
An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

A. The strict RPF check is run on the first sent and reply packet of any new session.
B. Strict RPF checks the best route back to the source using the incoming interface.
C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
D. Strict RPF allows packets back to sources with all active routes.

**Answer:** B

**Explanation:**
Strict Reverse Path Forwarding (RPF) is a security feature that is used to detect and prevent IP spoofing attacks on a network. It works by checking the routing information for incoming packets to ensure that they are coming from the source address that is indicated in the packet's header. In strict RPF mode, the firewall will check the best route back to the source of the incoming packet using the incoming interface. If the packet's source address does not match the route back to the source, the packet is dropped. This helps to prevent attackers from spoofing their IP address and attempting to access the network.

**NEW QUESTION 10**
An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

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

**Answer:** D

**NEW QUESTION 10**
Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

A. FortiGate points the collector agent to use a remote LDAP server.
B. FortiGate uses the AD server as the collector agent.
C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
D. FortiGate queries AD by using the LDAP to retrieve user group information.

**Answer:** CD

**Explanation:**
Fortigate Infrastructure 7.0 Study Guide P.272-273 https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

**NEW QUESTION 14**
Which three statements explain a flow-based antivirus profile? (Choose three.)

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

**Answer:** ADE

**NEW QUESTION 18**
Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

A. VDOMs without ports with connected devices are not displayed in the topology.
B. Downstream devices can connect to the upstream device from any of their VDOMs.
C. Security rating reports can be run individually for each configured VDOM.
D. Each VDOM in the environment can be part of a different Security Fabric.

**Answer:** A

**Explanation:**
FortiGate Security 7.2 Study Guide (p.436): "When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric."

**NEW QUESTION 21**
Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.
B. Only secondary FortiGate devices are rebooted.
C. Uninterruptable upgrade is enabled by default.
D. Traffic load balancing is temporally disabled while upgrading the firmware.

**Answer:** CD

**NEW QUESTION 25**
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning
B. Exempt
C. Allow
D. Learn

**Answer:** AC

**NEW QUESTION 30**
Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries
B. PKI
C. Traffic shaping
D. DNS

**Answer:** AD

**Explanation:**
FortiGate Infrastructure 7.2 Study Guide (p.73): "What about traffic originating from FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate. Traffic coming from FortiGate to those global services originates from the management VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM. It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate."

**NEW QUESTION 35**
FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.
In this scenario, what are two requirements for the VLAN ID? (Choose two.)

A. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.
B. The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs.
C. The two VLAN subinterfaces must have different VLAN IDs.
D. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

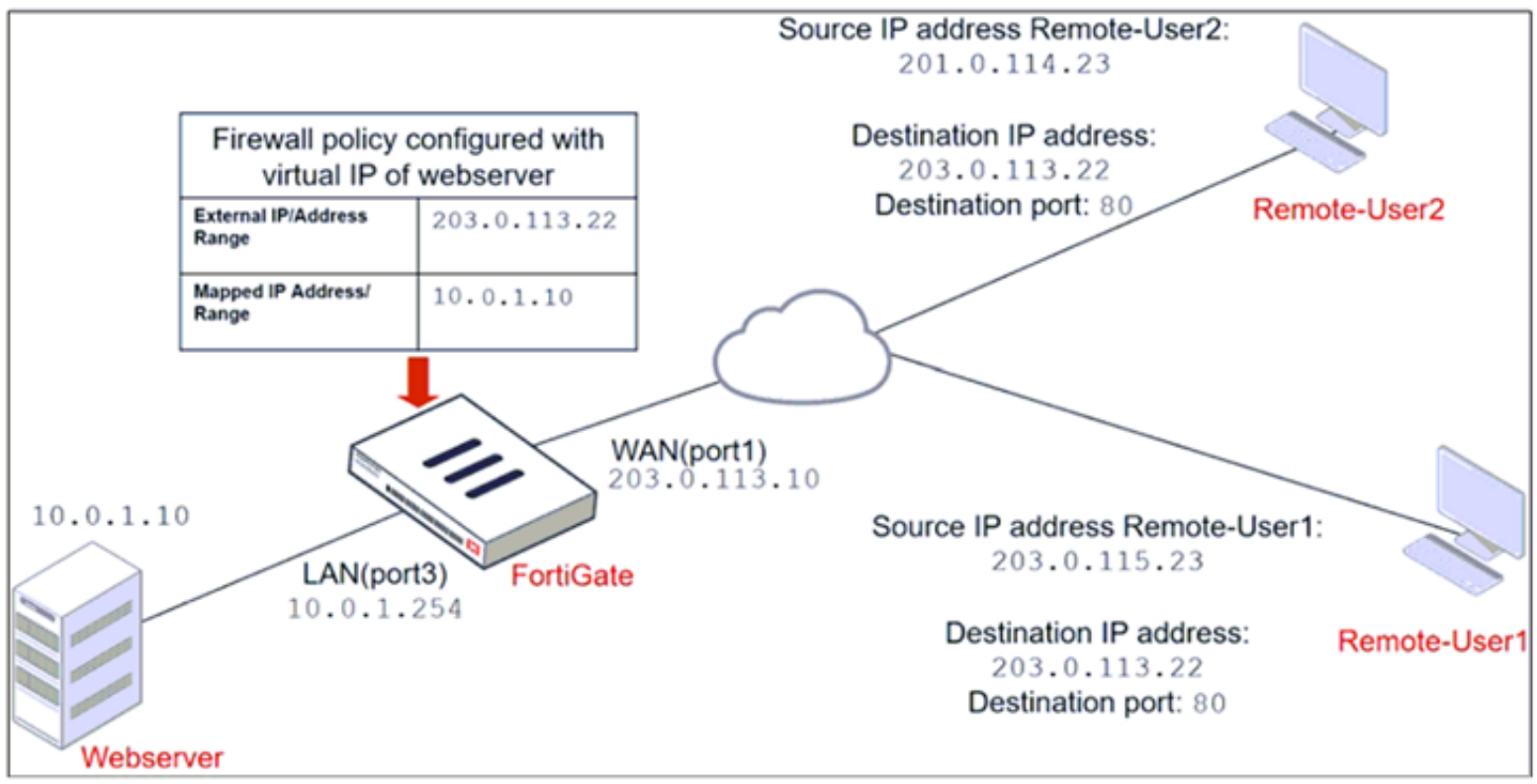
**Answer:** BC

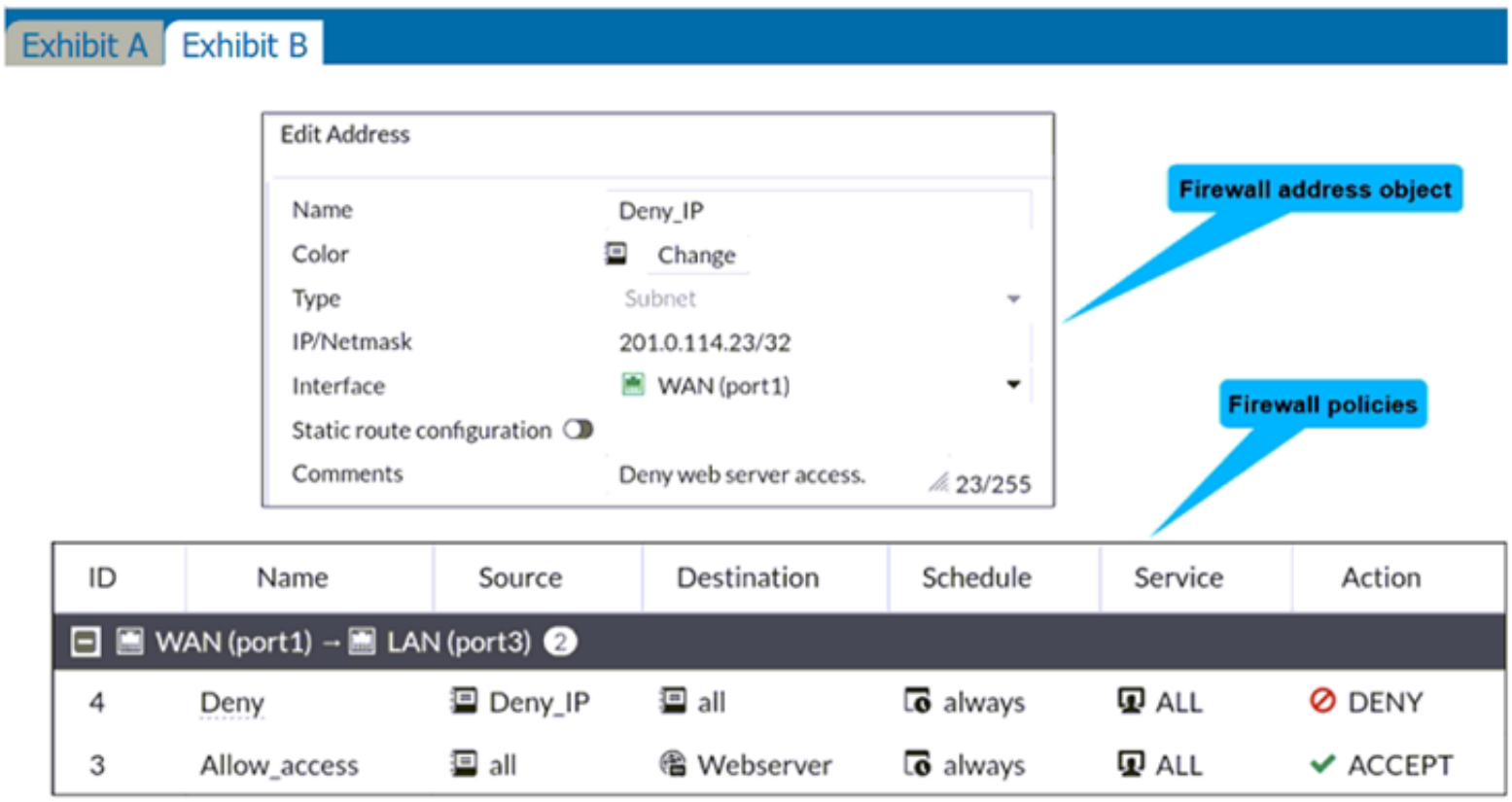
**Explanation:**
https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-use-emac-vlan-to-share-the-same-VLAN/t When FortiGate is operating in NAT mode, it means that it uses network address translation (NAT) to modify the source or destination IP addresses of the traffic passing through it1. NAT mode allows FortiGate to hide the IP addresses of the internal network from the external network, and to conserve IP addresses by using a single public IP address for multiple private IP addresses1.
A virtual LAN (VLAN) subinterface is a logical interface that allows traffic from different VLANs to enter
and exit the FortiGate unit2. A VLAN subinterface is created by adding a VLAN ID to a physical interface or an aggregate interface2. A VLAN ID is a numerical identifier that distinguishes one VLAN from another2.
In this scenario, there are two requirements for the VLAN ID of the VLAN subinterfaces added to the same physical interface:

- The two VLAN subinterfaces must have different VLAN IDs. This is because the VLAN ID is used to tag the traffic with the appropriate VLAN information, and to separate the traffic into different VLANs2. If the two VLAN subinterfaces have the same VLAN ID, they will not be able to distinguish the traffic from each other, and they will not be able to forward the traffic to the correct destination.
- The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different
VDOMs. This is because VDOMs are virtual instances of FortiGate that can have their own interfaces, policies, and routing tables3. Each VDOM operates independently from other VDOMs, and can have its own VLAN subinterfaces with different or identical VLAN IDs3. However, this requires inter-VDOM links to allow traffic between different VDOMs3.

**NEW QUESTION 40**
Refer to the exhibits.
The exhibits show a network diagram and firewall configurations.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver.
Remote-User2 must not be able to access the Webserver.

Exhibit A Exhibit B






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

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

**Answer:** BC

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

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

**NEW QUESTION 41**
Which scanning technique on FortiGate can be enabled only on the CLI?

A. Heuristics scan
B. Trojan scan
C. Antivirus scan
D. Ransomware scan

**Answer:** A

**NEW QUESTION 46**
Which of the following SD-WAN load balancing method use interface weight value to distribute traffic? (Choose two.)

A. Source IP
B. Spillover
C. Volume
D. Session

**Answer:** CD

**Explanation:**
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing

**NEW QUESTION 47**
In which two ways can RPF checking be disabled? (Choose two )

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

**Answer:** CD

**NEW QUESTION 48**
Which statement is correct regarding the use of application control for inspecting web applications?

A. Application control can identity child and parent applications, and perform different actions on them.
B. Application control signatures are organized in a nonhierarchical structure.
C. Application control does not require SSL inspection to identity web applications.
D. Application control does not display a replacement message for a blocked web application.

**Answer:** A

**Explanation:**
Application control is a feature that allows FortiGate to inspect and control the use of specific web applications on the network. When application control is enabled, FortiGate can identify child and parent applications, and can perform different actions on them based on the configuration.

**NEW QUESTION 49**
Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

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

**Answer:** ABE

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

**NEW QUESTION 54**
An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

A. Configure Source IP Pools.
B. Configure split tunneling in tunnel mode.
C. Configure different SSL VPN realms.
D. Configure host check .

**Answer:** D

**NEW QUESTION 58**
Which three statements are true regarding session-based authentication? (Choose three.)

A. HTTP sessions are treated as a single user.
B. IP sessions from the same source IP address are treated as a single user.
C. It can differentiate among multiple clients behind the same source IP address.
D. It requires more resources.
E. It is not recommended if multiple users are behind the source NAT

**Answer:** ACD

**NEW QUESTION 60**
A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.
What is the reason for the failed virus detection by FortiGate?

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

**Answer:** AC

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

**NEW QUESTION 65**
Which two statements are true when FortiGate is in transparent mode? (Choose two.)

A. By default, all interfaces are part of the same broadcast domain.
B. The existing network IP schema must be changed when installing a transparent mode.
C. Static routes are required to allow traffic to the next hop.
D. FortiGate forwards frames without changing the MAC address.

**Answer:** AD

**NEW QUESTION 66**
The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile. What order must FortiGate use when the web filter profile has features enabled, such as safe search?

A. DNS-based web filter and proxy-based web filter
B. Static URL filter, FortiGuard category filter, and advanced filters
C. Static domain filter, SSL inspection filter, and external connectors filters
D. FortiGuard category filter and rating filter

**Answer:** B

**Explanation:**
FortiGate Security 7.2 Study Guide (p.285): "Remember that the web filtering profile has several features. So, if you have enabled many of them, the inspection order flows as follows: 1. The local static URL filter 2. FortiGuard category filtering (to determine a rating) 3. Advanced filters (such as safe search or removing Active X components)"

**NEW QUESTION 69**
Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP elects the primary FortiGate device.
B. FGCP is not used when FortiGate is in transparent mode.
C. FGCP runs only over the heartbeat links.
D. FGCP is used to discover FortiGate devices in different HA groups.

**Answer:** AC

**Explanation:**
The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:
FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a variety of factors, such as the device's priority, to determine which device should be the primary.
FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices. FGCP does not run over other types of links, such as data links.

**NEW QUESTION 73**
What are two features of collector agent advanced mode? (Choose two.)

A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
B. In advanced mode, security profiles can be applied only to user groups, not individual users.
C. Advanced mode uses the Windows convention—NetBios: Domain\Username.
D. Advanced mode supports nested or inherited groups.

**Answer:** AD

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

**NEW QUESTION 78**
Which feature in the Security Fabric takes one or more actions based on event triggers?

A. Fabric Connectors
B. Automation Stitches
C. Security Rating
D. Logical Topology

**Answer:** B

**NEW QUESTION 80**
Which statement describes a characteristic of automation stitches?

A. They can have one or more triggers.
B. They can be run only on devices in the Security Fabric.
C. They can run multiple actions simultaneously.
D. They can be created on any device in the fabric.

**Answer:**

C

**Explanation:**
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/351998/creating-automation-stitches

**NEW QUESTION 82**
How does FortiGate act when using SSL VPN in web mode?

A. FortiGate acts as an FDS server.
B. FortiGate acts as an HTTP reverse proxy.
C. FortiGate acts as DNS server.
D. FortiGate acts as router.

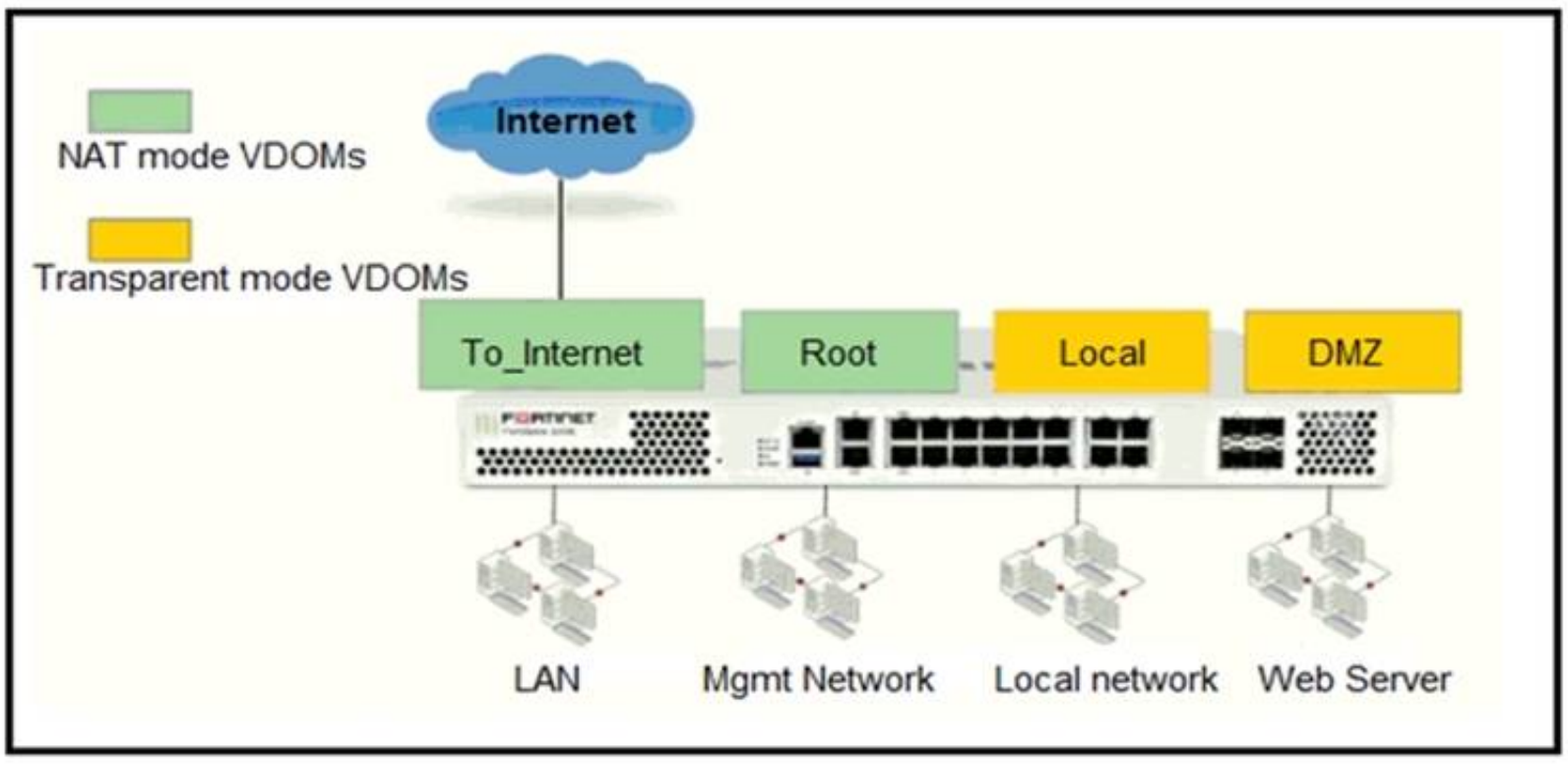
**Answer:** B

**NEW QUESTION 86**
Which two statements are true about the RPF check? (Choose two.)

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

**Answer:** AD

**NEW QUESTION 87**
Refer to the exhibit.

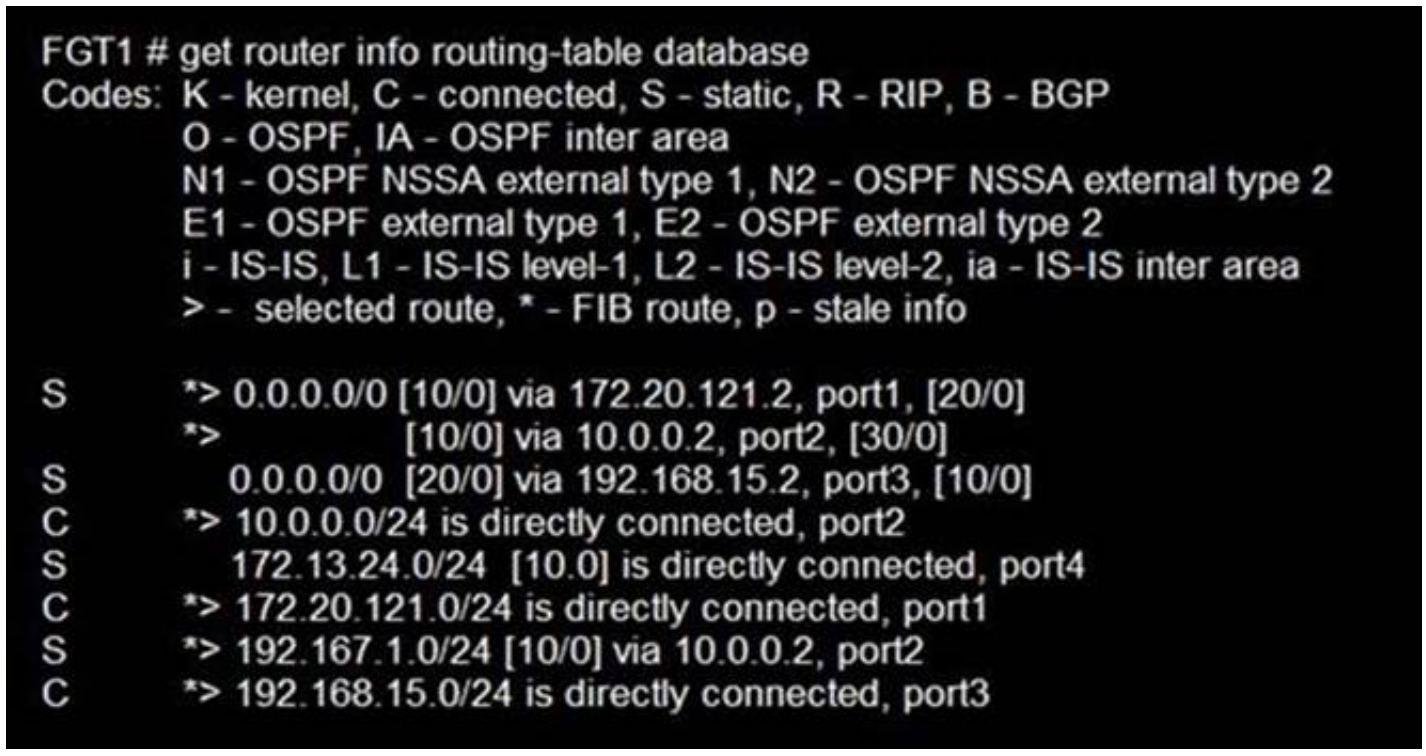



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem .
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

**Answer:** A

**NEW QUESTION 92**
Refer to the exhibit.




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

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

**Answer:** BC

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

**NEW QUESTION 93**
An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.
B. The interface is a member of a virtual wire pair.
C. The operation mode is transparent.
D. The interface is a member of a zone.
E. Captive portal is enabled in the interface.

**Answer:** ABC

**Explanation:**
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

**NEW QUESTION 98**
Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeou
B. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
C. It is a hard timeou
D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
E. It is an idle timeou
F. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
G. It is a hard timeou
H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

**Answer:** A

**NEW QUESTION 102**
A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not Which configuration option is the most effective way to support this request?

A. Implement a web filter category override for the specified website
B. Implement a DNS filter for the specified website.
C. Implement web filter quotas for the specified website
D. Implement web filter authentication for the specified website.

**Answer:** D

**NEW QUESTION 105**
FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.
In this scenario, which statement about VLAN IDs is true?

A. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.
B. The two VLAN subinterfaces must have different VLAN IDs.

C. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.
D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

**Answer:** CD

**NEW QUESTION 107**
Which of the following statements about central NAT are true? (Choose two.)

A. IP tool references must be removed from existing firewall policies before enabling central NAT .
B. Central NAT can be enabled or disabled from the CLI only.
C. Source NAT, using central NAT, requires at least one central SNAT policy.
D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

**Answer:** AB

**NEW QUESTION 110**
An administrator needs to increase network bandwidth and provide redundancy.
What interface type must the administrator select to bind multiple FortiGate interfaces?

A. VLAN interface
B. Software Switch interface
C. Aggregate interface
D. Redundant interface

**Answer:** C

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

**NEW QUESTION 115**
Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

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

**Answer:** D

**NEW QUESTION 118**
Refer to the exhibit.

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

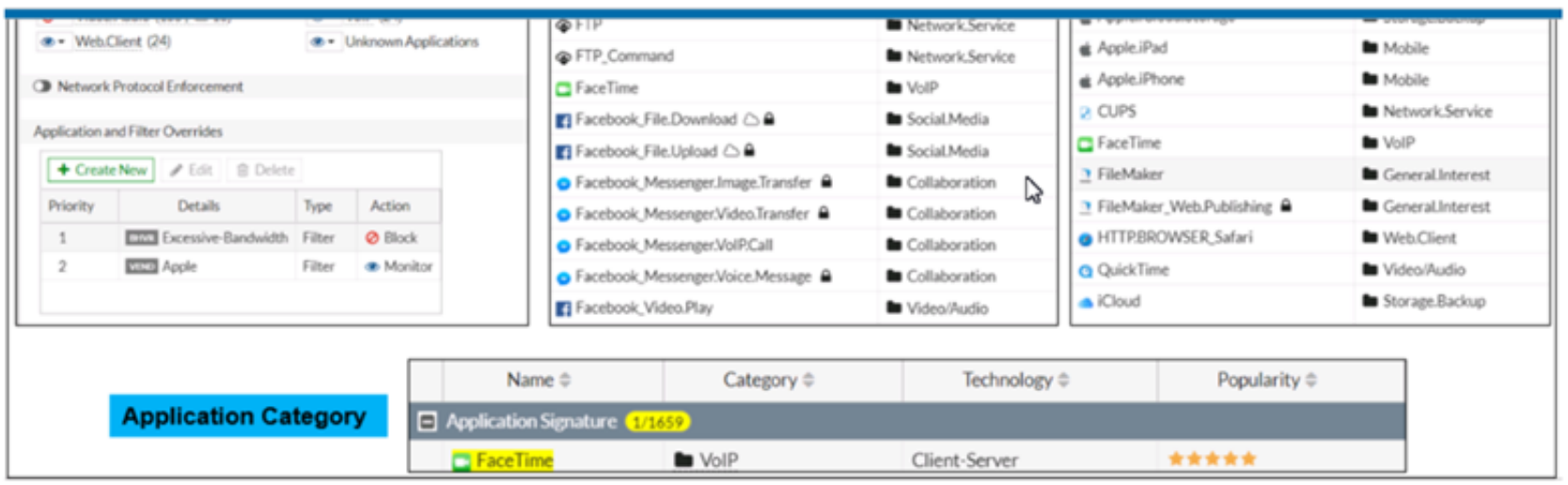
Examine the intrusion prevention system (IPS) diagnostic command.
Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

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

**Answer:** A

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

**NEW QUESTION 120**
Refer to the exhibit to view the application control profile.




Based on the configuration, what will happen to Apple FaceTime?

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

**Answer:** A

**NEW QUESTION 122**
FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning
B. File filter
C. DNS filter
D. Intrusion prevention

**Answer:** AD

**NEW QUESTION 125**
In an explicit proxy setup, where is the authentication method and database configured?

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

**Answer:** D

**NEW QUESTION 130**
An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value.
Which timeout option should be configured on FortiGate?

A. auth-on-demand
B. soft-timeout
C. idle-timeout
D. new-session
E. hard-timeout

**Answer:** E

**Explanation:**
https://community.fortinet.com/t5/FortiGate/Technical-TipExplanation:-of-auth-timeout-types-for-Firewall/ta-p/

**NEW QUESTION 131**
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status
B. get system performance status
C. diagnose sys top
D. get system arp

**Answer:** D

**Explanation:**
"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

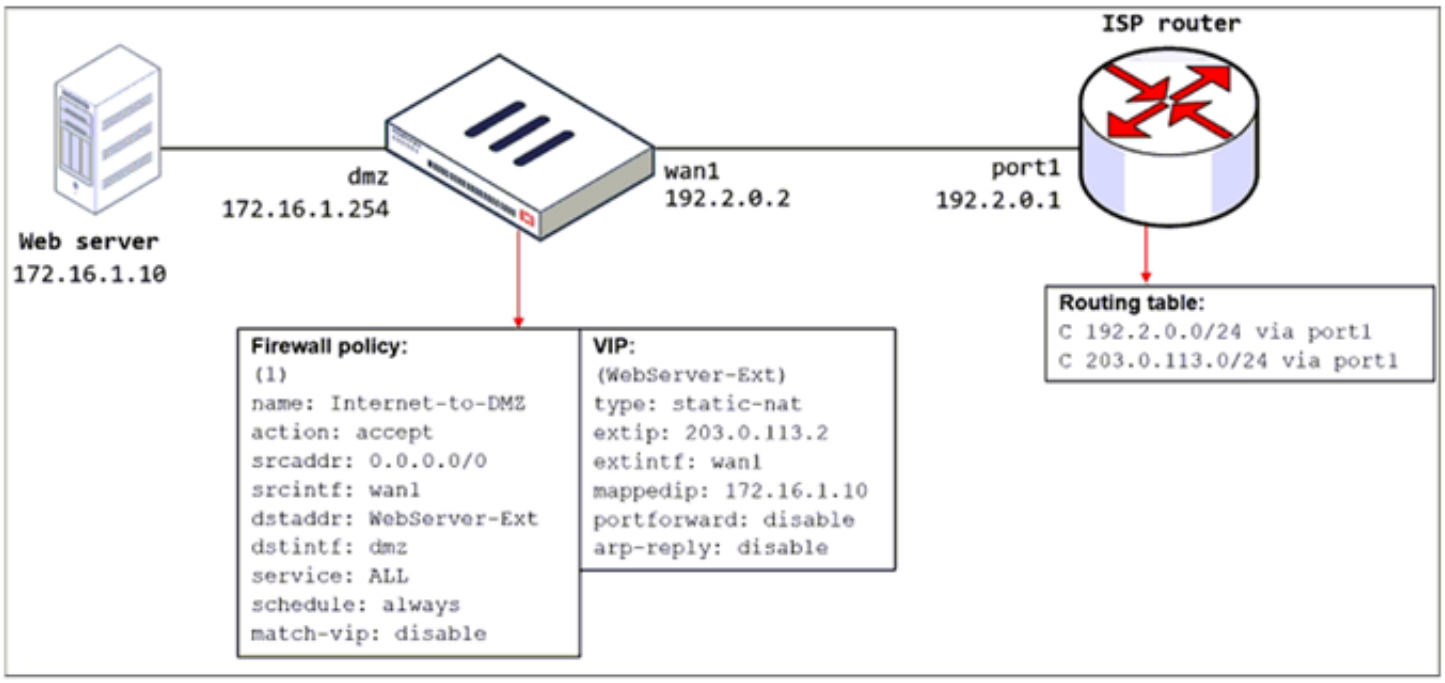
**NEW QUESTION 132**
Which statement is correct regarding the security fabric?

A. FortiManager is one of the required member devices.
B. FortiGate devices must be operating in NAT mode.
C. A minimum of two Fortinet devices is required.
D. FortiGate Cloud cannot be used for logging purposes.

**Answer:** B

**Explanation:**
FortiGate Security 7.2 Study Guide (p.428): "You must have a minimum of two FortiGate devices at the core of the Security Fabric, plus one FortiAnalyzer or cloud logging solution. FortiAnalyzer Cloud or FortiGate Cloud can act as the cloud logging solution. The FortiGate devices must be running in NAT mode."

**NEW QUESTION 136**
Refer to the exhibit.
The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.
When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



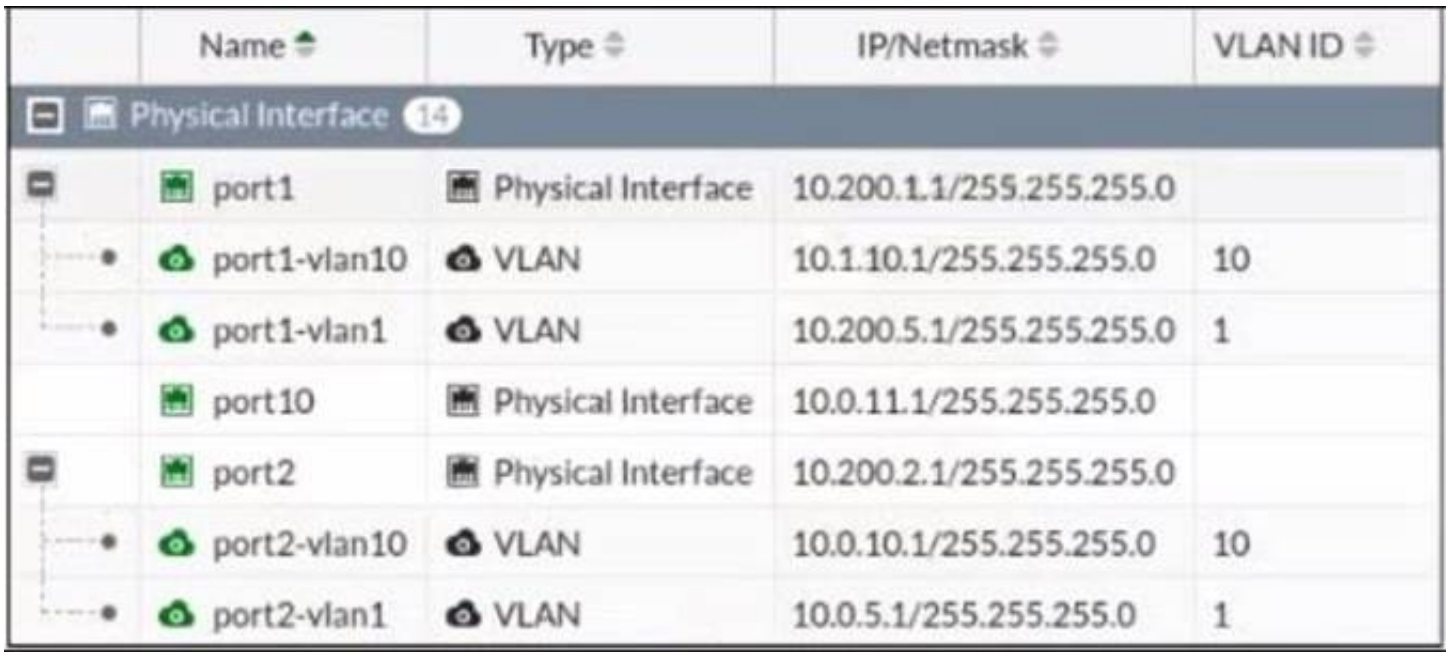

Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

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

**Answer:** B

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

**NEW QUESTION 140**
Refer to the exhibit.



| Name | Type | IP/Netmask | VLAN ID |
|---|---|---|---|
| Physical Interface 14 | | | |
| port1 | Physical Interface | 10.200.1.1/255.255.255.0 | |
| port1-vlan10 | VLAN | 10.1.10.1/255.255.255.0 | 10 |
| port1-vlan1 | VLAN | 10.200.5.1/255.255.255.0 | 1 |
| port10 | Physical Interface | 10.0.11.1/255.255.255.0 | |
| port2 | Physical Interface | 10.200.2.1/255.255.255.0 | |
| port2-vlan10 | VLAN | 10.0.10.1/255.255.255.0 | 10 |
| port2-vlan1 | VLAN | 10.0.5.1/255.255.255.0 | 1 |

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

A. Traffic between port2 and port2-vlan1 is allowed by default.
B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
C. port1 is a native VLAN.
D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

**Answer:** CD

**Explanation:**
https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

**NEW QUESTION 142**
An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

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

**Answer:** BC

**NEW QUESTION 147**
Which statement correctly describes the use of reliable logging on FortiGate?

A. Reliable logging is enabled by default in all configuration scenarios.
B. Reliable logging is required to encrypt the transmission of logs.
C. Reliable logging can be configured only using the CLI.
D. Reliable logging prevents the loss of logs when the local disk is full.

**Answer:** B

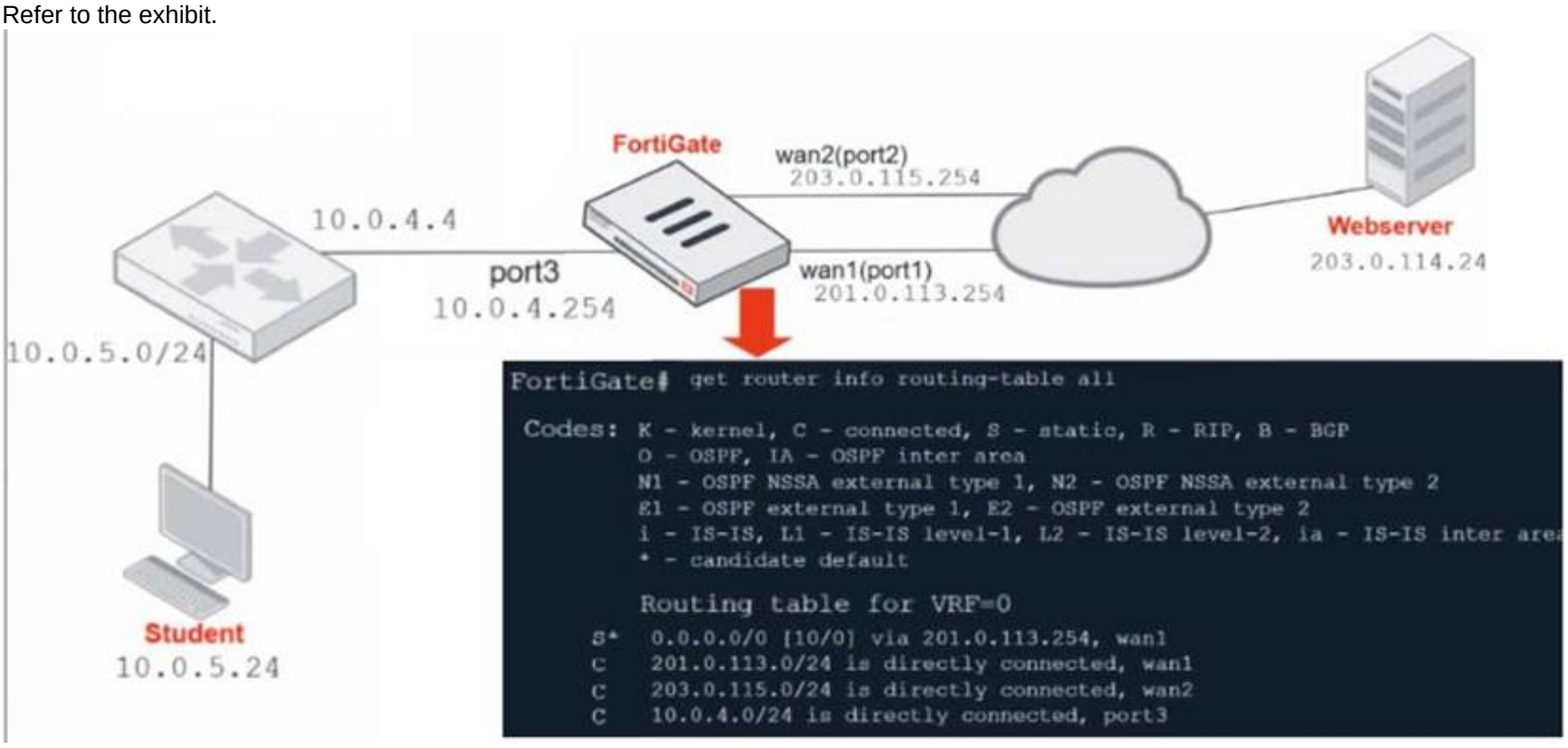
**Explanation:**
FortiGate Security 7.2 Study Guide (p.192): "if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm setting on the CLI."

**NEW QUESTION 151**
When configuring a firewall virtual wire pair policy, which following statement is true?

A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
B. Only a single virtual wire pair can be included in each policy.
C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
D. Exactly two virtual wire pairs need to be included in each policy.

**Answer:** A

**NEW QUESTION 152**
Refer to the exhibit.




Which contains a network diagram and routing table output. The Student is unable to access Webserver.
What is the cause of the problem and what is the solution for the problem?

A. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
B. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
C. The first reply packet for Student failed the RPF check .This issue can be resolved by adding a static route to 203.0. 114.24/32 through port3.
D. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 203.0. 114.24/32 through port3.

**Answer:** D

**NEW QUESTION 153**
You have enabled logging on a FortiGate device for event logs and all security logs, and you have set up logging to use the FortiGate local disk.

What is the default behavior when the local disk is full?

A. No new log is recorded after the warning is issued when log disk use reaches the threshold of 95%.
B. No new log is recorded until you manually clear logs from the local disk.
C. Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.
D. Logs are overwritten and the only warning is issued when log disk use reaches the threshold of 95%.

**Answer:** C

**Explanation:**
config log disk setting
set diskfull [ overwrite | nolog ]
Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full. (default --> overwrite)
config log memory global-setting
set full-first-warning-threshold {integer}
Log full first warning threshold as a percent. (default --> 75)

**NEW QUESTION 156**
Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) form port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) form local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)

A. The debug flow is of ICMP traffic.
B. A firewall policy allowed the connection.
C. A new traffic session is created.
D. The default route is required to receive a reply.

**Answer:** AC

**NEW QUESTION 160**
.....

# Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

## 100% Pass Your NSE4_FGT-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4_FGT-7.0-dumps.html