NSE4-5.4.exam.255q

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

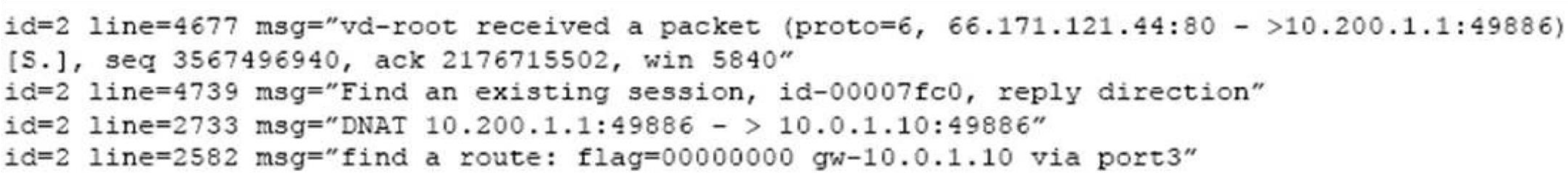
NSE4-5.4

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Exam A

QUESTION 1

Examine this output from a debug flow:



```
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"
```

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

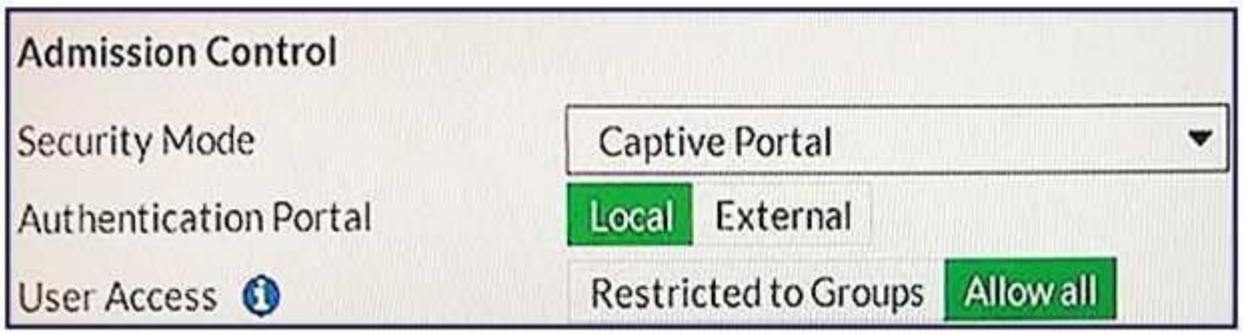
A. The packet was allowed by the firewall policy with the ID `00007fc0`.
B. FortiGate routed the packet through `port3`.
C. FortiGate received a TCP SYN/ACK packet.
D. The source IP address of the packet was translated to 10.0.1.10.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2

View the exhibit.



Admission Control

Security Mode: Captive Portal

Authentication Portal: Local | External

User Access: Restricted to Groups | Allow all

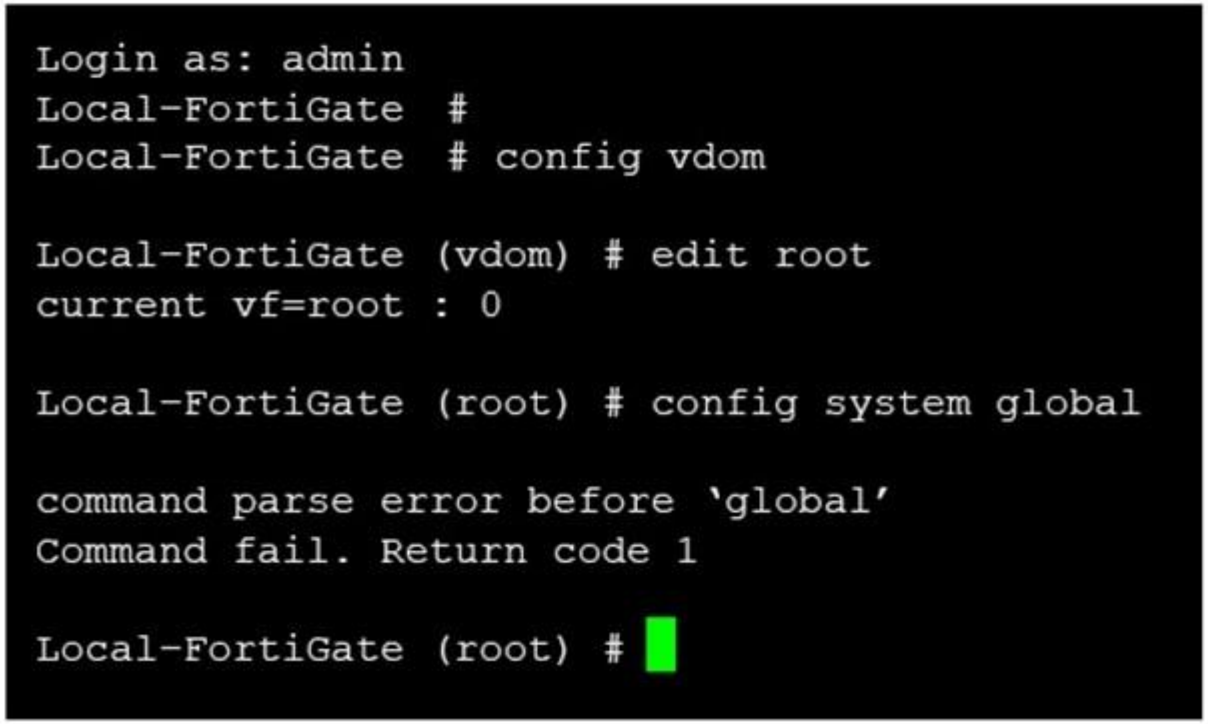
Which users and user groups are allowed access to the network through captive portal?

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 3
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 4

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 5
Which statements about the firmware upgrade process on an active-active high availability (HA) cluster are true? (Choose two.)

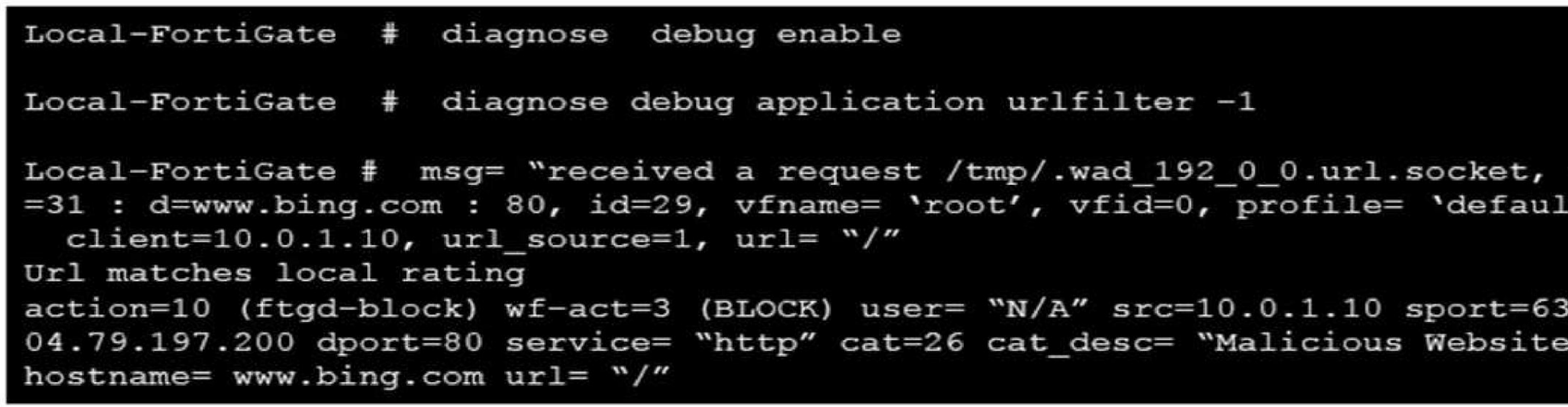
A. The firmware image must be manually uploaded to each FortiGate.
B. Only secondary FortiGate devices are rebooted.
C. Uninterruptable upgrade is enabled by default.
D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Examine the exhibit, which shows the output of a web filtering real time debug.
Why is the site `www.bing.com` being blocked?

A. The web server IP address 204.79.197.200 is categorized by FortiGuard as **Malicious Websites**.
B. The rating for the web site `www.bing.com` has been locally overridden to a category that is being blocked.
C. The web site `www.bing.com` is categorized by FortiGuard as Malicious Websites.
D. The user has not authenticated with the FortiGate yet.



```
Local-FortiGate  #  diagnose  debug enable

Local-FortiGate  #  diagnose debug application urlfilter -1

Local-FortiGate #  msg= “received a request /tmp/.wad_192_0_0.url.socket,
=31 : d=www.bing.com : 80, id=29, vfname= ‘root’, vfid=0, profile= ‘defaul
  client=10.0.1.10, url_source=1, url= “/”
Url matches local rating
action=10 (ftgd-block) wf-act=3 (BLOCK) user= “N/A” src=10.0.1.10 sport=63
04.79.197.200 dport=80 service= “http” cat=26 cat_desc= “Malicious Website
hostname= www.bing.com url= “/”
```

Correct Answer: A

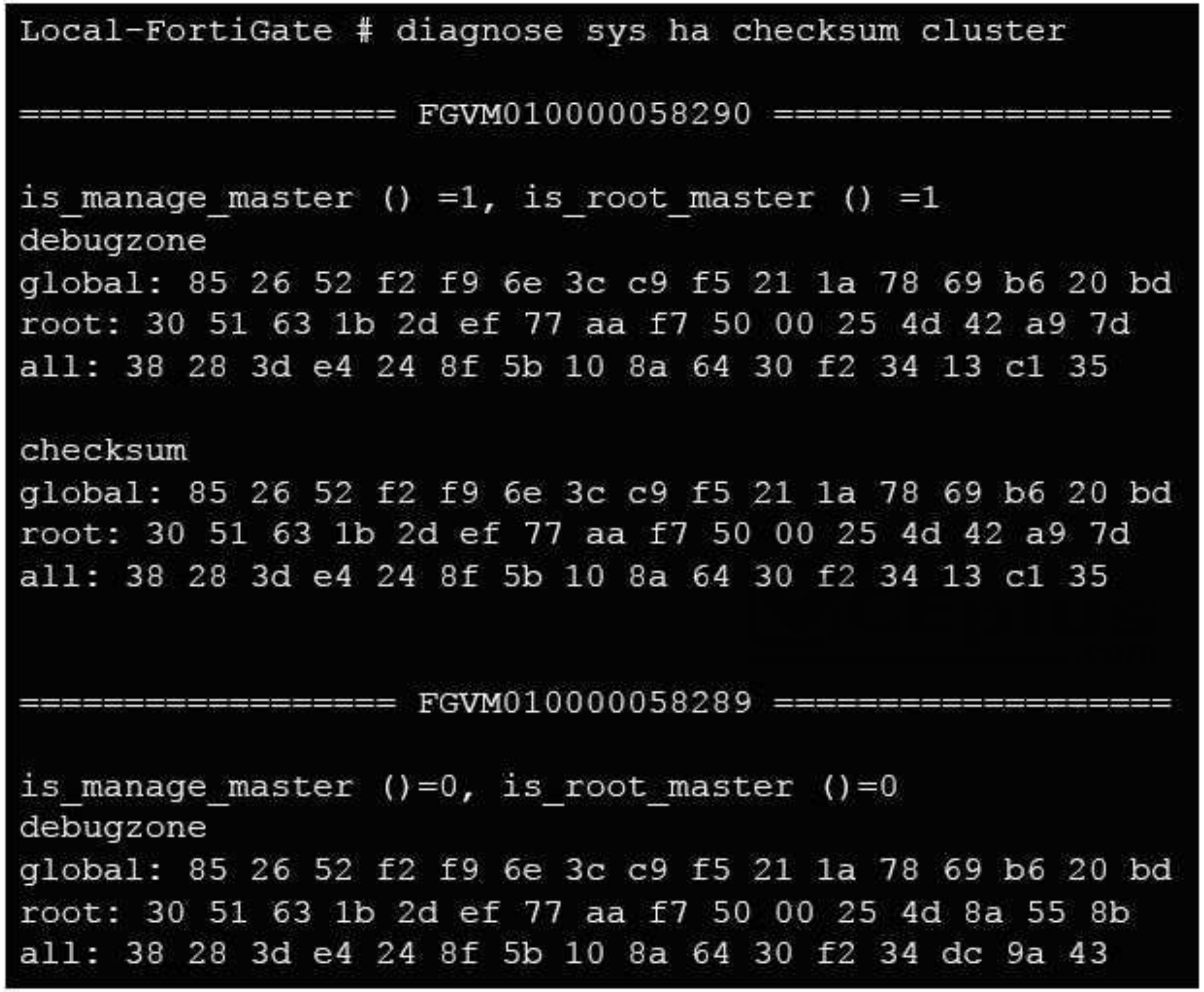
Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

View the exhibit.



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

================== FGVM010000058290 ===================

is_manage_master () =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_master ()=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
```

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

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

D. The root VDOM is not synchronized between the primary and secondary FortiGate.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What IPv6 extension header can be used to provide encryption and data confidentiality?

A. Mobility
B. ESP
C. Authentication

D. Destination options

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which two statements are true about IPsec VPNs and SSL VPNs? (Choose two.)

A. SSL VPN creates a HTTPS connection. IPsec does not.
B. Both SSL VPNs and IPsec VPNs are standard protocols.
C. Either a SSL VPN or an IPsec VPN can be established between two FortiGate devices.
D. Either a SSL VPN or an IPsec VPN can be established between an end-user workstation and a FortiGate device.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

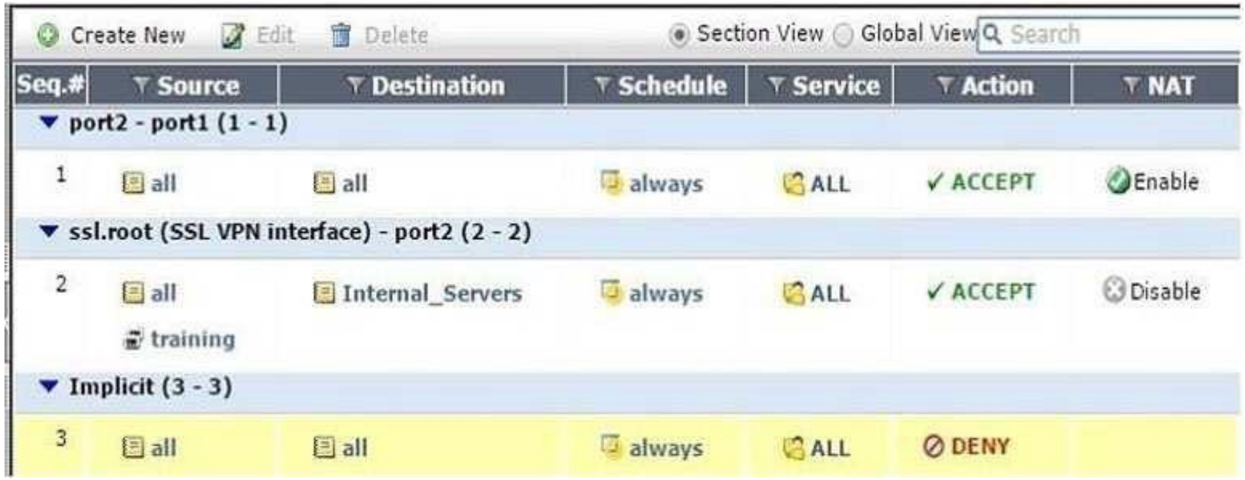
QUESTION 10
Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type.
Which of the following are some of the available event types in Web Config? (Select all that apply.)

A. Intrusion detected.
B. Successful firewall authentication.
C. Oversized file detected.
D. DHCP address assigned.
E. FortiGuard Web Filtering rating error detected.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A user logs into a SSL VPN portal and activates the tunnel mode.
The administrator has enabled split tunneling. The exhibit shows the firewall policy configuration:



Seq.#	Source	Destination	Schedule	Service	Action	NAT
▼ port2 - port1 (1 - 1)						
1	all	all	always	ALL	✓ ACCEPT	Enable
▼ ssl.root (SSL VPN interface) - port2 (2 - 2)						
2	all training	Internal_Servers	always	ALL	✓ ACCEPT	Disable
▼ Implicit (3 - 3)						
3	all	all	always	ALL	⊘ DENY	

Which static route is automatically added to the client's routing table when the tunnel mode is activated?

A. A route to a destination subnet matching the Internal_Servers address object.
B. A route to the destination subnet configured in the tunnel mode widget.
C. A default route.
D. A route to the destination subnet configured in the SSL VPN global settings.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

A. Split tunneling is supported.
B. It requires the installation of a VPN client.C. It requires the use of an Internet browser.
D. It does not support traffic from third-party network applications.
E. An SSL VPN IP address is dynamically assigned to the client by the FortiGate unit.
Correct Answer: ABE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
DLP archiving gives the ability to store session transaction data on a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

A. SNMP
B. IPSec
C. SMTP
D. POP3
E. HTTP

Correct Answer: CDE
Section: (none)
Explanation

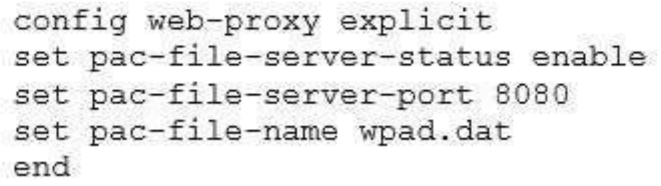
Explanation/Reference:

QUESTION 14
Which statements regarding banned words are correct? (Choose two.)

A. Content is automatically blocked if a single instance of a banned word appears.
B. The FortiGate updates banned words on a periodic basis.
C. The FortiGate can scan web pages and email messages for instances of banned words.
D. Banned words can be expressed as simple text, wildcards and regular expressions.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 15
Examine the following FortiGate web proxy configuration; then answer the question below:



```
config web-proxy explicit
set pac-file-server-status enable
set pac-file-server-port 8080
set pac-file-name wpad.dat
end
```

Assuming that the FortiGate proxy IP address is 10.10.1.1, which URL must an Internet browser use to download the PAC file?

A. https://10.10.1.1:8080
B. https://10.10.1.1:8080/wpad.dat
C. http://10.10.1.1:8080/
D. http://10.10.1.1:8080/wpad.dat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which statements are true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

A. Only one proxy is supported.
B. Can be manually imported to the browser.
C. The browser can automatically download it from a web server.
D. Can include a list of destination IP subnets where the browser can connect directly to without using a proxy.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 17
Which two methods are supported by the web proxy auto-discovery protocol (WPAD) to automatically learn the URL where a PAC file is located? (Choose two.)

A. DHCP

B. BOOTP
C. DNS
D. IPv6 auto configuration

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
What is a valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

A. Users are required to manually enter their credentials each time they connect to a different web site.
B. Proxy users are authenticated via FSSO.
C. There are multiple users sharing the same IP address.
D. Proxy users are authenticated via RADIUS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which two web filtering inspection modes inspect the full URL? (Choose two.)

A. DNS-based.
B. Proxy-based.
C. Flow-based.
D. URL-based

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20

Which web filtering inspection mode inspects DNS traffic?

A. DNS-based
B. FQDN-based
C. Flow-based
D. URL-based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21

Which statements are true regarding traffic shaping that is applied in an application sensor, and associated with a firewall policy? (Choose two.)

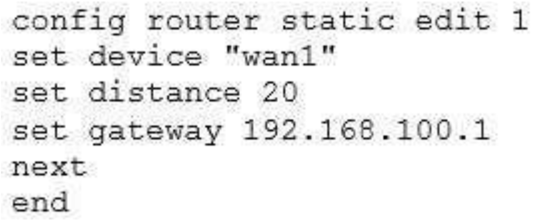
A. Shared traffic shaping cannot be used.
B. Only traffic matching the application control signature is shaped.
C. Can limit the bandwidth usage of heavy traffic applications.
D. Per-IP traffic shaping cannot be used.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

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 is NOT required for this static default route to be displayed in the FortiGate unit's routing table?

A. The Administrative Status of the wan1 interface is displayed as Up.
B. The Link Status of the wan1 interface is displayed as Up.
C. All other default routes should have an equal or higher distance.
D. You must disable DHCP client on that interface.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
When does a FortiGate load-share traffic between two static routes to the same destination subnet?

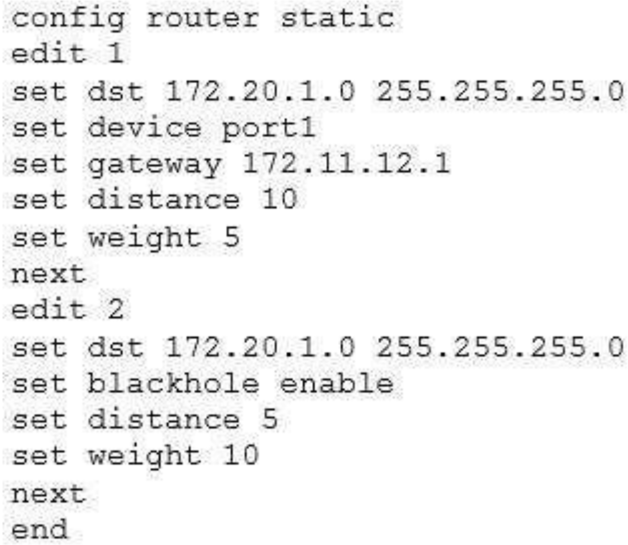
A. When they have the same cost and distance.
B. When they have the same distance and the same weight.
C. When they have the same distance and different priority.

D. When they have the same distance and same priority.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Examine the static route configuration shown below; then answer the question following it. (Choose two.)



```
config router static
edit 1
set dst 172.20.1.0 255.255.255.0
set device port1
set gateway 172.11.12.1
set distance 10
set weight 5
next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable
set distance 5
set weight 10
next
end
```

Which of the following statements correctly describes the static routing configuration provided? (Choose two.)

A. All traffic to 172.20.1.0/24 is dropped by the FortiGate.
B. As long as port1 is up, all traffic to 172.20.1.0/24 is routed by the static route number 1. If the interface port1 is down, the traffic is routed using the blackhole route.
C. The FortiGate unit does NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
D. The FortiGate unit creates a session entry in the session table when the traffic is being routed by the blackhole route.

Correct Answer: AC

Section: (none)
Explanation

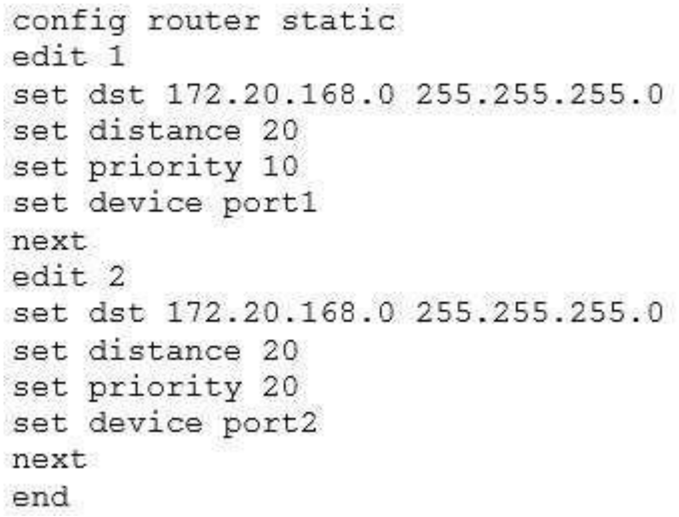
Explanation/Reference:
QUESTION 25
In the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate operating in NAT/Route mode, when searching for a suitable gateway?

A. A lookup is done only when the first packet coming from the client (SYN) arrives
B. A lookup is done when the first packet coming from the client (SYN) arrives, and a second one is performed when the first packet coming from the server (SYN/ ACK) arrives.
C. Three lookups are done during the TCP 3-way handshake (SYN, SYN/ACK, ACK).
D. A lookup is always done each time a packet arrives, from either the server or the client side.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.



```
config router static
edit 1
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 10
set device port1
next
edit 2
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 20
set device port2
next
end
```

Which of the following statements correctly describes the static routing configuration provided above?

A. The FortiGate evenly shares the traffic to 172.20.168.0/24 through both routes.

B. The FortiGate shares the traffic to 172.20.168.0/24 through both routes, but the port2 route will carry approximately twice as much of the traffic.

C. The FortiGate sends all the traffic to 172.20.168.0/24 through port1.

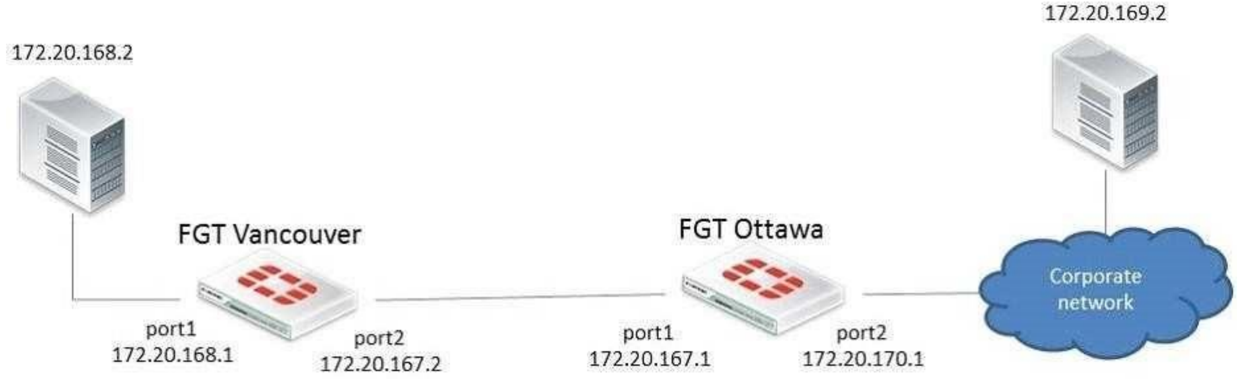
D. Only the route that is using port1 will show up in the routing table.

Correct Answer: C
Section: (none)
Explanation

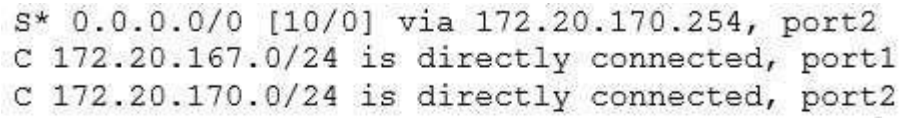
Explanation/Reference:

QUESTION 27

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



In this scenario, the FortiGate unit in Ottawa has the following routing table:



```
S* 0.0.0.0/0 [10/0] via 172.20.170.254, port2
C 172.20.167.0/24 is directly connected, port1
C 172.20.170.0/24 is directly connected, port2
```

Sniffer tests show that packets sent from the source IP address 172.20.168.2 to the destination IP address 172.20.169.2 are being dropped by the FortiGate located in Ottawa. Which of the following correctly describes the cause for the dropped packets?

A. The forward policy check.

B. The reverse path forwarding check.

C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate's routing table.

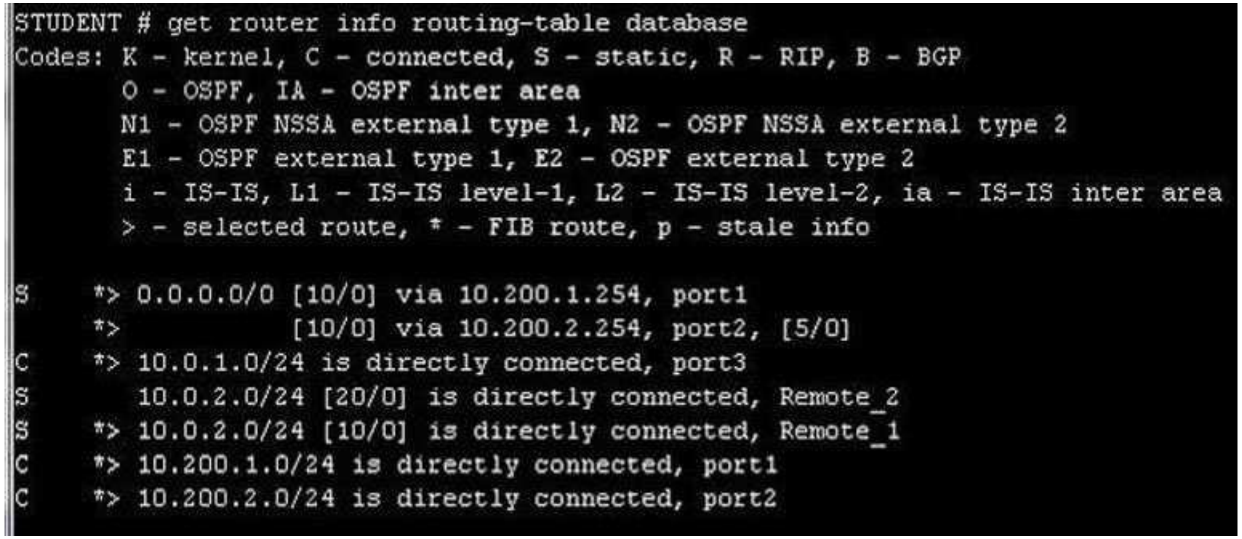
D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

Review the output of the command get router info routing-table database shown in the exhibit below; then answer the question following it.



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

S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
      *>           [10/0] via 10.200.2.254, port2, [5/0]
C     *> 10.0.1.0/24 is directly connected, port3
S        10.0.2.0/24 [20/0] is directly connected, Remote_2
S     *> 10.0.2.0/24 [10/0] is directly connected, Remote_1
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

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

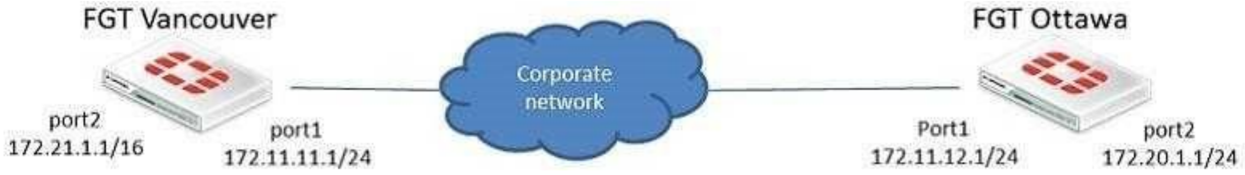
A. There will be six routes in the routing table.
B. There will be seven routes in the routing table.
C. There will be two default routes in the routing table.
D. There will be two routes for the 10.0.2.0/24 subnet in the routing table.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29

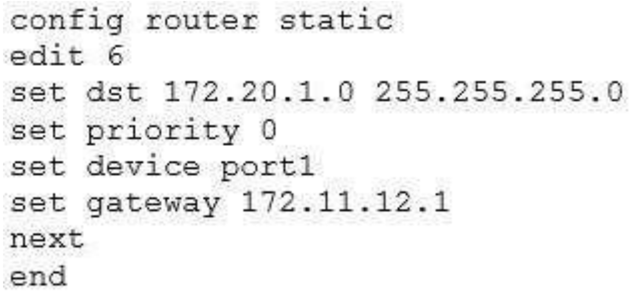
Examine the exhibit; then answer the question below.



The Vancouver FortiGate initially had the following information in its routing table:

S 172.20.0.0/16 [10/0] via 172.21.1.2, port2
C 172.21.0.0/16 is directly connected, port2
C 172.11.11.0/24 is directly connected, port1

Afterwards, the following static route was added:



```
config router static
edit 6
set dst 172.20.1.0 255.255.255.0
set priority 0
set device port1
set gateway 172.11.12.1
next
end
```

Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allowsubnet-overlap first.
B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.
C. The priority is 0, which means that the route will remain inactive.
D. The static route configuration is missing the distance setting.

Correct Answer: B
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?

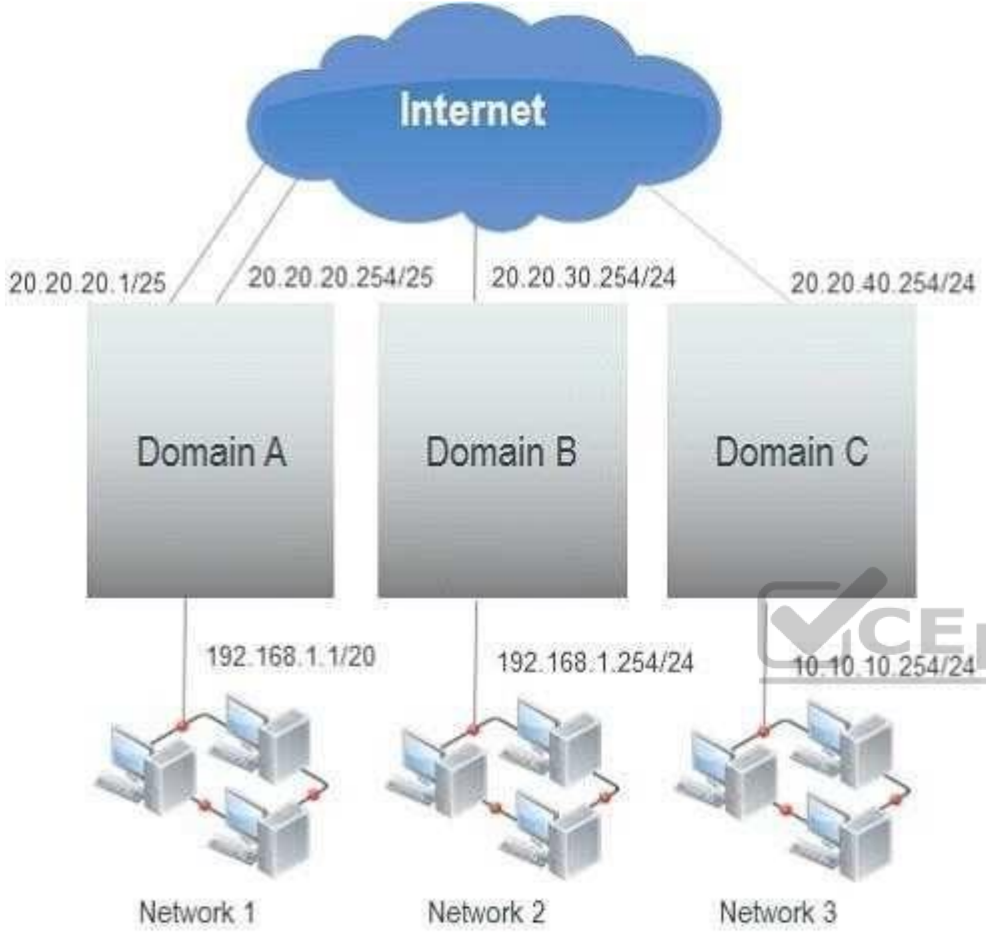
A. The administrator does not have the proper permissions to reassign the dmz interface.
B. The dmz interface is referenced in the configuration of another VDOM.
C. Non-management VDOMs cannot reference physical interfaces.
D. The dmz interface is in PPPoE or DHCP mode.

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

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.

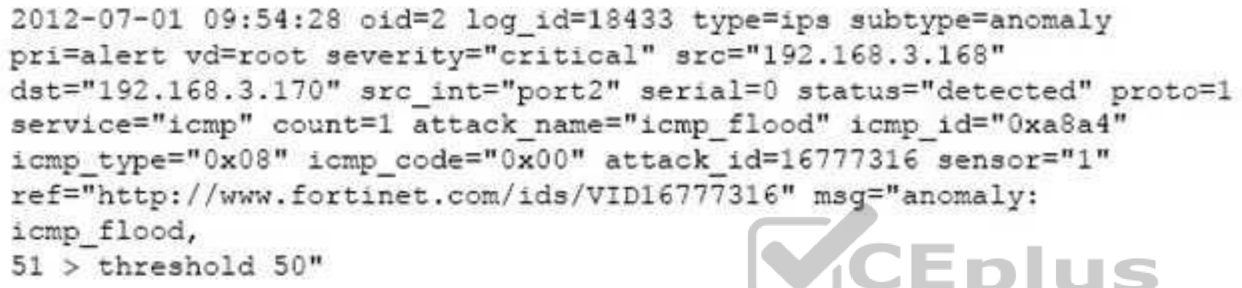
D. There are no hub locations in a partial mesh.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

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 43

Identify the statement which correctly describes the output of the following command:

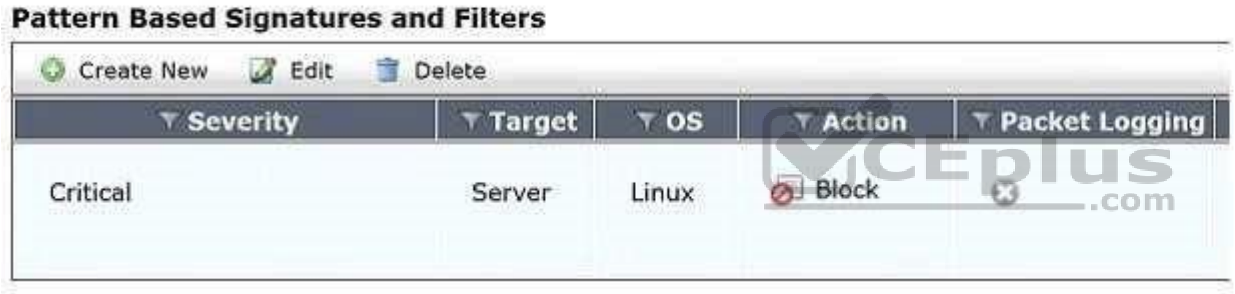
```
diagnose ips anomaly list
```

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 44
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 45

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 46

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 47

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 48
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 49
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 50

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 51
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 52
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 53

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 54

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 55
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 56
Which statements about virtual domains (VDOMs) are true? (Choose two.)

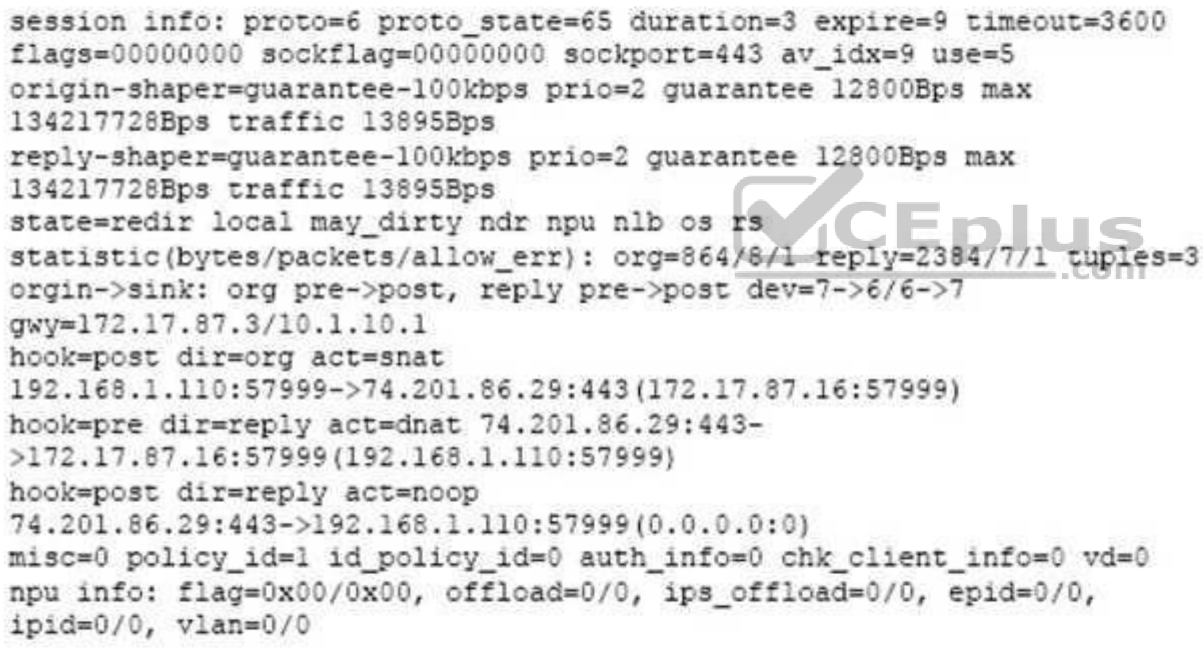
A. Transparent mode and NAT/Route mode VDOMs cannot be combined on the same FortiGate.
B. Each VDOM can be configured with different system hostnames.

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 57
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.)

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 58
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 59
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 60

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 61

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 62

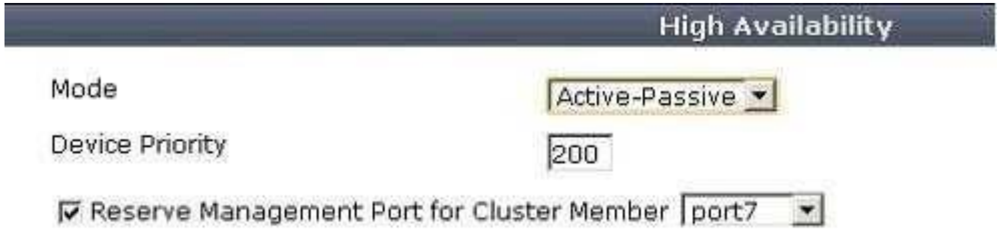
Regarding the header and body sections in raw log messages, which statement is correct?

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 63
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

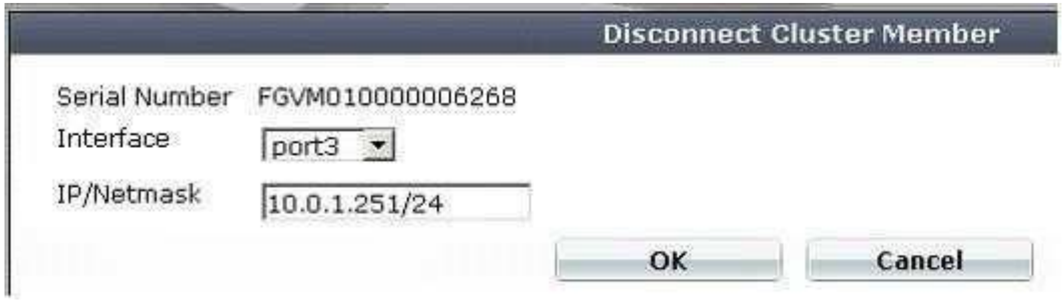
Which statements are correct regarding this setting? (Choose two.)

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 64
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 65
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 66

Which header field can be used in a firewall policy for traffic matching?

A. ICMP type and code.
B. DSCP.
C. TCP window size.
D. TCP sequence number.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 67

The order of the firewall policies is important. Policies can be re-ordered from either the GUI or the CLI. Which CLI command is used to perform this function?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68

Examine the following CLI configuration:

```
config system session-ttl
set default 1800 end
```

What statement is true about the effect of the above configuration line?

A. Sessions can be idle for more than 1800 seconds.
B. The maximum length of time a session can be open is 1800 seconds.
C. After 1800 seconds, the end user must re-authenticate.
D. After a session has been open for 1800 seconds, the FortiGate sends a keepalive packet to both client and server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
In which order are firewall policies processed on a FortiGate unit?
A. From top to down, according with their sequence number.
B. From top to down, according with their policy ID number.
C. Based on best match.
D. Based on the priority value.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which statements are true regarding local user authentication? (Choose two.)

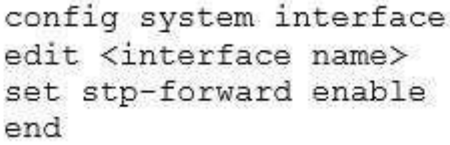
A. Two-factor authentication can be enabled on a per user basis.
B. Local users are for administration accounts only and cannot be used to authenticate network users.
C. Administrators can create the user accounts is a remote server and store the user passwords locally in the FortiGate.
D. Both the usernames and passwords can be stored locally on the FortiGate

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71

Examine the following spanning tree configuration on a FortiGate in transparent mode:



```
config system interface
edit <interface name>
set stp-forward enable
end
```

Which statement is correct for the above configuration?

A. The FortiGate participates in spanning tree.
B. The FortiGate device forwards received spanning tree messages.
C. Ethernet layer-2 loops are likely to occur.
D. The FortiGate generates spanning tree BPDU frames.

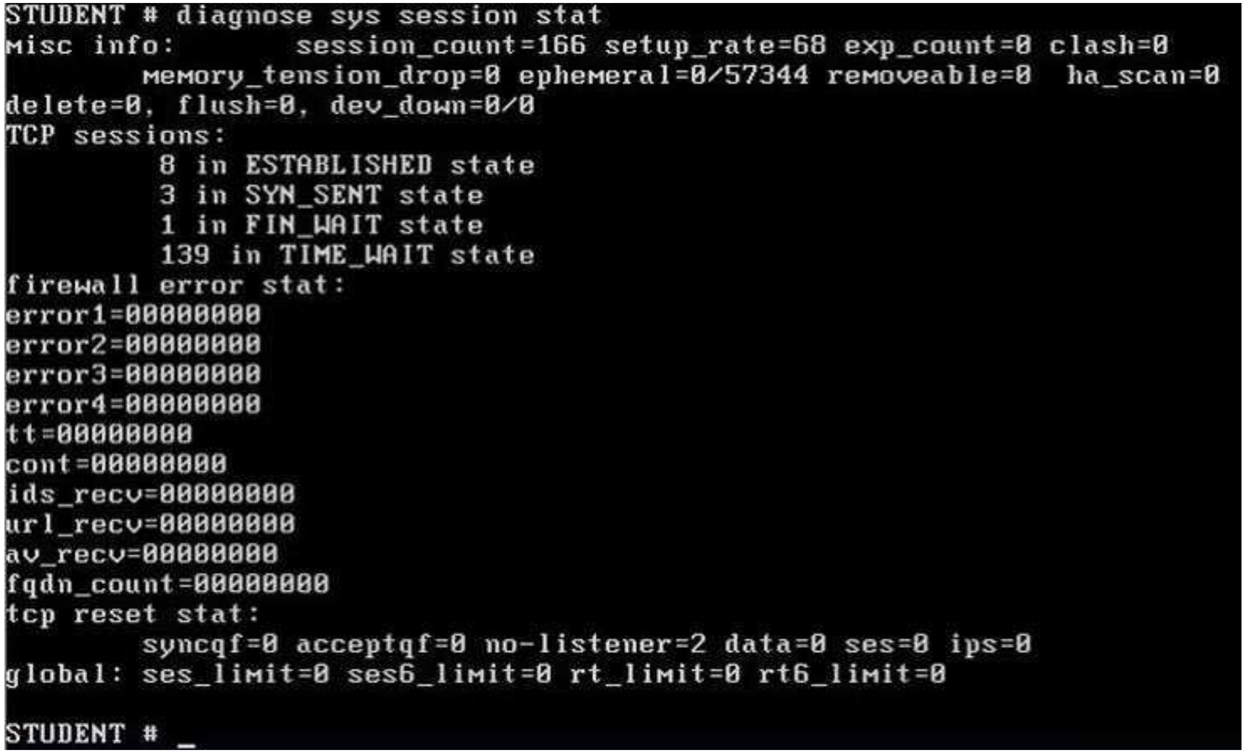
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72

Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of diagnose sys session stat for the STUDENT device. Exhibit B shows the command output of diagnose sys session stat for the REMOTE device.

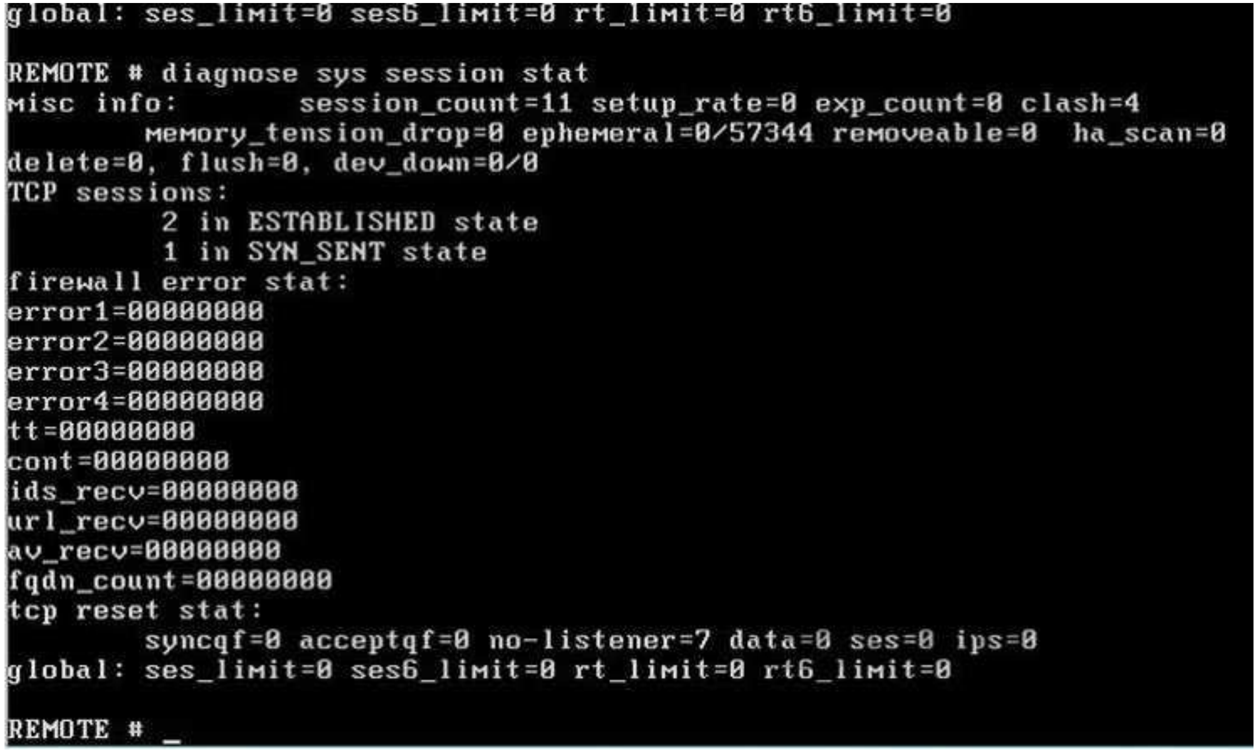
Exhibit A:



```
STUDENT # diagnose sys session stat
misc info:       session_count=166 setup_rate=68 exp_count=0 clash=0
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         8 in ESTABLISHED state
         3 in SYN_SENT state
         1 in FIN_WAIT state
         139 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=2 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

STUDENT # _
```

Exhibit B:



```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
misc info:       session_count=11 setup_rate=0 exp_count=0 clash=4
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         2 in ESTABLISHED state
         1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

Given the information provided in the exhibits, which of the following statements are correct? (Choose two.)

A. STUDENT is likely to be the master device.
B. Session-pickup is likely to be enabled.
C. The cluster mode is active-passive.
D. There is not enough information to determine the cluster mode.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73

An administrator has formed a high availability cluster involving two FortiGate units.

[Multiple upstream Layer 2 switches] -- [FortiGate HA Cluster] -- [Multiple downstream Layer 2 switches]

The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster. Which of the following options describes the best step the administrator can take? The administrator should_____________.

A. Increase the number of FortiGate units in the cluster and configure HA in active-active mode.
B. Enable monitoring of all active interfaces.
C. Set up a full-mesh design which uses redundant interfaces.
D. Configure the HA ping server feature to allow for HA failover in the event that a path is disrupted

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74

In a high availability 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 slave unit?

A. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
B. Request: internal host; slave FortiGate; Internet; web server.
C. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
D. Request: internal host; master FortiGate; slave FortiGate; Internet; web server.

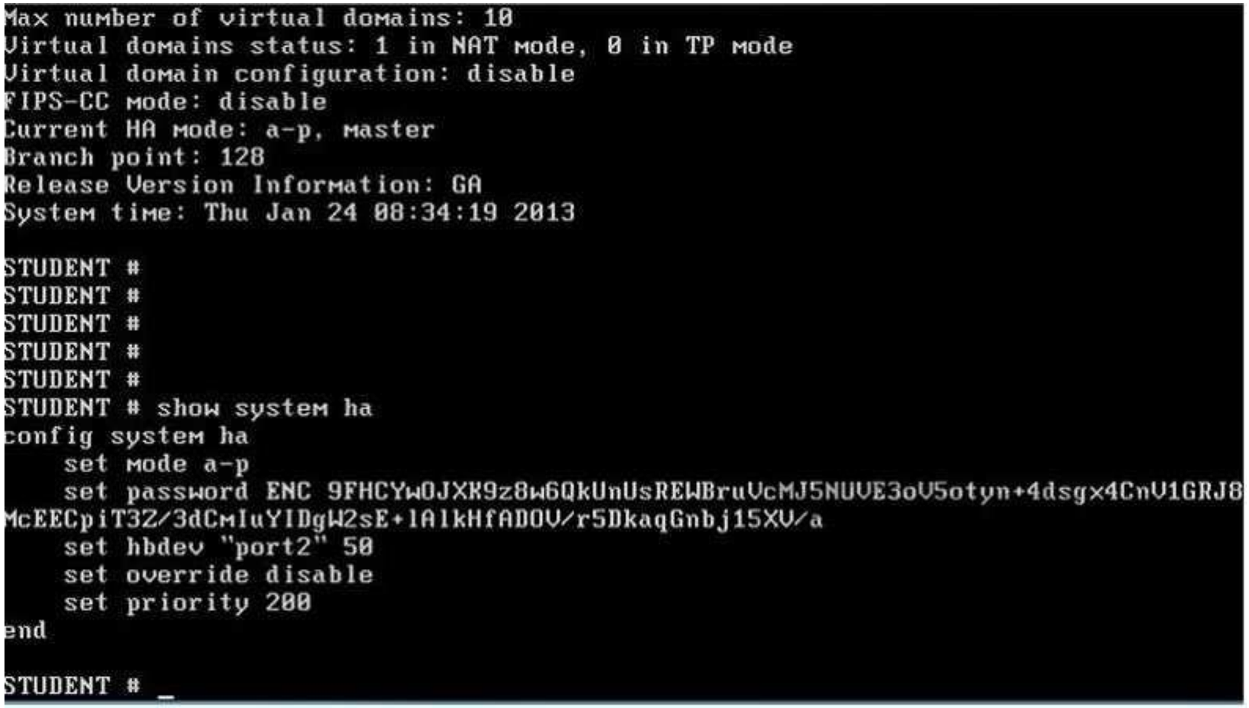
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75

Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of show system ha for the STUDENT device. Exhibit B shows the command output of show system ha for the REMOTE device.

Exhibit A:

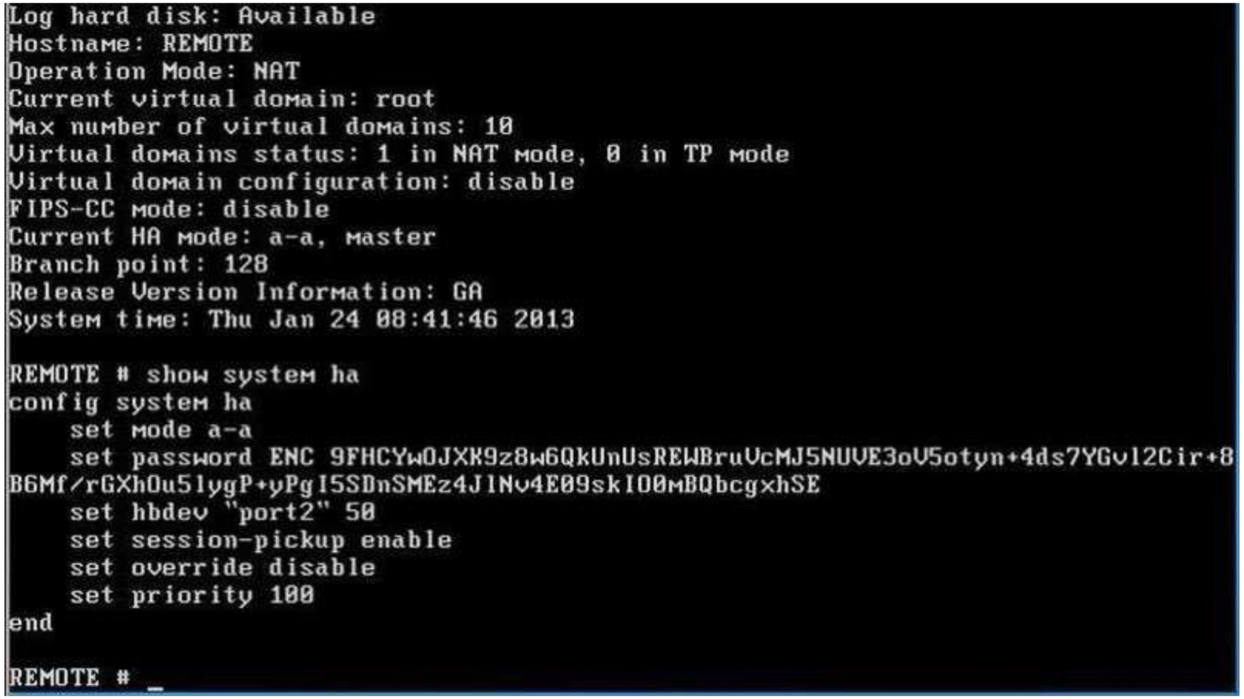


```
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT3Z/3dCmIuYIDgW2sE+lAlkHfADOV/r5DkaqGnbj15XV/a
    set hbdev "port2" 50
    set override disable
    set priority 200
end

STUDENT # _
```

Exhibit B



```
Log hard disk: Available
Hostname: REMOTE
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-a, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:41:46 2013

REMOTE # show system ha
config system ha
    set mode a-a
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4ds7YGvl2Cir+8
B6Mf/rGXhOu5lygP+yPgI5SDnSMEz4JlNv4E09skI00mBQbcgxhSE
    set hbdev "port2" 50
    set session-pickup enable
    set override disable
    set priority 100
end

REMOTE # _
```

Which one of the following is the most likely reason that the cluster fails to form?

A. Password
B. HA mode
C. Heartbeat
D. Override

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?.

A. Policy-based only.
B. Route-based only.
C. Either policy-based or route-based VPN.
D. GRE-based only.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using route- based mode. Users from either side must be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate already has a default route. Which two configuration steps are required to achieve these objectives? (Choose two.)

A. Create one firewall policy.
B. Create two firewall policies.
C. Add a route to the remote subnet.
D. Add two IPsec phases 2.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
An administrator wants to create an IPsec VPN tunnel between two FortiGate devices. Which three configuration steps must be performed on both units to support this scenario? (Choose three.)

A. Create firewall policies to allow and control traffic between the source and destination IP addresses.
B. Configure the appropriate user groups to allow users access to the tunnel.
C. Set the operating mode to IPsec VPN mode.
D. Define the phase 2 parameters.

E. Define the Phase 1 parameters.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
What is IPsec Perfect Forwarding Secrecy (PFS)?

A. A phase-1 setting that allows the use of symmetric encryption.
B. A phase-2 setting that allows the recalculation of a new common secret key each time the session key expires.
C. A `key-agreement' protocol.
D. A `security-association-agreement' protocol.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
An administrator has configured a route-based site-to-site IPsec VPN. Which statement is correct regarding this IPsec VPN configuration?

A. The IPsec firewall policies must be placed at the top of the list.
B. This VPN cannot be used as part of a hub and spoke topology.
C. Routes are automatically created based on the quick mode selectors.
D. A virtual IPsec interface is automatically created after the Phase 1 configuration is completed.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 81

A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received.
Which are two reasons for this problem? (Choose two.)

A. The FortiGate is connected to multiple ISPs.
B. There is a NAT device between the FortiGate and the FortiGuard Distribution Network.
C. The FortiGate is in Transparent mode.
D. The external facing interface of the FortiGate is configured to get the IP address from a DHCP server.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which statement is correct regarding virus scanning on a FortiGate unit?

A. Virus scanning is enabled by default.
B. Fortinet customer support enables virus scanning remotely for you.
C. Virus scanning must be enabled in a security profile, which must be applied to a firewall policy.
D. Enabling virus scanning in a security profile enables virus protection for all traffic flowing through the FortiGate.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

A. Proxy-based
B. DNS-basedC. Flow-based
D. Man-in-the-middle.
Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

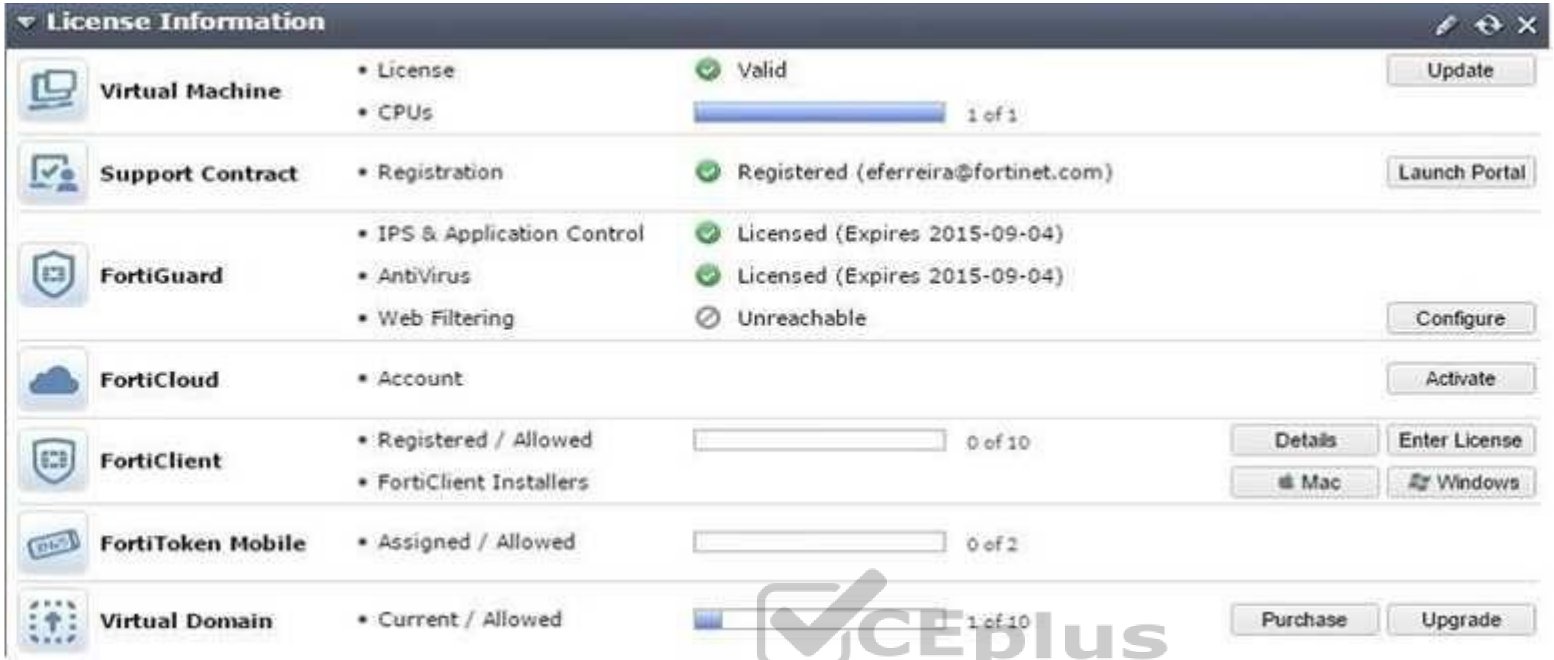
QUESTION 84
Which antivirus and attack definition update options are supported by FortiGate units? (Choose two.)

A. Manual update by downloading the signatures from the support site.
B. Pull updates from the FortiGate.
C. Push updates from a FortiAnalyzer.
D. execute fortiguard-AV-AS command from the CLI.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Examine the exhibit; then answer the question below.



License Information

Virtual Machine	• License	✓ Valid	
	• CPUs	1 of 1	
Support Contract	• Registration	✓ Registered (eferreira@fortinet.com)	
FortiGuard	• IPS & Application Control	✓ Licensed (Expires 2015-09-04)	
	• AntiVirus	✓ Licensed (Expires 2015-09-04)	
	• Web Filtering	⊘ Unreachable	
FortiCloud	• Account		
FortiClient	• Registered / Allowed	0 of 10	
	• FortiClient Installers		
FortiToken Mobile	• Assigned / Allowed	0 of 2	
Virtual Domain	• Current / Allowed	1 of 10	

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
For traffic that does match any configured firewall policy, what is the default action taken by the FortiGate?
A. The traffic is allowed and no log is generated.

B. The traffic is allowed and logged.
C. The traffic is blocked and no log is generated.
D. The traffic is blocked and logged.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

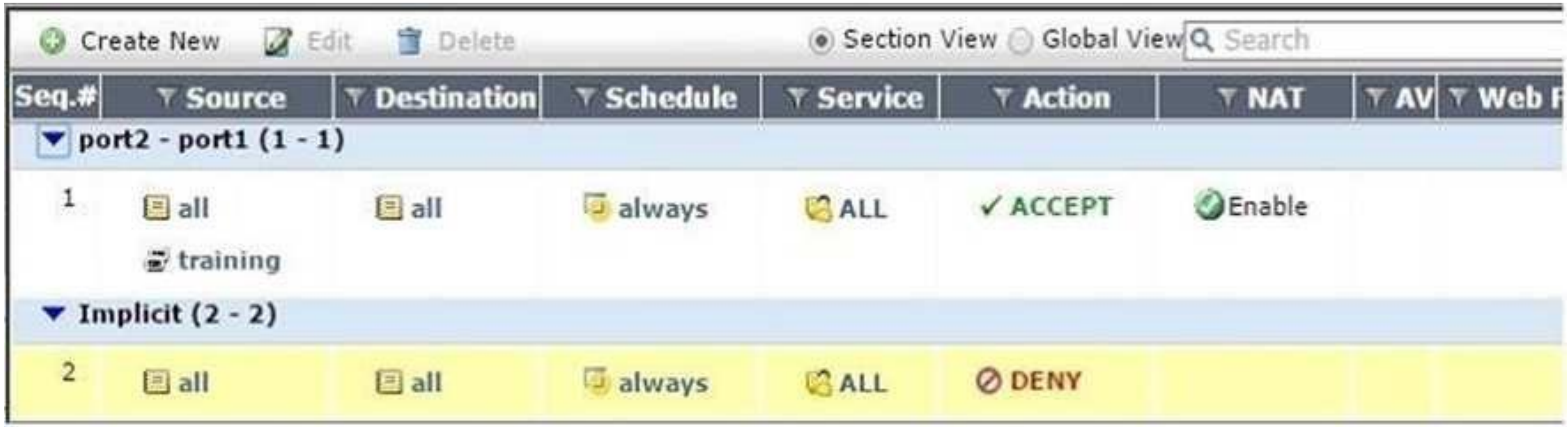
QUESTION 87
What methods can be used to deliver the token code to a user that is configured to use two-factor authentication? (Choose three.)

A. Browser pop-up window.
B. FortiToken.
C. Email.
D. Code books.
E. SMS phone message.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.



Create New | Edit | Delete | ● Section View ○ Global View | Search

Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web F
port2 - port1 (1 - 1)								
1	all training	all	always	ALL	✓ ACCEPT	Enable		
Implicit (2 - 2)								
2	all	all	always	ALL	⊘ DENY			

Based on the firewall configuration illustrated in the exhibit, which statement is correct?

A. A user that has not authenticated can access the Internet using any protocol that does not trigger an authentication challenge.
B. A user that has not authenticated can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP.
C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access all Internet services.
D. DNS Internet access is always allowed, even for users that has not authenticated.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
When firewall policy authentication is enabled, which protocols can trigger an authentication challenge? (Choose two.)

A. SMTP
B. POP3
C. HTTP
D. FTP

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which statement regarding the firewall policy authentication timeout is true?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which two statements are true regarding firewall policy disclaimers? (Choose two.)

A. They cannot be used in combination with user authentication.
B. They can only be applied to wireless interfaces.
C. Users must accept the disclaimer to continue.
D. The disclaimer page is customizable.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following items is NOT a packet characteristic matched by a firewall service object?

A. ICMP type and code
B. TCP/UDP source and destination ports
C. IP protocol number
D. TCP sequence number

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
When firewall policy authentication is enabled, only traffic on supported protocols will trigger an authentication challenge.
Select all supported protocols from the following:

A. SMTP
B. SSH
C. HTTP

D. FTP
E. SCP

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94

A client can create a secure connection to a FortiGate device using SSL VPN in web-only mode. Which one of the following statements is correct regarding the use of web-only mode SSL VPN?

A. Web-only mode supports SSL version 3 only.
B. A Fortinet-supplied plug-in is required on the web client to use web-only mode SSL VPN.
C. Web-only mode requires the user to have a web browser that supports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client to be able to connect to a web- only mode SSL VPN.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95

A client can establish a secure connection to a corporate network using SSL VPN in tunnel mode. Which of the following statements are correct regarding the use of tunnel mode SSL VPN? (Select all that apply.)

A. Split tunneling can be enabled when using tunnel mode SSL VPN.
B. Client software is required to be able to use a tunnel mode SSL VPN.
C. Users attempting to create a tunnel mode SSL VPN connection must be authenticated by at least one SSL VPN policy.
D. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96

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 97
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 98
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) QUESTION 99**
What are the valid sub-types for a Firewall type policy? (Select all that apply)

Explanation

Explanation/Reference:

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

Correct Answer: ABC
Section: (none) Explanation

Explanation/Reference:

QUESTION 100
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 101
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 102

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 103

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)
QUESTION 104

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?

Explanation

Explanation/Reference:

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 105
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 106
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 107

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 108

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) QUESTION 109**

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.

Explanation

Explanation/Reference:

Correct Answer: ABCD
Section: (none) Explanation

Explanation/Reference:

QUESTION 110 FILL BLANK
The____________ CLI command is used on the FortiGate unit to run static commands such as ping or to reset the FortiGate unit to factory defaults.

Correct Answer: execute
Section: (none) Explanation

Explanation/Reference:

QUESTION 111
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 112
When creating administrative users which of the following configuration objects determines access rights on the FortiGate unit.

A. profile
B. allowaccess interface settings
C. operation mode
D. local-in policy

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 113
Which of the following options can you use to update the virus definitions on a FortiGate unit? (Select all that apply.)

A. Push update.
B. Scheduled update
C. Manual update
D. FTP update

Correct Answer: ABC
Section: (none) Explanation

Explanation/Reference:

QUESTION 114
Which of the following statements are true of the FortiGate unit's factory default configuration?

A. `Port1' or `Internal' interface will have an IP of 192.168.1.99.
B. `Port1' or `Internal' interface will have a DHCP server set up and enabled (on devices that support DHCP Servers).
C. Default login will always be the username: admin (all lowercase) and no password.
D. The implicit firewall action is ACCEPT.

Correct Answer: ABC
Section: (none) Explanation

Explanation/Reference:

QUESTION 115
Under the System Information widget on the dashboard, which of the following actions are available for the system configuration? (Select all that apply.)

A. Backup
B. Restore
C. Revisions
D. Export

Correct Answer: ABC
Section: (none) Explanation

Explanation/Reference:

QUESTION 116
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 117
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 118

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 119
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 120
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 121
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 122
Which of the following authentication types are supported by FortiGate units? (Select all that apply.)

A. Kerberos
B. LDAP
C. RADIUS
D. Local Users

Correct Answer: BCD
Section: (none) Explanation

Explanation/Reference:

QUESTION 123

Which of the following are valid authentication user group types on a FortiGate unit? (Select all that apply.)

A. Firewall
B. Directory Service
C. Local
D. LDAP
E. PKI

Correct Answer: AB
Section: (none) Explanation

Explanation/Reference:

QUESTION 124
Users may require access to a web site that is blocked by a policy. Administrators can give users the ability to override the block. Which of the following statements regarding overrides are correct? (Select all that apply.)

A. A protection profile may have only one user group defined as an override group.
B. A firewall user group can be used to provide override privileges for FortiGuard Web Filtering.
C. Authentication to allow the override is based on a user's membership in a user group.
D. Overrides can be allowed by the administrator for a specific period of time.

Correct Answer: BCD
Section: (none) Explanation

Explanation/Reference:

QUESTION 125
Users may require access to a web site that is blocked by a policy. Administrators can give users the ability to override the block. Which of the following statements regarding overrides is NOT correct?

A. A web filter profile may only have one user group defined as an override group.
B. A firewall user group can be used to provide override privileges for FortiGuard Web Filtering.
C. When requesting an override, the matched user must belong to a user group for which the override capability has been enabled.
D. Overrides can be allowed by the administrator for a specific period of time.

Correct Answer: A

Section: (none) Explanation

Explanation/Reference:

QUESTION 126
An administrator has configured a FortiGate unit so that end users must authenticate against the firewall using digital certificates before browsing the Internet.
What must the user have for a successful authentication? (Select all that apply.)

A. An entry in a supported LDAP Directory.
B. A digital certificate issued by any CA server.
C. A valid username and password.
D. A digital certificate issued by the FortiGate unit.
E. Membership in a firewall user group.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
The FortiGate unit can be configured to allow authentication to a RADIUS server. The RADIUS server can use several different authentication protocols during the authentication process.
Which of the following are valid authentication protocols that can be used when a user authenticates to the RADIUS server? (Select all that apply.)

A. MS-CHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol v2)
B. PAP (Password Authentication Protocol)
C. CHAP (Challenge-Handshake Authentication Protocol)
D. MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol v1)
E. FAP (FortiGate Authentication Protocol)

Correct Answer: ABCD
Section: (none) Explanation
Explanation/Reference:

QUESTION 128
Which of the following are valid components of the Fortinet Server Authentication Extensions (FSAE)? (Select all that apply.)

A. Domain Local Security Agent.
B. Collector Agent.
C. Active Directory Agent.
D. User Authentication Agent.
E. Domain Controller Agent.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
A FortiGate unit can create a secure connection to a client using SSL VPN in tunnel mode. Which of the following statements are correct regarding the use of tunnel mode SSL VPN? (Select all that apply.)

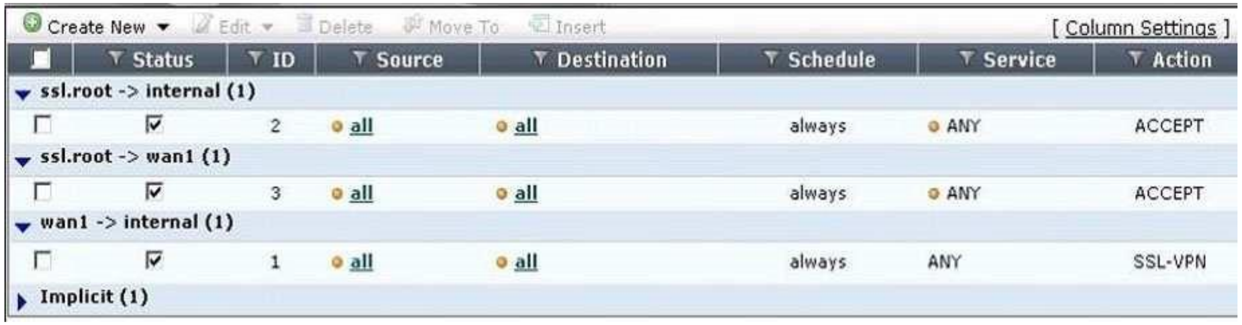
A. Split tunneling can be enabled when using tunnel mode SSL VPN.
B. Software must be downloaded to the web client to be able to use a tunnel mode SSL VPN.
C. Users attempting to create a tunnel mode SSL VPN connection must be members of a configured user group on the FortiGate unit.
D. Tunnel mode SSL VPN requires the FortiClient software to be installed on the user's computer.
E. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Correct Answer: ABCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
An end user logs into the SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has not enabled split tunneling and so the end user must access the Internet through the SSL VPN Tunnel.

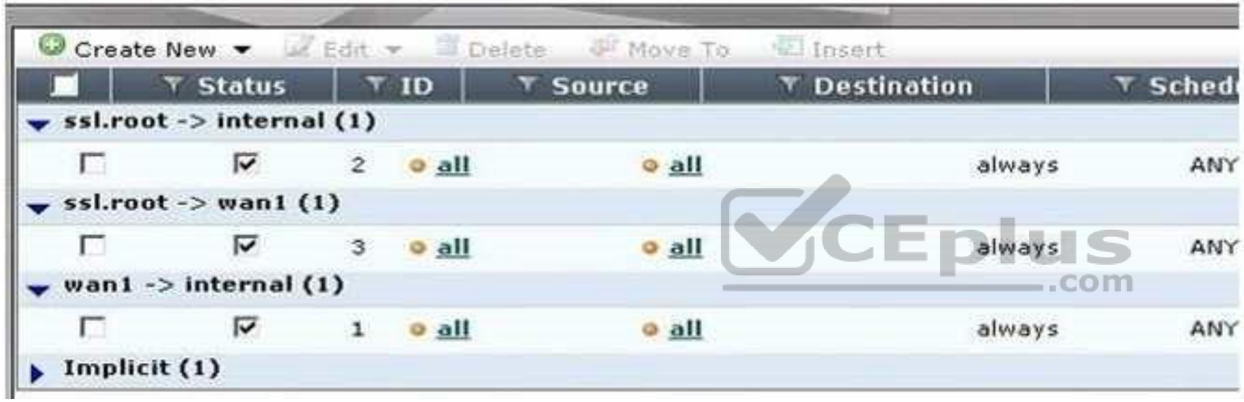
Which firewall policies are needed to allow the end user to not only access the internal network but also reach the Internet? A.



Create New ▾ | Edit ▾ | Delete | Move To | Insert | [Column Settings]

☐	Status	ID	Source	Destination	Schedule	Service	Action
ssl.root -> internal (1)							
☐	☑	2	all	all	always	ANY	ACCEPT
ssl.root -> wan1 (1)							
☐	☑	3	all	all	always	ANY	ACCEPT
wan1 -> internal (1)							
☐	☑	1	all	all	always	ANY	SSL-VPN
Implicit (1)							

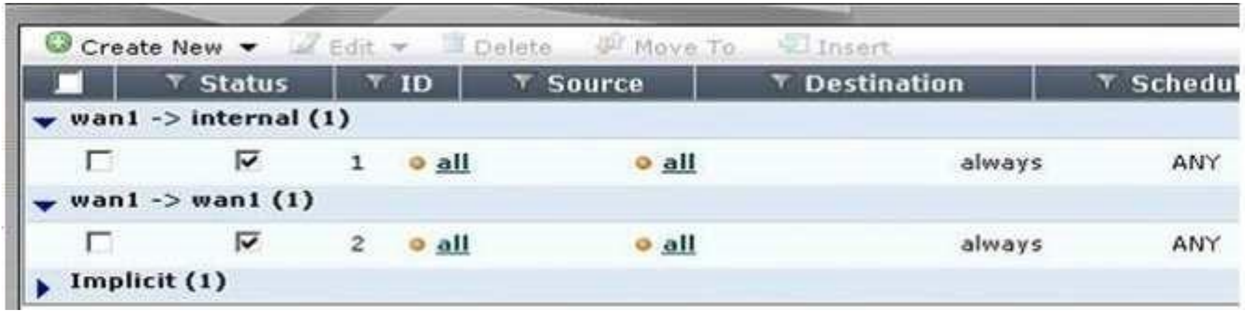
B.



Create New ▾ | Edit ▾ | Delete | Move To | Insert

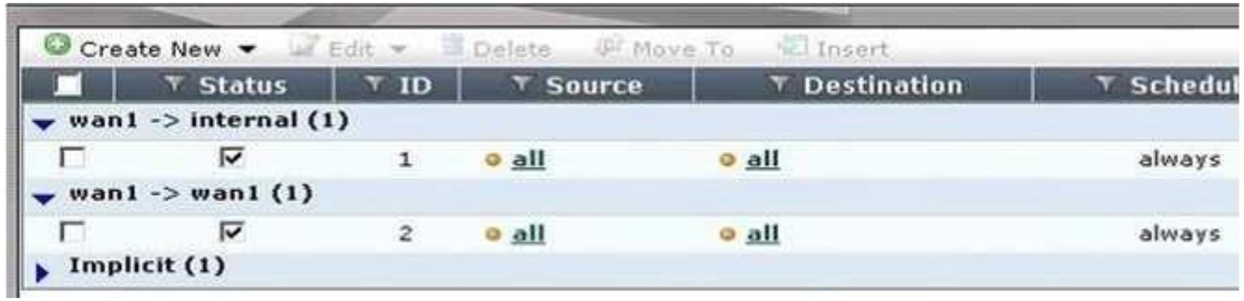
☐	Status	ID	Source	Destination	Sched
ssl.root -> internal (1)					
☐	☑	2	all	all	always ANY
ssl.root -> wan1 (1)					
☐	☑	3	all	all	always ANY
wan1 -> internal (1)					
☐	☑	1	all	all	always ANY
Implicit (1)					

C.



Create New ▾ | Edit ▾ | Delete | Move To | Insert

☐	Status	ID	Source	Destination	Schedul
wan1 -> internal (1)					
☐	☑	1	all	all	always ANY
wan1 -> wan1 (1)					
☐	☑	2	all	all	always ANY
Implicit (1)					

D. 

☐	Status	ID	Source	Destination	Schedul
▾ wan1 -> internal (1)					
☐	☑	1	● all	● all	always
▾ wan1 -> wan1 (1)					
☐	☑	2	● all	● all	always
▸ Implicit (1)					

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 131
Which of the following antivirus and attack definition update features are supported by FortiGate units? (Select all that apply.)

A. Manual, user-initiated updates from the FortiGuard Distribution Network.
B. Hourly, daily, or weekly scheduled antivirus and attack definition and antivirus engine updates from the FortiGuard Distribution Network.
C. Push updates from the FortiGuard Distribution Network.
D. Update status including version numbers, expiry dates, and most recent update dates and times.

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

Explanation/Reference:

QUESTION 132
By default, the Intrusion Protection System (IPS) on a FortiGate unit is set to perform which action?

A. Block all network attacks.
B. Block the most common network attacks.
C. Allows all traffic
D. Allow and log all traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
A FortiGate unit can scan for viruses on which types of network traffic? (Select all that apply.)

A. POP3
B. FTP
C. SMTP
D. SNMP
E. NetBios

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

Explanation/Reference:

QUESTION 134
Which of the following statements regarding Banned Words are correct? (Select all that apply.)

A. The FortiGate unit can scan web pages and email messages for instances of banned words.
B. When creating a banned word list, an administrator can indicate either specific words or patterns.
C. Banned words can be expressed as wildcards or regular expressions.
D. Content is automatically blocked if a single instance of a banned word appears.
E. The FortiGate unit includes a pre-defined library of common banned words.

Correct Answer: ABC
Section: (none) Explanation

Explanation/Reference:

QUESTION 135
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 136
Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The available actions for URL Filtering are Allow and Block.
B. Multiple URL Filter lists can be added to a single Web filter profile.
C. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.
D. The available actions for URL Filtering are Allow, Block and Exempt.

Correct Answer: D

Explanation/Reference:

Section: (none)
Explanation QUESTION 137
Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The FortiGate unit can filter URLs based on patterns using text and regular expressions.
B. The available actions for URL Filtering are Allow and Block.
C. Multiple URL Filter lists can be added to a single Web filter profile.
D. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
Which of the following Regular Expression patterns will make the term "bad language" case insensitive?

A. [bad language]
B. /bad language/i
C. i/bad language/
D. "bad language"
E. /bad language/c

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
SSL content inspection is enabled on the FortiGate unit. Which of the following steps is required to prevent a user from being presented with a web browser warning when accessing an SSL- encrypted website?

A. The root certificate of the FortiGate SSL proxy must be imported into the local certificate store on the user's workstation.

B. Disable the strict server certificate check in the web browser under Internet Options.
C. Enable transparent proxy mode on the FortiGate unit.
D. Enable NTLM authentication on the FortiGate unit. NTLM authentication suppresses the certificate warning messages in the web browser.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following statements describes the method of creating a policy to block access to an FTP site?

A. Enable Web Filter URL blocking and add the URL of the FTP site to the URL Block list.
B. Create a firewall policy with destination address set to the IP address of the FTP site, the Service set to FTP, and the Action set to Deny.
C. Create a firewall policy with a protection profile containing the Block FTP option enabled.
D. None of the above.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
UTM features can be applied to which of the following items?

A. Firewall policies
B. User groups
C. Policy routes
D. Address groups

Correct Answer: A

Explanation/Reference:

Section: (none) Explanation QUESTION 142

Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function. How are UTM features applied to traffic?

A. One or more UTM features are enabled in a firewall policy.
B. In the system configuration for that UTM feature, you can identify the policies to which the feature is to be applied.
C. Enable the appropriate UTM objects and identify one of them as the default.
D. For each UTM object, identify which policy will use it.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143

If no firewall policy is specified between two FortiGate interfaces and zones are not used, which of the following statements describes the action taken on traffic flowing between these interfaces?

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 144

Which of the following products can be installed on a computer running Windows XP to provide personal firewall protection, antivirus protection, web and mail filtering, spam filtering, and VPN functionality?

A. FortiGate
B. FortiAnalyzer

C. FortiClient
D. FortiManager
E. FortiReporter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
File blocking rules are applied before which of the following?

A. Firewall policy processing
B. Virus scanning
C. Web URL filtering
D. White/Black list filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Which of the following pieces of information can be included in the Destination Address field of a firewall policy?

A. An IP address pool, a virtual IP address, an actual IP address, and an IP address group.
B. A virtual IP address, an actual IP address, and an IP address group.
C. An actual IP address and an IP address group.
D. Only an actual IP address.

Correct Answer: B

Explanation/Reference:

Section: (none) Explanation QUESTION 147

FortiGate units are preconfigured with four default protection profiles. These protection profiles are used to control the type of content inspection to be performed. What action must be taken for one of these profiles to become active?

A. The protection profile must be assigned to a firewall policy.
B. The "Use Protection Profile" option must be selected in the Web Config tool under the sections for AntiVirus, IPS, WebFilter, and AntiSpam.
C. The protection profile must be set as the Active Protection Profile.
D. All of the above.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148

A FortiGate 60 unit is configured for your small office. The DMZ interface is connected to a network containing a web server and email server. The Internal interface is connected to a network containing 10 user workstations and the WAN1 interface is connected to your ISP.
You want to configure firewall policies so that your users can send and receive email messages to the email server on the DMZ network.
You also want the email server to be able to retrieve email messages from an email server hosted by your ISP using the POP3 protocol.
Which policies must be created for this communication? (Select all that apply.)

A. Internal > DMZ
B. DMZ > Internal
C. Internal > WAN1
D. WAN1 > Internal
E. DMZ > WAN1F. WAN1 > DMZ

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149

Which of the following network protocols can be used to access a FortiGate unit as an administrator?

Explanation/Reference:

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 150
Which of the following statements is correct regarding a FortiGate unit operating in NAT/Route mode?

A. The FortiGate unit requires only a single IP address for receiving updates and configuring from a management computer.
B. The FortiGate unit must use public IP addresses on both the internal and external networks.
C. The FortiGate unit commonly uses private IP addresses on the internal network but hides them using network address translation.
D. The FortiGate unit uses only DHCP-assigned IP addresses on the internal network.

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 151
Which of the following statements correctly describes how a FortiGate unit functions in Transparent mode?

A. To manage the FortiGate unit, one of the interfaces must be designated as the management interface. This interface may not be used for forwarding data.
B. An IP address is used to manage the FortiGate unit but this IP address is not associated with a specific interface.
C. The FortiGate unit must use public IP addresses on the internal and external networks.
D. The FortiGate unit uses private IP addresses on the internal network but hides them using address translation.

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 152

The Idle Timeout setting on a FortiGate unit applies to which of the following?

A. Web browsing
B. FTP connections
C. User authentication
D. Administrator access
E. Web filtering overrides

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 153

If a FortiGate unit has a dmz interface IP address of 210.192.168.2 with a subnet mask of 255.255.255.0, what is a valid dmz DHCP addressing range?

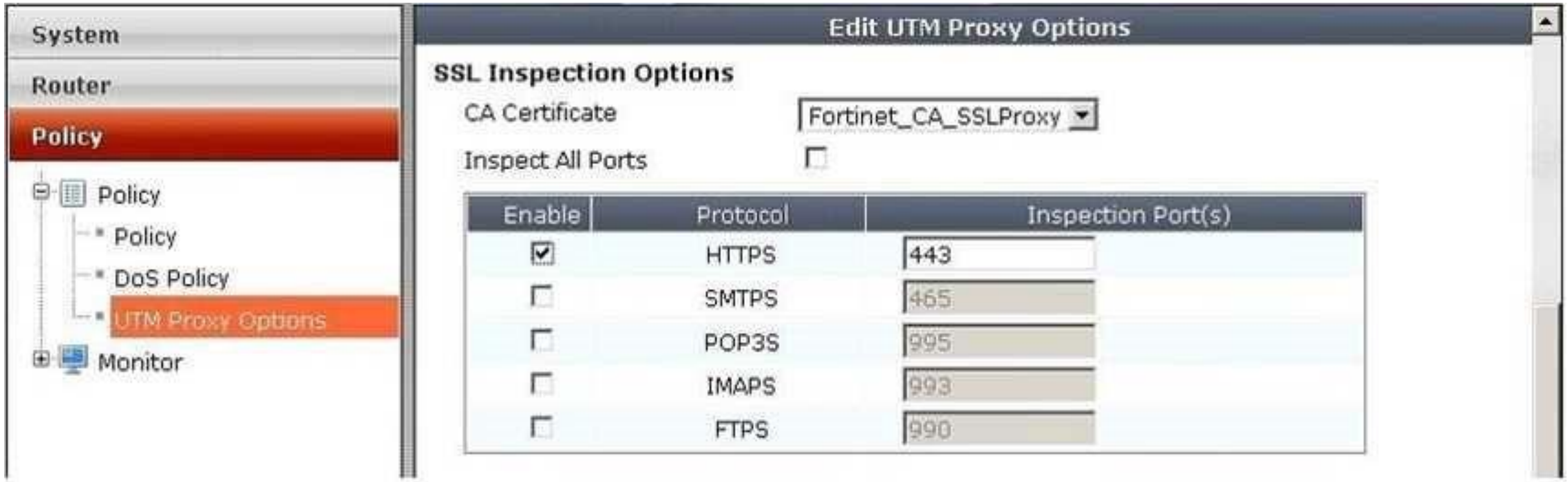
A. 172.168.0.1 - 172.168.0.10
B. 210.192.168.3 - 210.192.168.10C. 210.192.168.1 - 210.192.168.4
D. All of the above.

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 154

Examine the exhibit shown below then answer the question that follows it.



Edit UTM Proxy Options

SSL Inspection Options

CA Certificate: Fortinet_CA_SSLProxy

Inspect All Ports □

Enable	Protocol	Inspection Port(s)
☑	HTTPS	443
□	SMTPS	465
□	POP3S	995
□	IMAPS	993
□	FTPS	990

Within the UTM Proxy Options, the CA certificate Fortinet_CA_SSLProxy defines which of the following:

A. FortiGate unit's encryption certificate used by the SSL proxy.
B. FortiGate unit's signing certificate used by the SSL proxy.
C. FortiGuard's signing certificate used by the SSL proxy.
D. FortiGuard's encryption certificate used by the SSL proxy.

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 155
Shown below is a section of output from the debug command diag ip arp list.

```
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e state=00000004
use=4589 confirm=4589 update=2422 ref=1
```

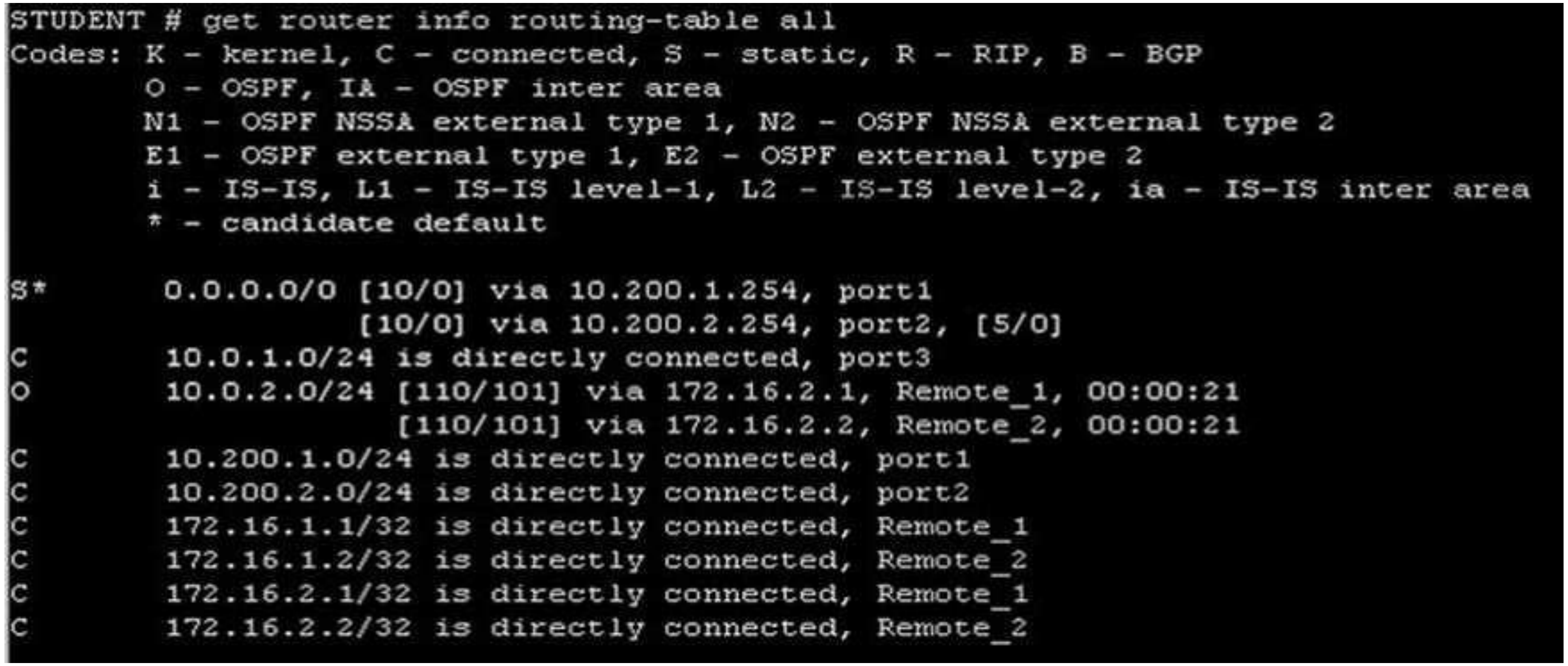
In the output provided, which of the following best describes the IP address 172.20.187.150?

A. It is the primary IP address of the port1 interface.
B. It is one of the secondary IP addresses of the port1 interface.
C. It is the IP address of another network device located in the same LAN segment as the FortiGate unit's port1 interface.

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 156
Review the output of the command get router info routing-table all shown in the Exhibit below; then answer the question following it.



```
STUDENT # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*       0.0.0.0/0 [10/0] via 10.200.1.254, port1
                   [10/0] via 10.200.2.254, port2, [5/0]
C        10.0.1.0/24 is directly connected, port3
O        10.0.2.0/24 [110/101] via 172.16.2.1, Remote_1, 00:00:21
                     [110/101] via 172.16.2.2, Remote_2, 00:00:21
C        10.200.1.0/24 is directly connected, port1
C        10.200.2.0/24 is directly connected, port2
C        172.16.1.1/32 is directly connected, Remote_1
C        172.16.1.2/32 is directly connected, Remote_2
C        172.16.2.1/32 is directly connected, Remote_1
C        172.16.2.2/32 is directly connected, Remote_2
```

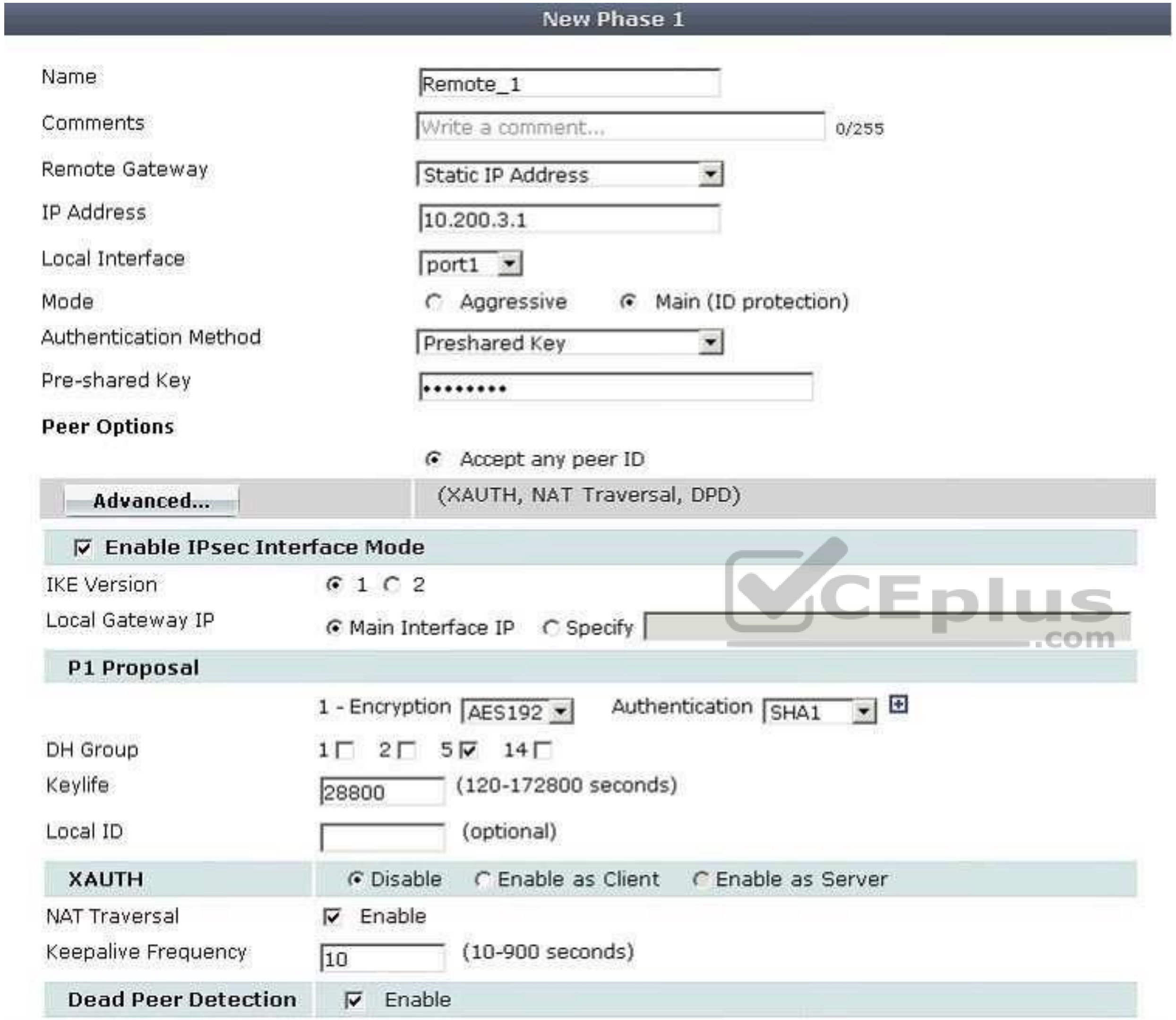
Which one of the following statements correctly describes this output?
A. The two routes to the 10.0.2.0/24 subnet are ECMP routes and traffic will be load balanced based on the configured ECMP settings.
B. The route to the 10.0.2.0/24 subnet via interface Remote_1 is the active and the route via Remote_2 is the backup.
C. OSPF does not support ECMP therefore only the first route to subnet 10.0.1.0/24 is used.

D. 172.16.2.1 is the preferred gateway for subnet 10.0.2.0/24.

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 157
Review the IPsec phase1 configuration in the Exhibit shown below; then answer the question following it.



New Phase 1

Name	Remote_1
Comments	Write a comment... 0/255
Remote Gateway	Static IP Address
IP Address	10.200.3.1
Local Interface	port1
Mode	○ Aggressive ● Main (ID protection)
Authentication Method	Preshared Key
Pre-shared Key	••••••••

Peer Options

● Accept any peer ID

Advanced... (XAUTH, NAT Traversal, DPD)

☑ **Enable IPsec Interface Mode**

IKE Version	● 1 ○ 2
Local Gateway IP	● Main Interface IP ○ Specify

P1 Proposal

	1 - Encryption AES192 Authentication SHA1
DH Group	1 □ 2 □ 5 ☑ 14 □
Keylife	28800 (120-172800 seconds)
Local ID	(optional)
XAUTH	● Disable ○ Enable as Client ○ Enable as Server
NAT Traversal	☑ Enable
Keepalive Frequency	10 (10-900 seconds)
Dead Peer Detection	☑ Enable

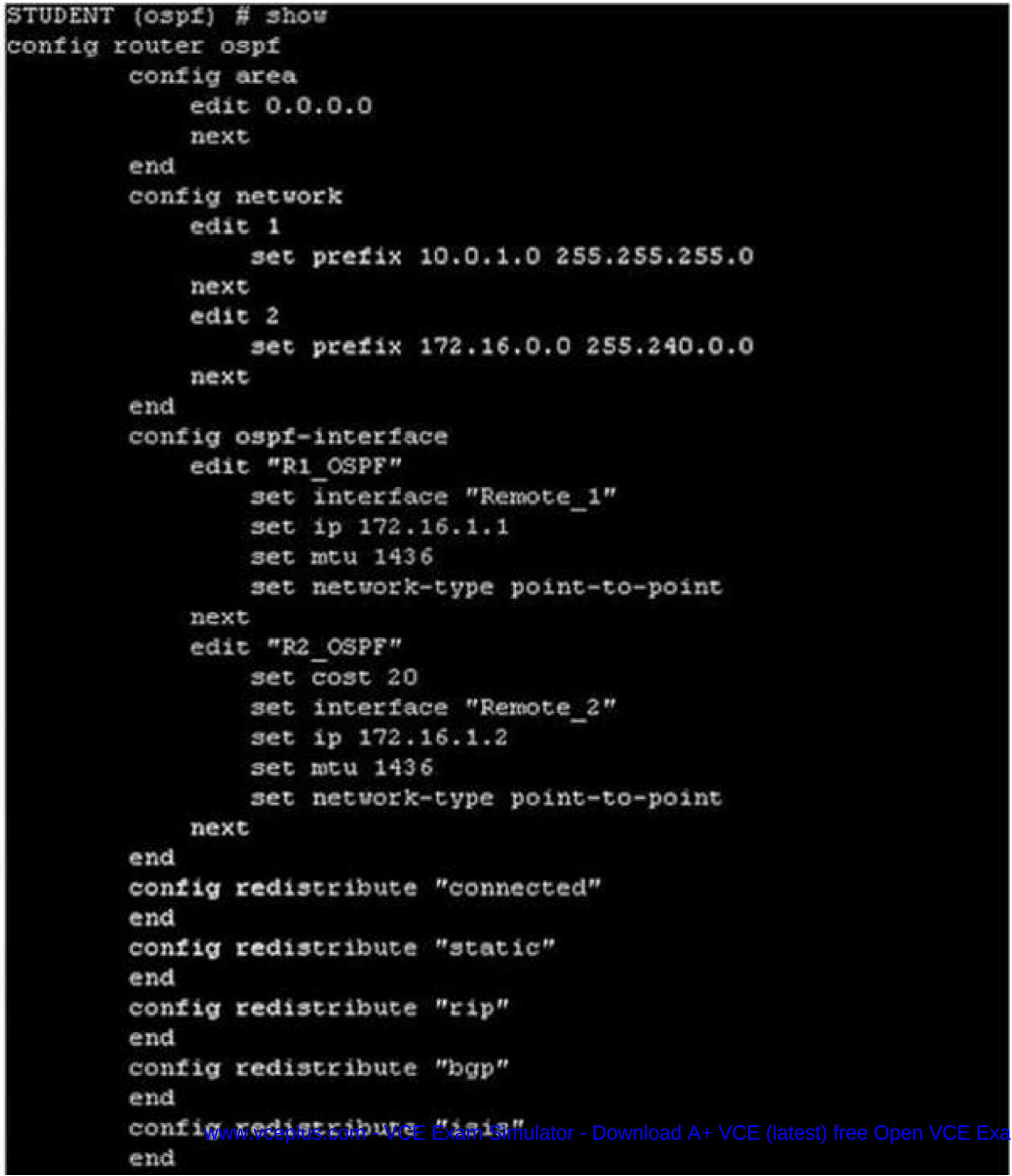
Which of the following statements are correct regarding this configuration? (Select all that apply).

A. The phase1 is for a route-based VPN configuration.
B. The phase1 is for a policy-based VPN configuration.
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 158
Review the output of the command config router ospf shown in the Exhibit below; then answer the question following it.



```
STUDENT (ospf) # show
config router ospf
        config area
            edit 0.0.0.0
            next
        end
        config network
            edit 1
                set prefix 10.0.1.0 255.255.255.0
            next
            edit 2
                set prefix 172.16.0.0 255.240.0.0
            next
        end
        config ospf-interface
            edit "R1_OSPF"
                set interface "Remote_1"
                set ip 172.16.1.1
                set mtu 1436
                set network-type point-to-point
            next
            edit "R2_OSPF"
                set cost 20
                set interface "Remote_2"
                set ip 172.16.1.2
                set mtu 1436
                set network-type point-to-point
            next
        end
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
```

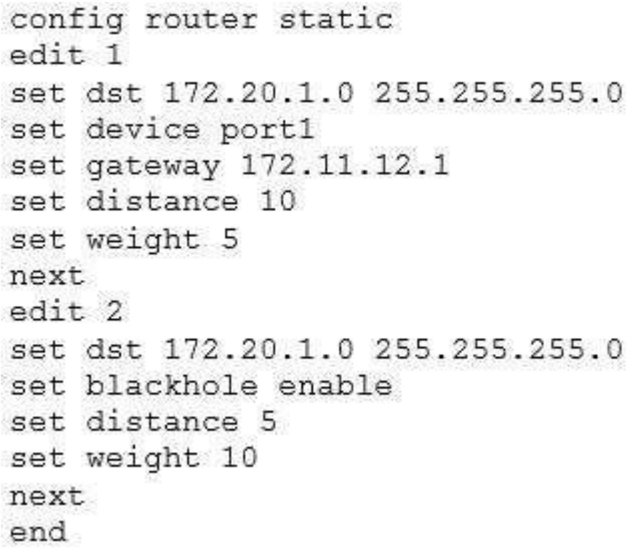
Which one of the following statements is correct regarding this output?

A. OSPF Hello packets will only be sent on interfaces configured with the IP addresses 172.16.1.1 and 172.16.1.2.
B. OSPF Hello packets will be sent on all interfaces of the FortiGate device.
C. OSPF Hello packets will be sent on all interfaces configured with an address matching the 10.0.1.0/24 and 172.16.0.0/12 networks.
D. OSPF Hello packets are not sent on point-to-point networks.

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 159
Examine the static route configuration shown below; then answer the question following it. (Select all that apply.)



```
config router static
edit 1
set dst 172.20.1.0 255.255.255.0
set device port1
set gateway 172.11.12.1
set distance 10
set weight 5
next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable
set distance 5
set weight 10
next
end
```

Which of the following statements correctly describes the static routing configuration provided? (Select all that apply.) A. All traffic to 172.20.1.0/24

will always be dropped by the FortiGate unit.

B. As long as port1 is up, all the traffic to 172.20.1.0/24 will be routed by the static route number 1. If the interface port1 is down, the traffic will be routed using the blackhole route.
C. The FortiGate unit will NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
D. The FortiGate unit will create a session entry in the session table when the traffic is being routed by the blackhole route.
E. Traffic to 172.20.1.0/24 will be shared through both routes.

Correct Answer: AC
Section: (none) Explanation

Explanation/Reference:

QUESTION 160
Which of the following statements are correct regarding virtual domains (VDOMs)? (Select all that apply.)

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. VDOMs share firmware versions, as well as antivirus and IPS databases.
D. Only administrative users with a 'super_admin' profile will be able to enter multiple VDOMs to make configuration changes.

Correct Answer: ABC
Section: (none) Explanation

Explanation/Reference:

QUESTION 161
Which of the following statements are TRUE for Port Pairing and Forwarding Domains? (Select all that apply.)

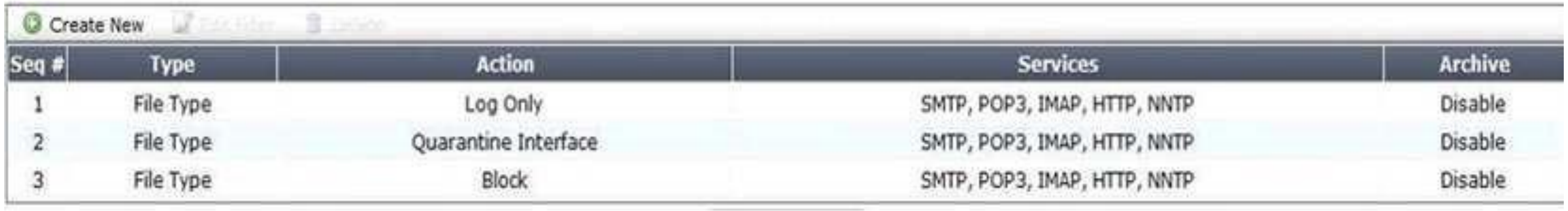
A. They both create separate broadcast domains.
B. Port Pairing works only for physical interfaces.
C. Forwarding Domains only apply to virtual interfaces.
D. They may contain physical and/or virtual interfaces.
E. They are only available in high-end models.

Correct Answer: AD
Section: (none) Explanation

Explanation/Reference:

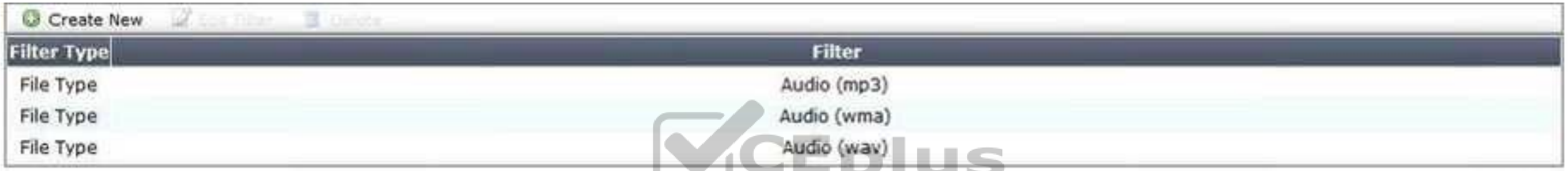
QUESTION 162

Examine the Exhibits shown below, then answer the question that follows. Review the following DLP Sensor (Exhibit 1):



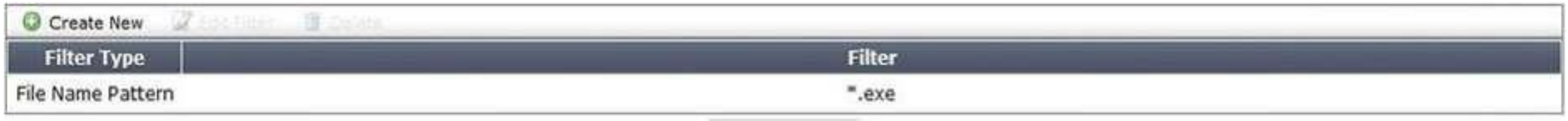
Seq #	Type	Action	Services	Archive
1	File Type	Log Only	SMTP, POP3, IMAP, HTTP, NNTP	Disable
2	File Type	Quarantine Interface	SMTP, POP3, IMAP, HTTP, NNTP	Disable
3	File Type	Block	SMTP, POP3, IMAP, HTTP, NNTP	Disable

Review the following File Filter list for rule #1 (Exhibit 2):



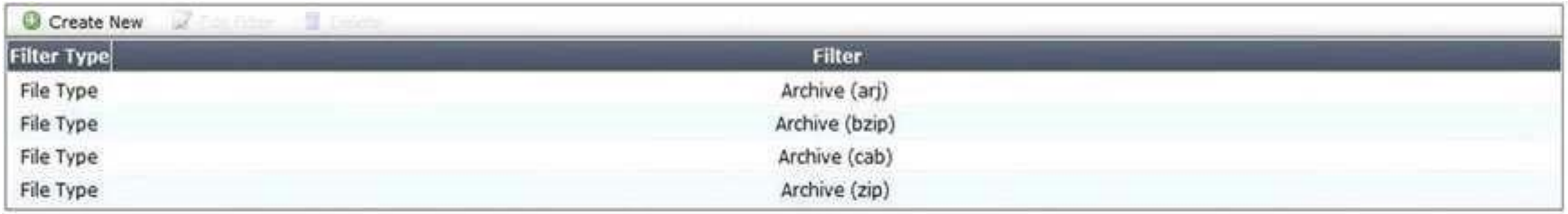
Filter Type	Filter
File Type	Audio (mp3)
File Type	Audio (wma)
File Type	Audio (wav)

Review the following File Filter list for rule #2 (Exhibit 3):



Filter Type	Filter
File Name Pattern	*.exe

Review the following File Filter list for rule #3 (Exhibit 4):



Filter Type	Filter
File Type	Archive (arj)
File Type	Archive (bzip)
File Type	Archive (cab)
File Type	Archive (zip)

An MP3 file is renamed to `workbook.exe' and put into a ZIP archive. It is then sent through the FortiGate device over HTTP. It is intercepted and processed by the configuration shown in the above Exhibits 1-4.
Assuming the file is not too large for the File scanning threshold, what action will the FortiGate unit take?

A. The file will be detected by rule #1 as an `Audio (mp3)', a log entry will be created and it will be allowed to pass through.
B. The file will be detected by rule #2 as a "*.exe", a log entry will be created and the interface that received the traffic will be brought down.
C. The file will be detected by rule #3 as an Archive(zip), blocked, and a log entry will be created.
D. Nothing, the file will go undetected.

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

Explanation/Reference:

QUESTION 163
What are the requirements for a cluster to maintain TCP connections after device or link failover? (Select all that apply.)

A. Enable session pick-up.
B. Only applies to connections handled by a proxy.
C. Only applies to UDP and ICMP connections.
D. Connections must not be handled by a proxy.

Correct Answer: AD
Section: (none) Explanation

Explanation/Reference:
QUESTION 164
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 because fewer tunnels are required.
C. Using a hub and spoke topology provides stronger encryption.
D. The routing at a spoke is simpler, compared to a meshed node.

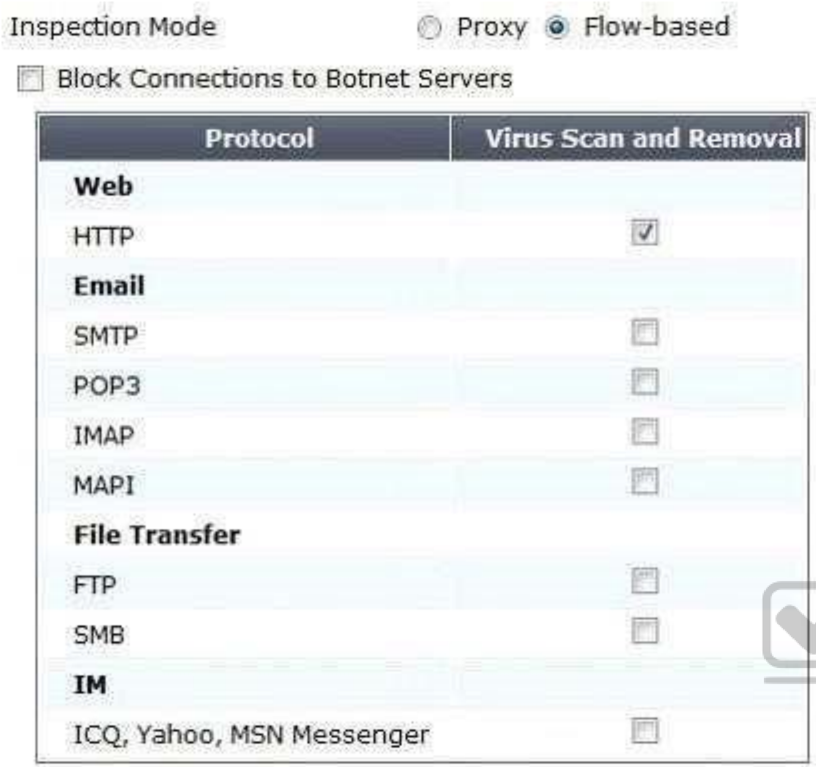
Correct Answer: BD
Section: (none) Explanation

Explanation/Reference:

QUESTION 165

The eicar test virus is put into a zip archive, which is given the password of "Fortinet" in order to open the archive. Review the configuration in the exhibits shown below; then answer the question that follows.

Exhibit A - Antivirus Profile:

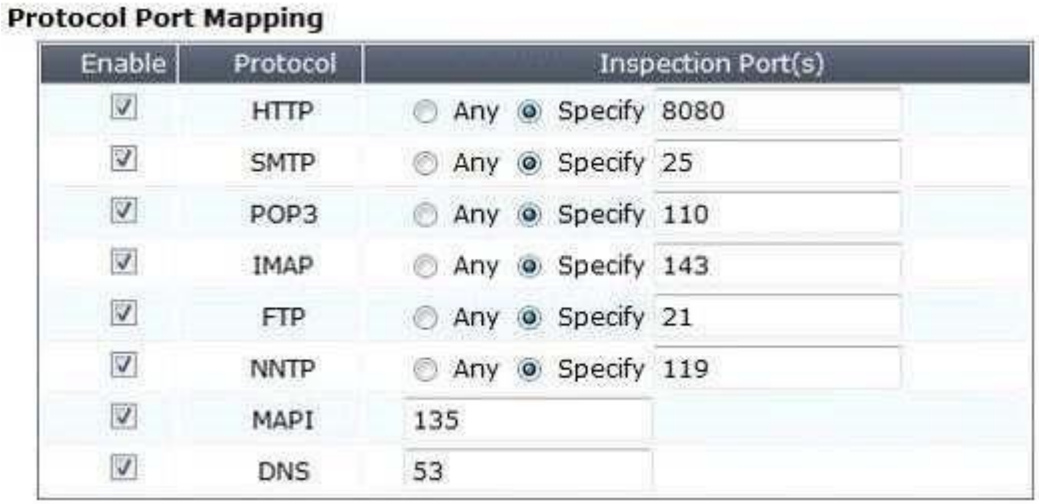


Inspection Mode ○ Proxy ● Flow-based

□ Block Connections to Botnet Servers

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

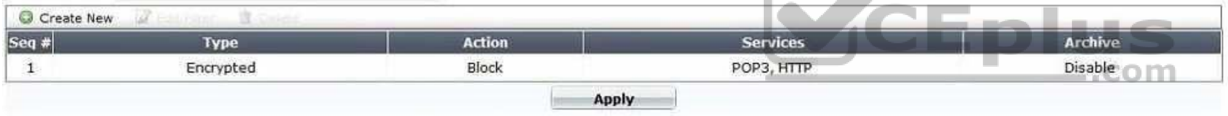
Exhibit B - Non-default UTM Proxy Options Profile:



Protocol Port Mapping

Enable	Protocol	Inspection Port(s)
☑	HTTP	○ Any ● Specify 8080
☑	SMTP	○ Any ● Specify 25
☑	POP3	○ Any ● Specify 110
☑	IMAP	○ Any ● Specify 143
☑	FTP	○ Any ● Specify 21
☑	NNTP	○ Any ● Specify 119
☑	MAPI	135
☑	DNS	53

Exhibit C - DLP Profile:



Seq #	Type	Action	Services	Archive
1	Encrypted	Block	POP3, HTTP	Disable

Which of one the following profiles could be enabled in order to prevent the file from passing through the FortiGate device over HTTP on the standard port for that protocol?

A. Only Exhibit A
B. Only Exhibit B
C. Only Exhibit C with default UTM Proxy settings.
D. All of the Exhibits (A, B and C)
E. Only Exhibit C with non-default UTM Proxy settings (Exhibit B).

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:
QUESTION 166

With FSSO, a domain user could authenticate either against the domain controller running the Collector Agent and Domain Controller Agent, or a domain controller running only the Domain Controller Agent.
If you attempt to authenticate with the Secondary Domain Controller running only the Domain Controller Agent, which of the following statements are correct? (Select all that apply.)

A. The login event is sent to the Collector Agent.
B. The FortiGate unit receives the user information from the Domain Controller Agent of the Secondary Controller.
C. The Collector Agent performs the DNS lookup for the authenticated client's IP address.
D. The user cannot be authenticated with the FortiGate device in this manner because each Domain Controller Agent requires a dedicated Collector Agent.

Correct Answer: AC
Section: (none) Explanation

Explanation/Reference:

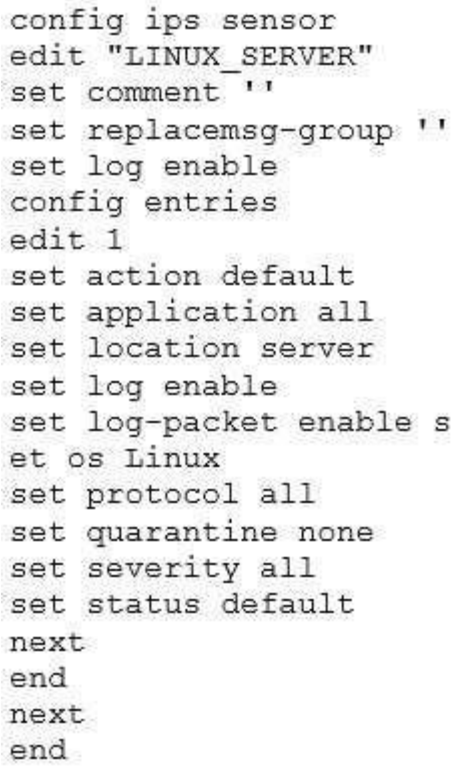
QUESTION 167
In Transparent Mode, forward-domain is an attribute of _______.

A. an interface
B. a firewall policy
C. a static route
D. a virtual domain

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 168
Review the CLI configuration below for an IPS sensor and identify the correct statements regarding this configuration from the choices below. (Select all that apply.)



```
config ips sensor
edit "LINUX_SERVER"
set comment ''
set replacemsg-group ''
set log enable
config entries
edit 1
set action default
set application all
set location server
set log enable
set log-packet enable s
et os Linux
set protocol all
set quarantine none
set severity all
set status default
next
end
next
end
```

A. The sensor will log all server attacks for all operating systems.
B. The sensor will include a PCAP file with a trace of the matching packets in the log message of any matched signature.
C. The sensor will match all traffic from the address object `LINUX_SERVER'.
D. The sensor will reset all connections that match these signatures.
E. The sensor only filters which IPS signatures to apply to the selected firewall policy.

Correct Answer: BE
Section: (none) Explanation

Explanation/Reference:
QUESTION 169
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:

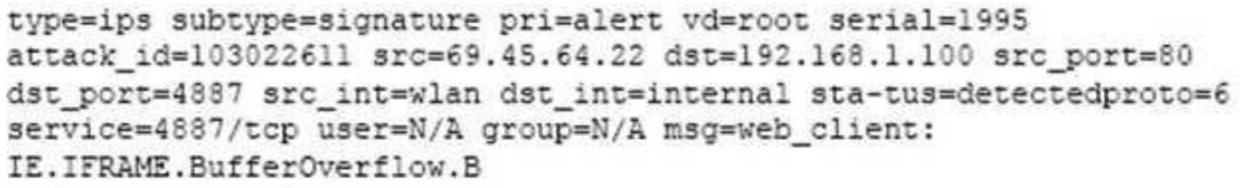
QUESTION 170
A DLP rule with an action of Exempt has been matched against traffic passing through the FortiGate unit. Which of the following statements is correct regarding how this transaction will be handled by the FortiGate unit?

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 171
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 172
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 173
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?

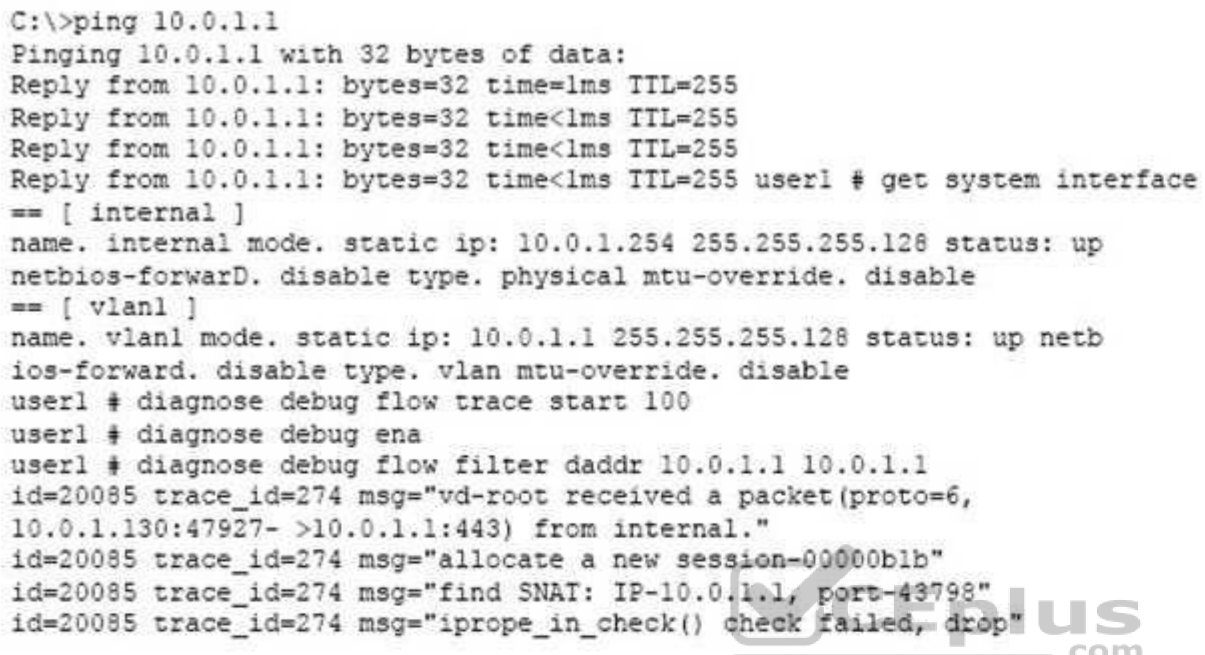
A. In the Service field of the Data Filter, type 80/tcp and select the NOT checkbox.
B. Add the following entry to the Generic Field section of the Data Filter: service="!web".
C. When editing the chart, uncheck wlog to indicate that Web Filtering data is being excluded when generating the chart.
D.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

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 174

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 175

A FortiGate administrator 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 Web Config in the management VDOM. What would be a possible cause for this problem?

A. The dmz interface is referenced in the configuration of another VDOM.
B. The administrator does not have the proper permissions to reassign the dmz interface.
C. Non-management VDOMs can not reference physical interfaces.
D. The dmz interface is in PPPoE or DHCP mode.
E. Reassigning an interface to a different VDOM can only be done through the CLI.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
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 177
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 178
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 179

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?

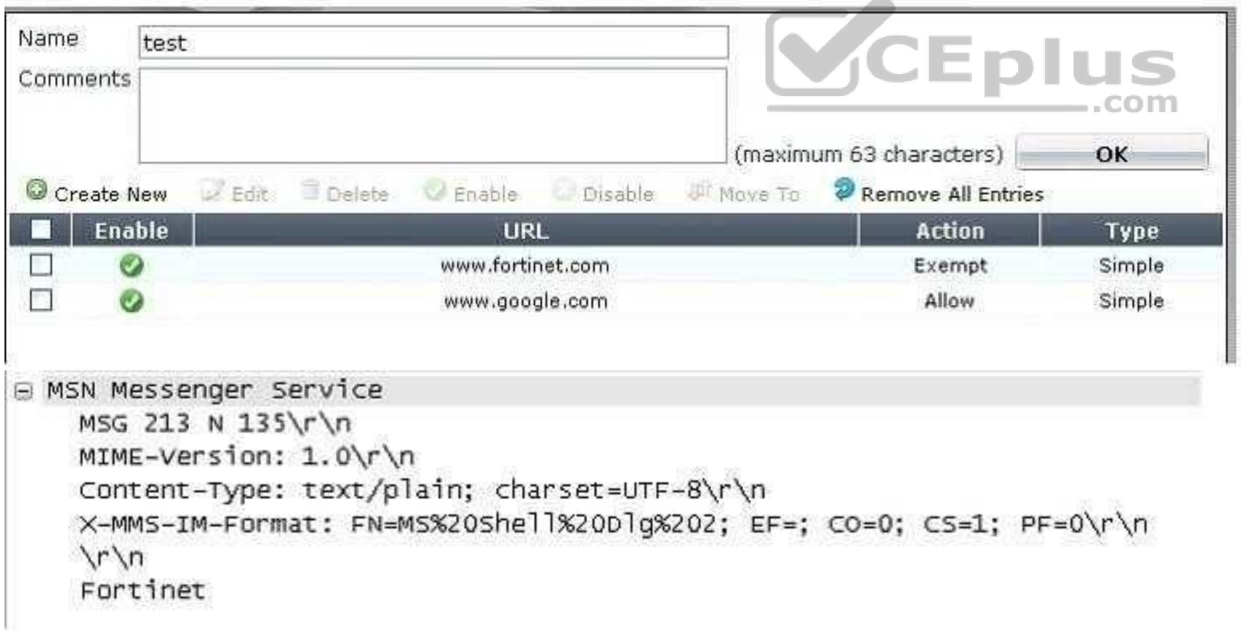
A. Common Name
B. Organization
C. Organizational Unit
D. Serial Number
E. Validity

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 180

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



□	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 181
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 182
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 183

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 184

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 185

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 186
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 187
Which of the following must be configured on a FortiGate unit to redirect content requests to remote web cache servers?

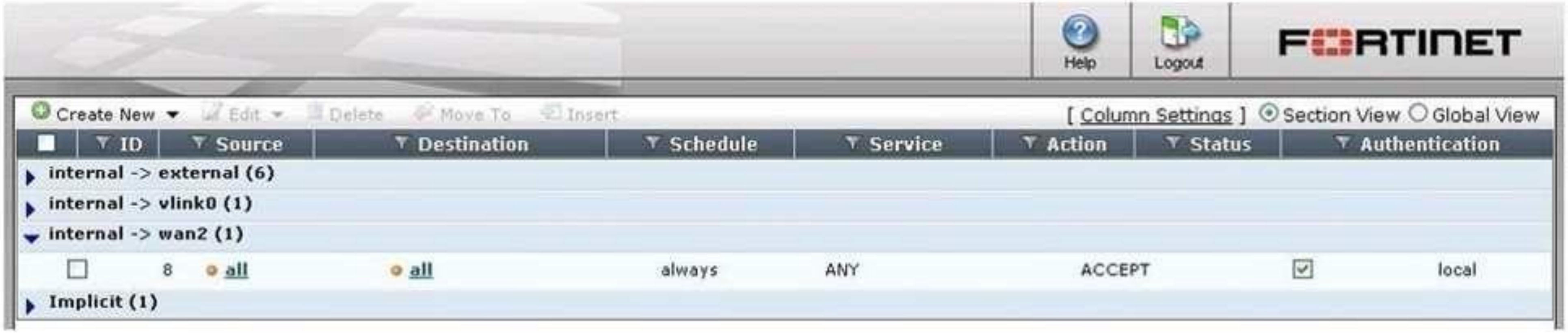
A. WCCP must be enabled on the interface facing the Web cache.
B. You must enabled explicit Web-proxy on the incoming interface.
C. WCCP must be enabled as a global setting on the FortiGate unit.
D. WCCP must be enabled on all interfaces on the FortiGate unit through which HTTP traffic is passing.

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 188

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 189

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 190
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 191
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 192
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 193
A network administrator needs to implement dynamic route redundancy between a FortiGate unit located in a remote office and a FortiGate unit located in the central office.
The remote office accesses central resources using IPSec VPN tunnels through two different Internet providers.
What is the best method for allowing the remote office access to the resources through the FortiGate unit used at the central office?

A. Use two or more route-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
B. Use two or more policy-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
C. Use route-based VPNs on the central office FortiGate unit to advertise routes with a dynamic routing protocol and use a policy-based VPN on the remote office with two or more static default routes.
D. Dynamic routing protocols cannot be used over IPSec VPN tunnels.

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 194
When performing a log search on a FortiAnalyzer, it is generally recommended to use the Quick Search option. What is a valid reason for using the Full Search option, instead?

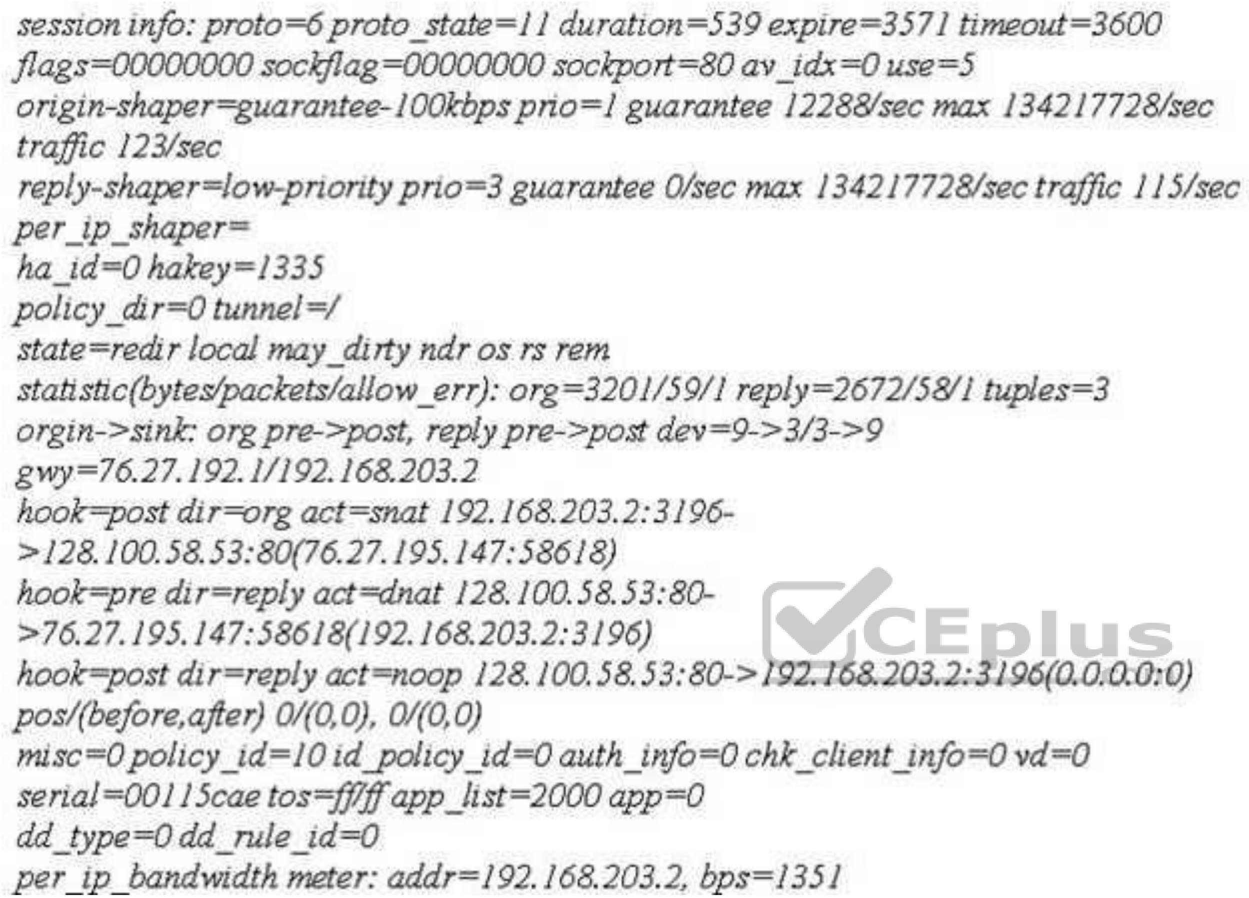
A. The search items you are looking for are not contained in indexed log fields.
B. A quick search only searches data received within the last 24 hours.
C. You want the search to include the FortiAnalyzer's local logs.

D. You want the search to include content archive data as well.

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 195
The diag sys session list command is executed in the CLI. The output of this command is shown in the exhibit.



```
session info: proto=6 proto_state=11 duration=539 expire=3571 timeout=3600
flags=00000000 sockflag=00000000 sockport=80 av_idx=0 use=5
origin-shaper=guarantee-100kbps prio=1 guarantee 12288/sec max 134217728/sec
traffic 123/sec
reply-shaper=low-priority prio=3 guarantee 0/sec max 134217728/sec traffic 115/sec
per_ip_shaper=
ha_id=0 hakey=1335
policy_dir=0 tunnel=/
state=redir local may_dirty ndr os rs rem
statistic(bytes/packets/allow_err): org=3201/59/1 reply=2672/58/1 tuples=3
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9
gwy=76.27.192.1/192.168.203.2
hook=post dir=org act=snat 192.168.203.2:3196-
>128.100.58.53:80(76.27.195.147:58618)
hook=pre dir=reply act=dnat 128.100.58.53:80-
>76.27.195.147:58618(192.168.203.2:3196)
hook=post dir=reply act=noop 128.100.58.53:80->192.168.203.2:3196(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=10 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00115cae tos=ff/ff app_list=2000 app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=192.168.203.2, bps=1351
```

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

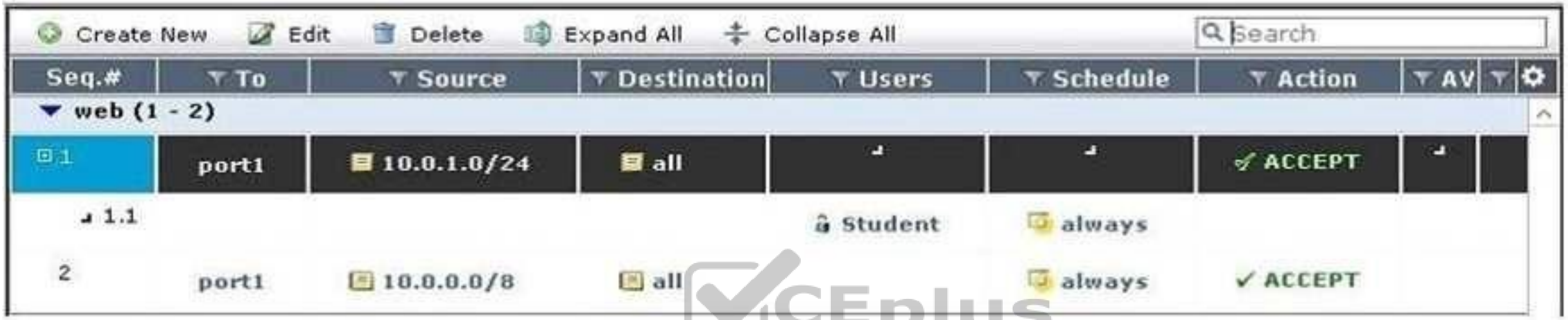
A. This is a UDP session.
B. Traffic shaping is being applied to this session.
C. This is an ICMP session.
D. This traffic has been authenticated.
E. This session matches a firewall policy with ID 5.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
Review the exhibit of an explicit proxy policy configuration. If there is a proxy connection attempt coming from the IP address 10.0.1.5, and from a user that has not authenticated yet, what action does the FortiGate proxy take?



Seq.#	To	Source	Destination	Users	Schedule	Action	AV
web (1 - 2)							
1	port1	10.0.1.0/24	all			✓ ACCEPT	
1.1				Student	always		
2	port1	10.0.0.0/8	all		always	✓ ACCEPT	

A. User is prompted to authenticate. Traffic from the user Student will be allowed by the policy #1. Traffic from any other user will be allowed by the policy #2.
B. User is not prompted to authenticate. The connection is allowed by the proxy policy #2.
C. User is not prompted to authenticate. The connection will be allowed by the proxy policy #1.
D. User is prompted to authenticate. Only traffic from the user Student will be allowed. Traffic from any other user will be blocked.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

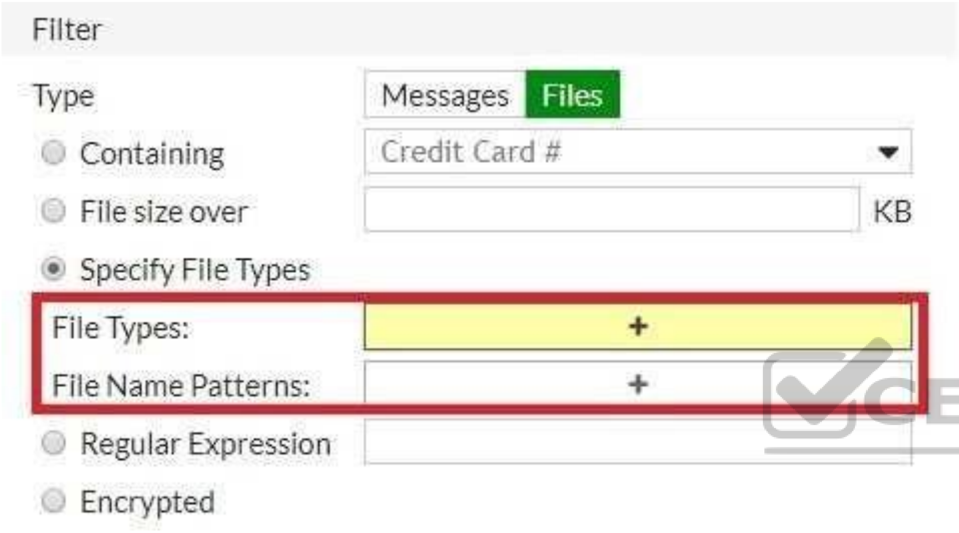
QUESTION 197
Which of the following statements are true regarding DLP File Type Filtering? (Choose two.)

A. Filters based on file extension
B. Filters based on fingerprints
C. Filters based on file content

D. File types are hard coded in the FortiOS

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference: Explanation:



Filter

Type Messages [✓ Files]

○ Containing Credit Card #

○ File size over KB

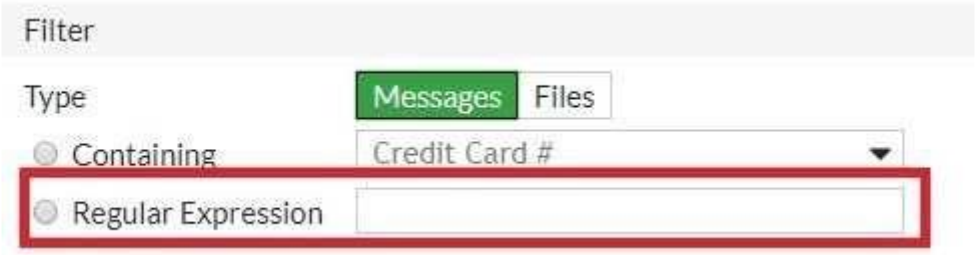
● Specify File Types

File Types: +

File Name Patterns: +

○ Regular Expression

○ Encrypted



Filter

Type [✓ Messages] Files

○ Containing Credit Card #

○ Regular Expression

QUESTION 198

Which of the following settings can be configured per VDOM? (Choose three.)

A. Operating mode (NAT/route or transparent)

B. Static routesC. Hostname

D. System time
E. Firewall Policies

Correct Answer: ABE
Section: (none) Explanation

Explanation/Reference:

QUESTION 199
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 200
What are examples of correct syntax for the session table diagnostics command? (Choose two.)

A. diagnose sys session filter clear
B. diagnose sys session src 10.0.1.254
C. diagnose sys session filter
D. diagnose sys session filter list dst.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201

Which statement best describes the objective of the SYN proxy feature available in SP processors?

A. Accelerate the TCP 3-way handshake
B. Collect statistics regarding traffic sessions
C. Analyze the SYN packet to decide if the new session can be offloaded to the SP processor
D. Protect against SYN flood attacks.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 202

Which of the following are possible actions for static URL filtering? (Choose three.)

A. Allow
B. Block
C. Exempt
D. Warning
E. Shape

Correct Answer: ABC
Section: (none)
Explanation
Explanation/Reference:

QUESTION 203
A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.

Which is one reason for this problem?

A. The FortiGate is connected to multiple ISPs.
B. FortiGuard scheduled updates are enabled in the FortiGate configuration.
C. The FortiGate is in Transparent mode.
D. The external facing interface of the FortiGate is configured to get the IP address from a DHCP server.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 204
Which best describe the mechanism of a TCP SYN flood?

A. The attacker keeps open many connections with slow data transmission so that other clients cannot start new connections.
B. The attacker sends a packet designed to "sync" with the FortiGate.
C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
D. The attacker starts many connections, but never acknowledges to fully form them.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 205
Which traffic can match a firewall policy's "Services" setting? (Choose three.)

A. HTTP
B. SSL C. DNS
D. RSS
E. HTTPS

Correct Answer: ACE
Section: (none) Explanation

Explanation/Reference:

QUESTION 206

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

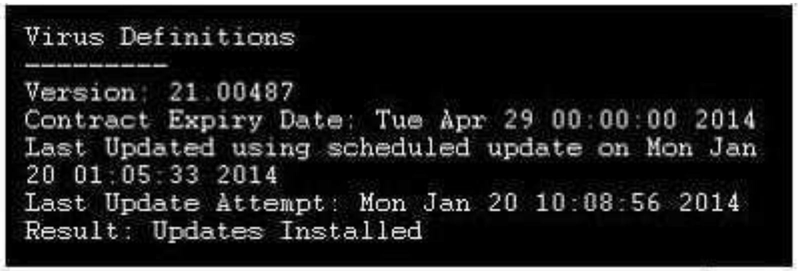
Explanation/Reference:

QUESTION 207

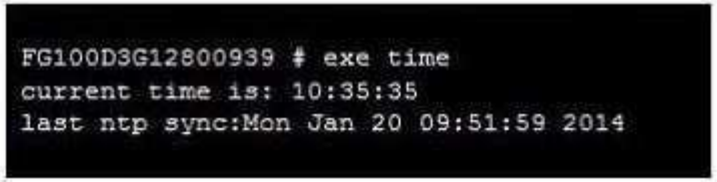
A FortiGate device is configure to perform an AV & IPS scheduled update every hour.

Section: (none)
Explanation

Explanation/Reference:



```
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 208
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

CD

QUESTION 209

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)
Explanat
ion

Explanation/Reference:

QUESTION 210

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)
Explanat
ion

Explanation/Reference:
Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 211

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 212

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 213

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.

B

QUESTION 214

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

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
Explanation/Reference:

QUESTION 215
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) Explanati

o
n

Explanation/Reference:

QUESTION 216
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 217
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 218
Which of the following statements are correct concerning IKE mode config? (Choose two)

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
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.

AB

QUESTION 219
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 220
Which action is taken by the FortiGate device when a file matches more than one rule in a Data Leak Prevention sensor?

A. The actions specified by the rule that most specifically matched the file
B. The actions specified in the first rule from top to bottom
C. All actions specified by all the matched rules.
D. The actions specified in the rule with the higher priority number

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 221

Which protocol can an Internet browser use to download the PAC file with the web proxy configuration?

Correct Answer:

A. HTTPS
B. FTP
C. TFTP
D. HTTP

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 222
Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

A. The whole VDOM is a single broadcast domain even when multiple VLAN are used.
B. Each VLAN is a separate broadcast domain.
C. Interfaces configured with the same VLAN ID can belong to different broadcast domains.
D. All the interfaces in the same broadcast domain must use the same VLAN ID.

Correct Answer: BC
Section: (none) Explanation

Explanation/Reference:

QUESTION 223
If you enable the option "Generate Logs when Session Starts", what effect does this have on the number of traffic log messages generated for each session?

A. No traffic log message is generated.
B. One traffic log message is generated.
C. Two traffic log messages are generated.
D. A log message is only generated if there is a security event.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224

Which of the following actions that can be taken by the Data Leak Prevention scanning? (Choose three.)

A. Block
B. Reject
C. Tag
D. Log only
E. Quarantine IP address

Correct Answer: ADE
Section: (none) Explanation

Explanation/Reference:

QUESTION 225

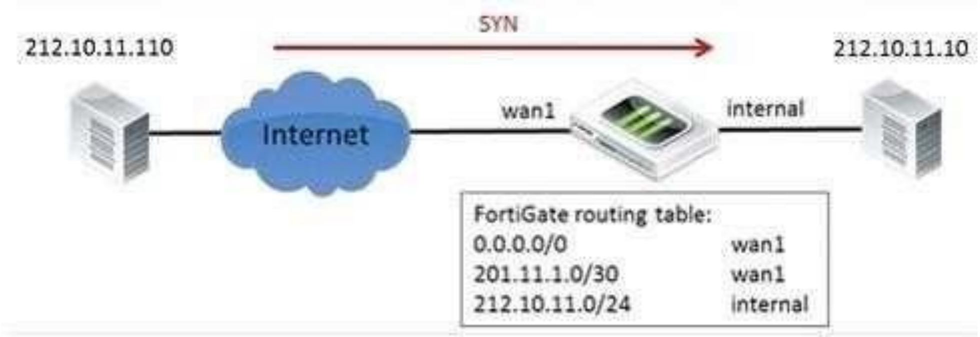
What is required in a FortiGate configuration to have more than one dialup IPsec VPN using aggressive mode?

A. All the aggressive mode dialup VPNs MUST accept connections from the same peer ID.
B. Each peer ID MUST match the FQDN of each remote peer.
C. Each aggressive mode dialup MUST accept connections from different peer ID.
D. The peer ID setting must NOT be used.

Correct Answer: C
Section: (none)

Explanation
Explanation/Reference:

QUESTION 226
Examine the network topology diagram in the exhibit; the workstation with the IP address 212.10.11.110 sends a TCP SYN packet to the workstation with the IP address 212.10.11.20.



FortiGate routing table:

0.0.0.0/0	wan1
201.11.1.0/30	wan1
212.10.11.0/24	internal

Which of the following sentences best describes the result of the reverse path forwarding (RFP) check executed by the FortiGate on the SYN packets? (Choose two).

A. Packets is allowed if RPF is configured as loose.
B. Packets is allowed if RPF is configured as strict.
C. Packets is blocked if RPF is configured as loose.
D. Packets is blocked if RPF is configured as strict.

Correct Answer: AD
Section: (none) Explanation

Explanation/Reference:

QUESTION 227
In a FSSO agentless polling mode solution, where must the collector agent be?

A. In any Windows server
B. In any of the AD domain controllers

C. In the master AD domain controller
D. The FortiGate device polls the AD domain controllers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
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 229
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 230

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 231
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:

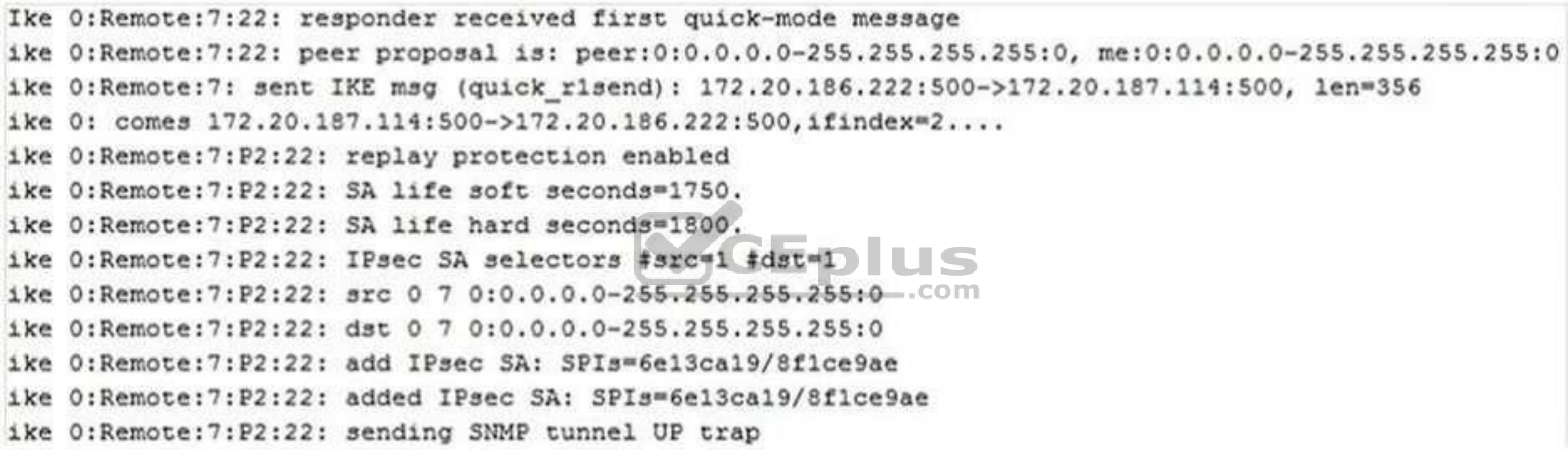
QUESTION 232
Which of the following network protocols can be inspected by the Data Leak Prevention scanning? (Choose three.)

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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
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 234
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 235
Which statement concerning IPS is false?

A. IPS packages contain an engine and signatures used by both IPS and other flow-based scans.
B. One-arm topology with sniffer mode improves performance of IPS blocking.
C. IPS can detect zero-day attacks.
D. The status of the last service update attempt from FortiGuard IPS is shown on System>Config>FortiGuard and in output from 'diag autoupdate version'

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 236
Which of the following statements are correct differences between NAT/route and transparent mode? (Choose two.)

A. In transparent mode, interfaces do not have IP addresses.
B. Firewall polices are only used in NAT/ route mode.
C. Static routers are only used in NAT/route mode.
D. Only transparent mode permits inline traffic inspection at layer 2.

Correct Answer: AC

Section: (none) Explanation

Explanation/Reference:

QUESTION 237
Which of the following statements are true regarding the web filtering modes? (Choose two.)

A. Proxy based mode allows for customizable block pages to display when sites are prevented.
B. Proxy based mode requires more resources than flow-based.
C. Flow based mode offers more settings under the advanced configuration section of the GUI.
D. Proxy based mode offers higher throughput than flow-based mode.

Correct Answer: AB
Section: (none) Explanation

Explanation/Reference:

QUESTION 238
Which of the following statements are characteristics of a FSSO solution using advanced access mode? (Choose three.)

A. Protection profiles can be applied to both individual users and user groups
B. Nested or inherited groups are supported
C. Usernames follow the LDAP convention: CN=User, OU=Name, DC=Domain D. Usernames follow the Windows convention: Domain\username
E. Protection profiles can be applied to user groups only.

Correct Answer: BCE
Section: (none) Explanation

Explanation/Reference:
QUESTION 239
Which of the following are operating mode supported in FortiGate devices? (Choose two)

A. Proxy
B. Transparent
C. NAT/route

D. Offline inspection

Correct Answer: BC
Section: (none) Explanation

Explanation/Reference:

QUESTION 240
Which of the following statements are correct regarding FortiGate virtual domains (VDOMs)? (Choose two)

A. VDOMs divide a single FortiGate unit into two or more independent firewall.
B. A management VDOM handles SNMP. logging, alert email and FortiGuard updates.
C. Each VDOM can run different firmware versions.
D. Administrative users with a 'super_admin' profile can administrate only one VDOM.

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

Explanation/Reference:

QUESTION 241
Which are the three different types of Conserve Mode that can occur on a FortiGate device? (Choose three.)

A. Proxy
B. Operating system
C. Kernel
D. System
E. Device

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242

Which of the following statements are correct about NTLM authentication? (Choose three)

A. NTLM negotiation starts between the FortiGate device and the user's browser.
B. It must be supported by the user's browser.
C. It must be supported by the domain controllers.
D. It does not require a collector agent.
E. It does not require DC agents.

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

Explanation/Reference:

QUESTION 243

Which of the following statements are true about IPsec VPNs? (Choose three.)

A. IPsec increases overhead and bandwidth.
B. IPsec operates at the layer 2 of the OSI model.
C. End-user's network applications must be properly pre-configured to send traffic across the IPsec VPN.
D. IPsec protects upper layer protocols.
E. IPsec operates at the layer 3 of the OSI model.

Correct Answer: ADE
Section: (none) Explanation

Explanation/Reference:

QUESTION 244

Which UTM feature sends a UDP query to FortiGuard servers each time FortiGate scans a packet (unless the response is locally cached)?

A. Antivirus
B. VPN
C. IPS
D. Web Filtering..

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
Which of the following combinations of two FortiGate device configurations (side A and side B), can be used to successfully establish an IPsec VPN between them?
(choose two)

A. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: aggressive mode, remote Gateway as static IP address policy-based VPN.
B. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: main mode, remote gateway as static IP address, route-based VPN
C. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: main mode, remote gateway as dialup, route-based VPN.
D. Side A: main mode, remote gateway as dialup policy based VPN, Side B: main mode, remote gateway as dialup, policy based VPN.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
QUESTION 246
A FortiGate devices has two VDOMs in NAT/route mode. Which of the following solutions can be implemented by a network administrator to route traffic between the two VDOMs. (Choose two.)

A. Use the inter-VDOMs links automatically created between all VDOMS.

B. Manually create and configured an inter-VDOM link between yours.
C. Interconnect and configure an external physical interface in one VDOM to another physical interface in the second VDOM.
D. Configure both VDOMs to share the same table.

Correct Answer: BC
Section: (none) Explanation

Explanation/Reference:

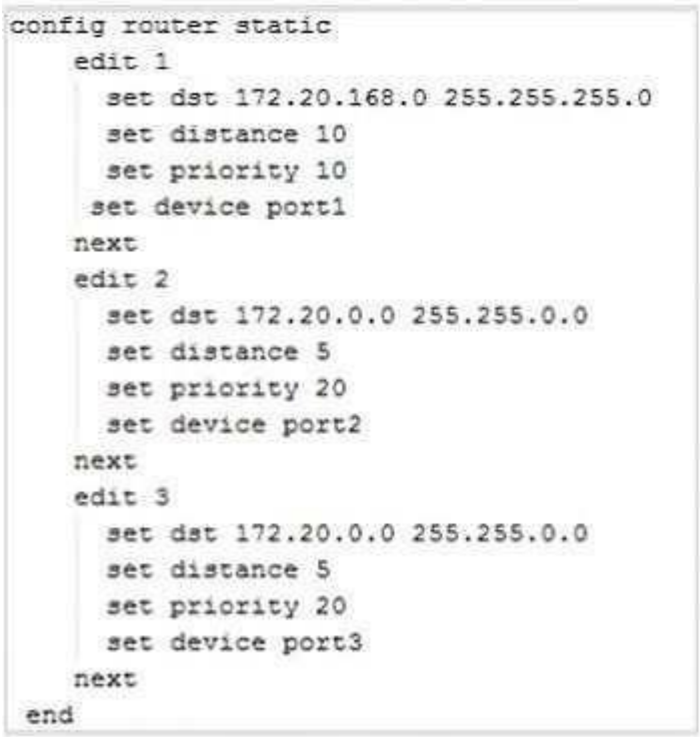
QUESTION 247
Which of the following are considered log types? (Choose three.)

A. Forward log
B. Traffic log
C. Syslog
D. Event log
E. Security log

Correct Answer: BDE
Section: (none) Explanation

Explanation/Reference:

QUESTION 248
The exhibit shoes three static routes.



```
config router static
    edit 1
      set dst 172.20.168.0 255.255.255.0
      set distance 10
      set priority 10
     set device port1
    next
    edit 2
      set dst 172.20.0.0 255.255.0.0
      set distance 5
      set priority 20
      set device port2
    next
    edit 3
      set dst 172.20.0.0 255.255.0.0
      set distance 5
      set priority 20
      set device port3
    next
 end
```

Which routes will be used to route the packets to the destination IP address 172.20.168.1?

A. The route with the ID number 2 and 3.
B. Only the route with the ID number 3.
C. Only the route with the ID number 2.
D. Only the route with the ID number 1.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:
QUESTION 249
Which of the following statements must be true for a digital certificate to be valid? (Choose two.)

A. It must be signed by a "trusted" CA
B. It must be listed as valid in a Certificate Revocation List (CRL)
C. The CA field must be "TRUE"
D. It must be still within its validity period

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250
Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

A. Asymmetric Keys
B. CA root digital certificates
C. RSA signature
D. Pre-shared keys

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
If you have lost your password for the "admin" account on your FortiGate, how should you reset it?

A. Log in with another administrator account that has "super_admin" profile permissions, then reset the password for the "admin" account.
B. Reboot the FortiGate. Via the local console, during the boot loader, use the menu to format the flash disk and reinstall the firmware. Then you can log in with the default password.
C. Power off the FortiGate. After several seconds, restart it. Via the local console, within 30 seconds after booting has completed, log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.
D. Reboot the FortiGate. Via the local console, during the boot loader, use the menu to log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
What actions are possible with Application Control? (Choose three.)

A. Warn
B. Allow
C. Block
D. Traffic Shaping
E. Quarantine

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

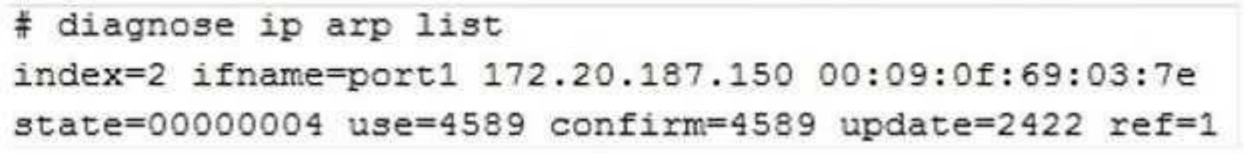
Explanation/Reference:

QUESTION 253
Which of the following statements are true about Man-in-the-middle SSL Content Inspection? (Choose three.)

A. The FortiGate device "re-signs" all the certificates coming from the HTTPS servers
B. The FortiGate device acts as a sub-CA
C. The local service certificate of the web server must be installed in the FortiGate device
D. The FortiGate device does man-in-the-middle inspection.
E. The required SSL Proxy certificate must first be requested to a public certificate authority (CA).

Correct Answer: BCE
Section: (none) Explanation

Explanation/Reference:
QUESTION 254
In the debug command output shown in the exhibit, which of the following best described the MAC address 00:09:0f:69:03:7e?



```
# diagnose ip arp list
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e
state=00000004 use=4589 confirm=4589 update=2422 ref=1
```

A. It is one of the secondary MAC addresses of the port1 interface.
B. It is the primary MAC address of the port interface.
C. It is the MAC address of another network devices located in the same LAN segment as the FortiGate unit's port1 interface.
D. It is the HA virtual MAC address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
Which correctly define "Section View" and "Global View" for firewall policies? (Choose two.)

A. Section View lists firewall policies primarily by their interface pairs.
B. Section View lists firewall policies primarily by their sequence number.
C. Global View lists firewall policies primarily by their interface pairs.
D. Global View lists firewall policies primarily by their policy sequence number.
E. The 'any' interface may be used with Section View.

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

Explanation/Reference: