Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

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
Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Source defined as Internet Services in the firewall policy.
B. Destination defined as Internet Services in the firewall policy.
C. Highest to lowest priority defined in the firewall policy.
D. Services defined in the firewall policy.
E. Lowest to highest policy ID number.

Answer: ABD

Explanation:
When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:
• Incoming Interface
• Outgoing Interface
• Source: IP address, user, internet services
• Destination: IP address or internet services
• Service: IP protocol and port number
• Schedule: Applies during configured times

NEW QUESTION 3
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

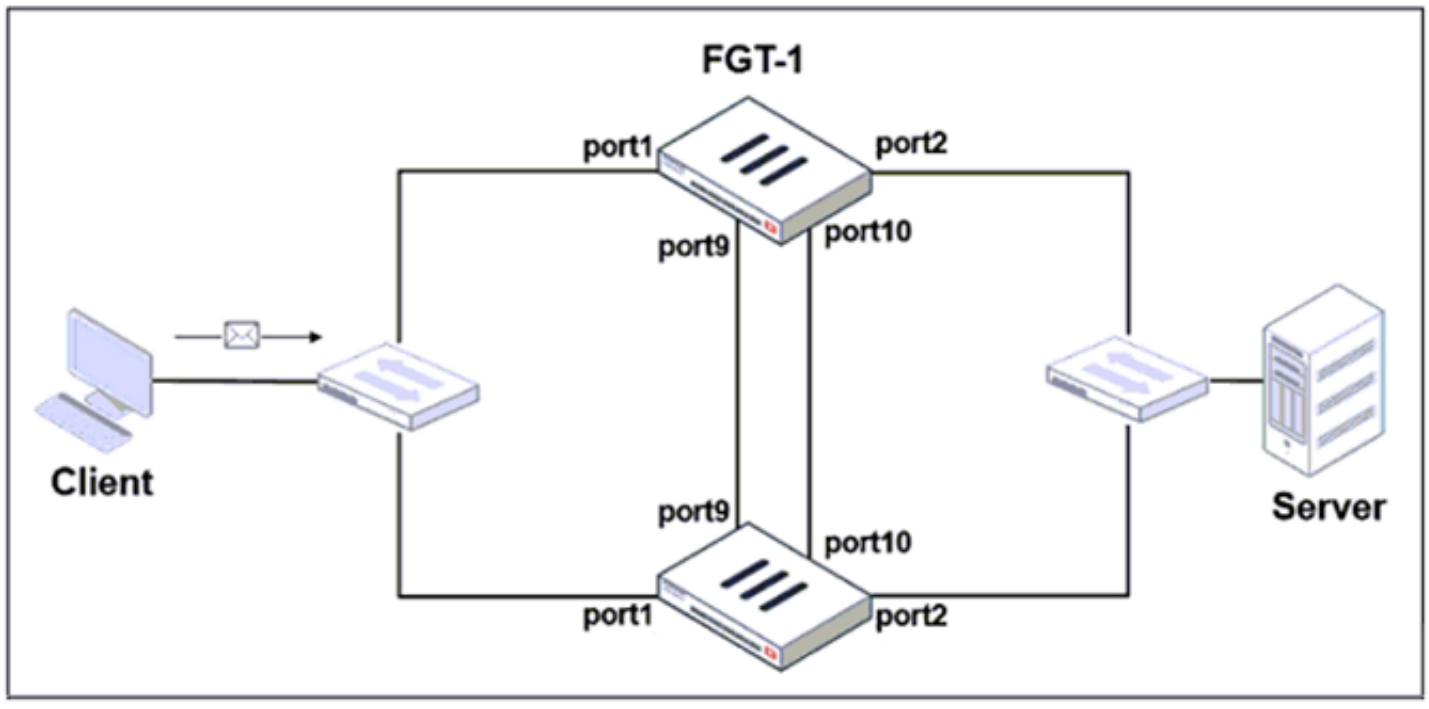


Exhibit A | Exhibit B

```
        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 4
To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

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

Answer: B

NEW QUESTION 5
An administrator wants to simplify remote access without asking users to provide user credentials. Which access control method provides this solution?

A. ZTNA IP/MAC filtering mode
B. ZTNA access proxy
C. SSL VPN
D. L2TP

Answer: B

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.165): "ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs."
This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials. ZTNA access proxy uses a secure tunnel between the user's device and the FortiGate, and authenticates the user based on device identity and context. The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile. This simplifies remote access and enhances security by reducing the attack surface12

NEW QUESTION 6
Which two statements are correct about SLA targets? (Choose two.)

A. You can configure only two SLA targets per one Performance SLA.
B. SLA targets are optional.
C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
D. SLA targets are used only when referenced by an SD-WAN rule.

Answer: BD

NEW QUESTION 7
Which two statements explain antivirus scanning modes? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

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

Answer: BC

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

NEW QUESTION 8
What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

A. Full Content inspection
B. Proxy-based inspection
C. Certificate inspection
D. Flow-based inspection

Answer: D

NEW QUESTION 9
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 10
Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

A. Antivirus engine
B. Intrusion prevention system engine
C. Flow engine
D. Detection engine

Answer: B

Explanation:
http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control

NEW QUESTION 10
In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.
B. The Incoming Interfac
C. Outgoing Interfac

D. Schedule, and Service fields can be shared with both IPv4 and IPv6.
E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
F. The IP version of the sources and destinations in a policy must match.
G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: BDE

NEW QUESTION 13
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 14
What are two functions of the ZTNA rule? (Choose two.)

A. It redirects the client request to the access proxy.
B. It applies security profiles to protect traffic.
C. It defines the access proxy.
D. It enforces access control.

Answer: BD

Explanation:
A ZTNA rule is a policy that enforces access control and applies security profiles to protect traffic between the client and the access proxy1. A ZTNA rule defines the following parameters1:

- Incoming interface: The interface that receives the client request.
- Source: The address and user group of the client.
- ZTNA tag: The tag that identifies the domain that the client belongs to.
- ZTNA server: The server that hosts the access proxy.
- Destination: The address of the application that the client wants to access.
- Action: The action to take for the traffic that matches the rule. It can be accept, deny, or redirect.
- Security profiles: The security features to apply to the traffic, such as antivirus, web filter, application control, and so on.

A ZTNA rule does not redirect the client request to the access proxy. That is the function of a policy route that matches the ZTNA tag and sends the traffic to the ZTNA server2.
A ZTNA rule does not define the access proxy. That is done by creating a ZTNA server object that specifies the IP address, port, and certificate of the access proxy3.
FortiGate Infrastructure 7.2 Study Guide (p.177): "A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic."

NEW QUESTION 19
Refer to the exhibit.

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

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

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

Answer: B

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

NEW QUESTION 21
An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

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

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821

NEW QUESTION 25
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 30
Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

A. SSH
B. HTTPS
C. FTM
D. FortiTelemetry

Answer: AB

NEW QUESTION 31
Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.
B. By default, the SSL VPN portal requires the installation of a client's certificate.
C. By default, split tunneling is enabled.
D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 34
Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

A. diagnose sys top
B. execute ping
C. execute traceroute
D. diagnose sniffer packet any
E. get system arp

Answer: BCD

NEW QUESTION 37
Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

A. The keyUsage extension must be set to keyCertSign.
B. The common name on the subject field must use a wildcard name.

C. The issuer must be a public CA.
D. The CA extension must be set to TRUE.

Answer: AD

Explanation:
"In order for FortiGate to act in these roles, its CA certificate must have the basic constraints extension set to cA=True and the value of the keyUsage extension set to keyCertSign."

NEW QUESTION 39
What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

A. FortiGate uses fewer resources.
B. FortiGate performs a more exhaustive inspection on traffic.
C. FortiGate adds less latency to traffic.
D. FortiGate allocates two sessions per connection.

Answer: AC

NEW QUESTION 43
An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSL/TLS connection.
Which FortiGate configuration can achieve this goal?

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

Answer: B

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

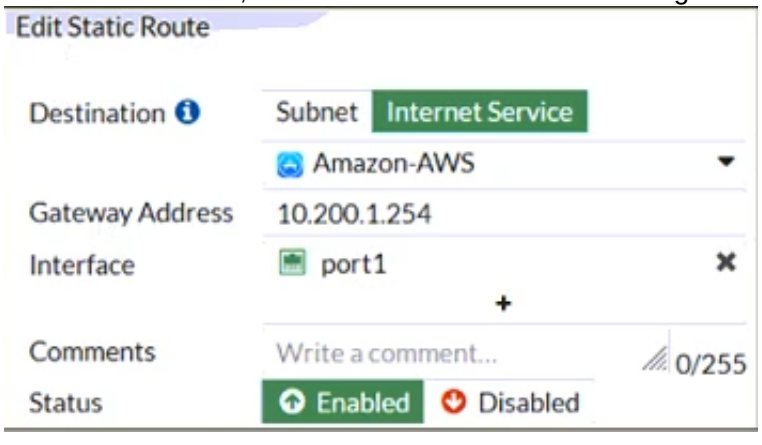
NEW QUESTION 48
An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

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 50
Refer to the exhibit, which contains a static route configuration. An administrator created a static route for Amazon Web Services.



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

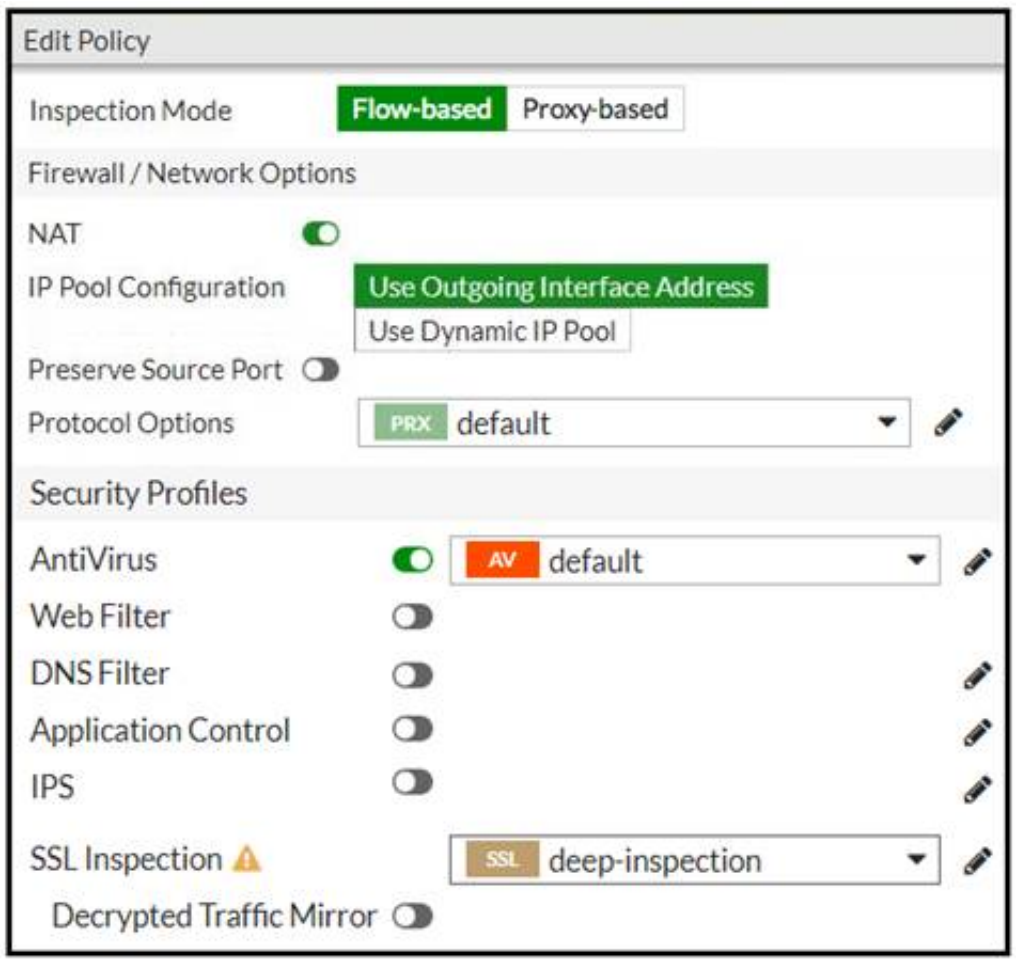
A. get router info routing-table database
B. diagnose firewall route list

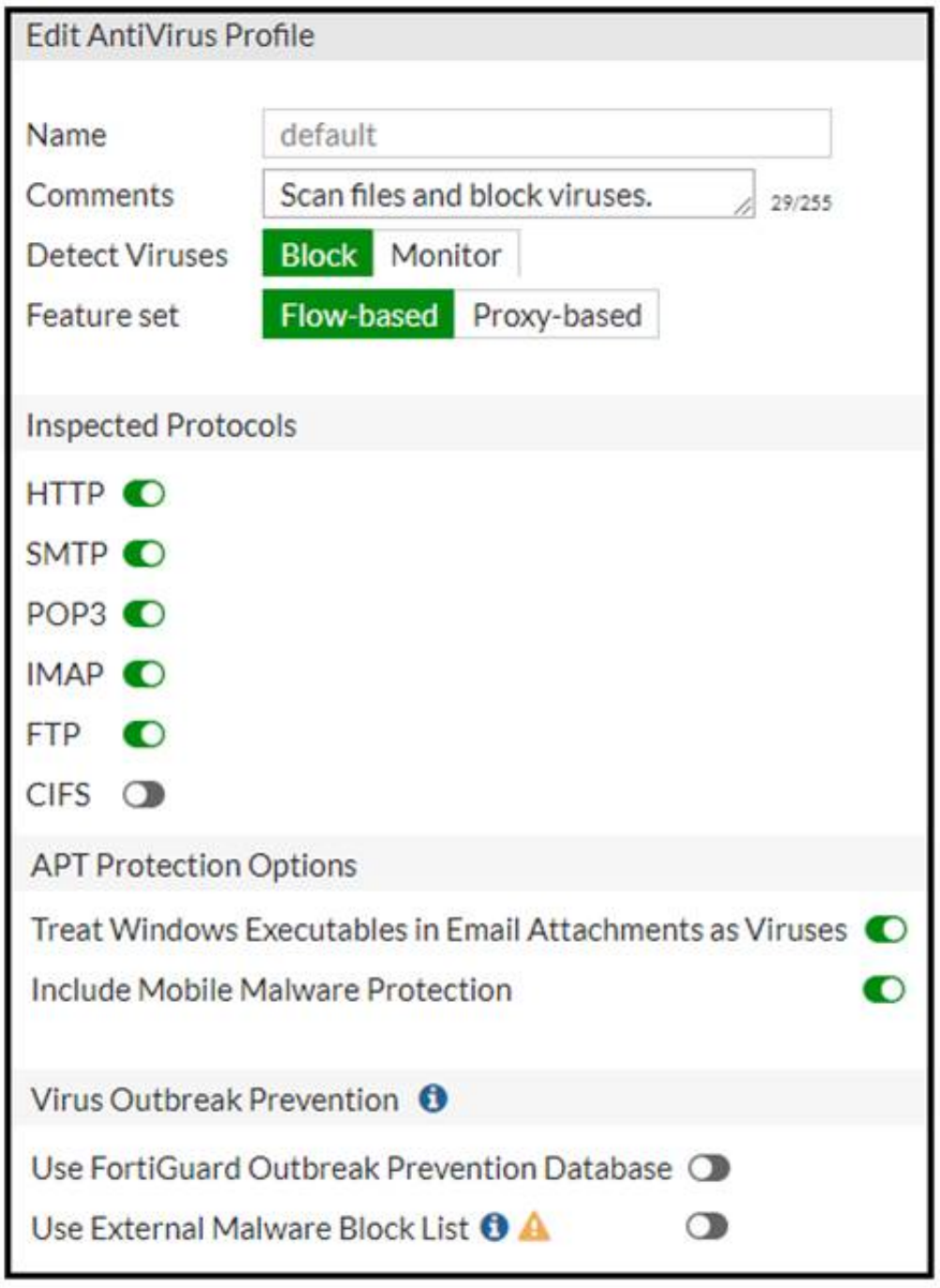
C. get internet-service route list
D. get router info routing-table all

Answer: B

Explanation:
ISDB static route will not create entry directly in routing-table. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/1
and here
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640
FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

NEW QUESTION 53
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).





Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The firewall policy performs the full content inspection on the file.
B. The flow-based inspection is used, which resets the last packet to the user.
C. The volume of traffic being inspected is too high for this model of FortiGate.
D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: B

Explanation:
· "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
· When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

NEW QUESTION 57
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 61
Refer to the exhibits.

Exhibit A | Exhibit B

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Exhibit A | Exhibit B

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

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

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

Answer: BD

NEW QUESTION 66
The IPS engine is used by which three security features? (Choose three.)

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

Answer: ABC

Explanation:
FortiGate Security 7.2 Study Guide (p.385): "The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It’s also responsible for application control, flow-based antivirus protection, web filtering, and email filtering."

NEW QUESTION 67
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 69
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 70
Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

A. The public key of the web server certificate must be installed on the browser.
B. The web-server certificate must be installed on the browser.
C. The CA certificate that signed the web-server certificate must be installed on the browser.
D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Answer: C

NEW QUESTION 74
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 75
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 79
Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

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

Answer: A

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

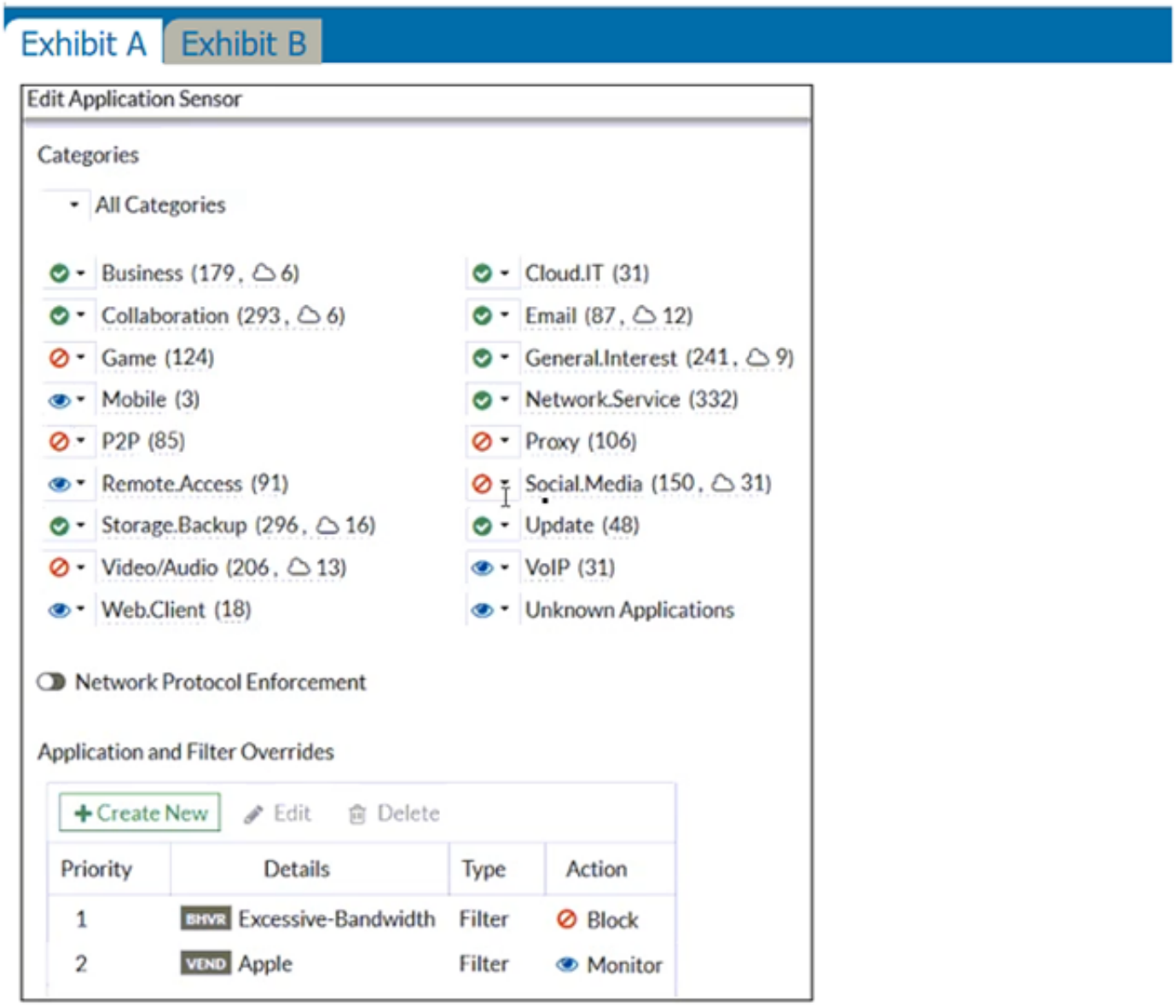
NEW QUESTION 82
Which of the following SD-WAN load balancing method use interface weight value to distribute traffic? (Choose two.)

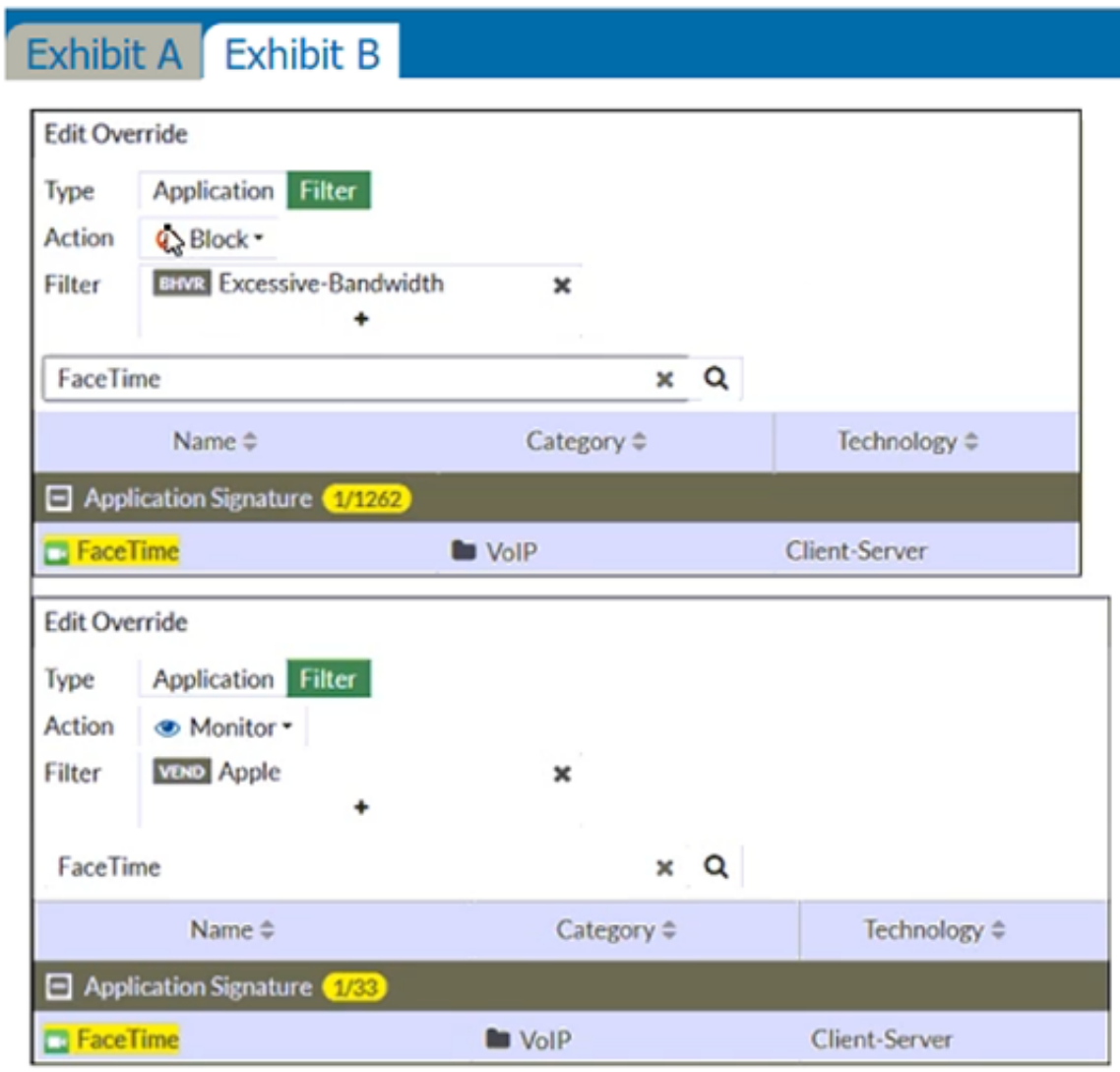
A. Source IP
B. Spillover
C. Volume
D. Session

Answer: CD

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

NEW QUESTION 85
Refer to the exhibits.
Exhibit A shows the application sensor configuration. Exhibit B shows 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?

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

Answer: B

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

NEW QUESTION 89
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 92
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 95
Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
C. Virtual IP addresses are used to distinguish between cluster members.
D. The primary device in the cluster is always assigned IP address 169.254.0.1.

Answer: BD

NEW QUESTION 98
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache
B. FortiSIEM
C. FortiAnalyzer
D. FortiSandbox
E. FortiCloud

Answer: BCE

NEW QUESTION 100
Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

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

Answer: CD

NEW QUESTION 102
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

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

Answer: A

NEW QUESTION 107

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
B. ADVPN is only supported with IKEv2.
C. Tunnels are negotiated dynamically between spokes.
D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Answer: AC

NEW QUESTION 108
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

NEW QUESTION 112
Refer to the web filter raw logs.

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

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

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

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

Answer: A

NEW QUESTION 114
Which timeout setting can be responsible for deleting SSL VPN associated sessions?

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

Answer: A

NEW QUESTION 115
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 119
An administrator configures outgoing interface any in a firewall policy. What is the result of the policy list view?

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

Answer: D

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

NEW QUESTION 124
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 127
When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

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

Answer: B

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

NEW QUESTION 128
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 129
An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an

administrator do to achieve this objective?

A. The administrator can register the same FortiToken on more than one FortiGate.
B. The administrator must use a FortiAuthenticator device
C. The administrator can use a third-party radius OTP server.
D. The administrator must use the user self-registration server.

Answer: B

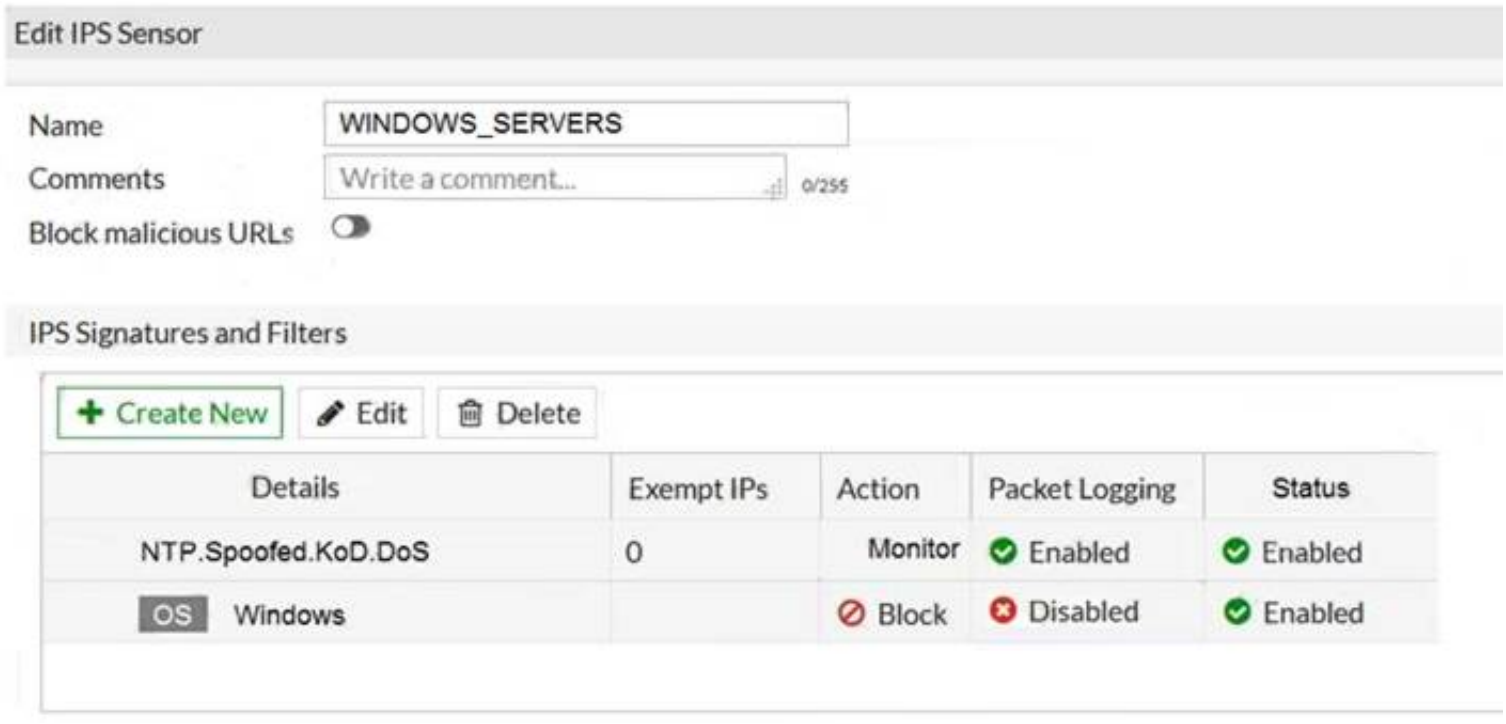
NEW QUESTION 133
FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.
Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

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

Answer: BC

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

NEW QUESTION 134
Refer to the exhibit.



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

A. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
B. The sensor will block all attacks aimed at Windows servers.
C. The sensor will reset all connections that match these signatures.
D. The sensor will gather a packet log for all matched traffic.

Answer: AB

NEW QUESTION 137
An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.
Which DPD mode on FortiGate will meet the above requirement?

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

Answer: D

NEW QUESTION 139
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 143
Examine this output from a debug flow:

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

Why did the FortiGate drop the packet?

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

Answer: D

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

NEW QUESTION 148
Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

A. FortiGate uses the AD server as the collector agent.
B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
C. FortiGate does not support workstation check .
D. FortiGate directs the collector agent to use a remote LDAP server.

Answer: BC

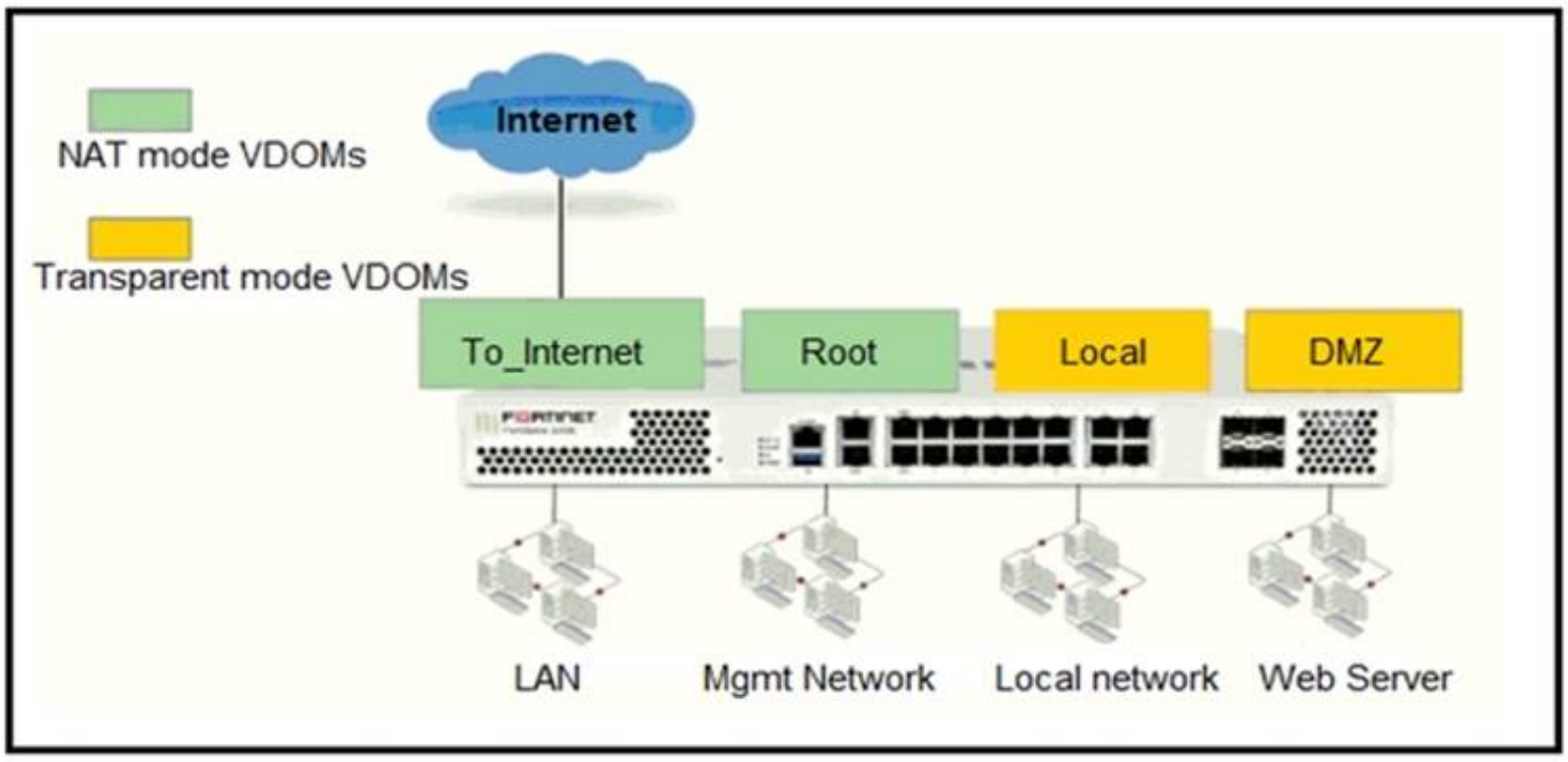
Explanation:
You can deploy FSSO w/o installing an agent. FG polls the DCs directly, instead of receiving logon info indirectly from a collector agent.
Because FG collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FG uses the SMB protocol to read the event viewer logs from the DCs.
FG acts as a collector. It 's responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

NEW QUESTION 152
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 157
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 162
Refer to the exhibit.

```
FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > -  selected route, * - FIB route, p - stale info

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

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

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

Answer: BC

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

NEW QUESTION 163
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 165
What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
B. FortiGate automatically negotiates a new security association after the existing security association expires.
C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=12069
FortiGate Infrastructure 7.2 Study Guide (p.264): "...then FortiGate might drop interesting traffic because of the absence of active SAs. To prevent this, you can enable Auto-negotiate. When you do this, FortiGate not only negotiates new SAs before the current SAs expire, but it also starts using the new SAs right away."
"Another benefit of enabling Auto-negotiate is that the tunnel comes up and stays up automatically, even when there is no interesting traffic. When you enable Autokey Keep Alive and keep Auto-negotiate disabled, the tunnel does not come up automatically unless there is interesting traffic. However, after the tunnel is up, it stays that way because FortiGate periodically sends keep alive packets over the tunnel. Note that when you enable Auto-negotiate, Autokey Keep Alive is implicitly enabled."

NEW QUESTION 169
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 173
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 177
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 180
Refer to the exhibit.

```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

A. The session is in SYN_SENT state.
B. The session is in FIN_ACK state.
C. The session is in FTN_WAIT state.
D. The session is in ESTABLISHED state.

Answer: A

Explanation:
Indicates TCP (proto=6) session in SYN_SENT state (proto=state=2) https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

NEW QUESTION 182
Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode
B. Can act as a Layer 2 switch as well as a Layer 3 router
C. All interfaces in the software switch share the same IP address
D. It can group only physical interfaces

Answer: AC

NEW QUESTION 185
Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

A. FortiGuard web filter cache
B. FortiGate hostname
C. NTP
D. DNS

Answer: CD

Explanation:
In the 7.2 Infrastructure Guide (page 306) the list of configuration settings that are NOT synchronized includes both 'FortiGate host name' and 'Cache'

NEW QUESTION 186
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 187
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 188
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 189
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 194
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view
B. Log backups from the CLI cannot be restored to another FortiGat
C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
D. Log downloads from the GUI are stored as LZ4 compressed files.

Answer: AB

NEW QUESTION 196
Which of statement is true about SSL VPN web mode?

A. The tunnel is up while the client is connected.
B. It supports a limited number of protocols.
C. The external network application sends data through the VPN.
D. It assigns a virtual IP address to the client.

Answer: B

Explanation:
FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

NEW QUESTION 198
Refer to the exhibit.

Exhibit A Exhibit B

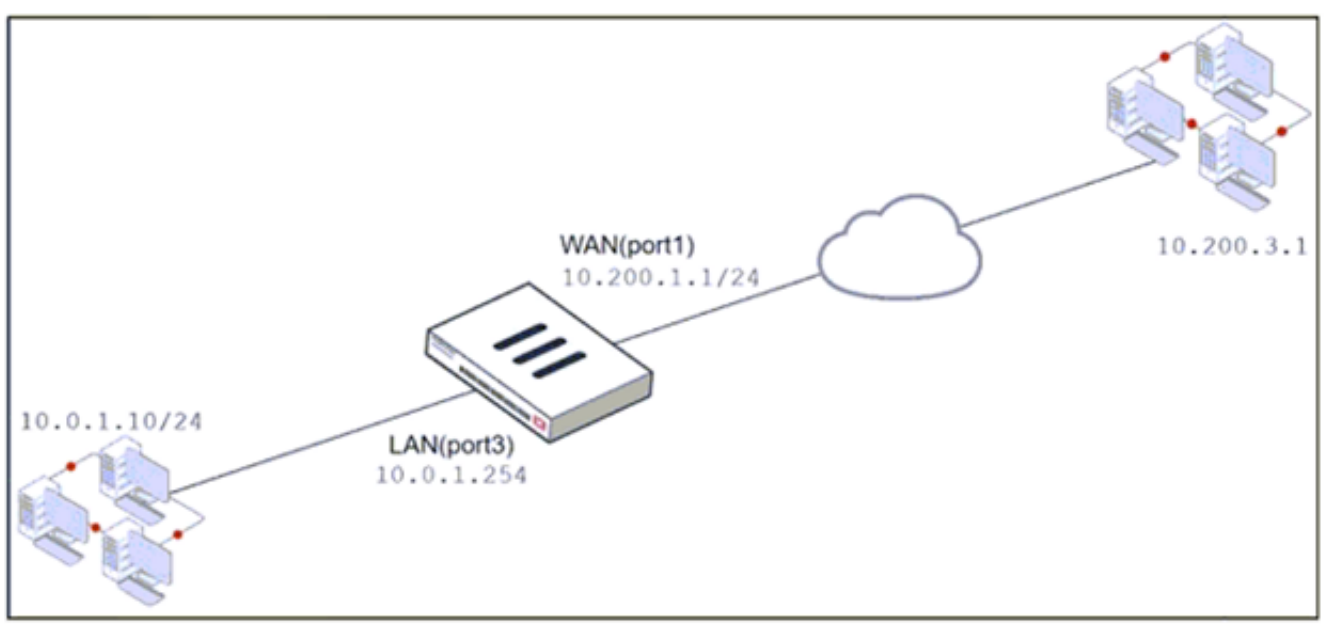


Exhibit A Exhibit B

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

Edit Virtual IP

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

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

Optional Filters

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

Edit Dynamic IP Pool

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

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

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

Answer: C

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

NEW QUESTION 203
If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

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

Answer: D

NEW QUESTION 205
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) from 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) from 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"
```

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

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

Answer: AC

Explanation:
The debug flow output shows the result of a diagnose command that captures the traffic flow between the source and destination IP addresses1. The debug flow output reveals the following information about the traffic flow1:

- The protocol is 1, which means that the traffic uses ICMP protocol2. ICMP is a protocol that is used to send error messages and test connectivity between devices2.
- The session state is 0, which means that a new traffic session was created3. A session is a data structure that stores information about a connection between two devices3.
- The policy ID is 1, which means that the traffic matched the firewall policy with ID 14. A firewall policy is a rule that defines how FortiGate processes traffic based on the source, destination, service, and action parameters4.
- The action is 0, which means that the traffic was allowed by the firewall policy. An action is a parameter that specifies what FortiGate does with the traffic that matches a firewall policy.

Therefore, two conclusions that can be made from the debug flow output are:

- The debug flow is for ICMP traffic.
- A new traffic session was created.

NEW QUESTION 206
Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.
B. It is available only on a proxy-based firewall policy.
C. It inspects video files hosted on file sharing services.
D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Answer: B

NEW QUESTION 208
An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

A. Device detection on all interfaces is enforced for 30 minutes.
B. Denied users are blocked for 30 minutes.
C. A session for denied traffic is created.
D. The number of logs generated by denied traffic is reduced.

Answer: CD

Explanation:
ses-denied-traffic
Enable/disable including denied session in the session table. https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/20620/config-system-settings block-session-timer
Duration in seconds for blocked sessions . integer
Minimum value: 1 Maximum value: 300
30
https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/1620/config-system-global

NEW QUESTION 209
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 214
What are two functions of ZTNA? (Choose two.)

A. ZTNA manages access through the client only.
B. ZTNA manages access for remote users only.
C. ZTNA provides a security posture check.

D. ZTNA provides role-based access.

Answer: CD

NEW QUESTION 218
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 222
Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53->10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

A. The session is a UDP unidirectional state.
B. The session is in TCP ESTABLISHED state.
C. The session is a bidirectional UDP connection.
D. The session is a bidirectional TCP connection.

Answer: C

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

NEW QUESTION 227
Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.
B. The application signature database inspects traffic only from the original web application server.
C. FortiGuard maintains only one signature of each web application that is unique.
D. FortiGate can inspect sub-application traffic regardless where it was originate

Answer: D

NEW QUESTION 230
Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

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

Answer: ADE

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

NEW QUESTION 233
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE4_FGT-7.0 Practice Exam Features:

* NSE4_FGT-7.0 Questions and Answers Updated Frequently

* NSE4_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE4_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year