# NSE4-5.4.exam.230q

Number: NSE4-5.4
Passing Score: 800
Time Limit: 120 min

**NSE4-5.4**

**Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4**

**Exam A**

**QUESTION 1**

In a high availability (HA) cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a secondary FortiGate?

A. Client > primary FortiGate> secondary FortiGate> primary FortiGate> web server.
B. Client > secondary FortiGate> web server.
C. Client >secondary FortiGate> primary FortiGate> web server.
D. Client> primary FortiGate> secondary FortiGate> web server.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**

A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub-interfaces added to the same physical interface.

Which statement about the VLAN IDs in this scenario is true?

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

**Correct Answer:** B

**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 3**
Which of the following statements are true when using Web Proxy Auto-discovery Protocol (WPAD) with the DHCP discovery method? (Choose two.)

A. The browser sends a DHCPINFORM request to the DHCP server.
B. The browser will need to be preconfigured with the DHCP server’s IP address.
C. The DHCP server provides the PAC file for download.
D. If the DHCP method fails, browsers will try the DNS method.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

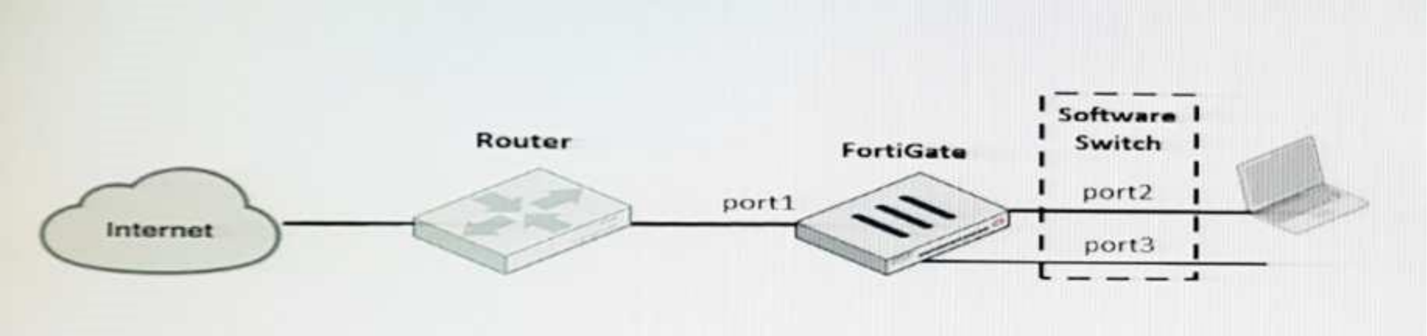
**QUESTION 4**
What inspections are executed by the IPS engine? (Choose three.)

A. Application control
B. Flow-based data leak prevention
C. Proxy-based antispam
D. Flow-based web filtering
E. Proxy-based antivirus

**Correct Answer:** ABD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
Examine the exhibit.



A client workstation is connected to FortiGate port2. The Fortigate port1 is connected to an ISP router. Port2 and port3 are both configured as a software switch.

What IP address must be configured in the workstation as the default gateway?

A. The port2's IP address.
B. The router's IP address.
C. The FortiGate's management IP address.
D. The software switch interface's IP address.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Which of the following statements about the FSSO collector agent timers is true?

A. The dead entry timeout interval is used to age out entries with an unverified status.
B. The workstation verify interval is used to periodically check if a workstation is still a domain member.
C. The user group cache expiry is used to age out the monitored groups.
D. The IP address change verify interval monitors the server IP address where the collector agent is installed, and updates the collector agent configuration if it changes.

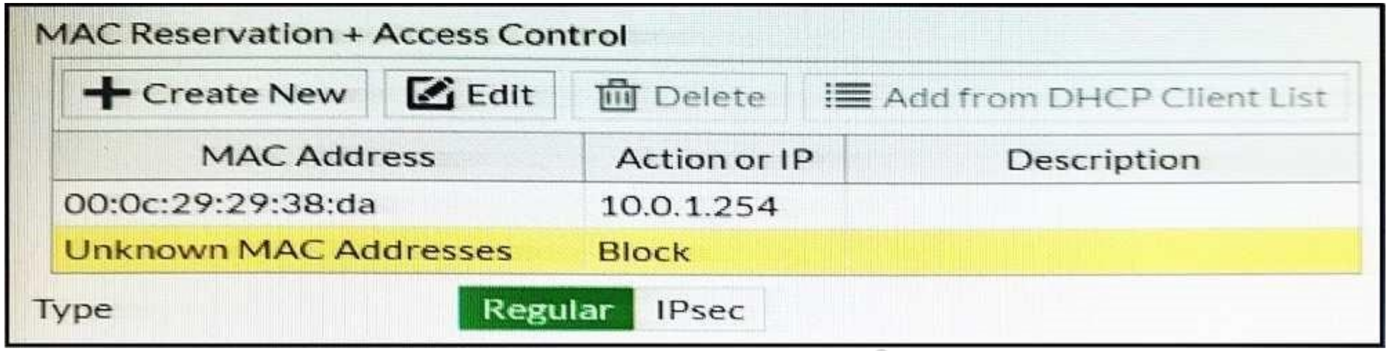
**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

An administrator has enabled the DHCP Server on the port1 interface and configured the following based on the exhibit.



MAC Reservation + Access Control

| MAC Address | Action or IP | Description |
|---|---|---|
| 00:0c:29:29:38:da | 10.0.1.254 | |
| Unknown MAC Addresses | Block | |

Type: Regular | IPsec

Which statement is correct based on this configuration?

A. The MAC address 00:0c:29:29:38:da belongs to the port1 interface.
B. Access to the network is blocked for the devices with the MAC address 00:0c:29:29:38:da and the IP address 10.0.1.254.
C. 00:0c:29:29:38:da is the virtual MAC address assigned to the secondary IP address (10.0.1.254) of the port1 interface.
D. The IP address 10.0.1.254 is reserves for the device with the MAC address 00:0c:29:29:38:da.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**

An administrator wants to create a policy-based IPsec VPN tunnel between two FortiGate devices.

Which configuration steps must be performed on both units to support this scenario? (Choose three.)

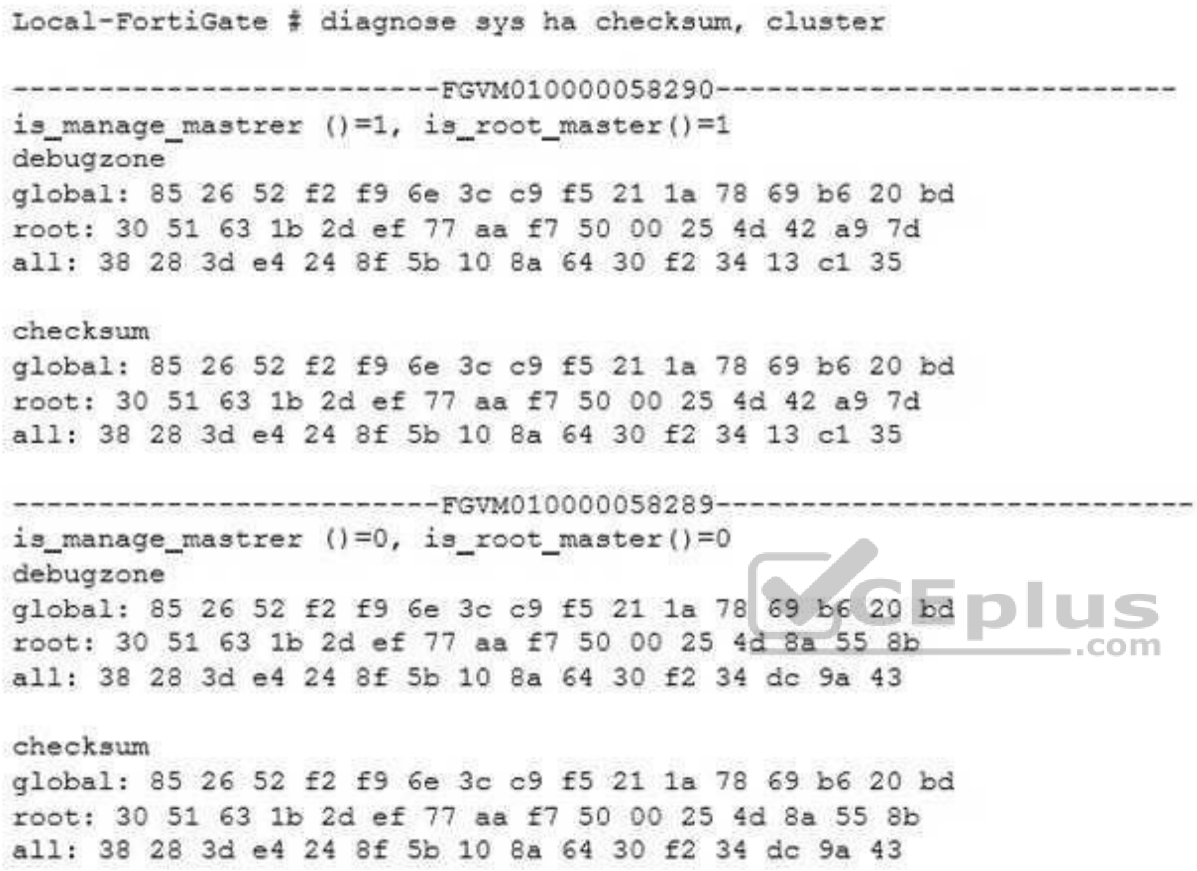
A. Define the phase 2 parameters.

B. Set the phase 2 encapsulation method to transport mode.
C. Define at least one firewall policy, with the action set to IPsec.
D. Define a route to the remote network over the IPsec tunnel.
E. Define the phase 1 parameters, without enabling IPsec interface mode.

**Correct Answer:** ACE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
View the Exhibit.



```
Local-FortiGate # diagnose sys ha checksum, cluster

-------------------------FGVM010000058290---------------------------
is_manage_mastrer ()=1, is_root_master()=1
debugzone
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 42 a9 7d
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 13 c1 35

checksum
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 42 a9 7d
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 13 c1 35

-------------------------FGVM010000058289----------------------------
is_manage_mastrer ()=0, is_root_master()=0
debugzone
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 8a 55 8b
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 dc 9a 43

checksum
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 8a 55 8b
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 dc 9a 43
```

Which statements are correct based on this output? (Choose two.)

A. The global configuration is synchronized between the primary and secondary FortiGate.
B. The all VDOM is not synchronized between the primary and secondary FortiGate.
C. The root VDOM is not synchronized between the primary and secondary FortiGate.
D. The FortiGates have three VDOMs.

**Correct Answer:** AC
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 10**

Which of the following statements about web caching are true? (Choose two.)

A. Web caching slows down web browsing due to constant read-write cycles from FortiGate memory.
B. When a client makes a web request, the proxy checks if the requested URL is already in memory.
C. Only heavy content is cached, for example, videos, images, audio and so on.
D. Web caching is supported in both explicit and implicit proxy.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**

What FortiGate configuration is required to actively prompt users for credentials?

A. You must enable one or more protocols that support active authentication on a firewall policy.
B. You must assign users to a group for active authentication.
C. You must place the firewall policy for active authentication before a firewall policy for passive authentication.
D. You must enable the **Authentication** setting on the firewall policy.

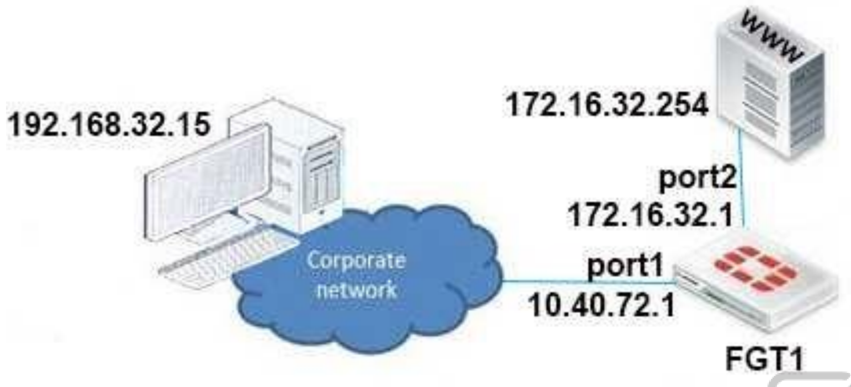
**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**

View the exhibit.



In this scenario, FGT1 has the following routing table:

```
S*    0. 0. 0. 0/0 [10/0] via 10. 40. 72. 2, port1
C    172. 16. 32. 0/24  is directly connected, port2
C    10. 40. 72. 0/30 is directly connected, port1
```

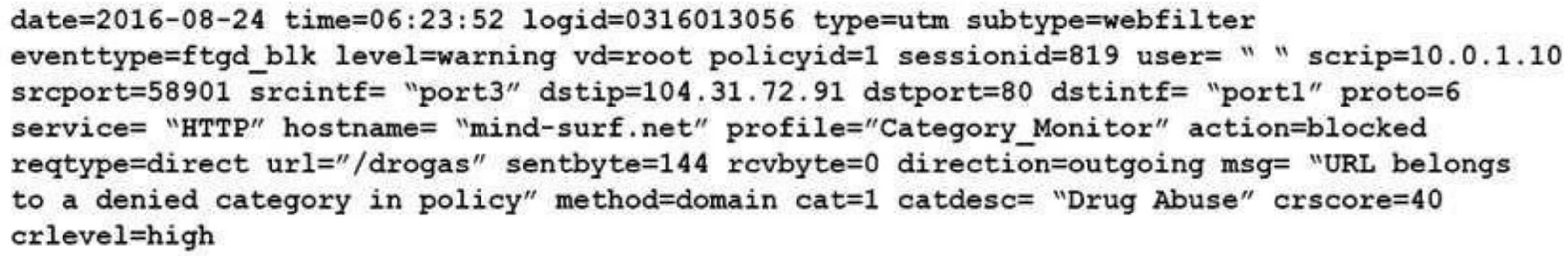
A user at 192.168.32.15 is trying to access the web server at 172.16.32.254. Which of the following statements best describe how the FortiGate will perform reverse path forwarding checks on this traffic? (Choose two.)

A. Strict RPF check will deny the traffic.
B. Strict RPF check will allow the traffic.
C. Loose RPF check will allow the traffic.
D. Loose RPF check will deny the traffic.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
View the exhibit.



```
date=2016-08-24 time=06:23:52 logid=0316013056 type=utm subtype=webfilter
eventtype=ftgd_blk level=warning vd=root policyid=1 sessionid=819 user= “ “ scrip=10.0.1.10
srcport=58901 srcintf= “port3” dstip=104.31.72.91 dstport=80 dstintf= “port1” proto=6
service= “HTTP” hostname= “mind-surf.net” profile=”Category_Monitor” action=blocked
reqtype=direct url=”/drogas” sentbyte=144 rcvbyte=0 direction=outgoing msg= “URL belongs
to a denied category in policy” method=domain cat=1 catdesc= “Drug Abuse” crscore=40
crlevel=high
```

What does the log message indicate? (Choose two.)

A. The log type is `utm`.
B. `10.0.1.10` is the IP address for `mind-surf.net`.
C. FortiGate blocked the traffic.
D. Firewall policy ID 6 matched the traffic.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

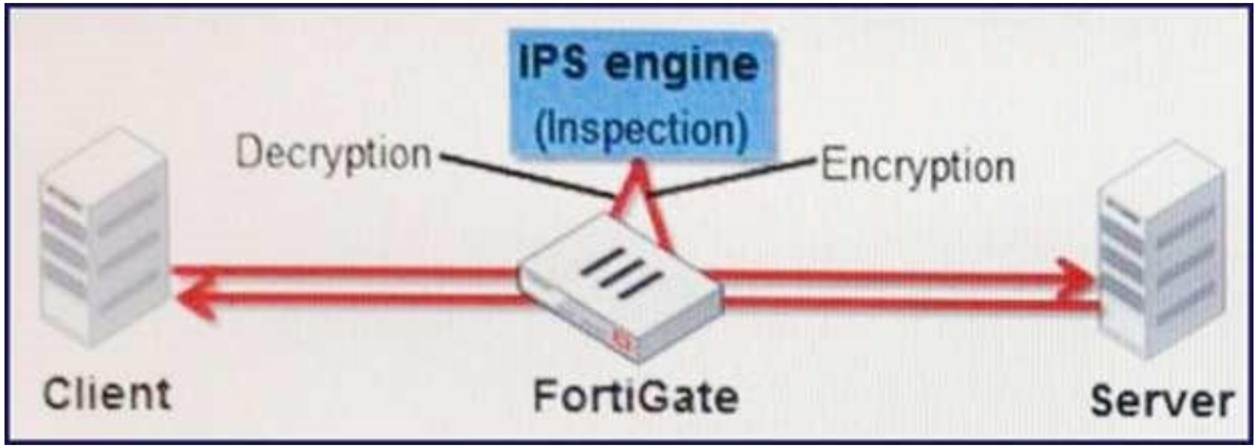
**Explanation/Reference:**

**QUESTION 14**
Which election criterion is used to elect the primary FortiGate in a high availability (HA) cluster when override is enabled?

A. uptime > priority > port monitor > serial number
B. port monitor > uptime > priority >serial number
C. priority > port monitor >uptime >serial number
D. port monitor > priority > uptime >serial number

**Correct Answer:** D
**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 15**
View the exhibit.



What does this exhibit represent?

A. SSL handshake
B. Interchanging digital certificates
C. Certificate signing request (CSR)
D. Inline SSL inspection

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
Which condition must be met to offload the encryption and decryption of IPsec traffic to an NP6 processor?

A. Phase 2 must use an encryption algorithm supported by the NP6.

B. Anti-replay must be disabled.
C. IPsec traffic must not be inspected by a session helper.

D. No content inspection can be applied to traffic that is going to be encrypted.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
What FortiGate feature can be used to prevent a cross-site scripting (XSS) attack?

A. Web application firewall (WAF)
B. DoS policies
C. Rate based IPS signatures
D. One-arm sniffer

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

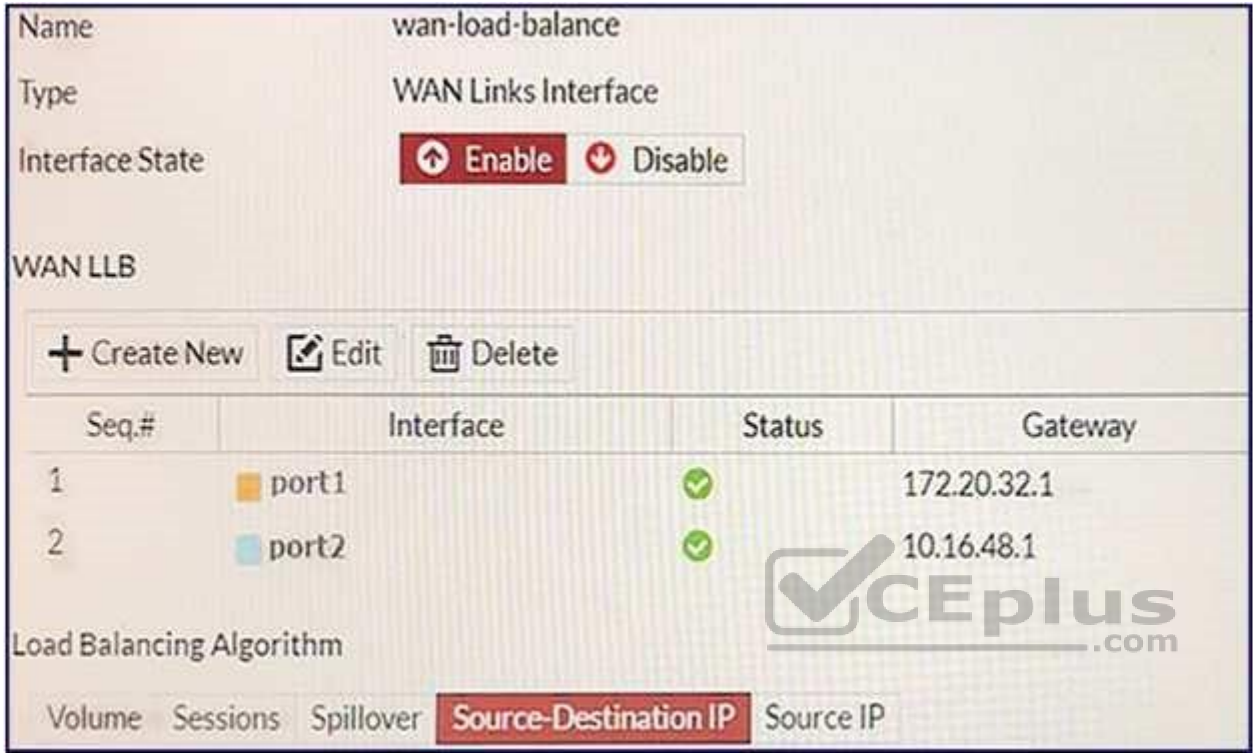
**QUESTION 18**
What is the purpose of the **Policy Lookup** feature?

A. It searches the matching policy based on an input criteria.
B. It enables hidden security profiles with full logging capabilities and generates **Learning Reports** based on an input criteria.
C. It finds duplicate objects in firewall policies.
D. It creates a new firewall policy based on an input criteria.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 19**

View the exhibit.



Name wan-load-balance

Type WAN Links Interface

Interface State [✓ Enable] Disable

WAN LLB

| Seq.# | Interface | Status | Gateway |
|---|---|---|---|
| 1 | port1 | ✓ | 172.20.32.1 |
| 2 | port2 | ✓ | 10.16.48.1 |

Load Balancing Algorithm

Volume Sessions Spillover [✓ Source-Destination IP] Source IP

Which of the following statements are correct? (Choose two.)

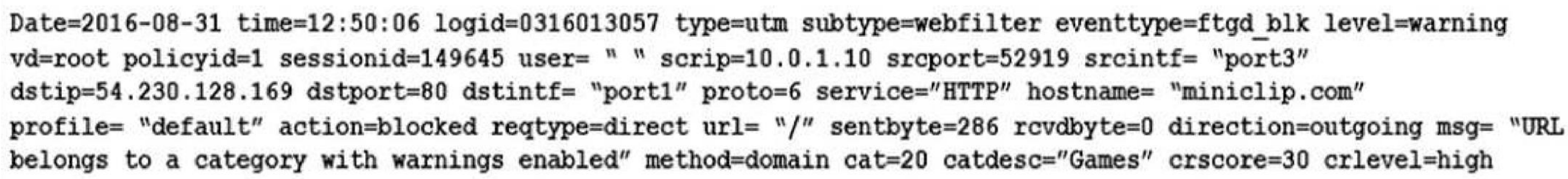
A. next-hop IP address is not required when configuring a static route that uses the wan-load balance interface.
B. Sessions will be load-balanced based on source and destination IP addresses.
C. Each member interface requires its own firewall policy to allow traffic.
D. The **wan-load-balance** interface must be manually created.

**Correct Answer:** AB
**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 20**
Examine the following web filtering log.

Which statement about the log message is true?

A. The action for the category **Games** is set to block.



```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked reqtype=direct url= "/" sentbyte=286 rcvdbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

B. The usage quota for the IP address 10.0.1.10 has expired.

C. The name of the applied web filter profile is `default`.

D. The web site `miniclip.com` matches a static URL filter whose action is set to **Warning**.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Examine this output from a debug flow:
Which statements about the output are correct? (Choose two.)

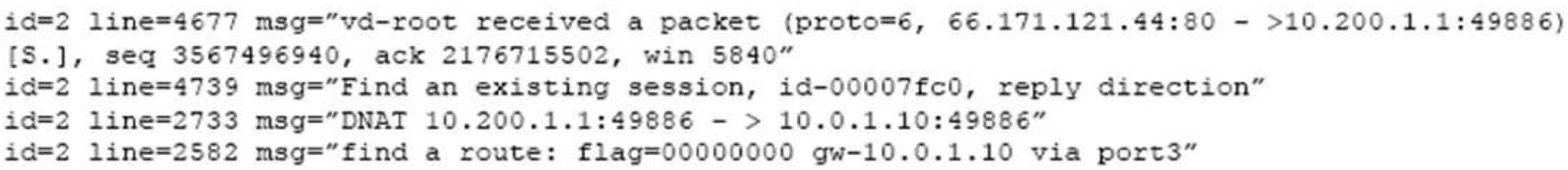
A. The packet was allowed by the firewall policy with the ID `00007fc0`.

B. FortiGate routed the packet through `port3`.

C. FortiGate received a TCP SYN/ACK packet.

D. The source IP address of the packet was translated to 10.0.1.10.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

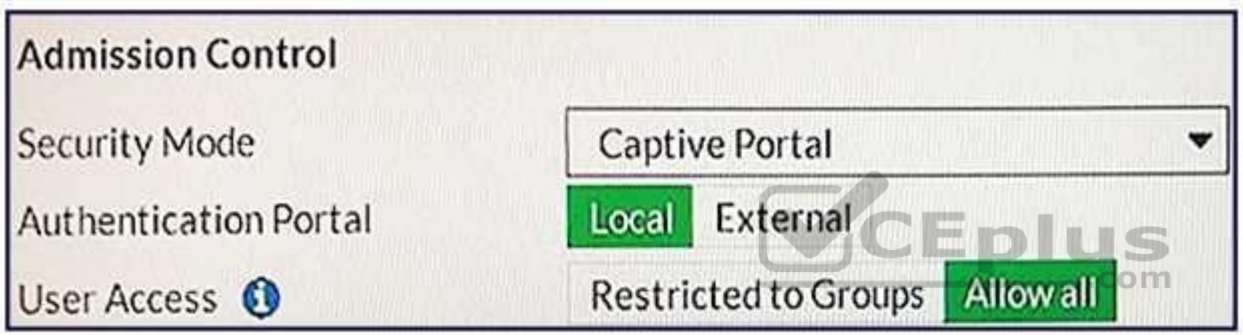


```
id=2 line=4677 msg="vd-root received a packet (proto=6, 66.171.121.44:80 - >10.200.1.1:49886)
[S.], seq 3567496940, ack 2176715502, win 5840"
id=2 line=4739 msg="Find an existing session, id-00007fc0, reply direction"
id=2 line=2733 msg="DNAT 10.200.1.1:49886 - > 10.0.1.10:49886"
id=2 line=2582 msg="find a route: flag=00000000 gw-10.0.1.10 via port3"
```

**Explanation/Reference:**

**QUESTION 22**

View the exhibit.



Admission Control

Security Mode: Captive Portal

Authentication Portal: [✓ Local] External

User Access: Restricted to Groups [✓ Allow all]

Which users and user groups are allowed access to the network through captive portal?

A. Only individual users–not groups–defined in the captive portal configuration.
B. Groups defined in the captive portal configuration
C. All users

D. Users and groups defined in the firewall policy.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
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.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
An administrator has disabled **Accept push updates** under **Antivirus & IPS Updates**. Which statements is true when this setting is disabled?

A. The extreme database is disabled.
B. New AV definitions are not added to FortiGate as soon as they are releases by FortiGuard.
C. Administrators cannot manually upload new AV definitions to the FortiGate.
D. FortiGate does not send files to FortiSandbox for inspection.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**

An administrator needs to create a tunnel mode SSLVPN to access an internal web server from the Internet. The web server is connected to `port1`. The Internet is connected to `port2`. Both interfaces belong to the VDOM named `Corporation`. What interface must be used as the source for the firewall policy that will allow this traffic?

A. `ssl.root`

B. `ssl.Corporation`

C. `port2`

D. `port1`

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**

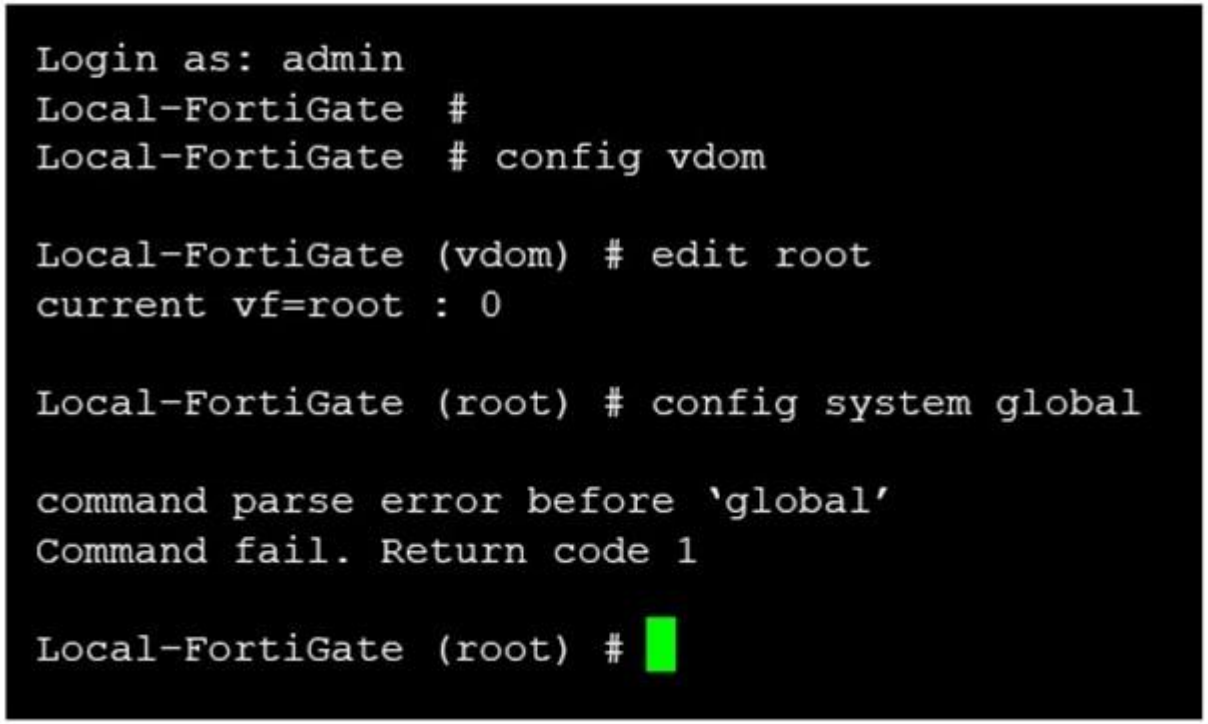
Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.
B. AH does not support perfect forward secrecy.
C. AH provides data integrity but no encryption.
D. AH provides strong data integrity but weak encryption.

**Correct Answer:** C
**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 27**

View the exhibit.



```
Login as: admin
Local-FortiGate  #
Local-FortiGate  # config vdom

Local-FortiGate (vdom) # edit root
current vf=root : 0

Local-FortiGate (root) # config system global

command parse error before 'global'
Command fail. Return code 1

Local-FortiGate (root) # █
```

Why is the administrator getting the error shown in the exhibit?

A. The administrator `admin` does not have the privileges required to configure global settings.
B. The global settings cannot be configured from the `root` VDOM context.
C. The command `config system global` does not exist in FortiGate.
D. The administrator must first enter the command `edit global`.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**

What FortiGate feature can be used to block a ping sweep scan from an attacker?

A. Web application firewall (WAF)
B. Rate based IPS signatures
C. One-arm sniffer
D. DoS policies

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**

Which statements about the firmware upgrade process on an active-active high availability (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.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**

A FortiGate is configured with three virtual domains (VDOMs). Which of the following statements is correct regarding multiple VDOMs?

A. The FortiGate must be a model 1000 or above to support multiple VDOMs.
B. A license has to be purchased and applied to the FortiGate before VDOM mode could be enabled.
C. Changing the operational mode of a VDOM requires a reboot of the FortiGate.
D. The FortiGate supports any combination of VDOMs in NAT/Route and transparent modes.

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
Which statements are correct regarding virtual domains (VDOMs)? (Choose two.)

A. VDOMs divide a single FortiGate unit into two or more virtual units that each have dedicated memory and CPUs.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. VDOMs share firmware versions, as well as antivirus and IPS databases.
D. Different time zones can be configured in each VDOM.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
A FortiGate is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root. Which of the following settings will this administrator be able to configure? (Choose two.)

A. Firewall addresses.
B. DHCP servers.
C. FortiGuard Distribution Network configuration.
D. System hostname.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**

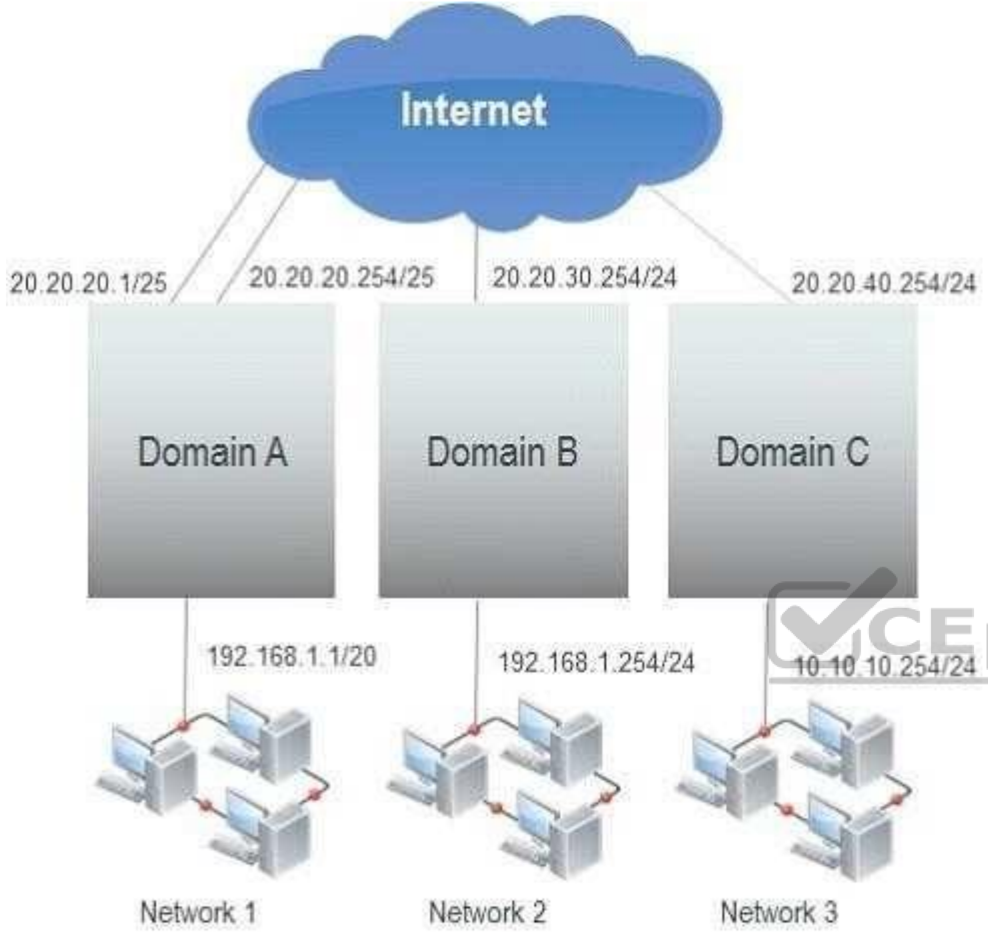
A FortiGate administrator with the super_admin profile configures a virtual domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in the GUI in the management VDOM. What would be a possible cause for this problem?

A. The administrator does not have the proper permissions to reassign the dmz interface.
B. The dmz interface is referenced in the configuration of another VDOM.
C. Non-management VDOMs cannot reference physical interfaces.
D. The dmz interface is in PPPoE or DHCP mode.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



Which of the following statements are true if the network administrator wants to route traffic between all the VDOMs? (Choose three.)

A. The administrator can configure inter-VDOM links to avoid using external interfaces and routers.

B. As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any interface, including inter-VDOM links.

C. This configuration requires a router to be positioned between the FortiGate unit and the Internet for proper routing.

D. Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached.

E. As each VDOM has an independent routing table, routing rules need to be set (for example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

**Correct Answer:** ABE

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub- interfaces added to the same physical interface. Which one of the following statements is correct regarding the VLAN IDs in this scenario?

A. The two VLAN sub-interfaces can have the same VLAN ID only if they have IP addresses in different subnets.
B. The two VLAN sub-interfaces must have different VLAN IDs.
C. The two VLAN sub-interfaces can have the same VLAN ID only if they belong to different VDOMs.
D. The two VLAN sub-interfaces can have the same VLAN ID if they are connected to different L2 IEEE 802.1Q compliant switches.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
Which statements are correct for port pairing and forwarding domains? (Choose two.)

A. They both create separate broadcast domains.
B. Port Pairing works only for physical interfaces.
C. Forwarding Domain only applies to virtual interfaces.
D. They may contain physical and/or virtual interfaces.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 37**
In transparent mode, forward-domain is an CLI setting associate with ___________.

A. static route

B. a firewall policy
C. an interface
D. a virtual domain

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Which of the following sequences describes the correct order of criteria used for the selection of a master unit within a FortiGate high availability (HA) cluster when override is disabled?

A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number.
B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number.
C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number.
D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Which of the following statements are correct about the HA command diagnose sys ha reset- uptime? (Choose two.)

A. The device this command is executed on is likely to switch from master to slave status if override is disabled.
B. The device this command is executed on is likely to switch from master to slave status if override is enabled.
C. This command has no impact on the HA algorithm.
D. This command resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**

What are the requirements for a HA cluster to maintain TCP connections after device or link failover? (Choose two.)

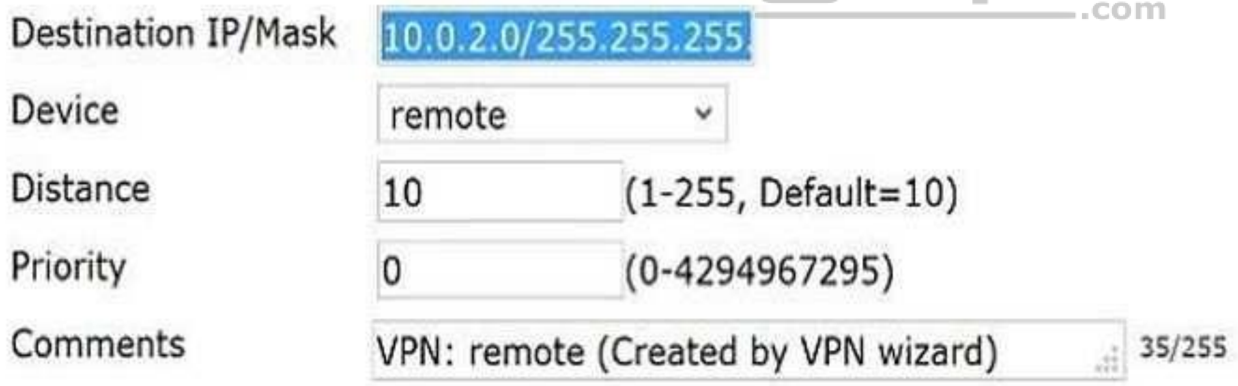
A. Enable session pick-up.
B. Enable override.
C. Connections must be UDP or ICMP.
D. Connections must not be handled by a proxy.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**

Review the static route configuration for IPsec shown in the exhibit; then answer the question below.



| | | |
|---|---|---|
| Destination IP/Mask | 10.0.2.0/255.255.255 | |
| Device | remote | |
| Distance | 10 | (1-255, Default=10) |
| Priority | 0 | (0-4294967295) |
| Comments | VPN: remote (Created by VPN wizard) | 35/255 |

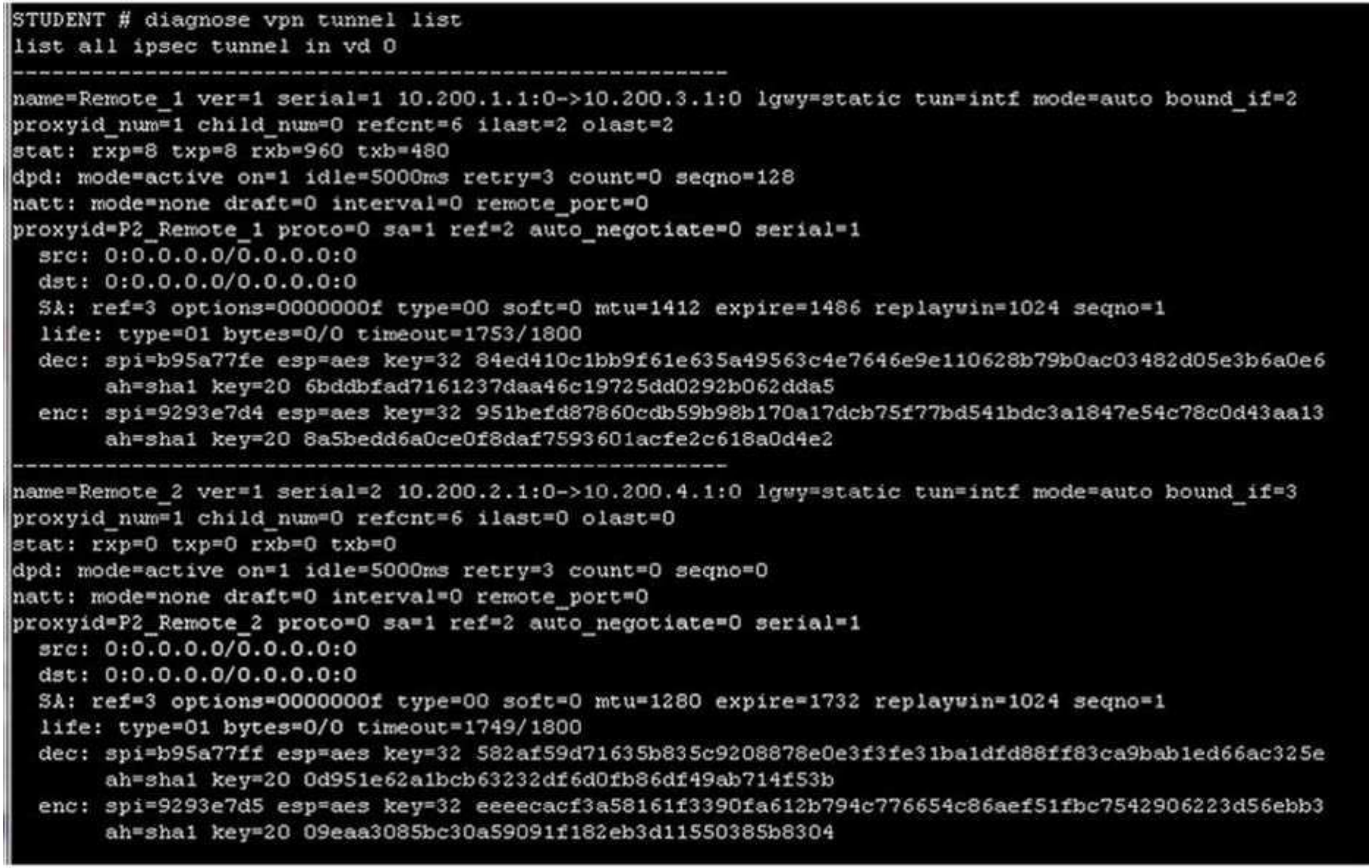
Which statements are correct regarding this configuration? (Choose two.)

A. Interface remote is an IPsec interface.
B. A gateway address is not required because the interface is a point-to-point connection.
C. A gateway address is not required because the default route is used.
D. Interface remote is a zone.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit.



```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=Remote_1 ver=1 serial=1 10.200.1.1:0->10.200.3.1:0 lgwy=static tun=intf mode=auto bound_if=2
proxyid_num=1 child_num=0 refcnt=6 ilast=2 olast=2
stat: rxp=8 txp=8 rxb=960 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=128
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_1 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=0000000f type=00 soft=0 mtu=1412 expire=1486 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1753/1800
  dec: spi=b95a77fe esp=aes key=32 84ed410c1bb9f61e635a49563c4e7646e9e110628b79b0ac03482d05e3b6a0e6
       ah=sha1 key=20 6bddbfad7161237daa46c19725dd0292b062dda5
  enc: spi=9293e7d4 esp=aes key=32 951befd87860cdb59b98b170a17dcb75f77bd541bdc3a1847e54c78c0d43aa13
       ah=sha1 key=20 8a5bedd6a0ce0f8daf7593601acfe2c618a0d4e2
------------------------------------------------------
name=Remote_2 ver=1 serial=2 10.200.2.1:0->10.200.4.1:0 lgwy=static tun=intf mode=auto bound_if=3
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_2 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=0000000f type=00 soft=0 mtu=1280 expire=1732 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1749/1800
  dec: spi=b95a77ff esp=aes key=32 582af59d71635b835c9208878e0e3f3fe31ba1dfd88ff83ca9bab1ed66ac325e
       ah=sha1 key=20 0d951e62a1bcb63232df6d0fb86df49ab714f53b
  enc: spi=9293e7d5 esp=aes key=32 eeeecacf3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
       ah=sha1 key=20 09eaa3085bc30a59091f182eb3d11550385b8304
```

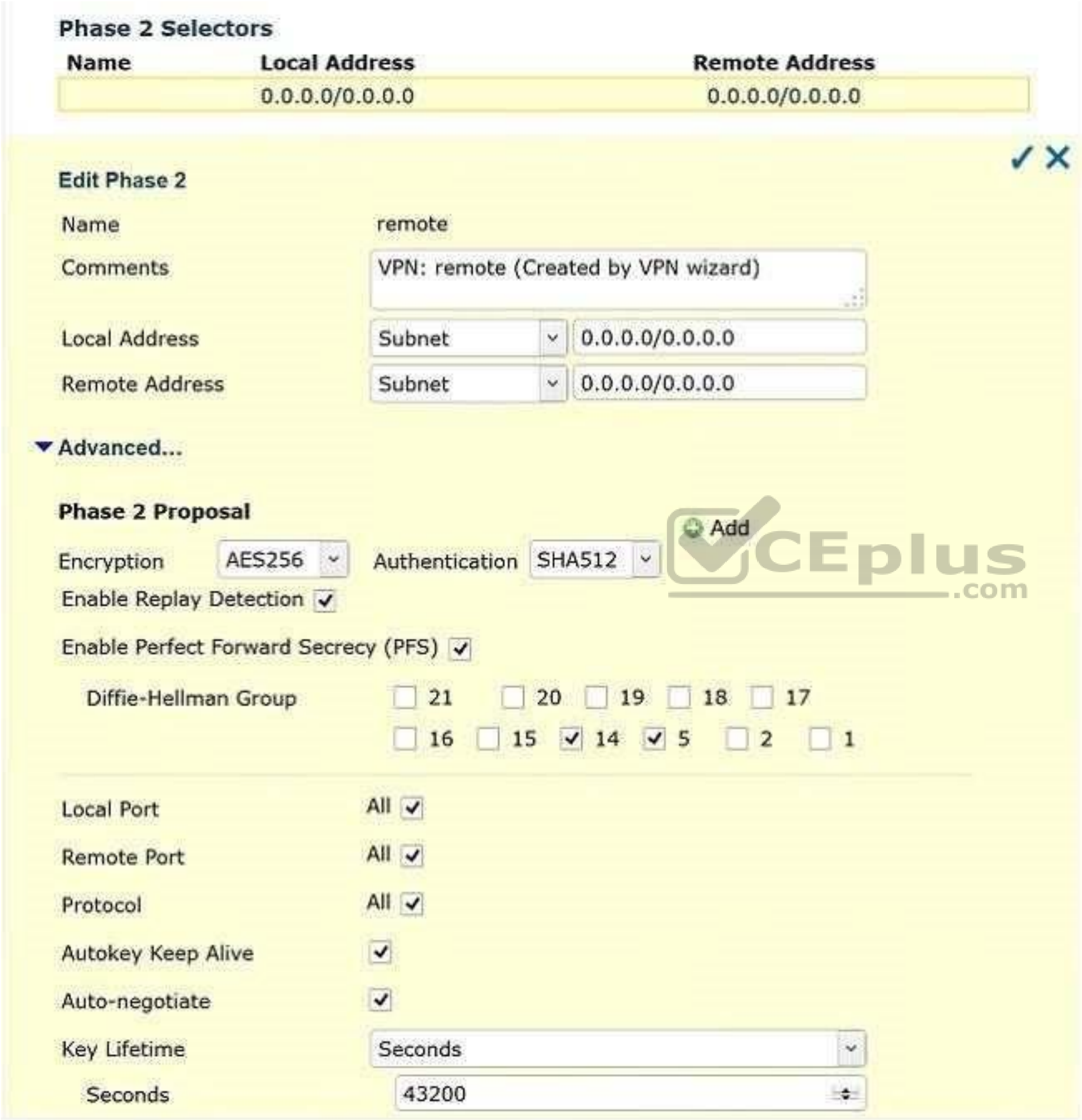
Which of the following statements is correct regarding this output? (Select one answer).

A. One tunnel is rekeying.
B. Two tunnels are rekeying.
C. Two tunnels are up.
D. One tunnel is up.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.



**Phase 2 Selectors**

| Name | Local Address | Remote Address |
|---|---|---|
| | 0.0.0.0/0.0.0.0 | 0.0.0.0/0.0.0.0 |

✓ ✕

**Edit Phase 2**

| | |
|---|---|
| Name | remote |
| Comments | VPN: remote (Created by VPN wizard) |
| Local Address | Subnet 0.0.0.0/0.0.0.0 |
| Remote Address | Subnet 0.0.0.0/0.0.0.0 |

▼ Advanced...

**Phase 2 Proposal**

Add

Encryption AES256 Authentication SHA512

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) ☑

Diffie-Hellman Group ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17
☐ 16 ☐ 15 ☑ 14 ☑ 5 ☐ 2 ☐ 1

| | |
|---|---|
| Local Port | All ☑ |
| Remote Port | All ☑ |
| Protocol | All ☑ |
| Autokey Keep Alive | ☑ |
| Auto-negotiate | ☑ |
| Key Lifetime | Seconds |
| Seconds | 43200 |

Which statements are correct regarding this configuration? (Choose two.).

A. The Phase 2 will re-key even if there is no traffic.
B. There will be a DH exchange for each re-key.
C. The sequence number of ESP packets received from the peer will not be checked.
D. Quick mode selectors will default to those used in the firewall policy.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

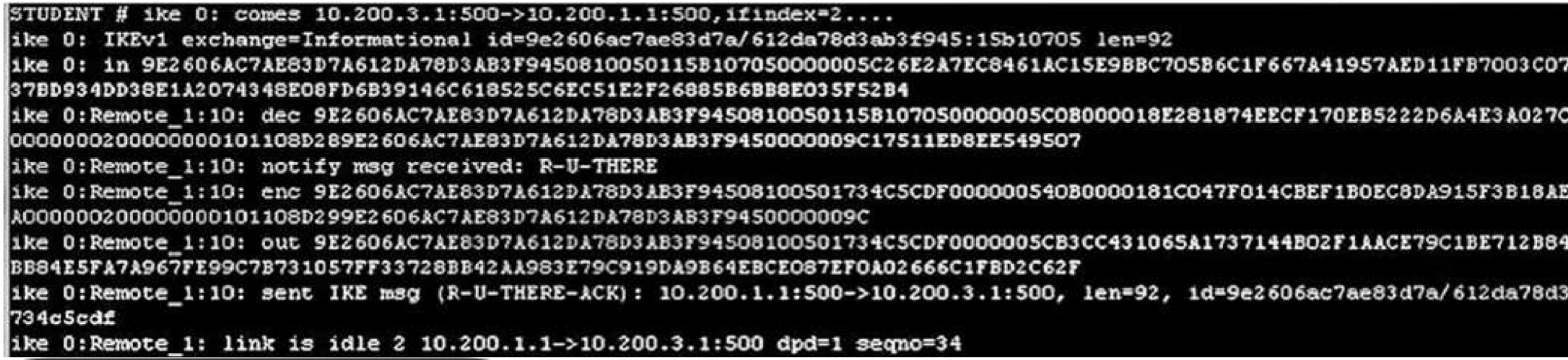
**QUESTION 44**
Which statement is an advantage of using a hub and spoke IPsec VPN configuration instead of a fully-meshed set of IPsec tunnels?

A. Using a hub and spoke topology provides full redundancy.
B. Using a hub and spoke topology requires fewer tunnels.
C. Using a hub and spoke topology uses stronger encryption protocols.
D. Using a hub and spoke topology requires more routes.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 45**
Review the IKE debug output for IPsec shown in the exhibit below.
Which statements is correct regarding this output?



```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07
37BD934DD38E1A2074348E08FD6B39146C618525C6EC51E2F26885B6BB8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C08000018E281874EECF170EB5222D6A4E3A027C
000000020000000010110 8D289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540B0000181C047F014CBEF1B0EC8DA915F3B18AE
A00000020000000010110 8D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AACE79C1BE712B84
BB84E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBCE087EF0A02666C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

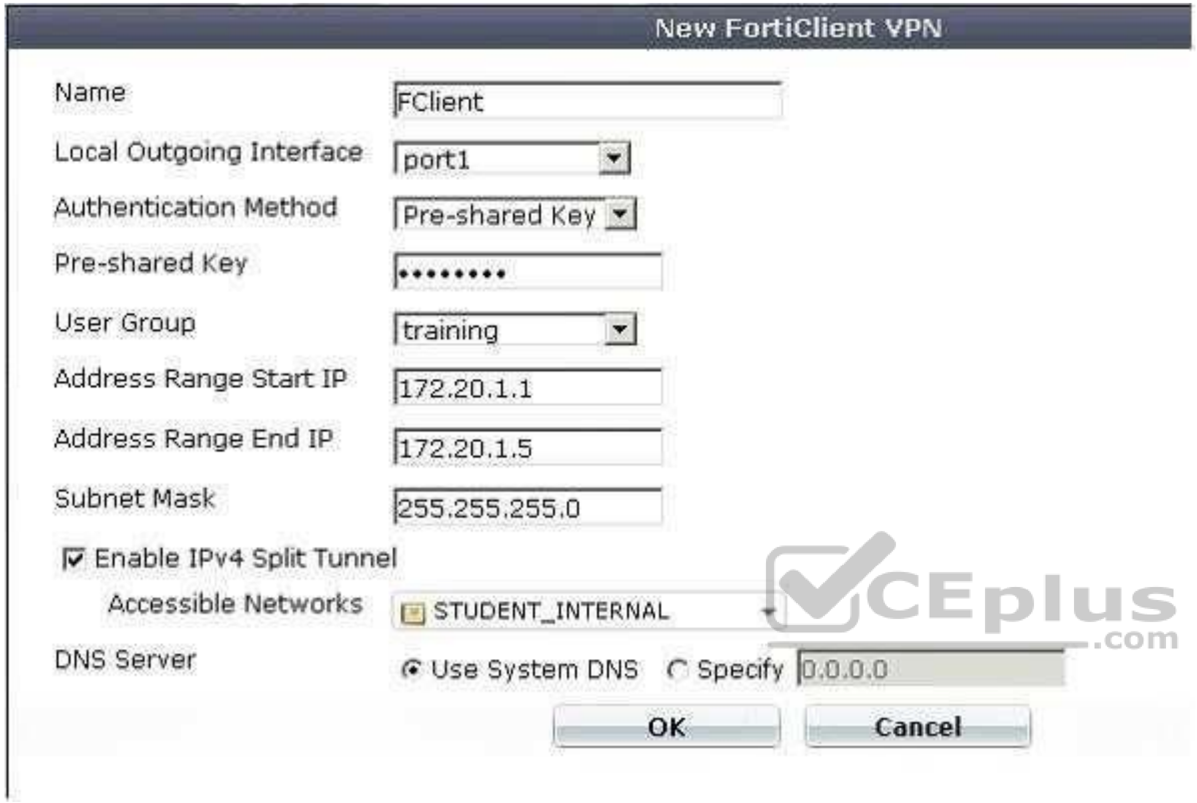
A. The output is a phase 1 negotiation.
B. The output is a phase 2 negotiation.
C. The output captures the dead peer detection messages.
D. The output captures the dead gateway detection packets.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 46**

Review the configuration for FortiClient IPsec shown in the exhibit.



New FortiClient VPN

| | |
|---|---|
| Name | FClient |
| Local Outgoing Interface | port1 |
| Authentication Method | Pre-shared Key |
| Pre-shared Key | •••••••• |
| User Group | training |
| Address Range Start IP | 172.20.1.1 |
| Address Range End IP | 172.20.1.5 |
| Subnet Mask | 255.255.255.0 |
| ☑ Enable IPv4 Split Tunnel | |
| Accessible Networks | STUDENT_INTERNAL |
| DNS Server | ● Use System DNS ○ Specify 0.0.0.0 |

Which statement is correct regarding this configuration?

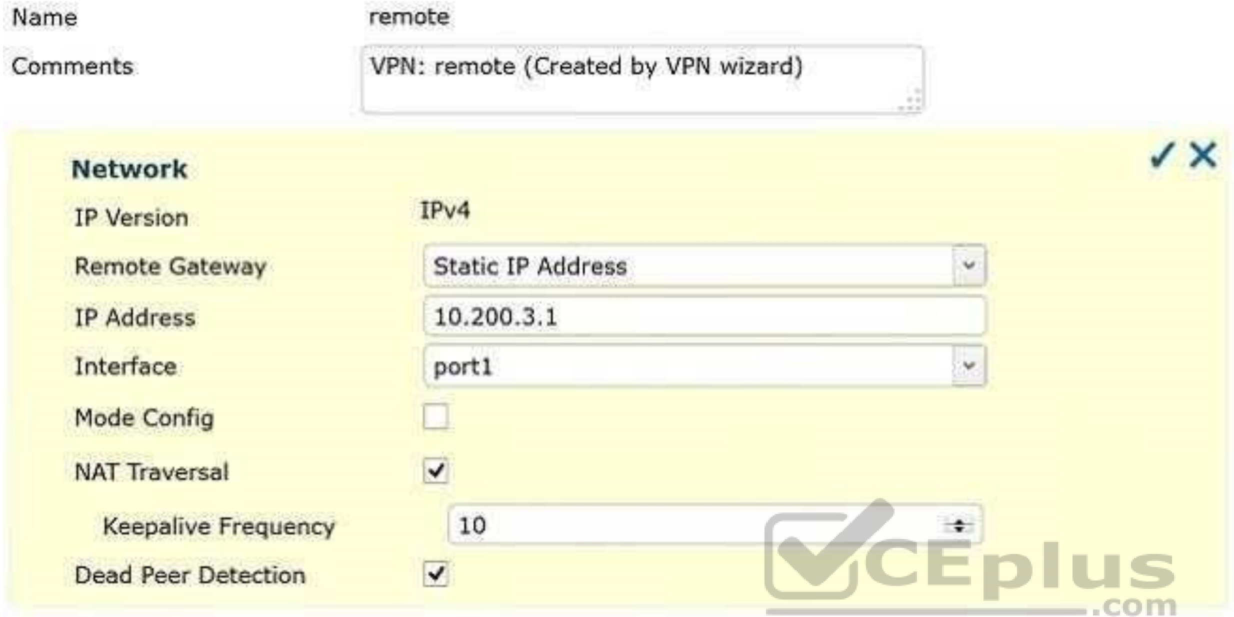
A. The connecting VPN client will install a route to a destination corresponding to the student_internal address object.
B. The connecting VPN client will install a default route.
C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range.
D. The connecting VPN client will connect in web portal mode and no route will be installed.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 47**

Review the IPsec phase 1 configuration in the exhibit; then answer the question below.



| | |
|---|---|
| Name | remote |
| Comments | VPN: remote (Created by VPN wizard) |

**Network**

| | |
|---|---|
| IP Version | IPv4 |
| Remote Gateway | Static IP Address |
| IP Address | 10.200.3.1 |
| Interface | port1 |
| Mode Config | □ |
| NAT Traversal | ☑ |
| Keepalive Frequency | 10 |
| Dead Peer Detection | ☑ |

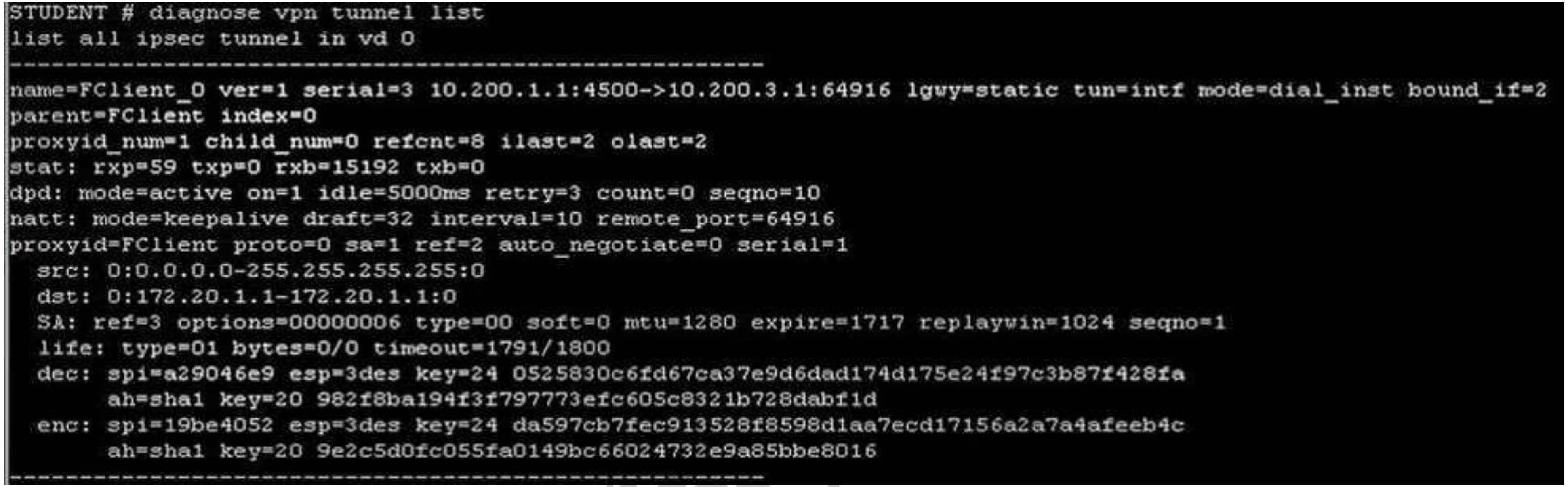
Which statements are correct regarding this configuration? (Choose two.)

A. The remote gateway address on 10.200.3.1.
B. The local IPsec interface address is 10.200.3.1.
C. The local gateway IP is the address assigned to port1.
D. The local gateway IP address is 10.200.3.1.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 48**

Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit below.



```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=FClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_inst bound_if=2
parent=FClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 olast=2
stat: rxp=59 txp=0 rxb=15192 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=10
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=FClient proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:172.20.1.1-172.20.1.1:0
  SA: ref=3 options=00000006 type=00 soft=0 mtu=1280 expire=1717 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1791/1800
  dec: spi=a29046e9 esp=3des key=24 0525830c6fd67ca37e9d6dad174d175e24f97c3b87f428fa
       ah=sha1 key=20 982f8ba194f3f797773efc605c8321b728dabf1d
  enc: spi=19be4052 esp=3des key=24 da597cb7fec913528f8598d1aa7ecd17156a2a7a4afeeb4c
       ah=sha1 key=20 9e2c5d0fc055fa0149bc66024732e9a85bbe8016
------------------------------------------------------
```

Which statements are correct regarding this output? (Choose two.)

A. The connecting client has been allocated address 172.20.1.1.
B. In the Phase 1 settings, dead peer detection is enabled.
C. The tunnel is idle.
D. The connecting client has been allocated address 10.200.3.1.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 49**
Which IPsec mode includes the peer id information in the first packet?

A. Main mode.

B. Quick mode.
C. Aggressive mode.
D. IKEv2 mode.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

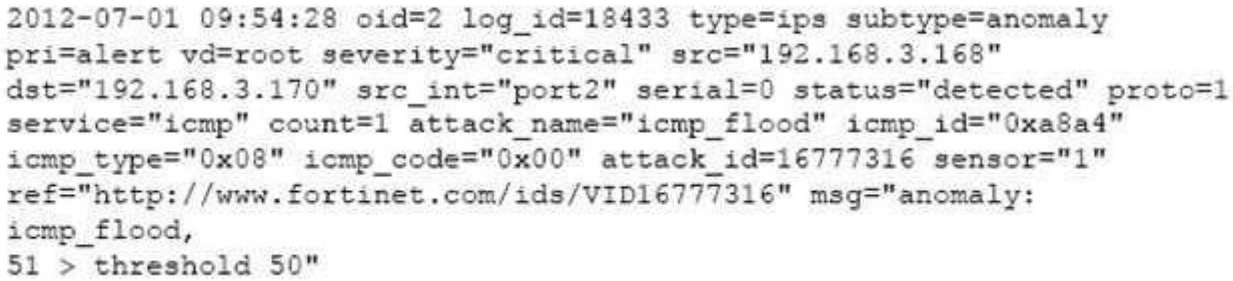
**QUESTION 50**
Which statements are correct properties of a partial mesh VPN deployment. (Choose two.)

A. VPN tunnels interconnect between every single location.
B. VPN tunnels are not configured between every single location.
C. Some locations are reached via a hub location.
D. There are no hub locations in a partial mesh.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 51**
Examine the following log message for IPS and identify the valid responses below. (Select all that apply.)



```
2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly
pri=alert vd=root severity="critical" src="192.168.3.168"
dst="192.168.3.170" src_int="port2" serial=0 status="detected" proto=1
service="icmp" count=1 attack_name="icmp_flood" icmp_id="0xa8a4"
icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1"
ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly:
icmp_flood,
51 > threshold 50"
```

A. The target is 192.168.3.168.
B. The target is 192.168.3.170.
C. The attack was detected and blocked.
D. The attack was detected only.
E. The attack was TCP based.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

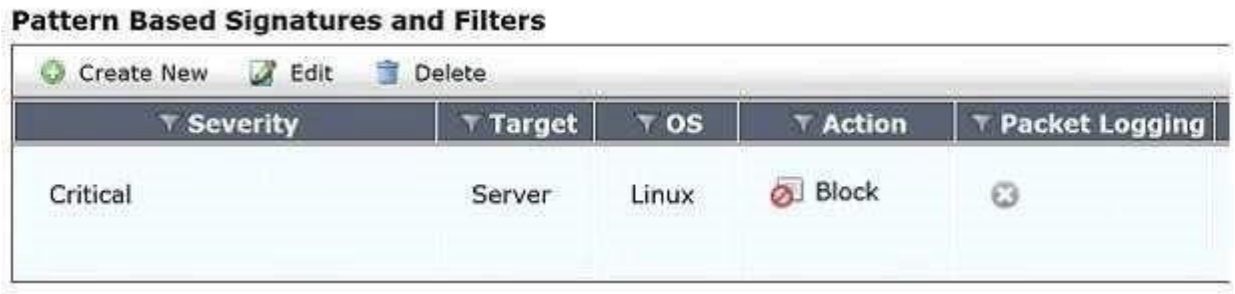
**QUESTION 52**
Identify the statement which correctly describes the output of the following command:

```
diagnose ips anomaly list
```

A. Lists the configured DoS policy.
B. List the real-time counters for the configured DoS policy. C. Lists the errors captured when compiling the DoS policy.
D. Lists the IPS signature matches.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 53**
Review the IPS sensor filter configuration shown in the exhibit



Pattern Based Signatures and Filters

| Severity | Target | OS | Action | Packet Logging |
|---|---|---|---|---|
| Critical | Server | Linux | Block | ⊗ |

Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

A. It does not log attacks targeting Linux servers.
B. It matches all traffic to Linux servers.
C. Its action will block traffic matching these signatures.
D. It only takes effect when the sensor is applied to a policy.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 54**
Which is the following statement are true regarding application control? (choose two)

A. Application control is based on TCP destination port numbers.
B. Application control is proxy based.
C. Encrypted traffic can be identified by application control.
D. Traffic Shaping can be applied to the detected application traffic.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 55**

FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory. Which of the following statements are correct regarding FSSO in a Windows domain environment when agent mode is used? (Choose two.)

A. An FSSO collector agent must be installed on every domain controller.
B. An FSSO domain controller agent must be installed on every domain controller.
C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.
D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 56**

Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode?

A. It requires a DC agent installed in some of the Windows DC.
B. It runs slower.
C. It might miss some logon events.
D. It requires access to a DNS server for workstation name resolution.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 57**

Which are two requirements for DC-agent mode FSSO to work properly in a Windows AD environment? (Choose two.)
A. DNS server must properly resolve all workstation names.
B. The remote registry service must be running in all workstations.
C. The collector agent must be installed in one of the Windows domain controllers.
D. A same user cannot be logged in into two different workstations at the same time.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 58**
Which statement describes what the CLI command diagnose debug authd fsso list is used for

A. Monitors communications between the FSSO collector agent and FortiGate unit.
B. Displays which users are currently logged on using FSSO.
C. Displays a listing of all connected FSSO collector agents.
D. Lists all DC Agents installed on all domain controllers.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 59**
When the SSL proxy is NOT doing man-in-the-middle interception of SSL traffic, which certificate field can be used to determine the rating of a website?

A. Organizational Unit.
B. Common Name.
C. Serial Number.
D. Validity.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 60**
Which tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Choose two.)

A. The web client SSL handshake.
B. The web server SSL handshake.
C. File buffering.
D. Communication with the URL filter process.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 61**
Bob wants to send Alice a file that is encrypted using public key cryptography.
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.
B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file
C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.
D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 62**
Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of sensitive data? (Select all that apply.)
A. Archive non-compliant outgoing e-mails using FortiMail.
B. Restrict unofficial methods of transferring files such as P2P using Application Control lists on a FortiGate.
C. Monitor database activity using FortiAnalyzer.
D. Apply a DLP sensor to a firewall policy.
E. Configure FortiClient to prevent files flagged as sensitive from being copied to a USB disk.

**Correct Answer:** ABD

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 63**
For data leak prevention, which statement describes the difference between the block and quarantine actions?

A. A block action prevents the transaction.
A quarantine action blocks all future transactions, regardless of the protocol.
B. A block action prevents the transaction. A quarantine action archives the data.
C. A block action has a finite duration.
A quarantine action must be removed by an administrator.
D. A block action is used for known users.
A quarantine action is used for unknown users.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 64**
In which process states is it impossible to interrupt/kill a process? (Choose two.)

A. S-Sleep
B. R-Running
C. D-Uninterruptable Sleep
D. Z-Zombie

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 65**

Which statements about virtual domains (VDOMs) are true? (Choose two.)

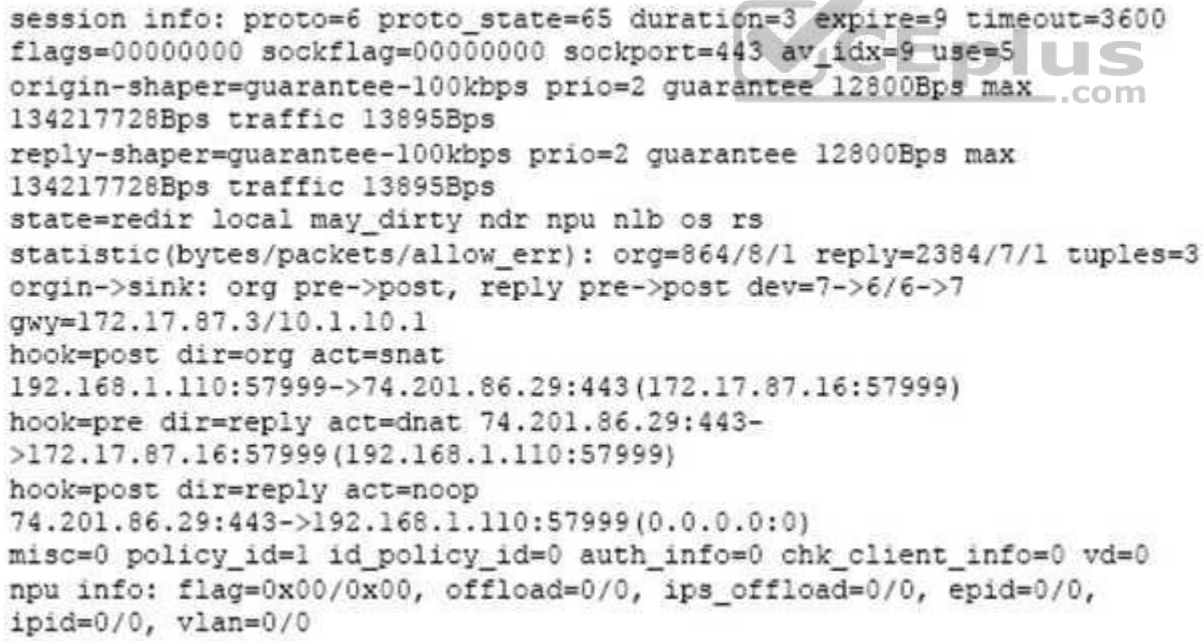
A. Transparent mode and NAT/Route mode VDOMs cannot be combined on the same FortiGate.
B. Each VDOM can be configured with different system hostnames.
C. Different VLAN sub-interfaces of the same physical interface can be assigned to different VDOMs.
D. Each VDOM has its own routing table.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 66**

Examine the following output from the diagnose sys session list command:



```
session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600
flags=00000000 sockflag=00000000 sockport=443 av_idx=9 use=5
origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max
134217728Bps traffic 13895Bps
reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max
134217728Bps traffic 13895Bps
state=redir local may_dirty ndr npu nlb os rs
statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7
gwy=172.17.87.3/10.1.10.1
hook=post dir=org act=snat
192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)
hook=pre dir=reply act=dnat 74.201.86.29:443-
>172.17.87.16:57999(192.168.1.110:57999)
hook=post dir=reply act=noop
74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0,
ipid=0/0, vlan=0/0
```

Which statements are true regarding the session above? (Choose two.)

https://vceplus.com/

A. Session Time-To-Live (TTL) was configured to 9 seconds.
B. FortiGate is doing NAT of both the source and destination IP addresses on all packets coming from the 192.168.1.110 address.
C. The IP address 192.168.1.110 is being translated to 172.17.87.16.
D. The FortiGate is not translating the TCP port numbers of the packets in this session.

**Correct Answer:** CD
**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 67**
Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

A. The source quick mode selector must be an IPv4 address.
B. The destination quick mode selector must be an IPv6 address.
C. The Local Gateway IP must be an IPv4 address.
D. The remote gateway IP must be an IPv6 address.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 68**

Which statements are true regarding IPv6 anycast addresses? (Choose two.)

A. Multiple interfaces can share the same anycast address.
B. They are allocated from the multicast address space.
C. Different nodes cannot share the same anycast address.
D. An anycast packet is routed to the nearest interface.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 69**
What functions can the IPv6 Neighbor Discovery protocol accomplish? (Choose two.)

A. Negotiate the encryption parameters to use.
B. Auto-adjust the MTU setting.
C. Autoconfigure addresses and prefixes.
D. Determine other nodes reachability.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 70**
Which is one of the conditions that must be met for offloading the encryption and decryption of IPsec traffic to an NP6 processor?

A. No protection profile can be applied over the IPsec traffic.
B. Phase-2 anti-replay must be disabled.
C. Both the phase 1 and phases 2 must use encryption algorithms supported by the NP6.
D. IPsec traffic must not be inspected by any FortiGate session helper.

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 71**
Which statements are true about offloading antivirus inspection to a Security Processor (SP)? (Choose two.)

A. Both proxy-based and flow-based inspection are supported.
B. A replacement message cannot be presented to users when a virus has been detected.
C. It saves CPU resources.
D. The ingress and egress interfaces can be in different SPs.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 72**
Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.)

A. Fragmented packet.
B. Multicast packet.C. SCTP packet
D. GRE packet.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 73**
Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

A. They are accelerated by hardware in the master unit.
B. They are not accelerated by hardware in the master unit.

C. They are accelerated by hardware in the slave unit.
D. They are not accelerated by hardware in the slave unit.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 74**
How is the FortiGate password recovery process?

A. Interrupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.
B. Log in through the console port using the "maintainer" account within several seconds of physically power cycling the FortiGate.
C. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.
D. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 75**
What are valid options for handling DNS requests sent directly to a FortiGates interface IP? (Choose three.)

A. Conditional-forward.
B. Forward-only.
C. Non-recursive.
D. Iterative.
E. Recursive.

**Correct Answer:** BCE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 76**

When creating FortiGate administrative users, which configuration objects specify the account rights?

A. Remote access profiles.
B. User groups.
C. Administrator profiles.
D. Local-in policies.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 77**

Which statements are true regarding the factory default configuration? (Choose three.)

A. The default web filtering profile is applied to the first firewall policy.
B. The `Port1' or `Internal' interface has the IP address 192.168.1.99.
C. The implicit firewall policy action is ACCEPT.
D. The `Port1' or `Internal' interface has a DHCP server set up and enabled (on device models that support DHCP servers).
E. Default login uses the username: admin (all lowercase) and no password.

**Correct Answer:** BDE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 78**

What methods can be used to access the FortiGate CLI? (Choose two.)

A. Using SNMP.
B. A direct connection to the serial console port.
C. Using the CLI console widget in the GUI.
D. Using RCP.

**Correct Answer:** BC

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 79**
What capabilities can a FortiGate provide? (Choose three.)

A. Mail relay.
B. Email filtering.
C. Firewall.
D. VPN gateway.
E. Mail server.

**Correct Answer:** BCD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 80**
Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

A. SNMP
B. WINS
C. HTTP
D. Telnet
E. SSH

**Correct Answer:** CDE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 81**
Which is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying a FortiGate unit?

A. MIB-based report uploads.
B. SNMP access limited by access lists.
C. Packet encryption.
D. Running SNMP service on a non-standard port is possible.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 82**
What logging options are supported on a FortiGate unit? (Choose two.)

A. LDAP
B. Syslog
C. FortiAnalyzer
D. SNMP

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 83**
What is the maximum number of FortiAnalyzer/FortiManager devices a FortiGate unit can be configured to send logs to?

A. 1
B. 2
C. 3
D. 4

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

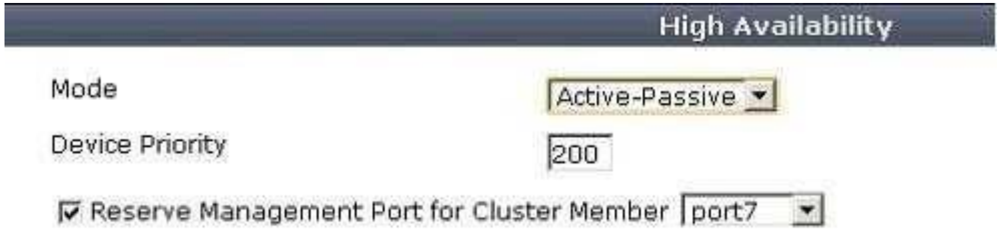
**QUESTION 84**
Regarding the header and body sections in raw log messages, which statement is correct?

A. The header and body section layouts change depending on the log type.
B. The header section layout is always the same regardless of the log type. The body section layout changes depending on the log type.
C. Some log types include multiple body sections.
D. Some log types do not include a body section.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 85**
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.



High Availability

Mode: Active-Passive

Device Priority: 200

☑ Reserve Management Port for Cluster Member: port7

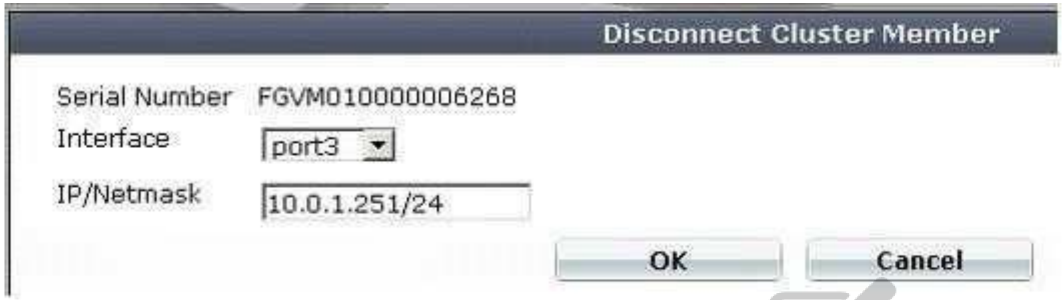
Which statements are correct regarding this setting? (Choose two.)

A. Interface settings on port7 will not be synchronized with other cluster members.
B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.
C. When connecting to port7 you always connect to the master device.
D. A gateway address may be configured for port7.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 86**
The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA members.



Disconnect Cluster Member

Serial Number FGVM010000006268
Interface port3
IP/Netmask 10.0.1.251/24

What is the effect of the Disconnect Cluster Member command as given in the exhibit. (Choose two.)

A. Port3 is configured with an IP address for management access.
B. The firewall rules are purged on the disconnected unit.
C. The HA mode changes to standalone.
D. The system hostname is set to the unit serial number.

**Correct Answer:** AC
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 87**
Which firewall objects can be included in the Destination Address field of a firewall policy? (Choose three.)

A. IP address pool.
B. Virtual IP address.
C. IP address.
D. IP address group.
E. MAC address

**Correct Answer:** BCD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 88**
In an IPSec gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks. Which of the following configuration steps must be performed on both FortiGate units to support this configuration? (Select all that apply.)

A. Create firewall policies to control traffic between the IP source and destination address.
B. Configure the appropriate user groups on the FortiGate units to allow users access to the IPSec VPN connection.
C. Set the operating mode of the FortiGate unit to IPSec VPN mode.
D. Define the Phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with the remote peer.
E. Define the Phase 1 parameters that the FortiGate unit needs to authenticate the remote peers.

**Correct Answer:** ADE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

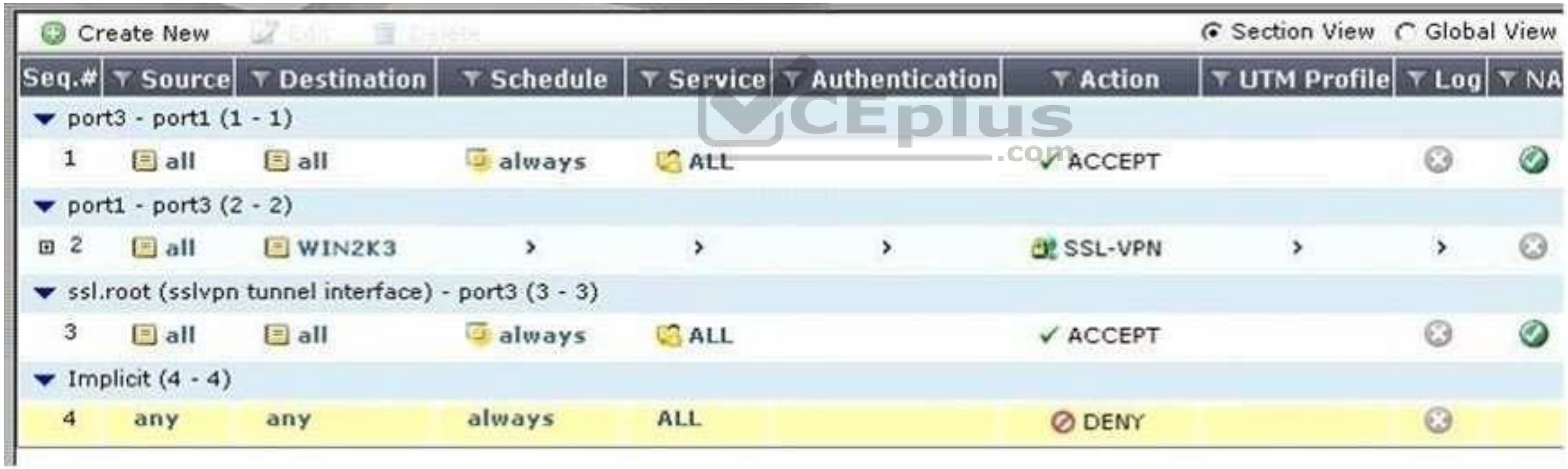
**QUESTION 89**

How is traffic routed onto an SSL VPN tunnel from the FortiGate unit side?

A. A static route must be configured by the administrator using the ssl.root interface as the outgoing interface.
B. Assignment of an IP address to the client causes a host route to be added to the FortiGate unit's kernel routing table.
C. A route back to the SSLVPN IP pool is automatically created on the FortiGate unit.
D. The FortiGate unit adds a route based upon the destination address in the SSL VPN firewall policy.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 90**
An end user logs into the full-access SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has enabled split tunneling.



| Seq.# | Source | Destination | Schedule | Service | Authentication | Action | UTM Profile | Log | NA |
|---|---|---|---|---|---|---|---|---|---|
| port3 - port1 (1 - 1) | | | | | | | | | |
| 1 | all | all | always | ALL | | ✓ ACCEPT | | ⊗ | ✓ |
| port1 - port3 (2 - 2) | | | | | | | | | |
| ⊞ 2 | all | WIN2K3 | › | › | › | SSL-VPN | › | › | ⊗ |
| ssl.root (sslvpn tunnel interface) - port3 (3 - 3) | | | | | | | | | |
| 3 | all | all | always | ALL | | ✓ ACCEPT | | ⊗ | ✓ |
| Implicit (4 - 4) | | | | | | | | | |
| 4 | any | any | always | ALL | | ⊘ DENY | | ⊗ | |

Given that the user authenticates against the SSL VPN policy shown in the image below, which statement below identifies the route that is added to the client's routing table.

A. A route to destination matching the `WIN2K3' address object.
B. A route to the destination matching the `all' address object.
C. A default route.

D. No route is added.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 91**
Which of the following antivirus and attack definition update options are supported by FortiGate units? (Select all that apply.)

A. Manual update by downloading the signatures from the support site.
B. Pull updates from the FortiGate device
C. Push updates from the FortiGuard Distribution Network.
D. "update-AV/AS" command from the CLI

**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 92**
A FortiGate AntiVirus profile can be configured to scan for viruses on SMTP, FTP, POP3, and SMB protocols using which inspection mode?

A. Proxy
B. DNS
C. Flow-based
D. Man-in-the-middle

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 93**
Which of the following items does NOT support the Logging feature?

A. File Filter
B. Application control
C. Session timeouts
D. Administrator activities
E. Web URL filtering

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 94**
Which of the following is true regarding Switch Port Mode?

A. Allows all internal ports to share the same subnet.
B. Provides separate routable interfaces for each internal port.
C. An administrator can select ports to be used as a switch.
D. Configures ports to be part of the same broadcast domain.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 95**
An administrator configures a FortiGate unit in Transparent mode on the 192.168.11.0 subnet. Automatic Discovery is enabled to detect any available FortiAnalyzers on the network.
Which of the following FortiAnalyzers will be detected? (Select all that apply.)

A. 192.168.11.100
B. 192.168.11.251
C. 192.168.10.100

D. 192.168.10.251

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 96**

Which of the following statements are correct regarding logging to memory on a FortiGate unit? (Select all that apply.)

A. When the system has reached its capacity for log messages, the FortiGate unit will stop logging to memory.
B. When the system has reached its capacity for log messages, the FortiGate unit overwrites the oldest messages.
C. If the FortiGate unit is reset or loses power, log entries captured to memory will be lost.
D. None of the above.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 97**

Which of the following spam filtering methods are supported on the FortiGate unit? (Select all that apply.)

A. IP Address Check
B. Open Relay Database List (ORDBL)
C. Black/White List
D. Return Email DNS Check
E. Email Checksum Check

**Correct Answer:** ABCDE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 98**

Which of the following email spam filtering features is NOT supported on a FortiGate unit?

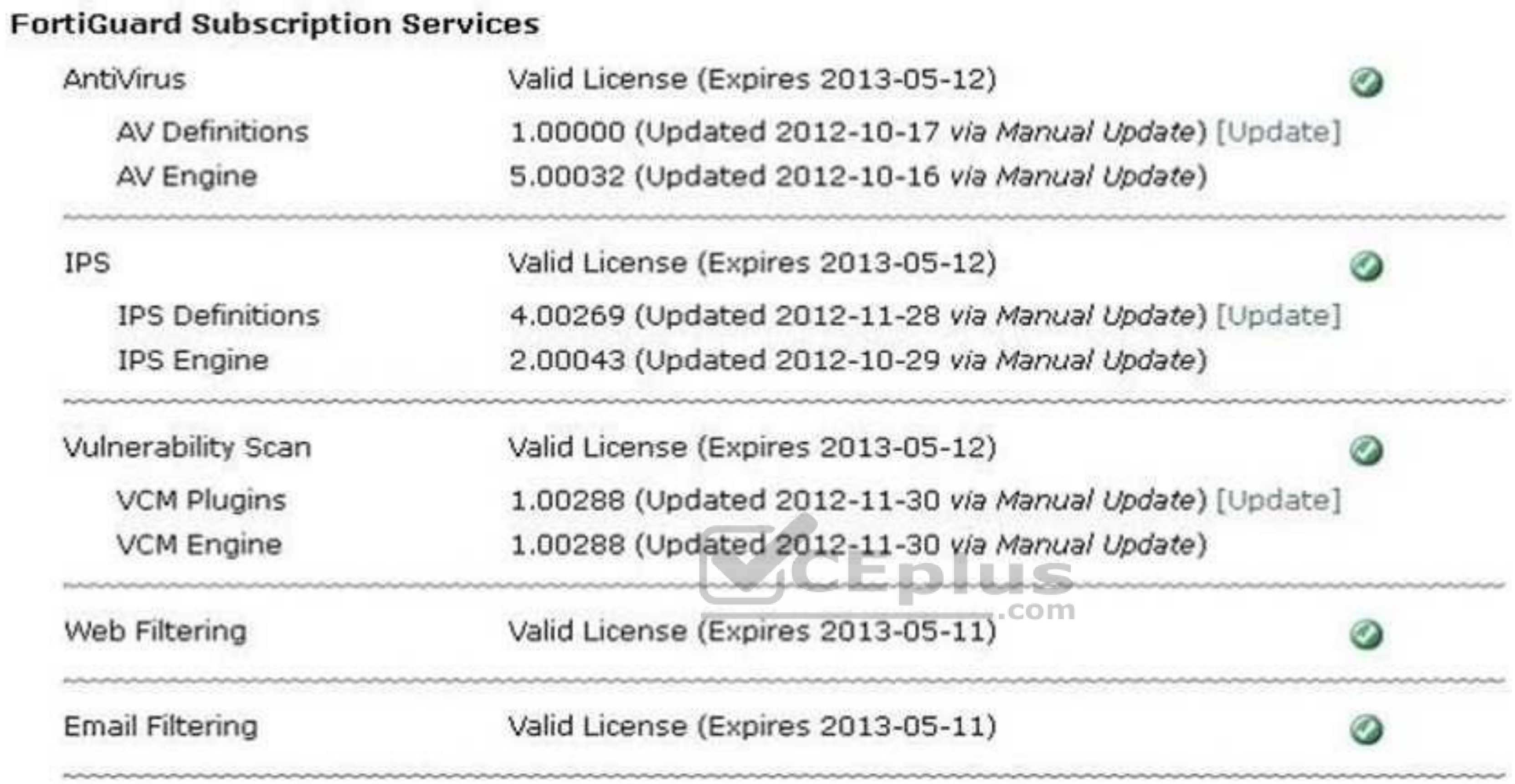
A. Multipurpose Internet Mail Extensions (MIME) Header Check
B. HELO DNS Lookup
C. Greylisting
D. Banned Word

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 99**

Examine the exhibit shown below; then answer the question following it.



FortiGuard Subscription Services

| | | |
|---|---|---|
| AntiVirus | Valid License (Expires 2013-05-12) | ✓ |
| AV Definitions | 1.00000 (Updated 2012-10-17 *via Manual Update*) [Update] | |
| AV Engine | 5.00032 (Updated 2012-10-16 *via Manual Update*) | |
| IPS | Valid License (Expires 2013-05-12) | ✓ |
| IPS Definitions | 4.00269 (Updated 2012-11-28 *via Manual Update*) [Update] | |
| IPS Engine | 2.00043 (Updated 2012-10-29 *via Manual Update*) | |
| Vulnerability Scan | Valid License (Expires 2013-05-12) | ✓ |
| VCM Plugins | 1.00288 (Updated 2012-11-30 *via Manual Update*) [Update] | |
| VCM Engine | 1.00288 (Updated 2012-11-30 *via Manual Update*) | |
| Web Filtering | Valid License (Expires 2013-05-11) | ✓ |
| Email Filtering | Valid License (Expires 2013-05-11) | ✓ |

Which of the following statements best describes the green status indicators that appear next to the different FortiGuard Distribution Network services as illustrated in the exhibit?

A. They indicate that the FortiGate unit is able to connect to the FortiGuard Distribution Network.
B. They indicate that the FortiGate unit has the latest updates that are available from the FortiGuard Distribution Network.
C. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.
D. They indicate that the FortiGate unit is in the process of downloading updates from the FortiGuard Distribution Network.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 100**

A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received. Which of the following statements are possible reasons for this? (Select all that apply.)

A. The external facing interface of the FortiGate unit is configured to use DHCP.

B. The FortiGate unit has not been registered.

C. There is a NAT device between the FortiGate unit and the FortiGuard Distribution Network and no override push IP is configured.

D. The FortiGate unit is in Transparent mode which does not support push updates.

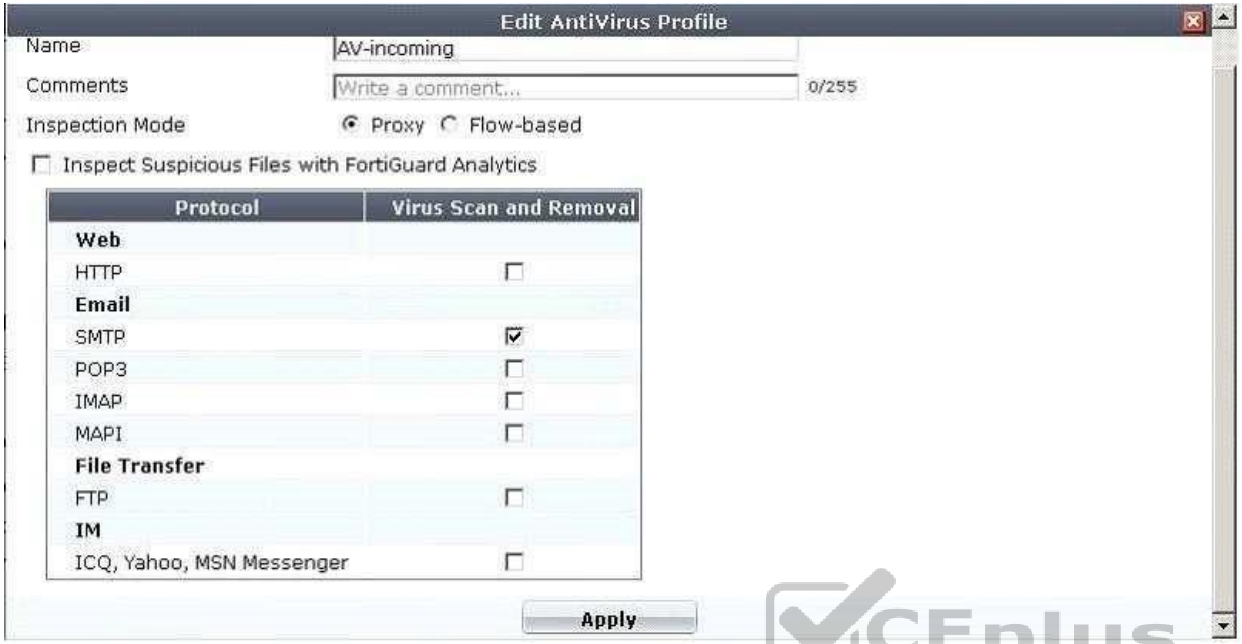
**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 101**

A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the antivirus and email filter profiles applied to this policy.

Exhibit A:

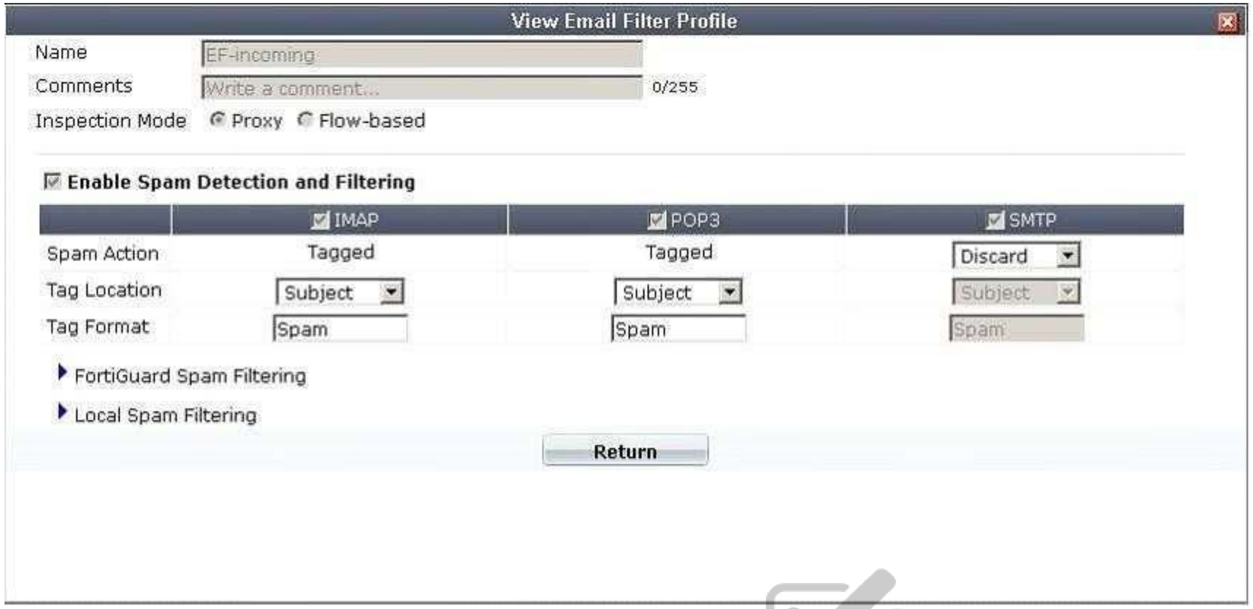


| | |
|---|---|
| Name | AV-incoming |
| Comments | Write a comment... 0/255 |
| Inspection Mode | ● Proxy ○ Flow-based |

□ Inspect Suspicious Files with FortiGuard Analytics

| Protocol | Virus Scan and Removal |
|---|---|
| **Web** | |
| HTTP | □ |
| **Email** | |
| SMTP | ☑ |
| POP3 | □ |
| IMAP | □ |
| MAPI | □ |
| **File Transfer** | |
| FTP | □ |
| **IM** | |
| ICQ, Yahoo, MSN Messenger | □ |

Exhibit B:



View Email Filter Profile

| | |
|---|---|
| Name | EF-incoming |
| Comments | Write a comment... 0/255 |
| Inspection Mode | ● Proxy ○ Flow-based |

☑ Enable Spam Detection and Filtering

| | ☑ IMAP | ☑ POP3 | ☑ SMTP |
|---|---|---|---|
| Spam Action | Tagged | Tagged | Discard |
| Tag Location | Subject | Subject | Subject |
| Tag Format | Spam | Spam | Spam |

What is the correct behavior when the email attachment is detected as a virus by the FortiGate antivirus engine?

A. The FortiGate unit will remove the infected file and deliver the email with a replacement message to alert the recipient that the original attachment was infected.
B. The FortiGate unit will reject the infected email and the sender will receive a failed delivery message.
C. The FortiGate unit will remove the infected file and add a replacement message. Both sender and recipient are notified that the infected file has been removed.
D. The FortiGate unit will reject the infected email and notify the sender.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 102**
Caching improves performance by reducing FortiGate unit requests to the FortiGuard server. Which of the following statements are correct regarding the caching of
FortiGuard responses? (Select all that apply.)

A. Caching is available for web filtering, antispam, and IPS requests.
B. The cache uses a small portion of the FortiGate system memory.
C. When the cache is full, the least recently used IP address or URL is deleted from the cache.
D. An administrator can configure the number of seconds to store information in the cache before the FortiGate unit contacts the FortiGuard server again.
E. The size of the cache will increase to accommodate any number of cached queries.

**Correct Answer:** BCD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 103**
Which of the following Fortinet products can receive updates from the FortiGuard Distribution Network? (Select all that apply.)

A. FortiGate
B. FortiClient
C. FortiMail
D. FortiAnalyzer

**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 104**
How can DLP file filters be configured to detect Office 2010 files? (Select all that apply.)

A. File TypE. Microsoft Office(msoffice)
B. File TypE. Archive(zip)
C. File TypE. Unknown Filetype(unknown)
D. File NamE. "*.ppt", "*.doc", "*.xls"
E. File NamE. "*.pptx", "*.docx", "*.xlsx"

**Correct Answer:** BE

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 105**
What are the valid sub-types for a Firewall type policy? (Select all that apply)

A. Device Identity
B. Address
C. User Identity
D. Schedule
E. SSL VPN

**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 106**
In NAT/Route mode when there is no matching firewall policy for traffic to be forwarded by the Firewall, which of the following statements describes the action taken on traffic?

A. The traffic is blocked.
B. The traffic is passed.
C. The traffic is passed and logged.
D. The traffic is blocked and logged.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 107**

In which order are firewall policies processed on the FortiGate unit?

A. They are processed from the top down according to their sequence number.
B. They are processed based on the policy ID number shown in the left hand column of the policy window.
C. They are processed on best match.
D. They are processed based on a priority value assigned through the priority column in the policy window.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 108**

Which of the following pieces of information can be included in the Destination Address field of a firewall policy? (Select all that apply.)

A. An IP address pool.
B. A virtual IP address.
C. An actual IP address or an IP address group.

D. An FQDN or Geographic value(s).

**Correct Answer:** BCD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 109**

The ordering of firewall policies is very important. Policies can be re-ordered within the FortiGate unit's GUI and also using the CLI. The command used in the CLI to perform this function is _________.

A. set order
B. edit policy
C. reorder
D. move

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 110**

You wish to create a firewall policy that applies only to traffic intended for your web server. The web server has an IP address of 192.168.2.2 and a /24 subnet mask. When defining the firewall address for use in this policy, which one of the following addresses is correct?

A. 192.168.2.0 / 255.255.255.0
B. 192.168.2.2 / 255.255.255.0
C. 192.168.2.0 / 255.255.255.255
D. 192.168.2.2 / 255.255.255.255

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 111**

A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

A. SSL
B. IPSec
C. direct serial connection
D. S/MIME

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 112**
Which of the following network protocols are supported for administrative access to a FortiGate unit?

A. HTTPS, HTTP, SSH, TELNET, PING, SNMP
B. FTP, HTTPS, NNTP, TCP, WINS
C. HTTP, NNTP, SMTP, DHCP
D. Telnet, FTP, RLOGIN, HTTP, HTTPS, DDNS
E. Telnet, UDP, NNTP, SMTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 113**
Which of the following statements is correct regarding a FortiGate unit operating in NAT/Route mode?

A. The FortiGate unit applies NAT to all traffic.
B. The FortiGate unit functions as a Layer 3 device.
C. The FortiGate unit functions as a Layer 2 device.
D. The FortiGate unit functions as a router and the firewall function is disabled.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 114**

A FortiGate unit can provide which of the following capabilities? (Select all that apply.)

A. Email filtering B.
Firewall

C. VPN gateway

D. Mail relay

E. Mail server

**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 115**

Which of the following methods can be used to access the CLI? (Select all that apply.)

A. By using a direct connection to a serial console.

B. By using the CLI console window in the GUI.

C. By using an SSH connection.

D. By using a Telnet connection.

**Correct Answer:** ABCD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 116**

When backing up the configuration file on a FortiGate unit, the contents can be encrypted by enabling the encrypt option and supplying a password. If the password is forgotten, the configuration file can still be restored using which of the following methods?

A. Selecting the recover password option during the restore process.

B. Having the password emailed to the administrative user by selecting the Forgot Password option.

C. Sending the configuration file to Fortinet Support for decryption.

D. If the password is forgotten, there is no way to use the file.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 117**

The FortiGate unit's GUI provides a link to update the firmware. Clicking this link will perform which of the following actions?

A. It will connect to the Fortinet Support site where the appropriate firmware version can be selected.
B. It will send a request to the FortiGuard Distribution Network so that the appropriate firmware version can be pushed down to the FortiGate unit.
C. It will present a prompt to allow browsing to the location of the firmware file.
D. It will automatically connect to the Fortinet Support site to download the most recent firmware version for the FortiGate unit.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 118**

Which of the following products is designed to manage multiple FortiGate devices?

A. FortiGate device
B. FortiAnalyzer device
C. FortiClient device
D. FortiManager device
E. FortiMail device
F. FortiBridge device

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 119**

Which of the following products provides dedicated hardware to analyze log data from multiple FortiGate devices?

A. FortiGate device
B. FortiAnalyzer device
C. FortiClient device
D. FortiManager device
E. FortiMail device
F. FortiBridge device

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 120**

Which of the following are valid FortiGate device interface methods for handling DNS requests? (Select all that apply.)

A. Forward-only
B. Non-recursive
C. Recursive
D. Iterative
E. Conditional-forward

**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 121**

The default administrator profile that is assigned to the default "admin" user on a FortGate device is: _______________.

A. trusted-admin
B. super_admin

C. super_user
D. admin
E. fortiner-root

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 122**
Which of the following logging options are supported on a FortiGate unit? (Select all that apply.)

A. LDAP
B. Syslog
C. FortiAnalyzer
D. Local disk and/or memory

**Correct Answer:** BCD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 123**
In order to match an identity-based policy, the FortiGate unit checks the IP information. Once inside the policy, the following logic is followed:

A. First, a check is performed to determine if the user's login credentials are valid. Next, the user is checked to determine if they belong to any of the groups defined for that policy. Finally, user restrictions are determined and port, time, and UTM profiles are applied.
B. First, user restrictions are determined and port, time, and UTM profiles are applied. Next, a check is performed to determine if the user's login credentials are valid. Finally, the user is checked to determine if they belong to any of the groups defined for that policy.
C. First, the user is checked to determine if they belong to any of the groups defined for that policy. Next, user restrictions are determined and port, time, and UTM profiles are applied. Finally, a check is performed to determine if the user's login credentials are valid.

**Correct Answer:** A

**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 124**
Which of the following statements regarding the firewall policy authentication timeout is true?

A. The authentication timeout is an idle timeout.
This means that the FortiGate unit will consider a user to be "idle" if it does not see any packets coming from the user's source IP.
B. The authentication timeout is a hard timeout.
This means that the FortiGate unit will remove the temporary policy for this user's source IP after this timer has expired.
C. The authentication timeout is an idle timeout.
This means that the FortiGate unit will consider a user to be "idle" if it does not see any packets coming from the user's source MAC.
D. The authentication timeout is a hard timeout.
This means that the FortiGate unit will remove the temporary policy for this user's source MAC after this timer has expired.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 125**
Two-factor authentication is supported using the following methods? (Select all that apply.)

A. FortiToken
B. Email
C. SMS phone message
D. Code books

**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 126**

Which of the following statements are true regarding Local User Authentication? (Select all that apply.)

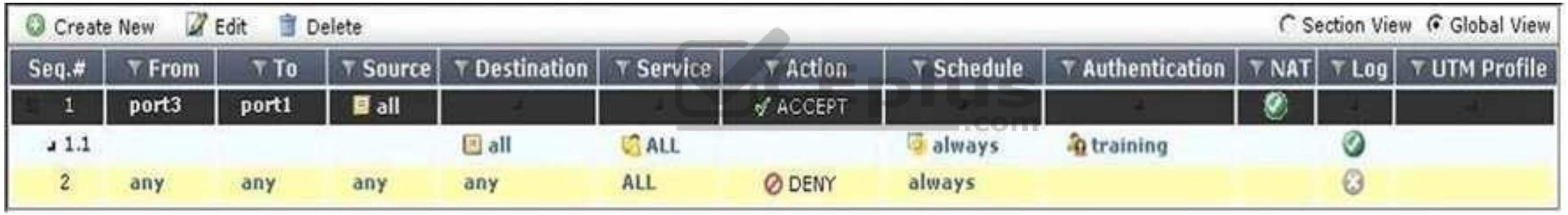
A. Local user authentication is based on usernames and passwords stored locally on the FortiGate unit.
B. Two-factor authentication can be enabled on a per user basis.
C. Administrators can create an account for the user locally and specify the remote server to verify the password.
D. Local users are for administration accounts only and cannot be used for identity policies.

**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 127**

Examine the firewall configuration shown below; then answer the question following it.



| Seq.# | From | To | Source | Destination | Service | Action | Schedule | Authentication | NAT | Log | UTM Profile |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | port3 | port1 | all | | | ACCEPT | | | ✓ | | |
| 1.1 | | | | all | ALL | | always | training | | ✓ | |
| 2 | any | any | any | any | ALL | DENY | always | | | ✗ | |

Which of the following statements are correct based on the firewall configuration illustrated in the exhibit? (Select all that apply.)

A. A user can access the Internet using only the protocols that are supported by user authentication.
B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP. These require authentication before the user will be allowed access.
C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services.
D. A user cannot access the Internet using any protocols unless the user has passed firewall authentication.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 128**

When browsing to an internal web server using a web-mode SSL VPN bookmark, from which of the following source IP addresses would the web server consider the HTTP request to be initiated?

A. The remote user's virtual IP address.
B. The FortiGate unit's internal IP address.
C. The remote user's public IP address.
D. The FortiGate unit's external IP address.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 129**

An issue could potentially occur when clicking Connect to start tunnel mode SSL VPN. The tunnel will start up for a few seconds, then shut down. Which of the following statements best describes how to resolve this issue?

A. This user does not have permission to enable tunnel mode.
Make sure that the tunnel mode widget has been added to that user's web portal.
B. This FortiGate unit may have multiple Internet connections.
To avoid this problem, use the appropriate CLI command to bind the SSL VPN connection to the original incoming interface.
C. Check the SSL adaptor on the host machine.
If necessary, uninstall and reinstall the adaptor from the tunnel mode portal.
D. Make sure that only Internet Explorer is used. All other browsers are unsupported.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 130**

You are the administrator in charge of a FortiGate unit which acts as a VPN gateway.

You have chosen to use Interface Mode when configuring the VPN tunnel and you want users from either side to be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate unit already has a default route.
Which of the following configuration steps are required to achieve these objectives? (Select all that apply.)

A. Create one firewall policy.
B. Create two firewall policies.

C. Add a route for the remote subnet.
D. Add a route for incoming traffic.
E. Create a phase 1 definition.
F. Create a phase 2 definition.

**Correct Answer:** BCEF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 131**
Which email filter is NOT available on a FortiGate device?

A. Sender IP reputation database.
B. URLs included in the body of known SPAM messages.
C. Email addresses included in the body of known SPAM messages.
D. Spam object checksums.
E. Spam grey listing.

**Correct Answer:** E

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 132**
A firewall policy has been configured such that traffic logging is disabled and a UTM function is enabled.
In addition, the system setting `utm-incident-traffic-log' has been enabled. In which log will a UTM event message be stored?

A. Traffic
B. UTM
C. System
D. None

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 133**
Which one of the following statements is correct about raw log messages?

A. Logs have a header and a body section.
The header will have the same layout for every log message.
The body section will change layout from one type of log message to another.
B. Logs have a header and a body section.
The header and body will change layout from one type of log message to another.
C. Logs have a header and a body section.
The header and body will have the same layout for every log message.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 134**
Which of the following is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying the FortiGate unit?

A. Packet encryption
B. MIB-based report uploads
C. SNMP access limits through access lists
D. Running SNMP service on a non-standard port is possible

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 135**
In which of the following report templates would you configure the charts to be included in the report?

A. Layout Template
B. Data Filter Template
C. Output Template
D. Schedule Template

**Correct Answer:** A
**Section: (none)**
**Explanation**

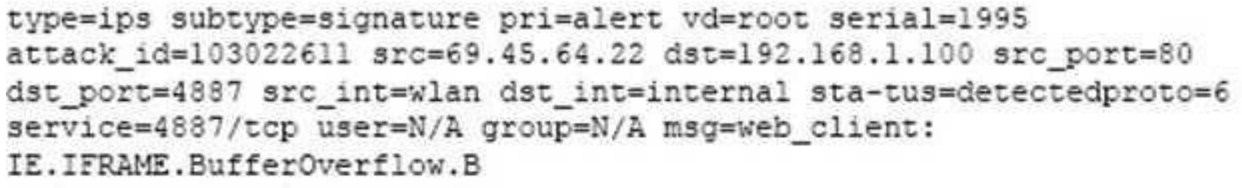
**Explanation/Reference:**

**QUESTION 136**
A DLP rule with an action of Exempt has been matched against traffic passing through the FortiGate unit. Which of the following statements is correct regarding how this transaction will be handled by the FortiGate unit?

A. Any other matched DLP rules will be ignored with the exception of Archiving.
B. Future files whose characteristics match this file will bypass DLP scanning.
C. The traffic matching the DLP rule will bypass antivirus scanning.
D. The client IP address will be added to a white list.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 137**
An administrator is examining the attack logs and notices the following entry:



```
type=ips subtype=signature pri=alert vd=root serial=1995
attack_id=103022611 src=69.45.64.22 dst=192.168.1.100 src_port=80
dst_port=4887 src_int=wlan dst_int=internal sta-tus=detectedproto=6
service=4887/tcp user=N/A group=N/A msg=web_client:
IE.IFRAME.BufferOverflow.B
```

Based on the information displayed in this entry, which of the following statements are correct? (Select all that apply.)

A. This is an HTTP server attack.
B. The attack was detected and blocked by the FortiGate unit.
C. The attack was against a FortiGate unit at the 192.168.1.100 IP address.
D. The attack was detected and passed by the FortiGate unit.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 138**
What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully- meshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a hub and spoke topology simplifies configuration.
C. Using a hub and spoke topology provides stronger encryption.
D. Using a hub and spoke topology reduces the number of tunnels.

**Correct Answer:** BD

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 139**

An administrator wishes to generate a report showing Top Traffic by service type. They notice that web traffic overwhelms the pie chart and want to exclude the web traffic from the report. Which of the following statements best describes how to do this?

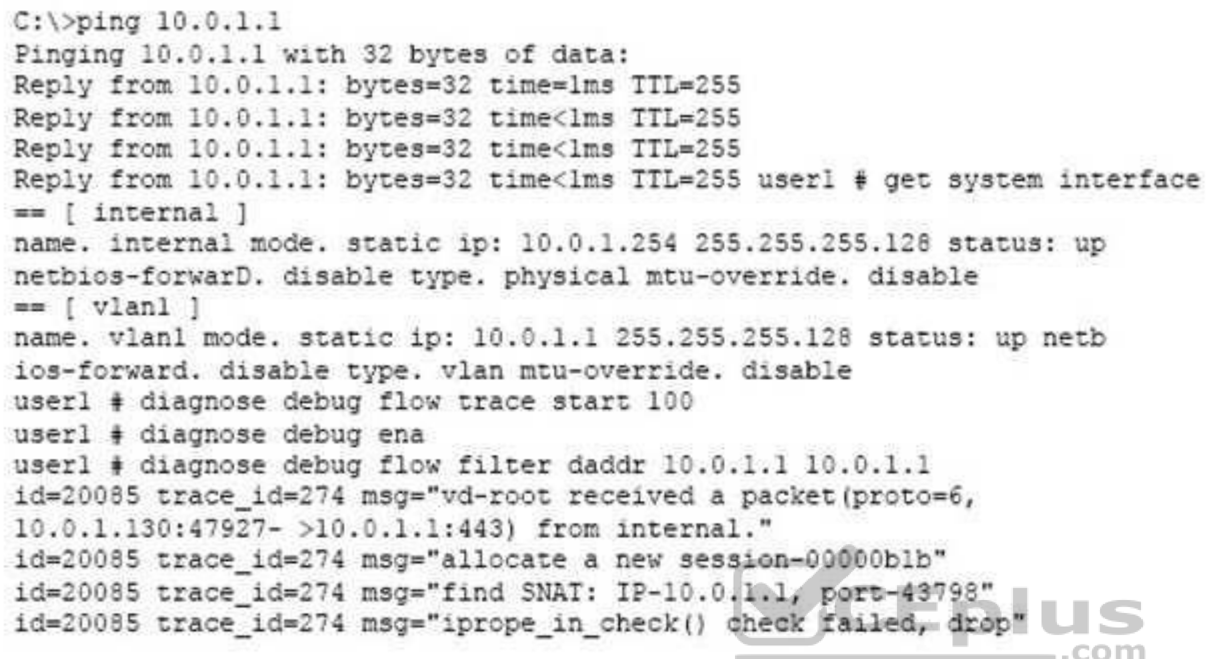
A. In the Service field of the Data Filter, type 80/tcp and select the NOT checkbox.
B. Add the following entry to the Generic Field section of the Data Filter: service="!web".
C. When editing the chart, uncheck wlog to indicate that Web Filtering data is being excluded when generating the chart.
D. When editing the chart, enter 'http' in the Exclude Service field.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 140**

A network administrator connects his PC to the INTERNAL interface on a FortiGate unit.
The administrator attempts to make an HTTPS connection to the FortiGate unit on the VLAN1 interface at the IP address of 10.0.1.1, but gets no connectivity.
The following troubleshooting commands are executed from the DOS prompt on the PC and from the CLI.



```
C:\>ping 10.0.1.1
Pinging 10.0.1.1 with 32 bytes of data:
Reply from 10.0.1.1: bytes=32 time=1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255 user1 # get system interface
== [ internal ]
name. internal mode. static ip: 10.0.1.254 255.255.255.128 status: up
netbios-forwarD. disable type. physical mtu-override. disable
== [ vlan1 ]
name. vlan1 mode. static ip: 10.0.1.1 255.255.255.128 status: up netb
ios-forward. disable type. vlan mtu-override. disable
user1 # diagnose debug flow trace start 100
user1 # diagnose debug ena
user1 # diagnose debug flow filter daddr 10.0.1.1 10.0.1.1
id=20085 trace_id=274 msg="vd-root received a packet(proto=6,
10.0.1.130:47927- >10.0.1.1:443) from internal."
id=20085 trace_id=274 msg="allocate a new session-00000b1b"
id=20085 trace_id=274 msg="find SNAT: IP-10.0.1.1, port-43798"
id=20085 trace_id=274 msg="iprope_in_check() check failed, drop"
```

Based on the output from these commands, which of the following explanations is a possible cause of the problem?

A. The Fortigate unit has no route back to the PC.
B. The PC has an IP address in the wrong subnet.
C. The PC is using an incorrect default gateway IP address.
D. The FortiGate unit does not have the HTTPS service configured on the VLAN1 interface.
E. There is no firewall policy allowing traffic from INTERNAL-> VLAN1.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 141**
Which of the following methods does the FortiGate unit use to determine the availability of a web cache using Web Cache Communication Protocol (WCCP)?

A. The FortiGate unit receives periodic "Here I am" messages from the web cache.
B. The FortiGate unit polls all globally-defined web cache servers at a regular intervals.
C. The FortiGate using uses the health check monitor to verify the availability of a web cache server.
D. The web cache sends an "I see you" message which is captured by the FortiGate unit.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 142**
A FortiGate unit is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root. Which of the following items would an administrator logging in using this account NOT be able to configure?

A. Firewall addresses
B. DHCP servers
C. FortiGuard Distribution Network configuration
D. PPTP VPN configuration

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 143**
Which of the following statements is correct regarding the antivirus scanning function on the FortiGate unit?

A. Antivirus scanning provides end-to-end virus protection for client workstations.
B. Antivirus scanning provides virus protection for the HTTP, Telnet, SMTP, and FTP protocols.
C. Antivirus scanning supports banned word checking.
D. Antivirus scanning supports grayware protection.

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

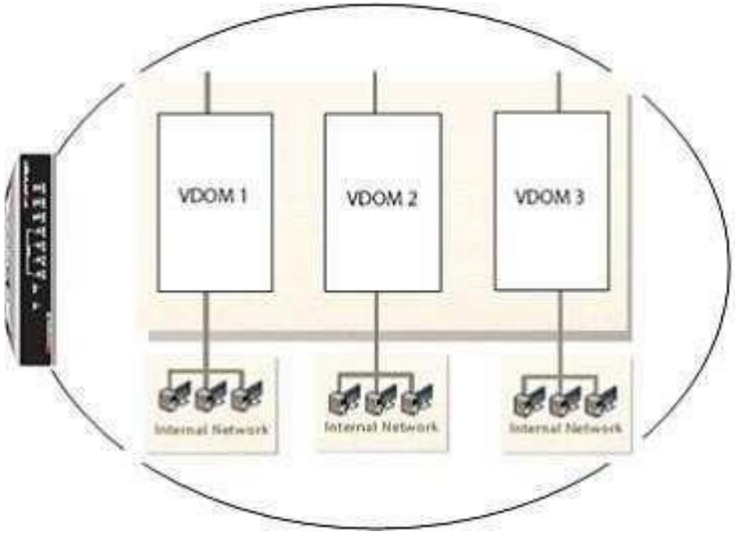
**QUESTION 144**
WAN optimization is configured in Active/Passive mode. When will the remote peer accept an attempt to initiate a tunnel?

A. The attempt will be accepted when the request comes from a known peer and there is a matching WAN optimization passive rule.
B. The attempt will be accepted when there is a matching WAN optimization passive rule.
C. The attempt will be accepted when the request comes from a known peer.
D. The attempt will be accepted when a user on the remote peer accepts the connection request.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 145**
A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



Which of the following statements are correct regarding these VDOMs? (Select all that apply.)

A. The FortiGate unit supports any combination of these VDOMs in NAT/Route and Transparent modes.
B. The FortiGate unit must be a model 1000 or above to support multiple VDOMs.
C. A license had to be purchased and applied to the FortiGate unit before VDOM mode could be enabled.
D. All VDOMs must operate in the same mode.
E. Changing a VDOM operational mode requires a reboot of the FortiGate unit.
F. An admin account can be assigned to one VDOM or it can have access to all three VDOMs.

**Correct Answer:** AF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

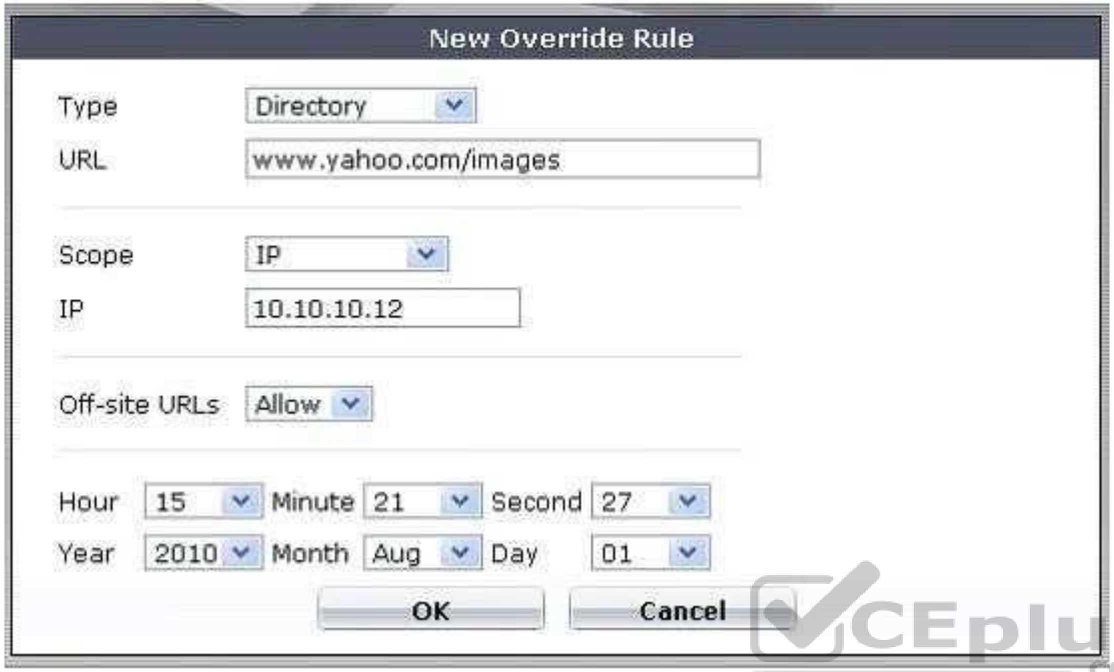
**QUESTION 146**
Both the FortiGate and FortiAnalyzer units can notify administrators when certain alert conditions are met.
Considering this, which of the following statements is NOT correct?

A. On a FortiGate device, the alert condition is based either on the severity level or on the log type, but not on a combination of the two.
B. On a FortiAnalyzer device, the alert condition is based either on the severity level or on the log type, but not on a combination of the two.
C. Only a FortiAnalyzer device can send the alert notification in the form of a syslog message.
D. Both the FortiGate and FortiAnalyzer devices can send alert notifications in the form of an email alert.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 147**
Which of the following statements is correct regarding the FortiGuard Services Web Filtering Override configuration as illustrated in the exhibit?



New Override Rule

Type: Directory

URL: www.yahoo.com/images

Scope: IP

IP: 10.10.10.12

Off-site URLs: Allow

Hour: 15 Minute: 21 Second: 27

Year: 2010 Month: Aug Day: 01

A. Any client on the same subnet as the authenticated user is allowed to access www.yahoo.com/images/.
B. A client with an IP of address 10.10.10.12 is allowed access to any subdirectory that is part of the www.yahoo.com web site.
C. A client with an IP address of 10.10.10.12 is allowed access to the www.yahoo.com/images/ web site and any of its offsite URLs.
D. A client with an IP address of 10.10.10.12 is allowed access to any URL under the www.yahoo.com web site, including any subdirectory URLs, until August 7, 2009.
E. Any client on the same subnet as the authenticated user is allowed to access www.yahoo.com/images/ until August 7, 2009.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 148**
SSL Proxy is used to decrypt the SSL-encrypted traffic. After decryption, where is the traffic buffered in preparation for content inspection?

A. The file is buffered by the application proxy.
B. The file is buffered by the SSL proxy.
C. In the upload direction, the file is buffered by the SSL proxy.
   In the download direction, the file is buffered by the application proxy.
D. No file buffering is needed since a stream-based scanning approach is used for SSL content inspection.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 149**
An administrator logs into a FortiGate unit using an account which has been assigned a super_admin profile. Which of the following operations can this administrator perform?

A. They can delete logged-in users who are also assigned the super_admin access profile.
B. They can make changes to the super_admin profile.
C. They can delete the admin account if the default admin user is not logged in.
D. They can view all the system configuration settings but can not make changes.
E. They can access configuration options for only the VDOMs to which they have been assigned.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 150**
Which of the following statements is correct about how the FortiGate unit verifies username and password during user authentication?

A. If a remote server is included in a user group, it will be checked before local accounts.
B. An administrator can define a local account for which the password must be verified by querying a remote server.
C. If authentication fails with a local password, the FortiGate unit will query the authentication server if the local user is configured with both a local password and an authentication server.
D. The FortiGate unit will only attempt to authenticate against Active Directory if Fortinet Server Authentication Extensions are installed and configured.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 151**
Which of the following cannot be used in conjunction with the endpoint compliance check?

A. HTTP Challenge Redirect to a Secure Channel (HTTPS) in the Authentication Settings.
B. Any form of firewall policy authentication.
C. WAN optimization.
D. Traffic shaping.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 152**
An administrator configures a VPN and selects the Enable IPSec Interface Mode option in the phase 1 settings.
Which of the following statements are correct regarding the IPSec VPN configuration?

A. To complete the VPN configuration, the administrator must manually create a virtual IPSec interface in Web Config under System > Network.
B. The virtual IPSec interface is automatically created after the phase1 configuration.
C. The IPSec policies must be placed at the top of the list.
D. This VPN cannot be used as part of a hub and spoke topology.
E. Routes were automatically created based on the address objects in the firewall policies.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 153**
Which of the following items are considered to be advantages of using the application control features on the FortiGate unit? Application control allows an administrator to:

A. set a unique session-ttl for select applications.
B. customize application types in a similar way to adding custom IPS signatures.
C. check which applications are installed on workstations attempting to access the network.
D. enable AV scanning per application rather than per policy.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 154**
In order to load-share traffic using multiple static routes, the routes must be configured with ...

A. the same distance and same priority.
B. the same distance and the same weight.
C. the same distance but each of them must be assigned a unique priority.
D. a distance equal to its desired weight for ECMP but all must have the same priority.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 155**
If Open Shortest Path First (OSPF) has already been configured on a FortiGate unit, which of the following statements is correct if the routes learned through OSPF need to be announced by Border Gateway Protocol (BGP)?

A. The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Autonomous System Boundary Router (ASBR).
B. The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Area Border Router (ABR).

C. At a minimum, the network administrator needs to enable Redistribute OSPF in the BGP settings.
D. The BGP local AS number must be the same as the OSPF area number of the routes learned that need to be redistributed into BGP.
E. By design, BGP cannot redistribute routes learned through OSPF.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 156**

Which of the following statements are correct regarding the configuration of a FortiGate unit as an SSL VPN gateway? (Select all that apply.)

A. Tunnel mode can only be used if the SSL VPN user groups have at least one Host Check option enabled.
B. The specific routes needed to access internal resources through an SSL VPN connection in tunnel mode from the client computer are defined in the routing widget associated with the SSL VPN portal.
C. In order to apply a portal to a user, that user must belong to an SSL VPN user group.
D. The portal settings specify whether the connection will operate in web-only or tunnel mode.

**Correct Answer:** CD
**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 157**

When the SSL proxy inspects the server certificate for Web Filtering only in SSL Handshake mode, which certificate field is being used to determine the site rating?

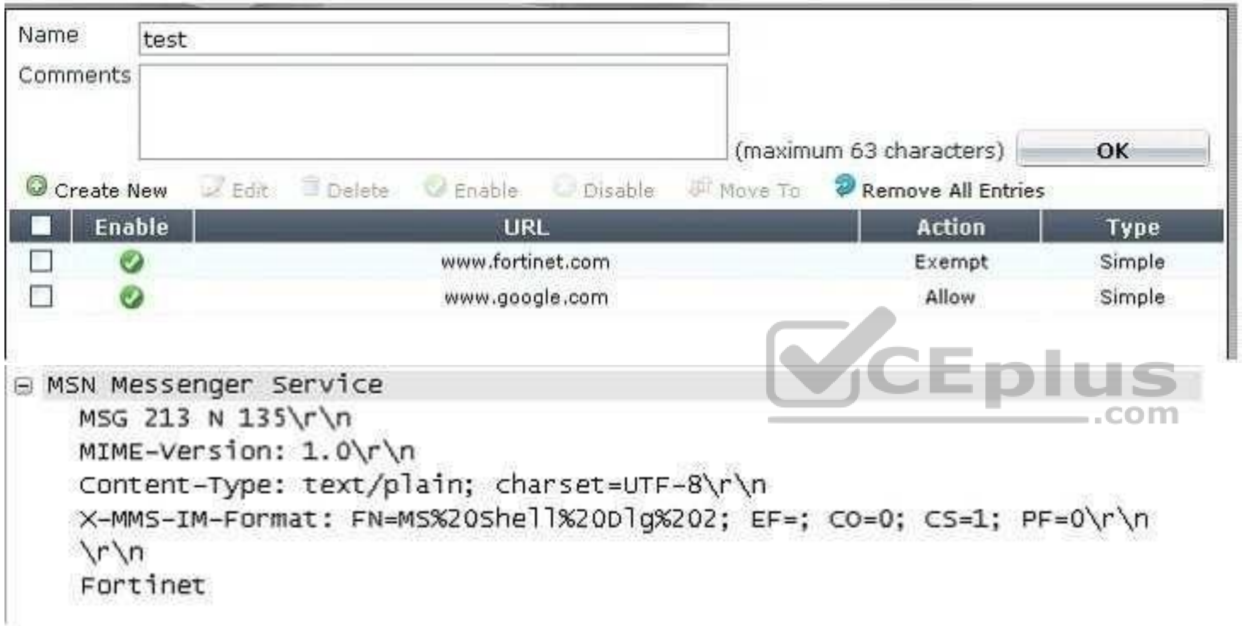
A. Common Name
B. Organization
C. Organizational Unit
D. Serial Number
E. Validity

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 158**
Which of the following describes the best custom signature for detecting the use of the word "Fortinet" in chat applications?



| | |
|---|---|
| Name | test |
| Comments | |

(maximum 63 characters)

| ☐ | Enable | URL | Action | Type |
|---|---|---|---|---|
| ☐ | ✓ | www.fortinet.com | Exempt | Simple |
| ☐ | ✓ | www.google.com | Allow | Simple |

```
⊟ MSN Messenger Service
    MSG 213 N 135\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    X-MMS-IM-Format: FN=MS%20Shell%20Dlg%202; EF=; CO=0; CS=1; PF=0\r\n
    \r\n
    Fortinet
```

A. The sample packet trace illustrated in the exhibit provides details on the packet that requires detection. F-SBID( --protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; -- no_case; )
B. F-SBID( --protocol tcp; --flow from_client; --pattern "fortinet"; --no_case; )
C. F-SBID( --protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; -- within 20; --no_case; )
D. F-SBID( --protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; -- within 20; )

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 159**
When configuring a server load balanced virtual IP, which of the following is the best distribution algorithm to be used in applications where the same physical destination server must be maintained between sessions?

A. Static
B. Round robin
C. Weighted round robin
D. Least connected

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 160**
Which of the following Session TTL values will take precedence?

A. Session TTL specified at the system level for that port number
B. Session TTL specified in the matching firewall policy
C. Session TTL dictated by the application control list associated with the matching firewall policy
D. The default session TTL specified at the system level

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 161**
If Routing Information Protocol (RIP) version 1 or version 2 has already been configured on a FortiGate unit, which of the following statements is correct if the routes learned through RIP need to be advertised into Open Shortest Path First (OSPF)?

A. The FortiGate unit will automatically announce all routes learned through RIP v1 or v2 to its OSPF neighbors.

B. The FortiGate unit will automatically announce all routes learned only through RIP v2 to its OSPF neighbors.
C. At a minimum, the network administrator needs to enable Redistribute RIP in the OSPF Advanced Options.
D. The network administrator needs to configure a RIP to OSPF announce policy as part of the RIP settings.
E. At a minimum, the network administrator needs to enable Redistribute Default in the OSPF Advanced Options.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 162**
In the Tunnel Mode widget of the web portal, the administrator has configured an IP Pool and enabled split tunneling.
Which of the following statements is true about the IP address used by the SSL VPN client?

A. The IP pool specified in the SSL-VPN Tunnel Mode Widget Options will override the IP address range defined in the SSL-VPN Settings.

B. Because split tunneling is enabled, no IP address needs to be assigned for the SSL VPN tunnel to be established.
C. The IP address range specified in SSL-VPN Settings will override the IP address range in the SSL-VPN Tunnel Mode Widget Options.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 163**

The Host Check feature can be enabled on the FortiGate unit for SSL VPN connections. When this feature is enabled, the FortiGate unit probes the remote host computer to verify that it is "safe" before access is granted.
Which of the following items is NOT an option as part of the Host Check feature?

A. FortiClient Antivirus software
B. Microsoft Windows Firewall software
C. FortiClient Firewall software
D. Third-party Antivirus software

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 164**
Which of the following report templates must be used when scheduling report generation?

A. Layout Template
B. Data Filter Template
C. Output Template
D. Chart Template

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 165**
Which of the following statements is not correct regarding virtual domains (VDOMs)?

A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. A backup management VDOM will synchronize the configuration from an active management VDOM.
D. VDOMs share firmware versions, as well as antivirus and IPS databases.

E. Only administrative users with a super_admin profile will be able to enter all VDOMs to make configuration changes.

**Correct Answer:** C
**Section: (none)**
**Explanation**

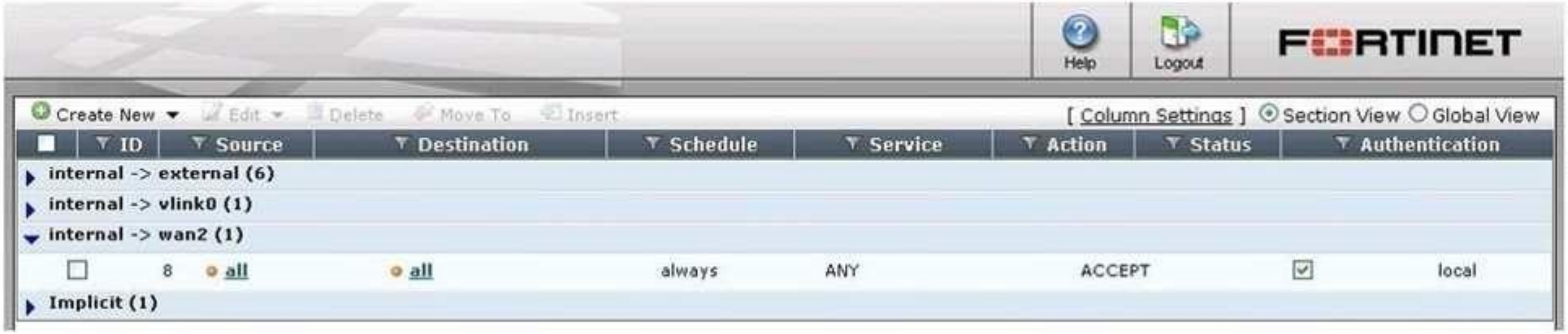
**Explanation/Reference:**

**QUESTION 166**
Which of the following must be configured on a FortiGate unit to redirect content requests to remote web cache servers?

A. WCCP must be enabled on the interface facing the Web cache.
B. You must enabled explicit Web-proxy on the incoming interface.
C. WCCP must be enabled as a global setting on the FortiGate unit.
D. WCCP must be enabled on all interfaces on the FortiGate unit through which HTTP traffic is passing.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 167**
Which of the following statements is correct based on the firewall configuration illustrated in the exhibit?



| ☐ | ID | Source | Destination | Schedule | Service | Action | Status | Authentication |
|---|---|---|---|---|---|---|---|---|
| internal -> external (6) | | | | | | | | |
| internal -> vlink0 (1) | | | | | | | | |
| internal -> wan2 (1) | | | | | | | | |
| ☐ | 8 | all | all | always | ANY | ACCEPT | ☑ | local |
| Implicit (1) | | | | | | | | |

A. A user can access the Internet using only the protocols that are supported by user authentication.

B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP. These require authentication before the user will be allowed access.
C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services.
D. A user cannot access the Internet using any protocols unless the user has passed firewall authentication.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 168**
Which of the following statements is correct regarding the NAC Quarantine feature?

A. With NAC quarantine, files can be quarantined not only as a result of antivirus scanning, but also for other forms of content inspection such as IPS and DLP.
B. NAC quarantine does a client check on workstations before they are permitted to have administrative access to FortiGate.
C. NAC quarantine allows administrators to isolate clients whose network activity poses a security risk.
D. If you chose the quarantine action, you must decide whether the quarantine type is NAC quarantine or File quarantine.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 169**
What advantages are there in using a fully Meshed IPSec VPN configuration instead of a hub and spoke set of IPSec tunnels?

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a full mesh topology simplifies configuration.
C. Using a full mesh topology provides stronger encryption.
D. Full mesh topology is the most fault-tolerant configuration.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 170**

An administrator wishes to generate a report showing Top Traffic by service type, but wants to exclude SMTP traffic from the report.
Which of the following statements best describes how to do this?

A. In the Service field of the Data Filter, type 25/smtp and select the NOT checkbox.
B. Add the following entry to the Generic Field section of the Data Filter: service="!smtp".
C. When editing the chart, uncheck mlog to indicate that Mail Filtering data is being excluded when generating the chart.
D. When editing the chart, enter 'dns' in the Exclude Service field.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 171**

An organization wishes to protect its SIP Server from call flooding attacks. Which of the following configuration changes can be performed on the FortiGate unit to fulfill this requirement?

A. Apply an application control list which contains a rule for SIP and has the "Limit INVITE Request" option configured.
B. Enable Traffic Shaping for the appropriate SIP firewall policy.
C. Reduce the session time-to-live value for the SIP protocol by running the configure system session-ttl CLI command.
D. Run the set udp-idle-timer CLI command and set a lower time value.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 172**

In a High Availability configuration operating in Active-Active mode, which of the following correctly describes the path taken by a load-balanced HTTP session?

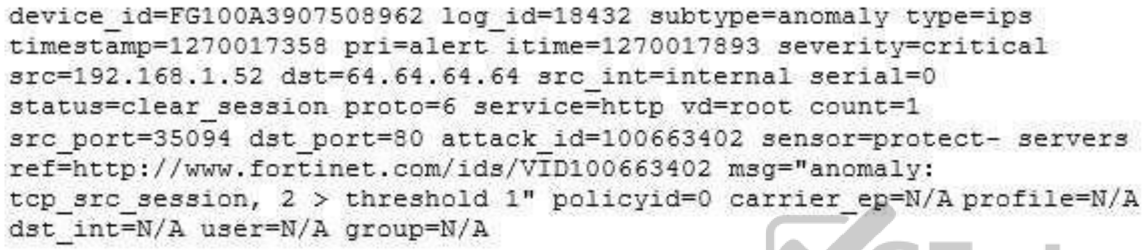
A. Request: Internal Host -> Master FG -> Slave FG -> Internet -> Web Server
B. Request: Internal Host -> Master FG -> Slave FG -> Master FG -> Internet -> Web Server
C. Request: Internal Host -> Slave FG -> Internet -> Web Server

D. Request: Internal Host -> Slave FG -> Master FG -> Internet -> Web Server

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 173**
An administrator is examining the attack logs and notices the following entry:



```
device_id=FG100A3907508962 log_id=18432 subtype=anomaly type=ips
timestamp=1270017358 pri=alert itime=1270017893 severity=critical
src=192.168.1.52 dst=64.64.64.64 src_int=internal serial=0
status=clear_session proto=6 service=http vd=root count=1
src_port=35094 dst_port=80 attack_id=100663402 sensor=protect- servers
ref=http://www.fortinet.com/ids/VID100663402 msg="anomaly:
tcp_src_session, 2 > threshold 1" policyid=0 carrier_ep=N/A profile=N/A
dst_int=N/A user=N/A group=N/A
```

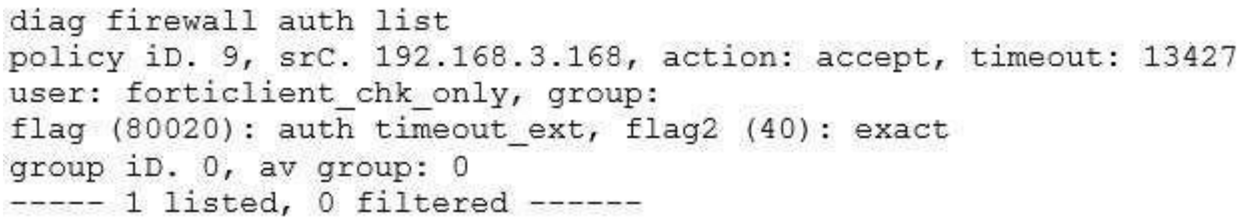
Based solely upon this log message, which of the following statements is correct?

A. This attack was blocked by the HTTP protocol decoder.
B. This attack was caught by the DoS sensor "protect-servers".
C. This attack was launched against the FortiGate unit itself rather than a host behind the FortiGate unit.
D. The number of concurrent connections to destination IP address 64.64.64.64 has exceeded the configured threshold.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 174**
The following diagnostic output is displayed in the CLI:



```
diag firewall auth list
policy iD. 9, srC. 192.168.3.168, action: accept, timeout: 13427
user: forticlient_chk_only, group:
flag (80020): auth timeout_ext, flag2 (40): exact
group iD. 0, av group: 0
----- 1 listed, 0 filtered ------
```

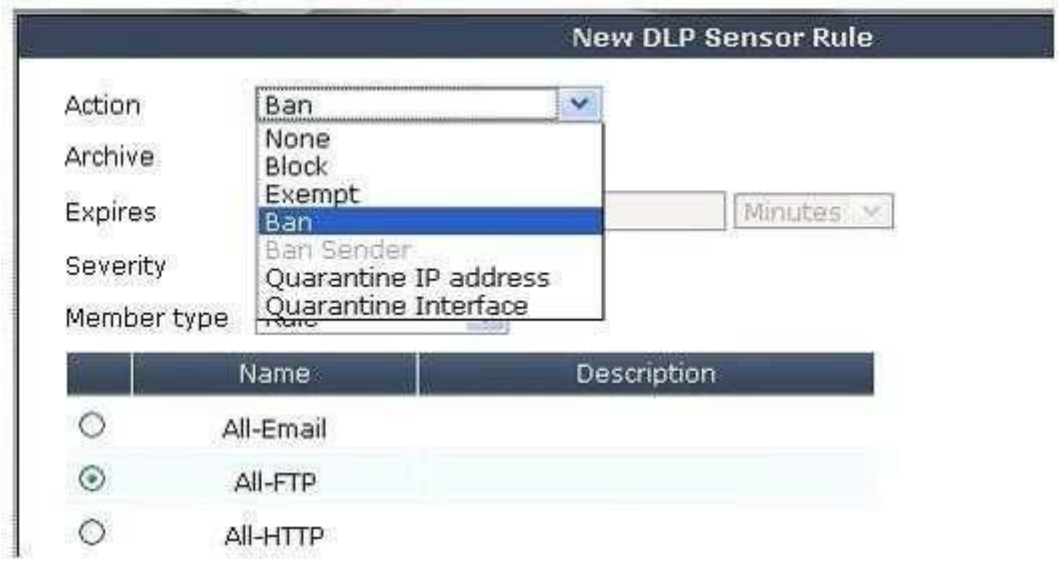
Based on this output, which of the following statements is correct?

A. Firewall policy 9 has endpoint compliance enabled but not firewall authentication.
B. The client check that is part of an SSL VPN connection attempt failed.
C. This user has been associated with a guest profile as evidenced by the group id of 0.
D. An auth-keepalive value has been enabled.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 175**
An administrator is configuring a DLP rule for FTP traffic. When adding the rule to a DLP sensor,



New DLP Sensor Rule

Action: Ban

Archive

Expires: Minutes

Severity

Member type: Rule

| | Name | Description |
|---|---|---|
| ○ | All-Email | |
| ● | All-FTP | |
| ○ | All-HTTP | |

the administrator notes that the Ban Sender action is not available (greyed-out), as shown in the exhibit.
Which of the following is the best explanation for the Ban Sender action NOT being available?

A. The Ban Sender action is never available for FTP traffic.
B. The Ban Sender action needs to be enabled globally for FTP traffic on the FortiGate unit before configuring the sensor.
C. Firewall policy authentication is required before the Ban Sender action becomes available.
D. The Ban Sender action is only available for known domains. No domains have yet been added to the domain list.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 176**

Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

A. SSH
B. Telnet
C. NTLM

D. HTTPS

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 177**
Acme Web Hosting is replacing one of their firewalls with a FortiGate. It must be able to apply port forwarding to their back-end web servers while blocking virus uploads and TCP SYN floods from attackers. Which operation mode is the best choice for these requirements?

A. NAT/route
B. NAT mode with an interface in one-arm sniffer mode
C. Transparent mode
D. No appropriate operation mode exists

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 178**
Which of the following statements are true about the SSL Proxy certificate that must be used for SSL Content Inspection? (Choose two.)

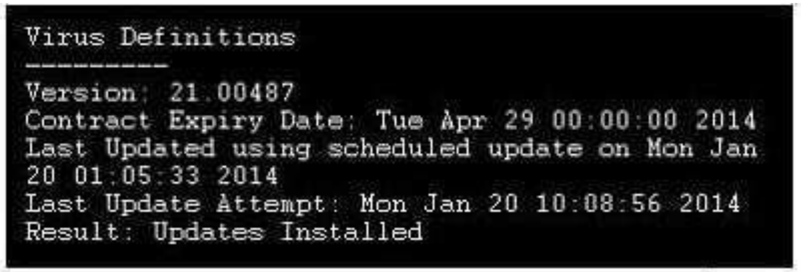
A. It cannot be signed by a private CA
B. It must have either the field "CA=True" or the filed "Key Usage=KeyCertSign"
C. It must be installed in the FortiGate device
D. The subject filed must contain either the FQDN, or the IP address of the FortiGate device

**Correct Answer:** CD
**Section: (none)**
**Explanation**

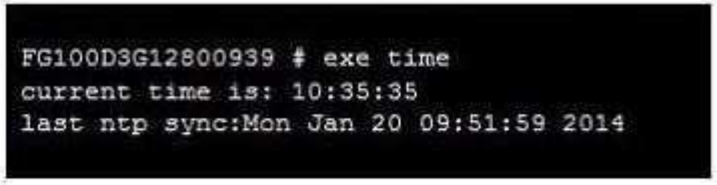
**Explanation/Reference:**

**QUESTION 179**

A FortiGate device is configure to perform an AV & IPS scheduled update every hour.



```
Virus Definitions
----------
Version: 21.00487
Contract Expiry Date: Tue Apr 29 00:00:00 2014
Last Updated using scheduled update on Mon Jan
20 01:05:33 2014
Last Update Attempt: Mon Jan 20 10:08:56 2014
Result: Updates Installed
```



```
FG100D3G12800939 # exe time
current time is: 10:35:35
last ntp sync:Mon Jan 20 09:51:59 2014
```

Given the information in the exhibit, when will the next update happen?

A. 01:00
B. 02:05
C. 11:00
D. 11:08

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 180**

Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

A. In symmetric cryptography, the keys are publicly available. In asymmetric cryptography, the keys must be kept secret.
B. Asymmetric cryptography can encrypt data faster than symmetric cryptography
C. Symmetric cryptography uses one pre-shared key. Asymmetric cryptography uses a pair or keys
D. Asymmetric keys can be sent to the remote peer via digital certificates. Symmetric keys cannot

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 181**
An Internet browser is using the WPAD DNS method to discover the PAC file's URL. The DNS server replies to the browser's request with the IP address 10.100.1.10. Which URL will the browser use to download the PAC file?

A. http://10.100.1.10/proxy.pac
B. https://10.100.1.10/
C. http://10.100.1.10/wpad.dat
D. https://10.100.1.10/proxy.pac

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 182**
Which of the following IPsec configuration modes can be used for implementing L2TP- over- IPSec VPNs?

A. Policy-based IPsec only. B.
Route-based IPsec only.
C. Both policy-based and route-based VPN.
D. L2TP-over-IPSec is not supported by FortiGate devices.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 183**
Which of the following statements best describes the role of a DC agents in an FSSO DC?

A. Captures the login events and forward them to the collector agent.
B. Captures the user IP address and workstation name and forward that information to the FortiGate devices.
C. Captures the login and logoff events and forward them to the collector agent.
D. Captures the login events and forward them to the FortiGate devices.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 184**
Which statement is correct concerning creating a custom signature?

A. It must start with the name
B. It must indicate whether the traffic flow is from the client or the server.
C. It must specify the protocol. Otherwise, it could accidentally match lower-layer protocols.
D. It is not supported by Fortinet Technical Support.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 185**
Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (Choose three)

A. Irix
B. QNIX
C. Linux
D. Mac OS
E. BSD

**Correct Answer:** CDE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 186**
Which is true of FortiGate's session table?

A. NAT/PAT is shown in the central NAT table, not the session table.
B. It shows TCP connection states.
C. It shows IP, SSL, and HTTP sessions.
D. It does not show UDP or ICMP connection state codes, because those protocols are connectionless.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 187**
Which of the following statements are correct concerning the FortiGate session life support protocol? (Choose two)

A. By default, UDP sessions are not synchronized.
B. Up to four FortiGate devices in standalone mode are supported.
C. only the master unit handles the traffic.
D. Allows per-VDOM session synchronization.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 188**
Which FSSO agents are required for a FSSO agent-based polling mode solution?

A. Collector agent and DC agents
B. Polling agent only

C. Collector agent only
D. DC agents only

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 189**
Which are outputs for the command `diagnose hardware deviceinfo nic'? (Choose two.)

A. ARP cache
B. Physical MAC address
C. Errors and collisions
D. Listening TCP ports**Correct Answer:** BC **Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 190**
There are eight (8) log severity levels that indicate the importance of an event. Not including Debug, which is only needed to log diagnostic data, what are both the lowest AND highest severity levels?

A. Notification, Emergency
B. Information, Critical
C. Error, Critical
D. Information, Emergency
E. Information, Alert

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 191**
Which of the following statements best describe the main requirements for a traffic session to be offload eligible to an NP6 processor? (Choose three.)

A. Session packets do NOT have an 802.1Q VLAN tag.
B. It is NOT multicast traffic.
C. It does NOT require proxy-based inspection.
D. Layer 4 protocol must be UDP, TCP, SCTP or ICMP.
E. It does NOT require flow-based inspection.

**Correct Answer:** CDE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 192**
Which of the following statements are correct concerning IPsec dialup VPN configurations for FortiGate devices? (Choose two)

A. Main mode mist be used when there is no more than one IPsec dialup VPN configured on the same FortiGate device.
B. A FortiGate device with an IPsec VPN configured as dialup can initiate the tunnel connection to any remote IP address.
C. Peer ID must be used when there is more than one aggressive-mode IPsec dialup VPN on the same FortiGate device.
D. The FortiGate will automatically add a static route to the source quick mode selector address received from each remote peer.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 193**
Which of the following statements are correct concerning IKE mode config? (Choose two)

A. It can dynamically assign IP addresses to IPsec VPN clients.
B. It can dynamically assign DNS settings to IPsec VPN clients.
C. It uses the ESP protocol.
D. It can be enabled in the phase 2 configuration.

**Correct Answer:** AB

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 194**
For FortiGate devices equipped with Network Processor (NP) chips, which are true? (Choose three.)

A. For each new IP session, the first packet always goes to the CPU.
B. The kernel does not need to program the NPU. When the NPU sees the traffic, it determines by itself whether it can process the traffic
C. Once offloaded, unless there are errors, the NP forwards all subsequent packets. The CPU does not process them.
D. When the last packet is sent or received, such as a TCP FIN or TCP RST signal, the NP returns this session to the CPU for tear down.
E. Sessions for policies that have a security profile enabled can be NP offloaded.

**Correct Answer:** ACD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 195**
In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

A. The DC agents get each user IP address from the event logs and forward that information to the collector agent
B. The collector agent does not know, and does not need, each user IP address. Only workstation names are known by the collector agent.
C. The collector agent frequently polls the AD domain controllers to get each user IP address.
D. The DC agent learns the workstation name from the event logs and DNS is then used to translate those names to the respective IP addresses.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 196**
Which of the following statements are true regarding WAN Link Load Balancing? (Choose two).

A. There can be only one virtual WAN Link per VDOM.
B. FortiGate can measure the quality of each link based on latency, jitter, or packets percentage.
C. Link health checks can be performed over each link member if the virtual WAN interface.
D. Distance and priority values are configured in each link member if the virtual WAN interface.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 197**
Which of the following statements best describes what the Document Fingerprinting feature is for?

A. Protects sensitive documents from leakage
B. Appends a fingerprint signature to all documents sent by users
C. Appends a fingerprint signature to all the emails sent by users
D. Validates the fingerprint signature in users' emails

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 198**
Which statement describes how traffic flows in sessions handled by a slave unit in an active- active HA cluster?

A. Packet are sent directly to the slave unit using the slave physical MAC address.
B. Packets are sent directly to the slave unit using the HA virtual MAC address.
C. Packets arrived at both units simultaneously, but only the salve unit forwards the session.
D. Packets are first sent to the master unit, which then forwards the packets to the slave unit.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 199**
Which of the following statements is correct concerning multiple vdoms configured in a FortiGate device?

A. FortiGate devices,from the FGT/FWF 60D and above, all support VDOMS.

B. All FortiGate devices scale to 250 VDOMS.
C. Each VDOM requires its own FortiGuard license.
D. FortiGate devices support more NAT/route VDOMs than Transparent Mode VDOMs.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 200**
Files that are larger than the oversized limit are subjected to which Antivirus check?

A. Grayware
B. Virus
C. SandboxD. Heuristic

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 201**

Which of the following traffic shaping functions can be offloaded to a NP processor? (Choose two.)

A. Que prioritization
B. Traffic cap (bandwidth limit)
C. Differentiated services field rewriting
D. Guarantee bandwidth

**Correct Answer:** CD
**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 202**

Which statement best describes what a Fortinet System on a Chip (SoC) is?

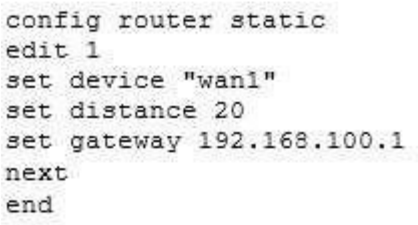
A. Low-power chip that provides general purpose processing power
B. Chip that combines general purpose processing power with Fortinet's custom ASIC technology
C. Light-version chip (with fewer features) of an SP processor
D. Light-version chip (with fewer features) of a CP processor

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 203**

A static route is configured for a FortiGate unit from the CLI using the following commands:



```
config router static
edit 1
set device "wan1"
set distance 20
set gateway 192.168.100.1
next
end
```

Which of the following conditions are required for this static default route to be displayed in the FortiGate unit's routing table? (Choose two.)

A. The administrative status of the wan1 interface is displayed as down.
B. The link status of the wan1 interface is displayed as up.
C. All other default routers should have a lower distance.
D. The wan1 interface address and gateway address are on the same subnet.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 204**
A FortiGate devices is configured with four VDOMs: 'root' and 'vdom1' are in NAT/route mode; 'vdom2' and 'vdom2' are in transparent mode. The management VDOM is 'root'. Which of the following statements are true? (Choose two.)

A. An inter-VDOM link between 'root' and 'vdom1' can be created.
B. An inter-VDOM link between 'vdom1' and vdom2' can created.
C. An inter-VDOM link between 'vdom2' and vdom3' can created.
D. Inter-VDOM link links must be manually configured for FortiGuard traffic.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 205**

You have created a new administrator account, and assign it the prof_admin profile. Which is false about that account's permissions?

A. It cannot upgrade or downgrade firmware.
B. It can create and assign administrator accounts to parts of its own VDOM.
C. It can reset forgotten passwords for other administrator accounts such as "admin".
D. It has a smaller permissions scope than accounts with the "super_admin" profile.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 206**

In FortiOS session table output, what are the two possible `proto_state' values for a UDP session? (Choose two.)

A. 00
B. 11
C. 01
D. 05

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 207**

Which of the following statements are true regarding traffic accelerated by an NP processor? (Choose two.)

A. TCP SYN packets are always handled by the NP Processor
B. The initial packets go to the NP Processor, where a decision is taken on if the session can be offloaded or not.
C. Packets for a session termination are always handled by the CPU.
D. The initial packets go to the CPU, where a decision is taken on if the session can be offloaded or not.

**Correct Answer:** AD

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 208**
Which authentication methods does FortiGate support for firewall authentication? (Choose two.)

A. Remote Authentication Dial in User Service (RADIUS)
B. Lightweight Directory Access Protocol (LDAP)
C. Local Password Authentication
D. POP3
E. Remote Password Authentication

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 209**
How many packets are interchanged between both IPSec ends during the negotiation of a main- mode phase 1?

A. 5
B. 3
C. 2
D. 6

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 210**
Which is NOT true about the settings for an IP pool type port block allocation?

A. A Block Size defines the number of connections.
B. Blocks Per User defines the number of connection blocks for each user.
C. An Internal IP Range defines the IP addresses permitted to use the pool.
D. An External IP Range defines the IP addresses in the pool.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 211**
You have configured the DHCP server on a FortiGate's port1 interface (or internal, depending on the model) to offer IPs in a range of 192.168.1.65-192.168.1.253.

When the first host sends a DHCP request, what IP will the DHCP offer?
A. 192.168.1.99
B. 192.168.1.253
C. 192.168.1.65
D. 192.168.1.66

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 212**
Regarding the use of web-only mode SSL VPN, which statement is correct?

A. It support SSL version 3 only.
B. It requires a Fortinet-supplied plug-in on the web client.
C. It requires the user to have a web browser that suppports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client.

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 213**
Which of the following network protocols can be inspected by the Data Leak Prevention scanning? (Choose three.)

A. SMTP
B. HTTP-POST
C. AIM
D. MAPI
E. ICQ

**Correct Answer:** ABD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 214**
Which of the following IPsec configuration modes can be used when the FortiGate is running in NAT mode?

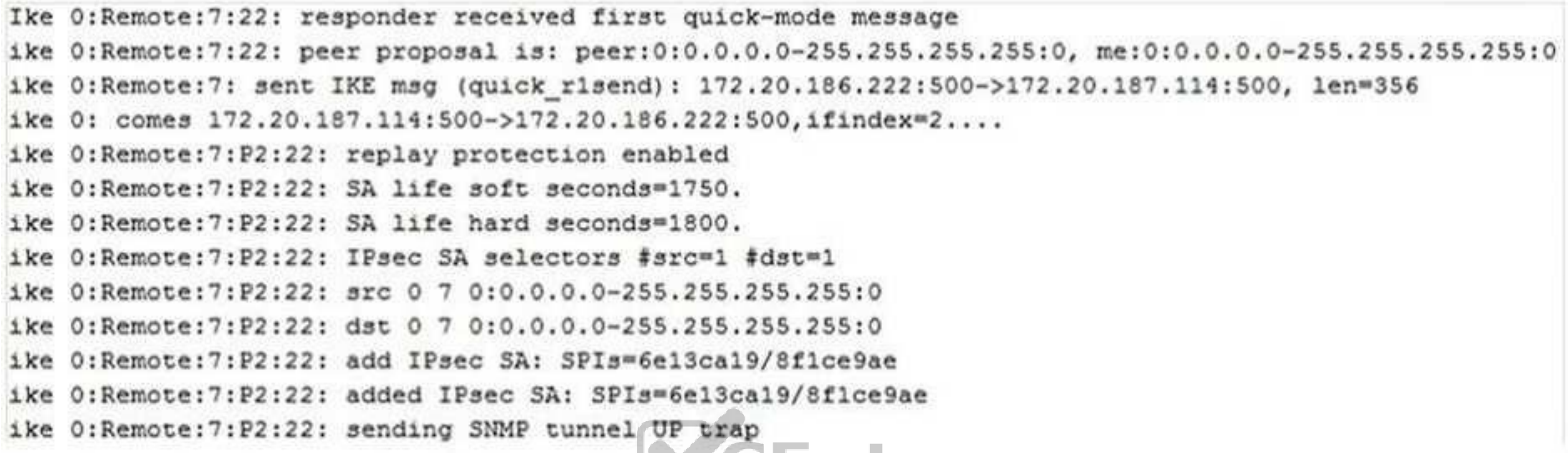
A. Policy-based VPN only
B. Both policy-based and route-based VPN.
C. Route-based VPN only.
D. IPSec VPNs are not supported when the FortiGate is running in NAT mode.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 215**

The exhibit shows a part output of the diagnostic command 'diagnose debug application ike 255', taken during establishment of a VPN. Which of the following statement are correct concerning this output? (Choose two)



```
Ike 0:Remote:7:22: responder received first quick-mode message
ike 0:Remote:7:22: peer proposal is: peer:0:0.0.0.0-255.255.255.255:0, me:0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7: sent IKE msg (quick_r1send): 172.20.186.222:500->172.20.187.114:500, len=356
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:7:P2:22: replay protection enabled
ike 0:Remote:7:P2:22: SA life soft seconds=1750.
ike 0:Remote:7:P2:22: SA life hard seconds=1800.
ike 0:Remote:7:P2:22: IPsec SA selectors #src=1 #dst=1
ike 0:Remote:7:P2:22: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: dst 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: add IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: added IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: sending SNMP tunnel UP trap
```

A. The quick mode selectors negotiated between both IPsec VPN peers is 0.0.0.0/32 for both source and destination addresses.
B. The output corresponds to a phase 2 negotiation
C. NAT-T enabled and there is third device in the path performing NAT of the traffic between both IPsec VPN peers.
D. The IP address of the remote IPsec VPN peer is 172.20.187.114

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 216**
Which statement best describes what SSL.root is?

A. The name of the virtual network adapter required in each user's PC for SSL VPN Tunnel mode.
B. The name of a virtual interface in the root VDOM where all the SSL VPN user traffic comes from.
C. A Firewall Address object that contains the IP addresses assigned to SSL VPN users.

D. The virtual interface in the root VDOM that the remote SSL VPN tunnels connect to.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 217**

Which is NOT true about source matching with firewall policies?

A. A source address object must be selected in the firewall policy.
B. A source user/group may be selected in the firewall policy.
C. A source device may be defined in the firewall policy.
D. A source interface must be selected in the firewall policy.
E. A source user/group and device must be specified in the firewall policy.

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 218**

Files reported as "suspicious" were subject to which Antivirus check"?

A. Grayware
B. Virus
C. SandboxD. Heuristic

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 219**

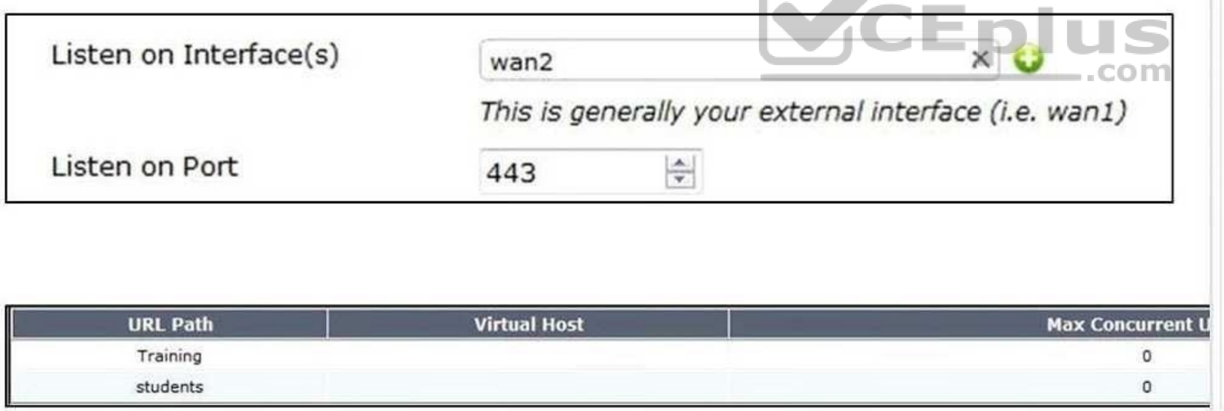
Which profile could IPS engine use on an interface that is in sniffer mode? (Choose three)

A. Antivirus (flow based
B. Web filtering (PROXY BASED)
C. Intrusion Protection
D. Application Control
E. Endpoint control

**Correct Answer:** ABD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 220**
A FortiGate is configured with the 1.1.1.1/24 address on the wan2 interface and HTTPS Administrative Access, using the default tcp port, is enabled for that interface. Given the SSL VPN settings in the exhibit.



Listen on Interface(s): wan2
This is generally your external interface (i.e. wan1)
Listen on Port: 443

| URL Path | Virtual Host | Max Concurrent U |
|---|---|---|
| Training | | 0 |
| students | | 0 |

Which of the following SSL VPN login portal URLs are valid? (Choose two.)

A. http://1.1.1.1:443/Training
B. https://1.1.1.1:443/STUDENTS
C. https://1.1.1.1/login
D. https://1.1.1.1/

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 221**
Which of the following fields contained in the IP/TCP/UDP headers can be used to make a routing decision when using policy-based routing? (Choose three)

A. Source IP address.
B. TCP flags
C. Source TCP/UDP ports
D. Type of service.
E. Checksum

**Correct Answer:** ACD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 222**
Which of the following protocols are defined in the IPsec Standard? (Choose two)

A. AH
B. GRE
C. SSL/TLS
D. ESP

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 223**
Which action does the FortiGate take when link health monitor times out?

A. All routes to the destination subnet configured in the link health monitor are removed from the routing table.
B. The distance values of all routes using interface configured in the link health monitor are increased.
C. The priority values of all routes using configured in the link health monitor are increased.
D. All routes using the next-hop gateway configured in the link health monitor are removed from the routing table.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 224**
Which of the following statements are true regarding application control? (Choose two.)

A. Application control is based on TCP destination port numbers.
B. Application control is proxy based.
C. Encrypted traffic can be identified by application control.
D. Traffic shaping can be applied to the detected application traffic.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 225**
Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

A. More than one proxy is supported.
B. Can contain a list of destinations that will be exempt from the use of any proxy.
C. Can contain a list of URLs that will be exempted from the FortiGate web filtering inspection.
D. Can contain a list of users that will be exempted from the use of any proxy.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 226**

Where are most of the security events logged?

A. Security log
B. Forward Traffic log
C. Event log
D. Alert log
E. Alert Monitoring Console

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 227**

Which commands are appropriate for investigating high CPU? (Choose two.)

A. diag sys top
B. diag hardware sysinfo mem
C. diag debug flow
D. get system performance status

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 228**

Which statement is correct concerning an IPsec VPN with the remote gateway setting configured as 'Dynamic DNS'?

A. The FortiGate will accept IPsec VPN connection from any IP address.
B. The FQDN resolution of the local FortiGate IP address where the VPN is terminated must be provided by a dynamic DNS provider.
C. The FortiGate will Accept IPsec VPN connections only from IP addresses included on a dynamic DNS access list.
D. The remote gateway IP address can change dynamically.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 229**
Which of the following statements describes the objectives of the gratuitous ARP packets sent by an HA cluster?

A. To synchronize the ARp tables in all the FortiGate Unis that are part of the HA cluster.
B. To notify the network switches that a new HA master unit has been elected.
C. To notify the master unit that the slave devices are still up and alive.
D. To notify the master unit about the physical MAC addresses of the slave units.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 230**

How do application control signatures update on a FortiGate device?

A. Through FortiGuard updates.

B. Upgrade the FortiOS firmware to a newer release.
C. By running the Application Control auto-learning feature.
D. Signatures are hard coded to the device and cannot be updated.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**