Braindumps.FCNSP.v5.119.QA

Number: FCNSP.v5
Passing Score: 800
Time Limit: 120 min
File Version: 32.1

VCEplus.com

Brain-dumps

FCNSP

Fortinet Certified Network Security Professional (V5)

- Now sum up more relevant and up to dated questions in this VCE file.
- Best ever training material, It's really helps you to maximize the exam preparation.
- Superb!!! It's a key to success and it's fully according to your exam requirements.
- I found this format very refreshing and very informative.
- I passed the test the first time using your wonderful dump! it is so comprehensive and easy to read and everything is memorable for the exam.
- A big success is waiting for you :) Just study it.

Sections

Exam A

QUESTION 1
How can DLP file filters be configured to detect Office 2010 files? (Select all that apply.)

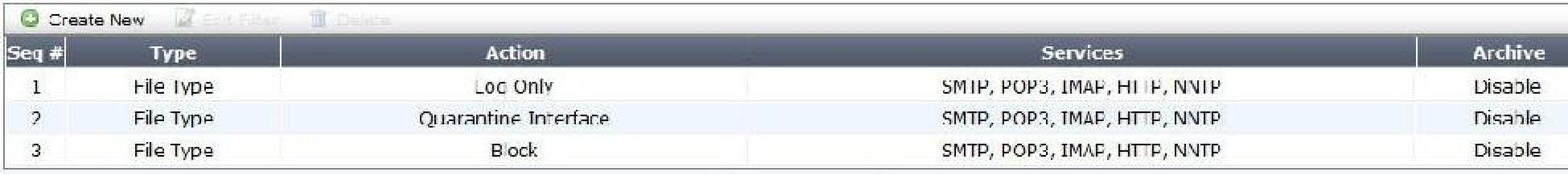
A. File TypE. Microsoft Office(msoffice)
B. File TypE. Archive(zip)
C. File TypE. Unknown Filetype(unknown)
D. File NamE. "*.ppt", "*.doc", "*.xls"
E. File NamE. "*.pptx", "*.docx", "*.xlsx"

Correct Answer: BE
Section: Volume A
Explanation

Explanation/Reference:

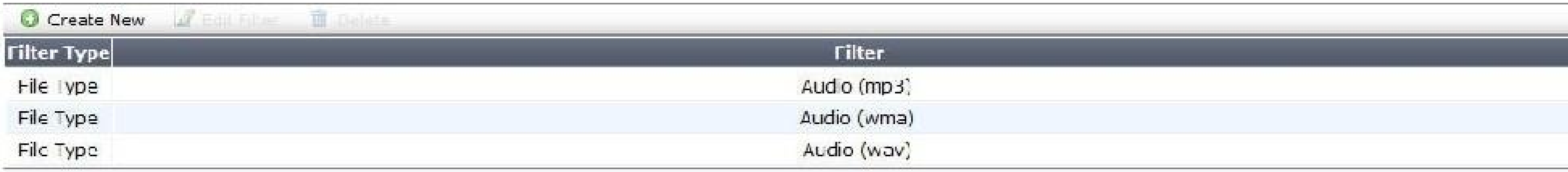
QUESTION 2
Examine the Exhibits shown below, then answer the question that follows.

Review the following DLP Sensor (Exhibit 1):



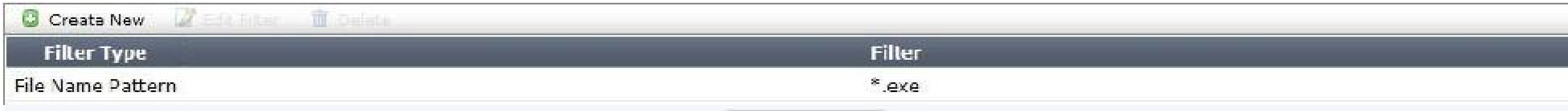
Seq #	Type	Action	Services	Archive
1	File Type	Log Only	SMTP, POP3, IMAP, HTTP, NNTP	Disable
2	File Type	Quarantine Interface	SMTP, POP3, IMAP, HTTP, NNTP	Disable
3	File Type	Block	SMTP, POP3, IMAP, HTTP, NNTP	Disable

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



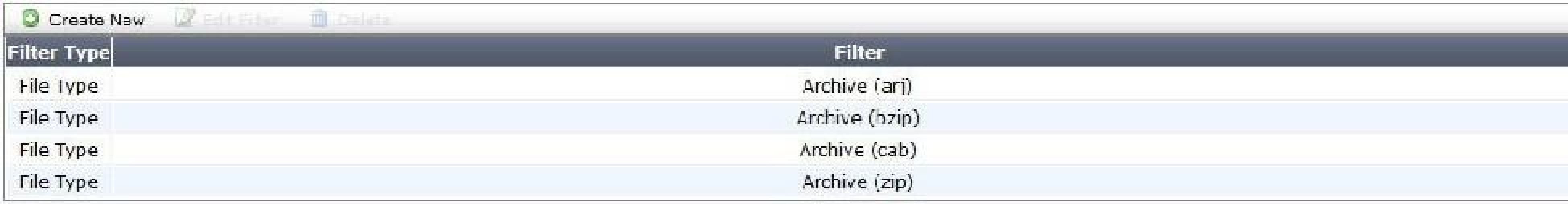
Filter Type	Filter
File Type	Audio (mp3)
File Type	Audio (wma)
File Type	Audio (wav)

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?

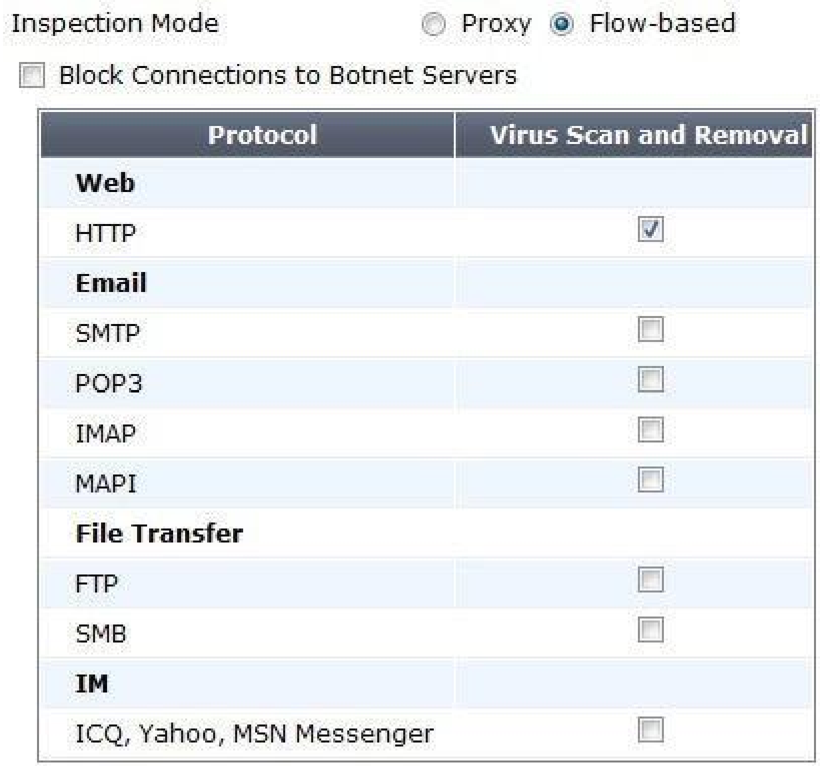
A. The file will be detected by rule #1 as an `Audio (mp3)', a log entry will be created and it will be allowed to pass through.
B. The file will be detected by rule #2 as a "*.exe", a log entry will be created and the interface that received the traffic will be brought down.
C. The file will be detected 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: Volume A
Explanation

Explanation/Reference:
Rechecked.

QUESTION 3
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:

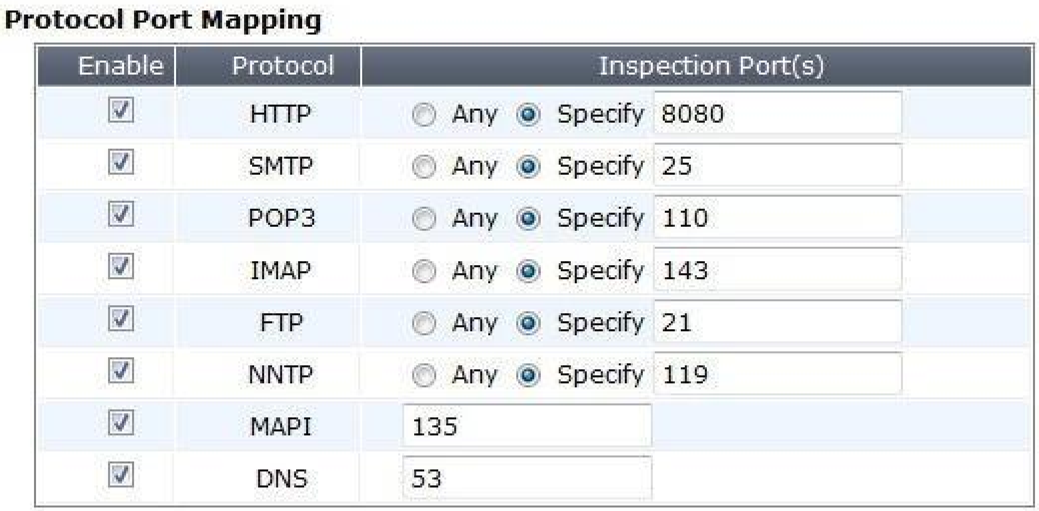


Inspection Mode ○ Proxy ● Flow-based

☐ 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	☐

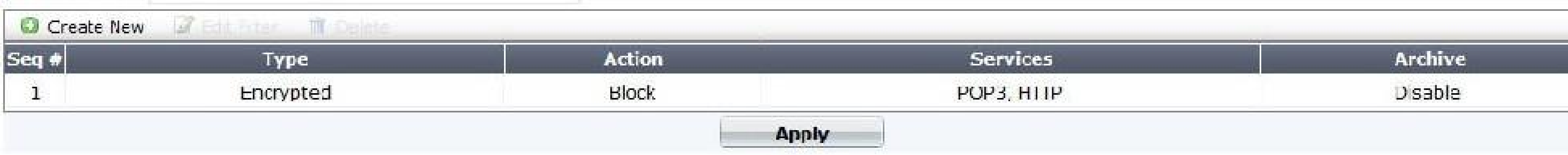
Exhibit B Non-default UTM Proxy Options Profile:



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: Volume A
Explanation

Explanation/Reference:

QUESTION 4
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: Volume A
Explanation

Explanation/Reference:
QUESTION NO:14
Select the answer that describes what the CLI command diag 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.

Answer: B

QUESTION 5
What are the requirements for a cluster to maintain TCP connections after device or link failover? (Select all that apply.)

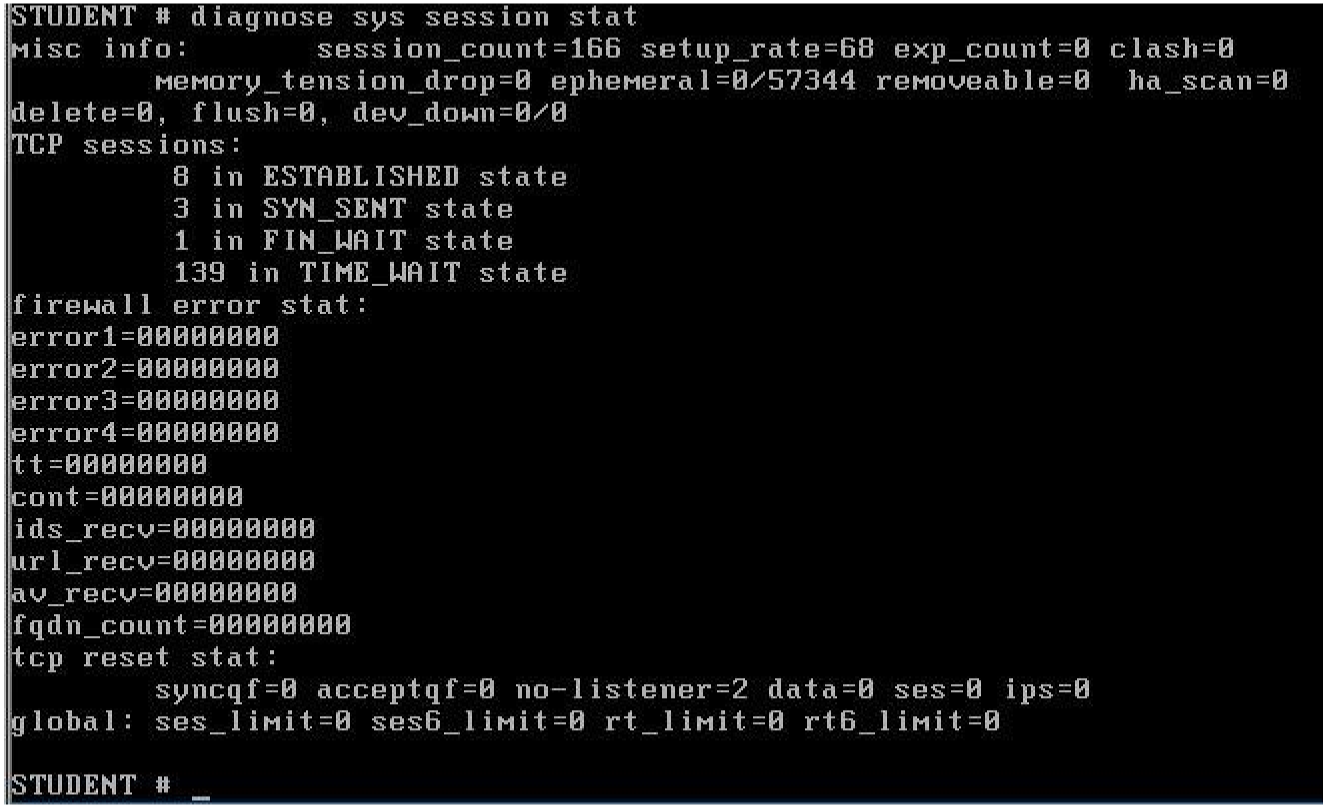
A. Enable session pick-up.
B. Only applies to connections handled by a proxy.
C. Only applies to UDP and ICMP connections.
D. Connections must not be handled by a proxy.

Correct Answer: AD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 6
Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of 'diag sys session stat' for the STUDENT device. Exhibit B shows the command output of 'diag sys session stat' for the REMOTE device.

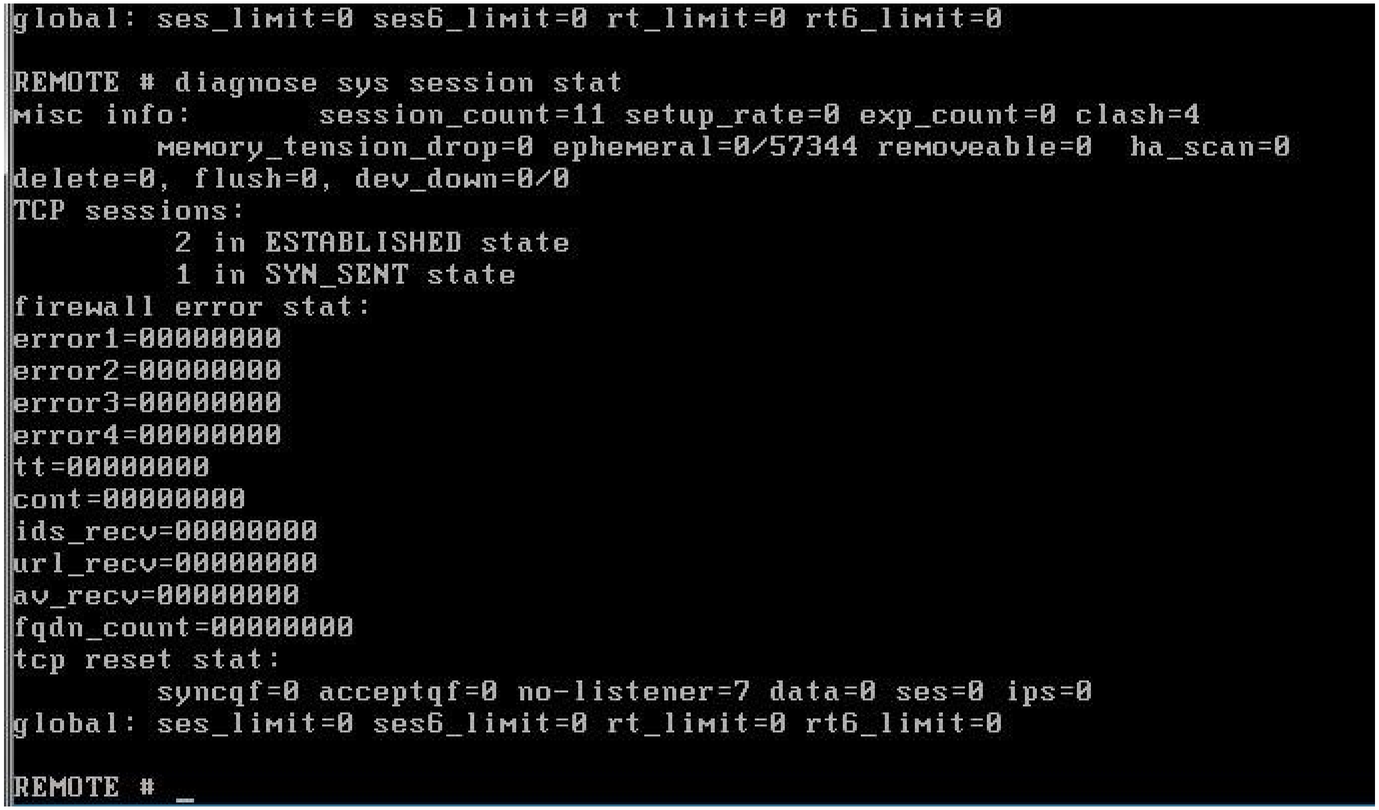
Exhibit A:



```
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? (Select all that apply.)

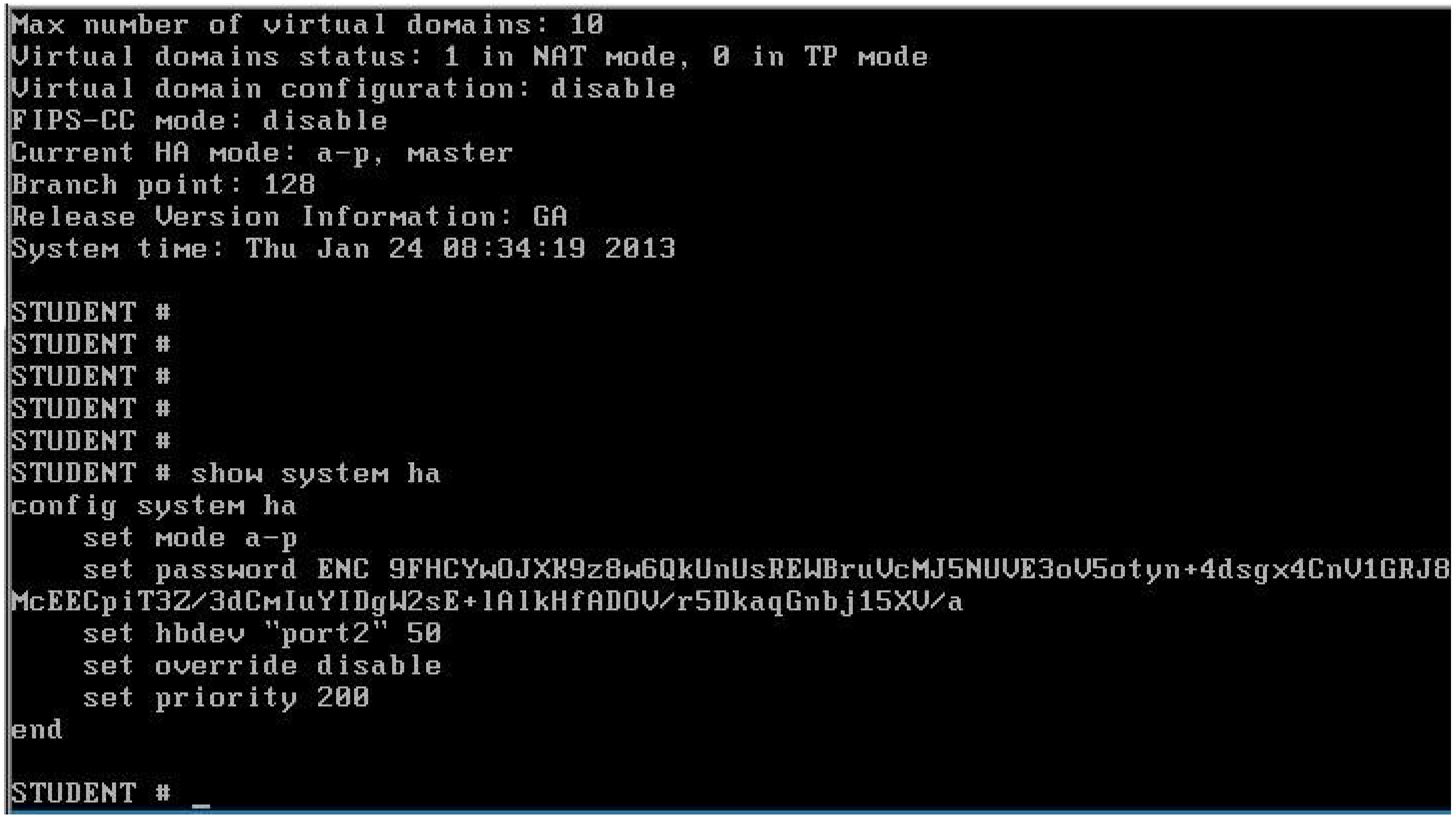
A. STUDENT is likely to be the master device.
B. Session-pickup is likely to be enabled.
C. The cluster mode is definitely Active-Passive.
D. There is not enough information to determine the cluster mode.

Correct Answer: AD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 7
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:

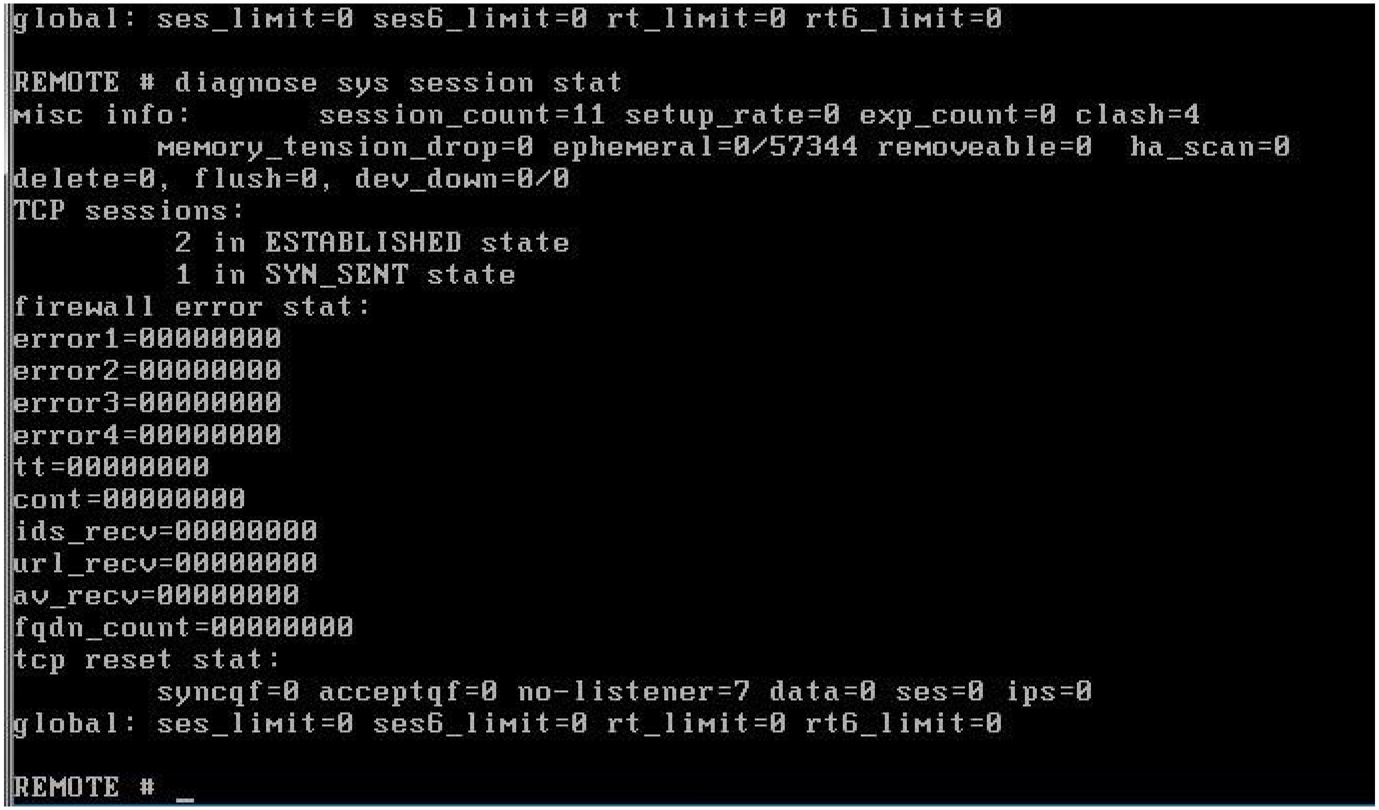


```
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

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



```
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 # _
```

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

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 8
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: Volume A
Explanation

Explanation/Reference:

QUESTION 9
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.

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 10
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
set 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: Volume A
Explanation

Explanation/Reference:

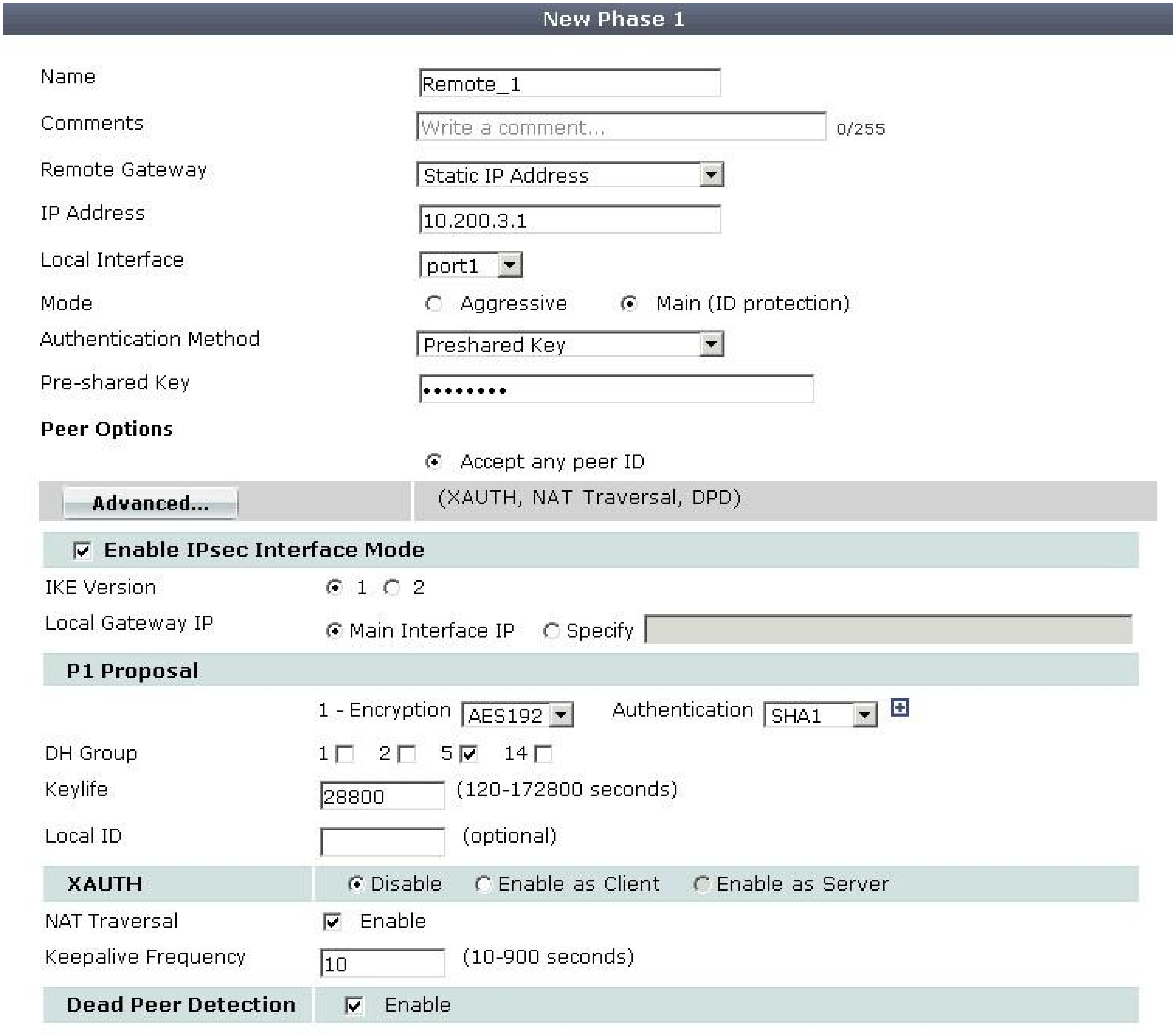
QUESTION 11
Identify the correct properties of a partial mesh VPN deployment:

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: Volume A
Explanation

Explanation/Reference:

QUESTION 12
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

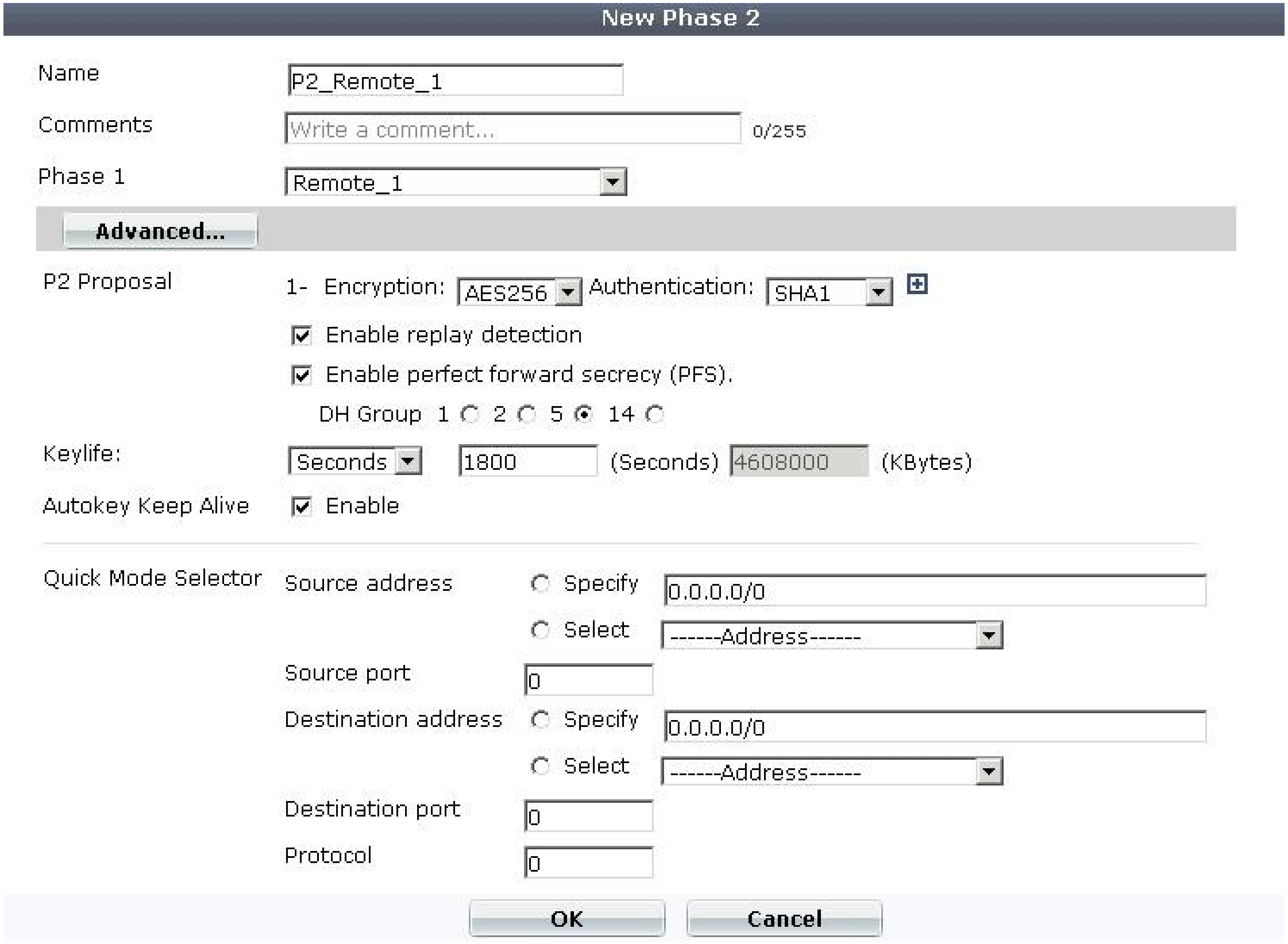
Which of the following statements are correct regarding this configuration? (Select all that apply).

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: Volume A
Explanation

Explanation/Reference:
Updated.

QUESTION 13
Review the IPsec Phase2 configuration shown in the Exhibit; then answer the question following it.



New Phase 2

Name: P2_Remote_1

Comments: Write a comment... 0/255

Phase 1: Remote_1

Advanced...

P2 Proposal: 1- Encryption: AES256 Authentication: SHA1

☑ Enable replay detection

☑ Enable perfect forward secrecy (PFS).

DH Group 1 ○ 2 ○ 5 ● 14 ○

Keylife: Seconds 1800 (Seconds) 4608000 (KBytes)

Autokey Keep Alive: ☑ Enable

Quick Mode Selector

Source address: ○ Specify 0.0.0.0/0 ○ Select ------Address------

Source port: 0

Destination address: ○ Specify 0.0.0.0/0 ○ Select ------Address------

Destination port: 0

Protocol: 0

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

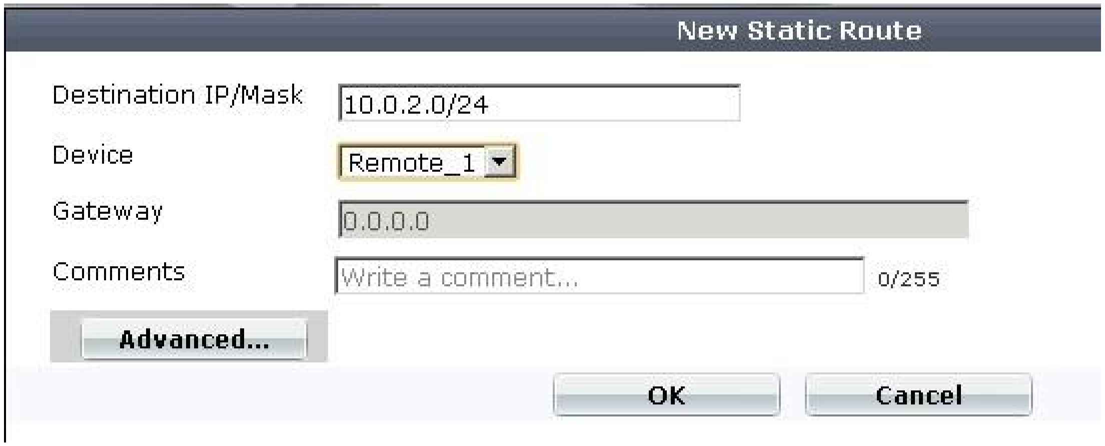
A. The Phase 2 will re-key even if there is no traffic.
B. There will be a DH exchange for each re-key.

C. The sequence number of ESP packets received from the peer will not be checked.
D. Quick mode selectors will default to those used in the firewall policy.

Correct Answer: AB
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 14
Review the static route configuration for IPsec shown in the Exhibit below; then answer the question following it.



New Static Route

Destination IP/Mask: 10.0.2.0/24
Device: Remote_1
Gateway: 0.0.0.0
Comments: Write a comment... 0/255

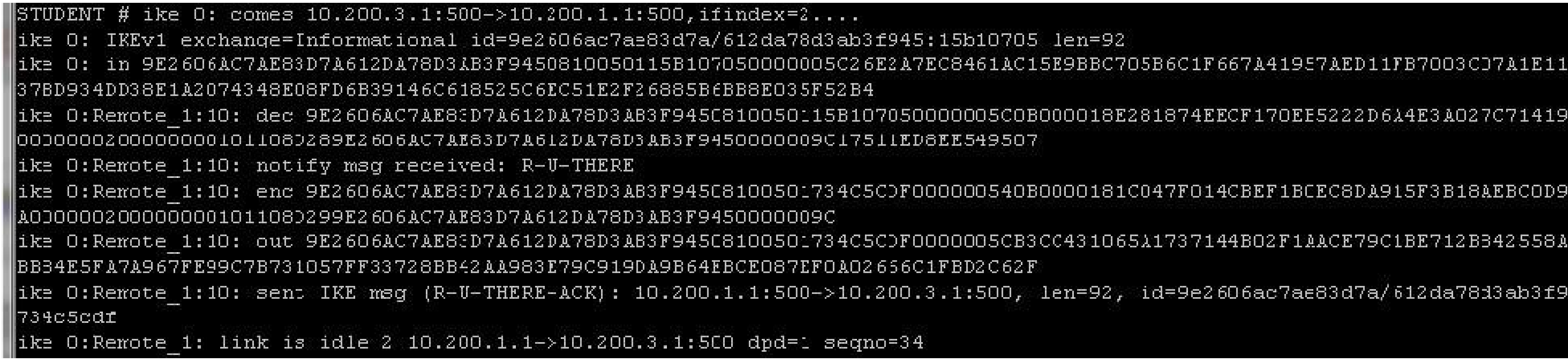
Which of the following statements are correct regarding this configuration? (Select all that apply).

A. Remote_1 is a Phase 1 object with interface mode enabled
B. The gateway address is not required because the interface is a point-to-point connection
C. The gateway address is not required because the default route is used
D. Remote_1 is a firewall zone

Correct Answer: AB
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 15
Review the IKE debug output for IPsec shown in the Exhibit below.



```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B10705000005C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07A1E11
37BD934DD38E1A2074348E08FD6B39146C618525C6EC51E2F26885B6BB8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C0B000018E281874EECF170EE5222D6A4E3A027C71419
00000002000000000101108D289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540B0000181C047F014CBEF1BCEC8DA915F3B18AEBC0D9
A0000002000000000101108D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AACE79C1BE712B342558A
BB34E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBCE087EF0A02656C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3ab3f9
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

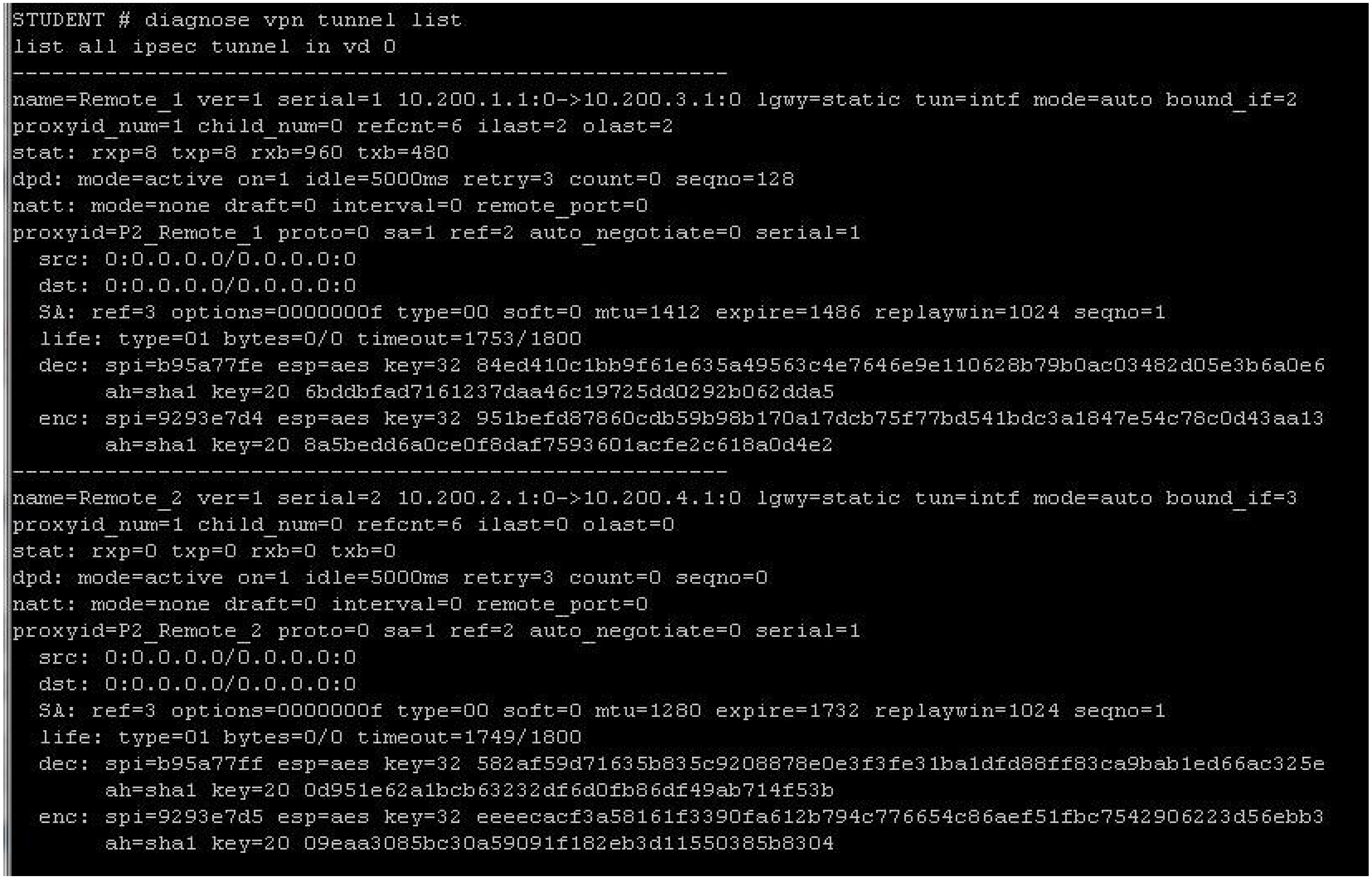
Which one of the following statements is correct regarding this output?

A. The output is a Phase 1 negotiation.
B. The output is a Phase 2 negotiation.
C. The output captures the Dead Peer Detection messages.
D. The output captures the Dead Gateway Detection packets.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 16
Review the IPsec diagnostics output of the command diag vpn tunnel list shown in the Exhibit.



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

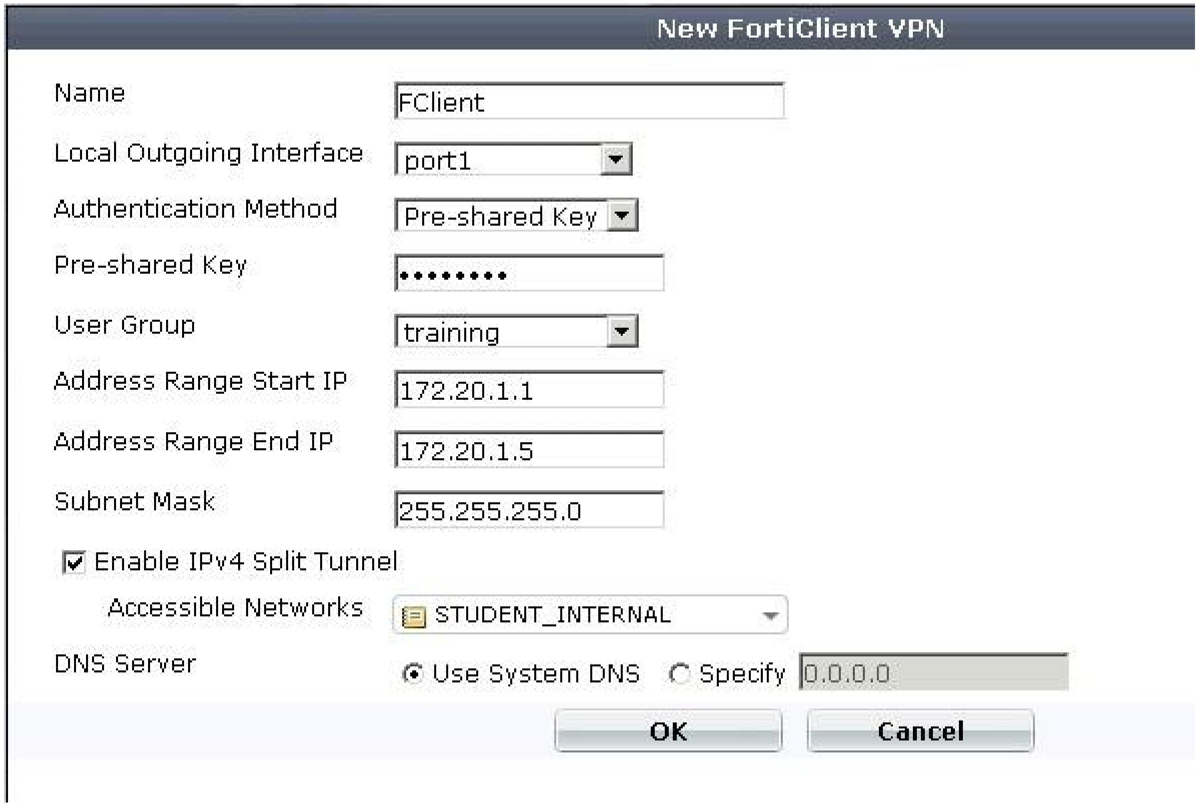
Which of the following statements is correct regarding this output? (Select one answer).

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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 17
Review the configuration for FortiClient IPsec shown in the Exhibit below.



New FortiClient VPN

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

Which of the following statements is correct regarding this configuration?

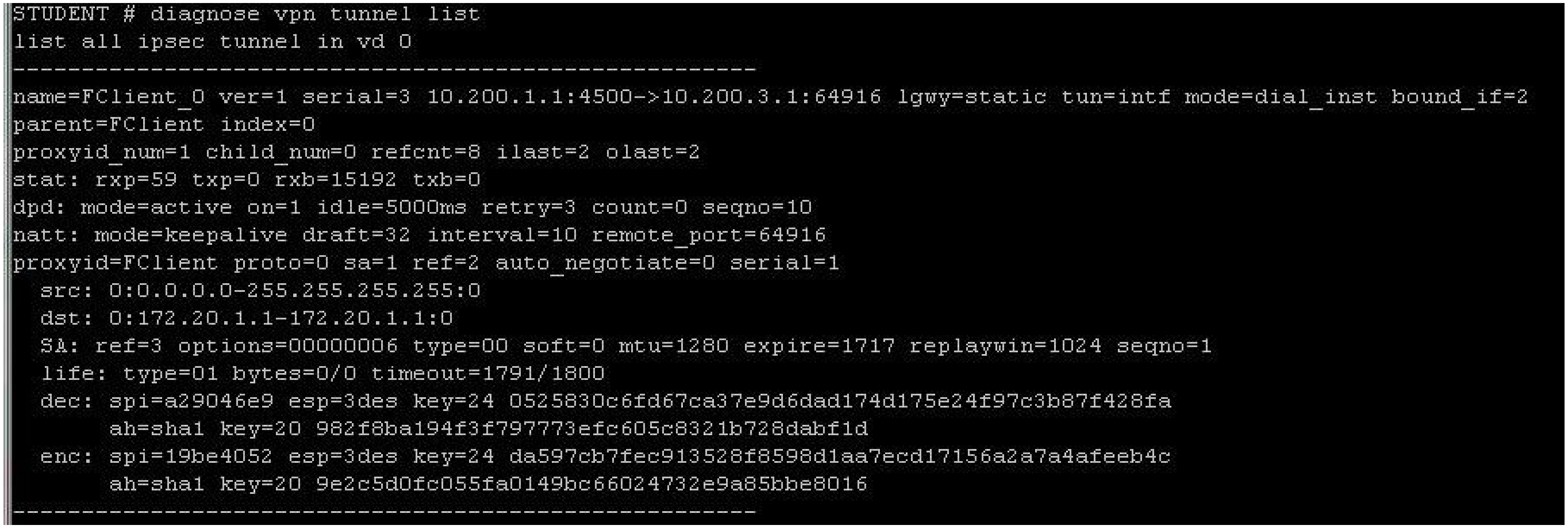
A. The connecting VPN client will install a route to a destination corresponding to the STUDENT_INTERNAL address object
B. The connecting VPN client will install a default route

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 18
Review the IPsec diagnostics output of the command diag vpn tunnel list shown in the Exhibit below.



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

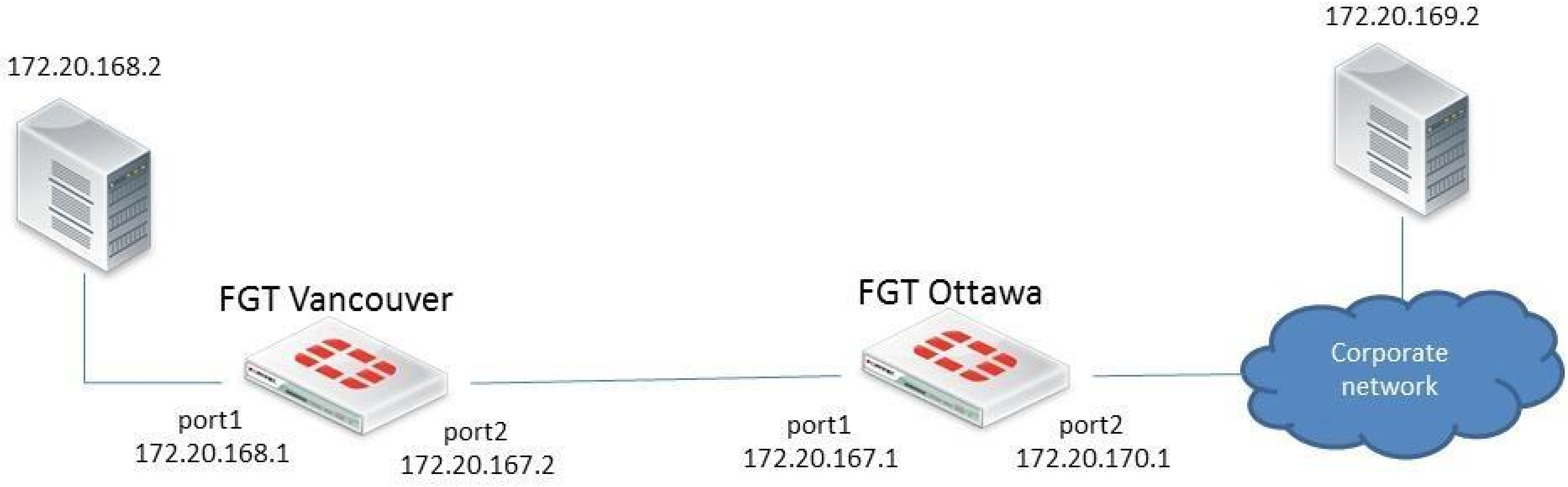
Which of the following statements are correct regarding this output? (Select all that apply.)

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

Correct Answer: AB
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 19
Examine the Exhibit shown 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 unit 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 unit'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: Volume A
Explanation

Explanation/Reference:

QUESTION 20
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 unit will evenly share the traffic to 172.20.168.0/24 through both routes.

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

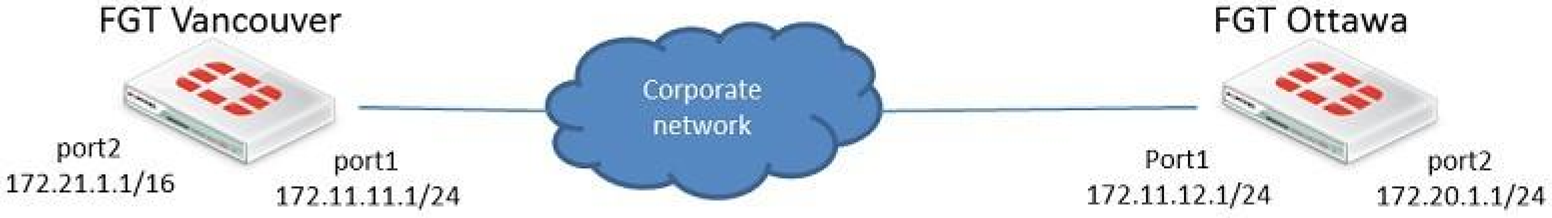
C. The FortiGate unit will send all the traffic to 172.20.168.0/24 through port1.

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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 21
Examine the Exhibit shown below; then answer the question following it.



The Vancouver FortiGate unit 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 pririoty 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 allow-subnet-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: Volume A
Explanation

Explanation/Reference:

QUESTION 22

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

```
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: Volume A
Explanation

Explanation/Reference:

QUESTION 23

In the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate unit when searching for a suitable gateway?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 24
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
```

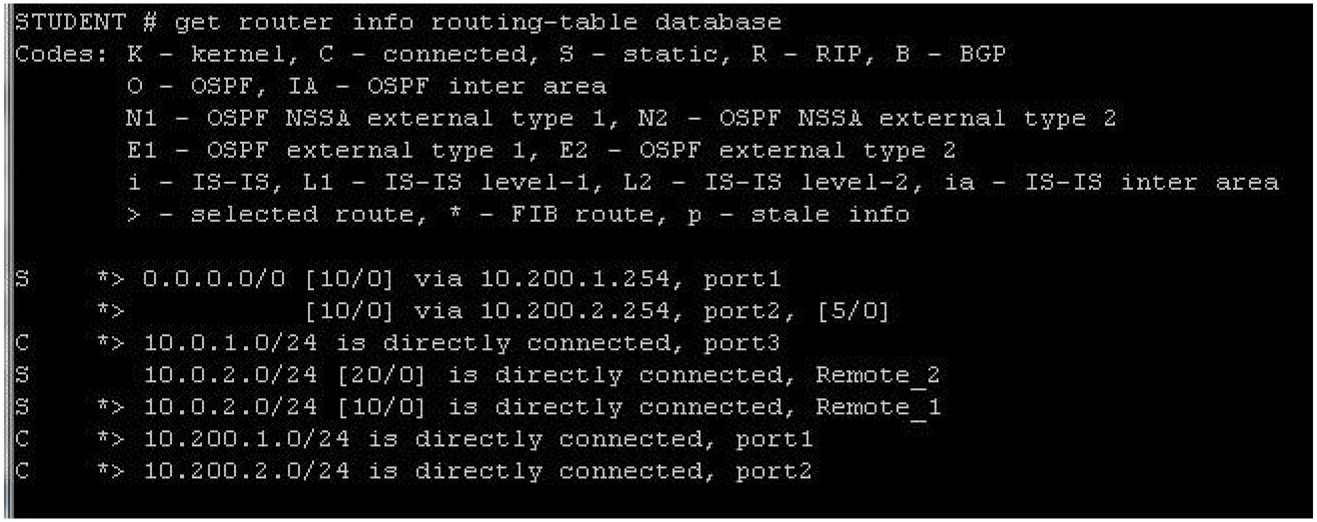
In the output provided, which of the following best describes the IP address 172.20.187.150?

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: Volume A
Explanation

Explanation/Reference:

QUESTION 25
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 of the following statements are correct regarding this output? (Select all that apply).

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: Volume A
Explanation

Explanation/Reference:

QUESTION 26
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: Volume B
Explanation

Explanation/Reference:

QUESTION 27
Which of the following statements is correct about configuring web filtering overrides?

A. The Override option for FortiGuard Web Filtering is available for any user group type.
B. Admin overrides require an administrator to manually allow pending override requests which are listed in the Override Monitor.
C. The Override Scopes of User and User Group are only for use when Firewall Policy Authentication is also being used.
D. Using Web Filtering Overrides requires the use of Firewall Policy Authentication.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 28
The FortiGate Server Authentication Extensions (FSAE) provide 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 FSAE in a Windows domain environment when NTLM is not used? (Select all that apply.)

A. An FSAE Collector Agent must be installed on every domain controller.
B. An FSAE Domain Controller Agent must be installed on every domain controller.
C. The FSAE Domain Controller Agent will regularly update user logon information on the FortiGate unit.
D. The FSAE Collector Agent will retrieve user information from the Domain Controller Agent and will send the user logon information to the FortiGate unit.
E. For non-domain computers, an FSAE client must be installed on the computer to allow FSAE authentication.

Correct Answer: BD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 29
Bob wants to send Alice a file that is encrypted using public key cryptography.

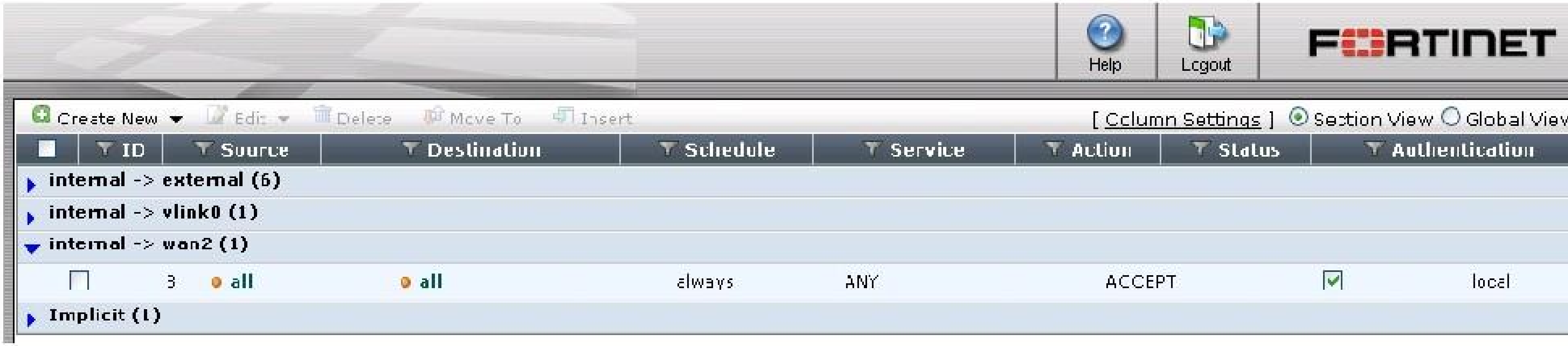
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

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.
E. Bob will use Alice's public key to encrypt the file and Alice will use Bob's public key to decrypt the file.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 30
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)								
□	3	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: Volume B
Explanation

Explanation/Reference:

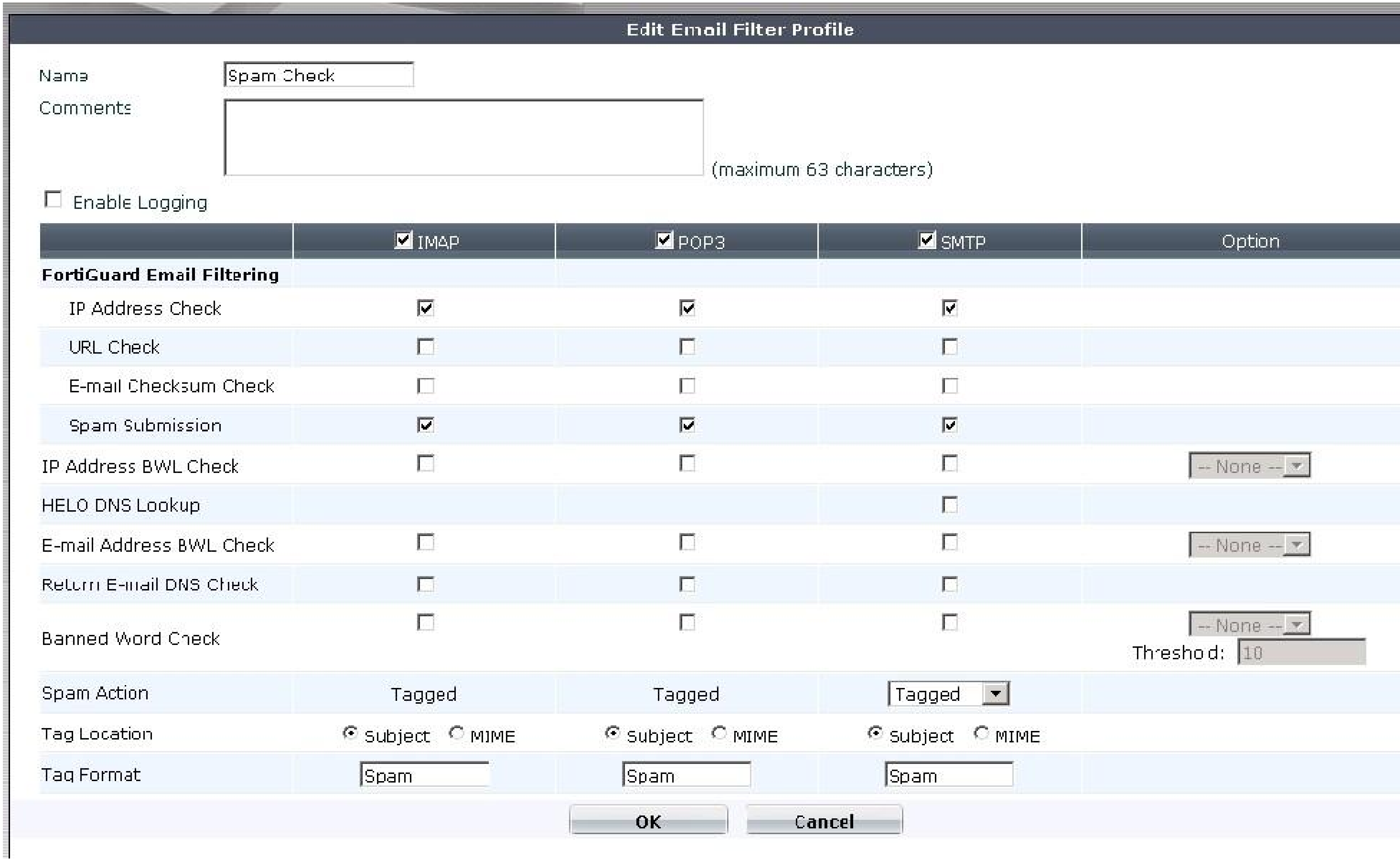
QUESTION 31
Which of the following statements is correct regarding the antivirus scanning function on the FortiGate unit?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 32
A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the AntiVirus and Email Filter profiles applied to this policy.



Edit Email Filter Profile

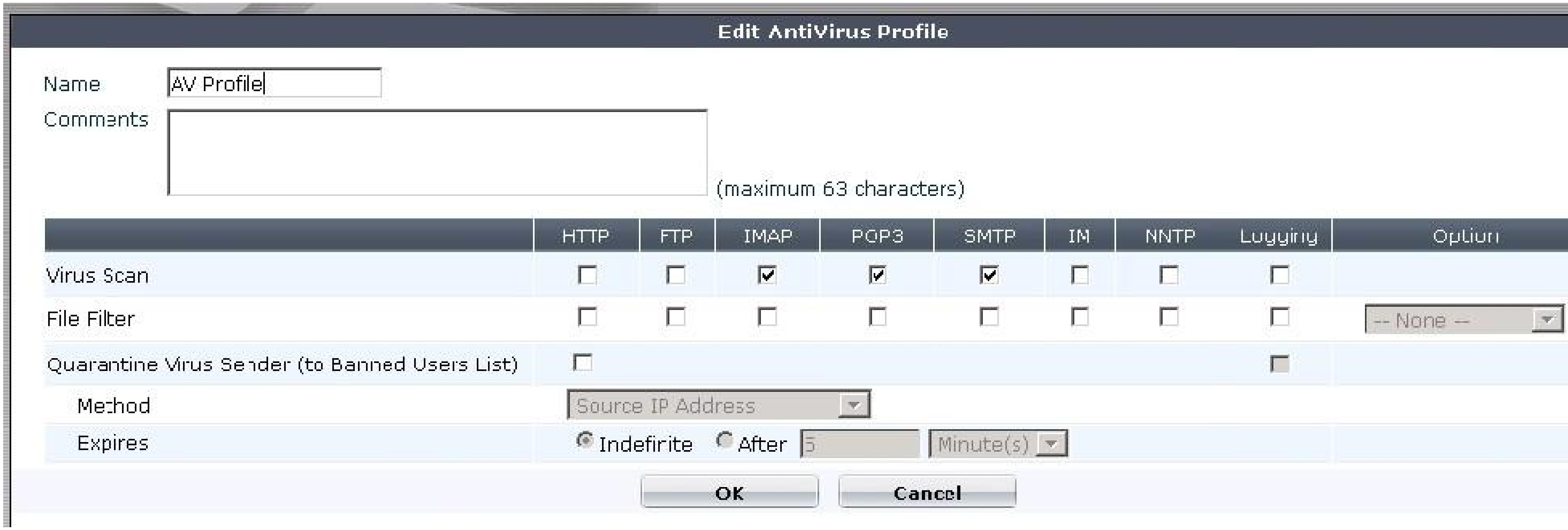
Name: Spam Check

Comments:

(maximum 63 characters)

□ Enable Logging

	☑ IMAP	☑ POP3	☑ SMTP	Option
FortiGuard Email Filtering				
IP Address Check	☑	☑	☑	
URL Check	□	□	□	
E-mail Checksum Check	□	□	□	
Spam Submission	☑	☑	☑	
IP Address BWL Check	□	□	□	-- None --
HELO DNS Lookup			□	
E-mail Address BWL Check	□	□	□	-- None --
Return E-mail DNS Check	□	□	□	
Banned Word Check	□	□	□	-- None -- Threshold: 10
Spam Action	Tagged	Tagged	Tagged ▾	
Tag Location	● Subject ○ MIME	● Subject ○ MIME	● Subject ○ MIME	
Tag Format	Spam	Spam	Spam	



Edit AntiVirus Profile

Name: AV Profile

Comments: (maximum 63 characters)

	HTTP	FTP	IMAP	POP3	SMTP	IM	NNTP	Logging	Option
Virus Scan	□	□	☑	☑	☑	□	□	□	
File Filter	□	□	□	□	□	□	□	□	-- None --
Quarantine Virus Sender (to Banned Users List)	□							□	
Method	Source IP Address								
Expires	● Indefinite ○ After 5 Minute(s)								

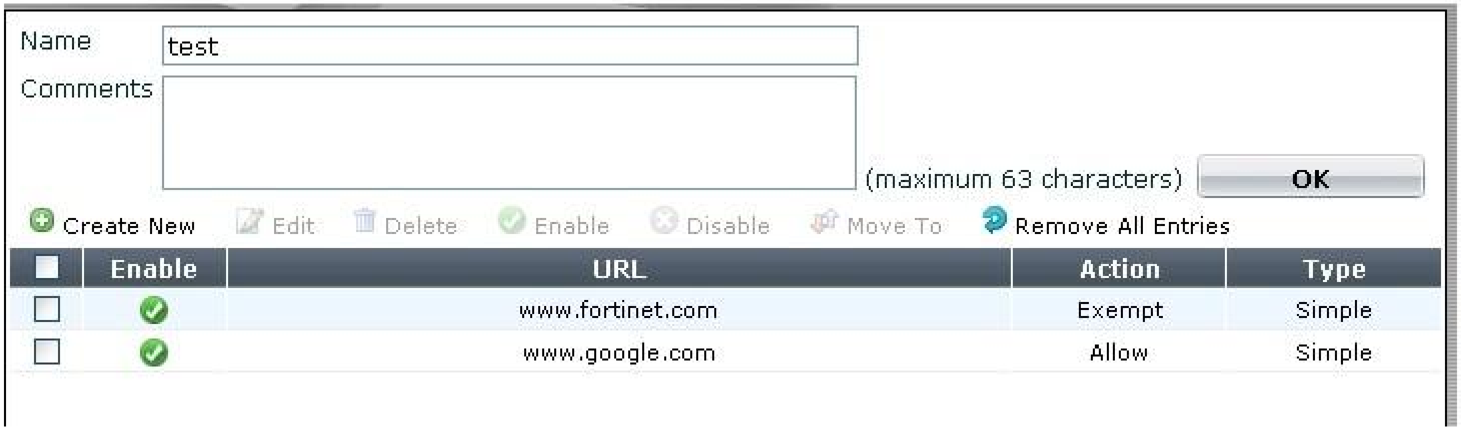
What is the correct behavior when the email attachment is detected as a virus by the FortiGate AntiVirus engine?

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

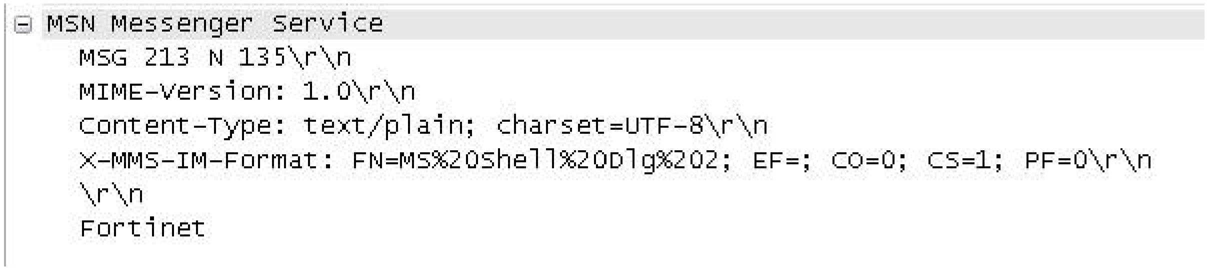
QUESTION 33
Which of the following describes the best custom signature for detecting the use of the word "Fortinet" in chat applications?



Name: test

Comments:

□	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: Volume B
Explanation

Explanation/Reference:

QUESTION 34
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 status=detected proto=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: Volume B
Explanation

Explanation/Reference:

QUESTION 35
An administrator is examining the attack logs and notices the following entry:

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

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

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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 36
Which of the following items are considered to be advantages of using the application control features on the FortiGate unit?

Application control allows an administor to:

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 37
Which of the following features could be used by an administrator to block FTP uploads while still allowing FTP downloads?

A. Anti-Virus File-Type Blocking
B. Data Leak Prevention
C. Network Admission Control
D. FortiClient Check

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

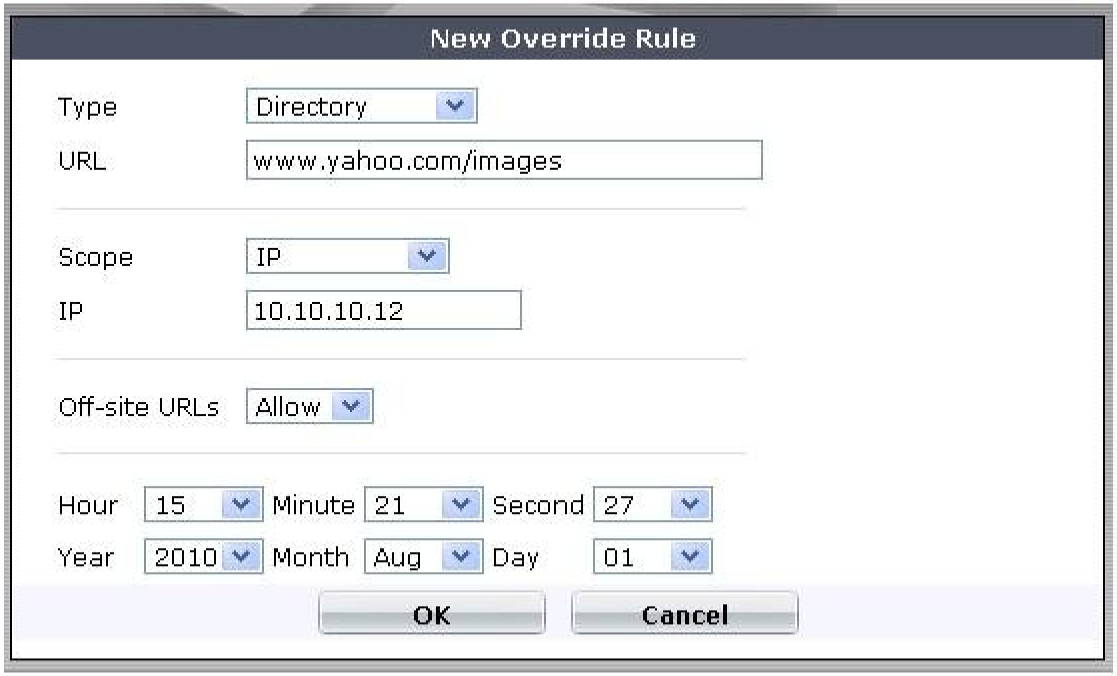
QUESTION 38
An organization wishes to protect its SIP Server from call flooding attacks. Which of the following configuration changes can be performed on the FortiGate unit to fulfill this requirement?

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: Volume B
Explanation

Explanation/Reference:

QUESTION 39
Which of the following statements is correct regarding the FortiGuard Services Web Filtering Override configuration as illustrated in the exhibit?



New Override Rule

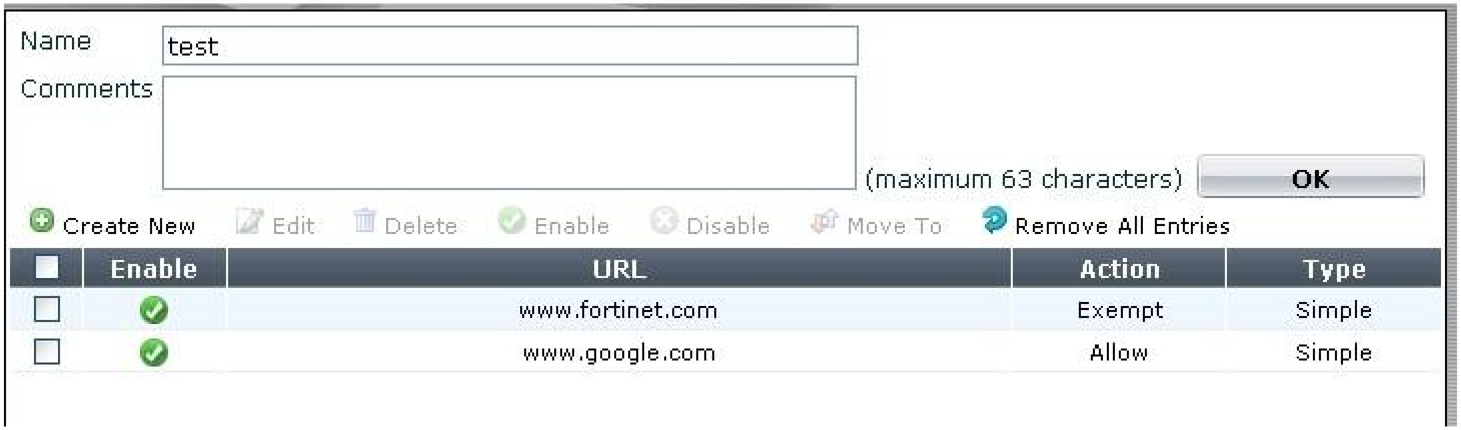
Type: Directory
URL: www.yahoo.com/images
Scope: IP
IP: 10.10.10.12
Off-site URLs: Allow
Hour: 15 Minute: 21 Second: 27
Year: 2010 Month: Aug Day: 01

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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 40
Based on the web filtering configuration illustrated in the exhibit,



Name: test

Comments:

(maximum 63 characters)

□	Enable	URL	Action	Type
□	✓	www.fortinet.com	Exempt	Simple
□	✓	www.google.com	Allow	Simple

which one of the following statements is not a reasonable conclusion?

A. Users can access both the www.google.com site and the www.fortinet.com site.
B. When a user attempts to access the www.google.com site, the FortiGate unit will not perform web filtering on the content of that site.
C. When a user attempts to access the www.fortinet.com site, any remaining web filtering will be bypassed.
D. Downloaded content from www.google.com will be scanned for viruses if antivirus is enabled.

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 41
Which spam 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: Volume B
Explanation

Explanation/Reference:

QUESTION 42
Which part of an email message exchange is NOT inspected by the POP3 and IMAP proxies?

A. TCP connection
B. File attachments
C. Message headers
D. Message body

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 43
Which of the following statements best decribes the proxy behavior on a FortiGate unit during an FTP client upload when FTP splice is disabled?

A. The proxy buffers the entire file from the client, only sending the file to the server if the file is clean. One possible consequence of buffering is that the server could time out.
B. The proxy sends the file to the server while simultaneously buffering it.
C. The proxy removes the infected file from the server by sending a delete command on behalf of the client.
D. If the file being scanned is determined to be clean, the proxy terminates the connection and leaves the file on the server.

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Answer is Valid.

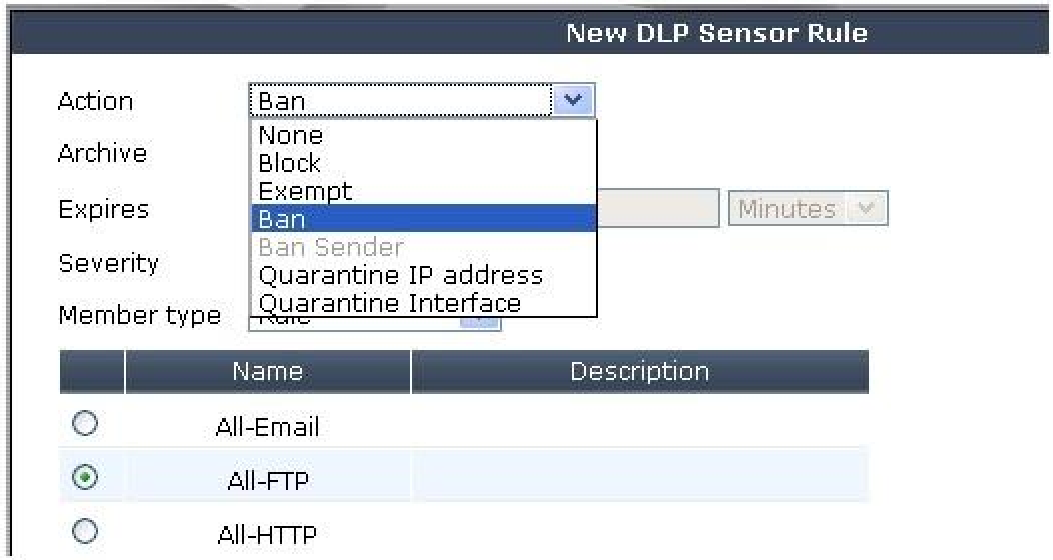
QUESTION 44
Which of the following describes the difference between the ban and quarantine actions?

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 45
An administrator is configuring a DLP rule for FTP traffic. When adding the rule to a DLP sensor,



New DLP Sensor Rule

Action: Ban

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

the administrator notes that the Ban Sender action is not available (greyed-out), as shown in the exhibit.

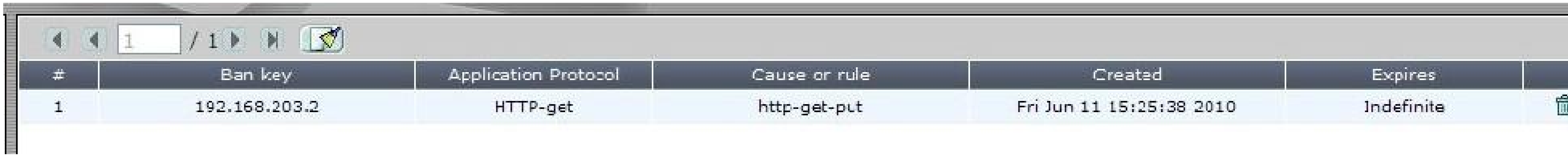
Which of the following is the best explanation for the Ban Sender action NOT being available?

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 46
When viewing the Banned User monitor in Web Config, the administrator notes the entry illustrated in the exhibit.



#	Ban key	Application Protocol	Cause or rule	Created	Expires	
1	192.168.203.2	HTTP-get	http-get-put	Fri Jun 11 15:25:38 2010	Indefinite	🗑

Which of the following statements is correct regarding this entry?

A. The entry displays a ban that has been added as a result of traffic triggering a configured DLP rule.

B. The entry displays a ban that was triggered by HTTP traffic matching an IPS signature. This client is banned from receiving or sending any traffic through the FortiGate.

C. The entry displays a quarantine, which could have been added by either IPS or DLP.

D. This entry displays a ban entry that was added manually by the administrator on June11th.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 47
The following ban list entry is displayed through the CLI.

```
get user ban list
id cause src-ip-addr dst-ip-addr expires created
531 protect_client 10.177.0.21 207.1.17.1 indefinite Wed Dec 24 :21:33 2008
```

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

A. The administrator has specified the Attack and Victim Address method for the quarantine.

B. This diagnostic entry results from the administrator running the diag ips log test command.
This command has no effect on traffic.

C. A DLP rule has been matched.

D. An attack has been repeated more than once during the holddown period; the expiry time has been reset to indefinite.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 48
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: Volume B
Explanation

Explanation/Reference:

QUESTION 49
Which of the following DLP actions will override any other action?

A. Exempt
B. Quarantine Interface
C. Block
D. None

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 50
Which of the following DLP actions will always be performed if it is selected?

A. Archive
B. Quarantine Interface
C. Ban Sender

D. Block
E. None
F. Ban
G. Quarantine IP Address

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 51
The transfer of encrypted files or the use of encrypted protocols between users and servers on the internet can frustrate the efforts of administrators attempting to monitor traffic passing through the FortiGate unit and ensuring user compliance to corporate rules.

Which of the following items will allow the administrator to control the transfer of encrypted data through the FortiGate unit? (Select all that apply.)

A. Encrypted protocols can be scanned through the use of the SSL proxy.
B. DLP rules can be used to block the transmission of encrypted files.
C. Firewall authentication can be enabled in the firewall policy, preventing the use of encrypted communications channels.
D. Application control can be used to monitor the use of encrypted protocols; alerts can be sent to the administrator through email when the use of encrypted protocols is attempted.

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 52
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: Volume B
Explanation

Explanation/Reference:

QUESTION 53
The following diagnostic output is displayed in the CLI:

```
diag firewall auth list

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

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

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 54
Which of the following cannot be used in conjunction with the endpoint compliance check?

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

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:

QUESTION 55
SSL Proxy is used to decrypt the SSL-encrypted traffic. After decryption, where is the traffic buffered in preparation for content inspection?

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 56
Which of the following statements correctly describes the deepscan option for HTTPS?

A. When deepscan is disabled, only the web server certificate is inspected; no decryption of content occurs.
B. Enabling deepscan will perform further checks on the server certificate.
C. Deepscan is only applicable to mail protocols, where all IP addresses in the header are checked.
D. With deepscan enabled, archived files will be decompressed before scanning for a more comprehensive file inspection.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 57
Which of the following tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Select all that apply.)

A. The web client SSL handshake.
B. The web server SSL handshake.

C. File buffering.
D. Communication with the urlfilter process.

Correct Answer: AB
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 58
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: Volume B
Explanation

Explanation/Reference:

QUESTION 59
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: Volume B
Explanation

Explanation/Reference:

QUESTION 60

Both the FortiGate and FortiAnalyzer units can notify administrators when certain alert conditions are met.

Considering this, which of the following statements is NOT correct?

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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 61

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: Volume B
Explanation

Explanation/Reference:

QUESTION 62

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: Volume B
Explanation

Explanation/Reference:

QUESTION 63
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: Volume B
Explanation

Explanation/Reference:

QUESTION 64
An administrator wishes to generate a report showing Top Traffic by service type, but wants to exclude SMTP traffic from the report.

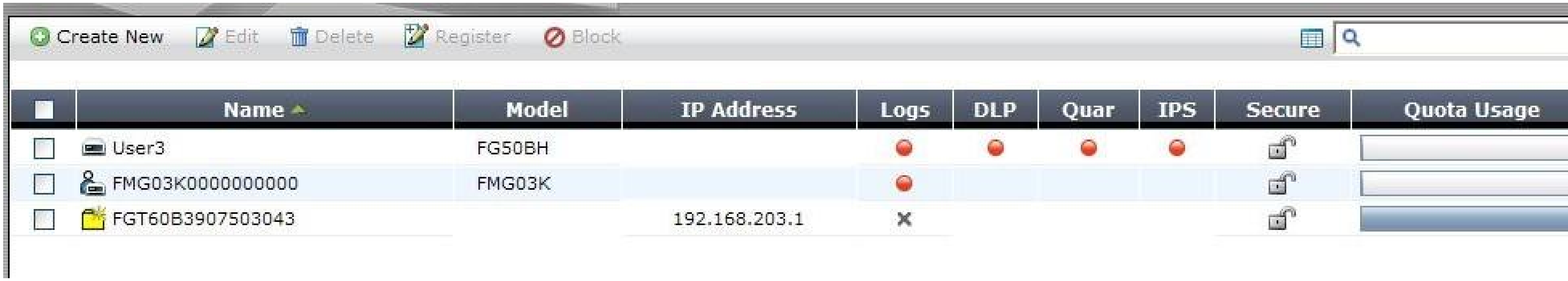
Which of the following statements best describes how to do this?

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: Volume B
Explanation

Explanation/Reference:

QUESTION 65
A portion of the device listing for a FortiAnalyzer unit is displayed in the exhibit.



□	Name ▲	Model	IP Address	Logs	DLP	Quar	IPS	Secure	Quota Usage
□	User3	FG50BH		●	●	●	●	🔓	
□	FMG03K0000000000	FMG03K		●				🔓	
□	FGT60B3907503043		192.168.203.1	✕				🔓	

Which of the following statements best describes the reason why the FortiGate 60B unit is unable to archive data to the FortiAnalyzer unit?

A. The FortiGate unit is considered an unregistered device.
B. The FortiGate unit has been blocked from sending archive data to the FortiAnalyzer device by the administrator.
C. The FortiGate unit has insufficient privileges. The administrator should edit the device entry in the FortiAnalyzer and modify the privileges.
D. The FortiGate unit is being treated as a syslog device and is only permitted to send log data.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 66
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: Volume B
Explanation

Explanation/Reference:

QUESTION 67
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: Volume B
Explanation

Explanation/Reference:

QUESTION 68
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: Volume B
Explanation

Explanation/Reference:

QUESTION 69
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: Volume B
Explanation

Explanation/Reference:

QUESTION 70
An administrator has formed a High Availability cluster involving two FortiGate 310B 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. set up a full-mesh design which uses redundant interfaces.
B. increase the number of FortiGate units in the cluster and configure HA in Active-Active mode.
C. enable monitoring of all active interfaces.

D. configure the HA ping server feature to allow for HA failover in the event that a path is disrupted.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Absolutely correct.

QUESTION 71
In a High Availability configuration operating in Active-Active mode, which of the following correctly describes the path taken by a load-balanced HTTP session?

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 72
Which of the following statements is not correct regarding virtual domains (VDOMs)?

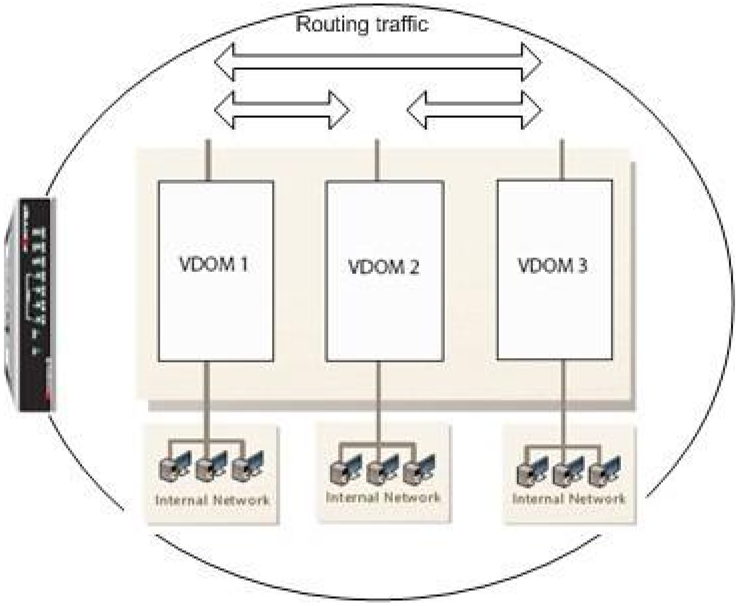
A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. A backup management VDOM will synchronize the configuration from an active management VDOM.
D. VDOMs share firmware versions, as well as antivirus and IPS databases.
E. Only administrative users with a super_admin profile will be able to enter all VDOMs to make configuration changes.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 73

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? (Select all that apply.)

A. The administrator should 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. This provides the same level of security internally as externally.

C. This configuration requires the use of an external router.

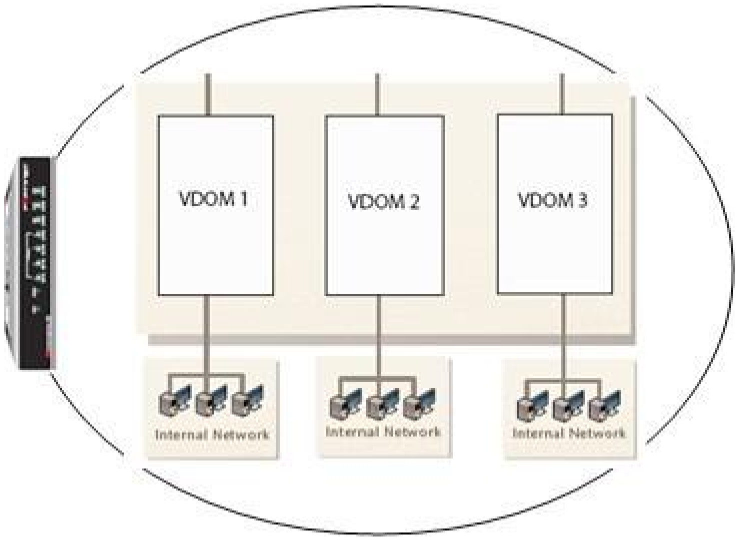
D. Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached.

E. As each VDOM has an independant 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: Volume B
Explanation

Explanation/Reference:

QUESTION 74
A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



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

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

Correct Answer: AF
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 75
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: Volume B
Explanation

Explanation/Reference:

QUESTION 76
A FortiGate unit is operating in NAT/Route mode and is configured with two Virtual LAN (VLAN) sub-interfaces added to the same physical interface.

Which 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: Volume B
Explanation

Explanation/Reference:

QUESTION 77
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: Volume B
Explanation

Explanation/Reference:

QUESTION 78
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: Volume B
Explanation

Explanation/Reference:

QUESTION 79
WAN optimization is configured in Active/Passive mode. When will the remote peer accept an attempt to initiate a tunnel?

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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 80
Which of the following methods does the FortiGate unit use to determine the availability of a web cache using Web Cache Communication Protocol (WCCP)?

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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 81
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: Volume B
Explanation

Explanation/Reference:

QUESTION 82
Which of the following represents the method used on a FortiGate unit running FortiOS version 4.2 to apply traffic shaping to P2P traffic, such as BitTorrent?

A. Apply a Traffic Shaper to a BitTorrent entry in an Application Control List.
B. Enable the Shape option in a Firewall policy with a Service set to BitTorrent.
C. Define a DLP Rule to match against BitTorrent traffic and include the rule in a DLP Sensor with Traffic Shaping enabled.

D. Specify the amount of Rate Limiting to be applied to BitTorrent traffic through the P2P settings of the Firewall Policy Protocol Options.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 83
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 NTLM and Polling Mode are not used? (Select all that apply.)

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 retrieve user information from the Domain Controller Agent and will send the user logon information to the FortiGate unit.
E. For non-domain computers, the only way to allow FSSO authentication is to install an FSSO client.

Correct Answer: BD
Section: Volume A
Explanation

Explanation/Reference:
Corrected.

QUESTION 84
Which of the following represents the correct order of criteria used for the selection of a Master unit within a FortiGate High Availability (HA) cluster when master 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: Volume A
Explanation

Explanation/Reference:

QUESTION 85
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 subordinate unit?

A. Request: Internal Host; Master FortiGate; Slave FortiGate; Internet; Web Server
B. Request: Internal Host; Master FortiGate; Slave FortiGate; Master FortiGate; Internet; Web Server
C. Request: Internal Host; Slave FortiGate; Internet; Web Server
D. Request: Internal Host; Slave FortiGate; Master FortiGate; Internet; Web Server

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 86
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: Volume A
Explanation

Explanation/Reference:

QUESTION 87
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: Volume A
Explanation

Explanation/Reference:

QUESTION 88
Data Leak Prevention archiving gives the ability to store files and message data onto 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: Volume A
Explanation

Explanation/Reference:

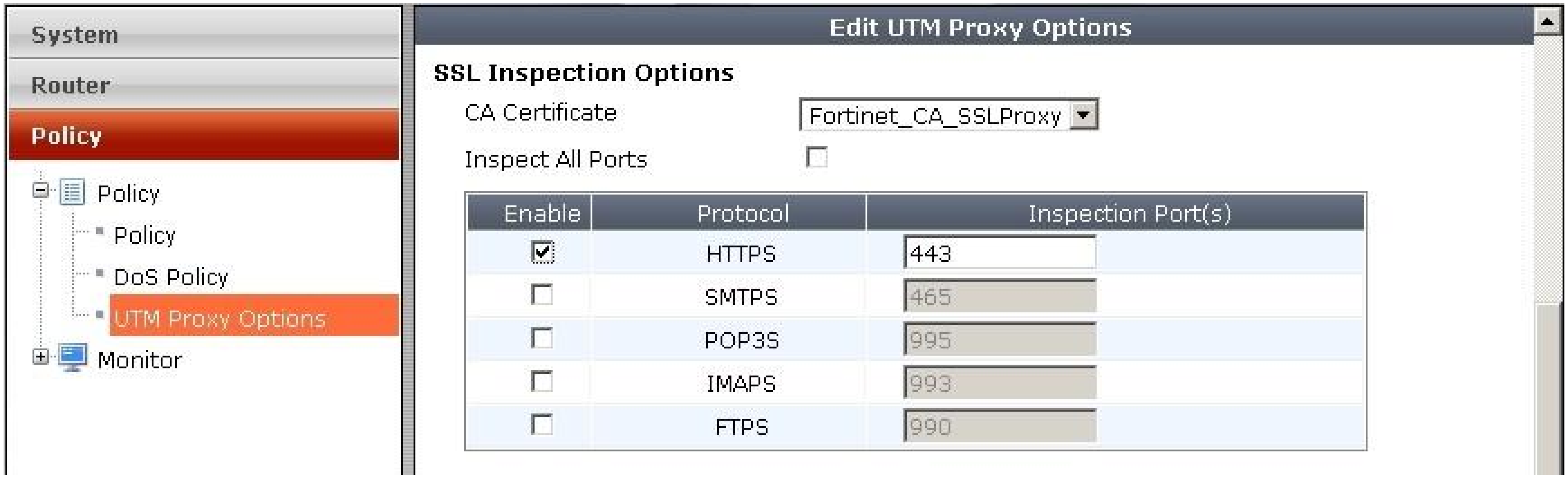
QUESTION 89
Which of the following statements are correct regarding Application Control?

A. Application Control is based on the IPS engine.
B. Application Control is based on the AV engine.
C. Application Control can be applied to SSL encrypted traffic.
D. Application Control cannot be applied to SSL encrypted traffic.

Correct Answer: AC
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 90
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: Volume A
Explanation

Explanation/Reference:

QUESTION 91
For Data Leak Prevention, which of the following describes the difference between the block and quarantine actions?

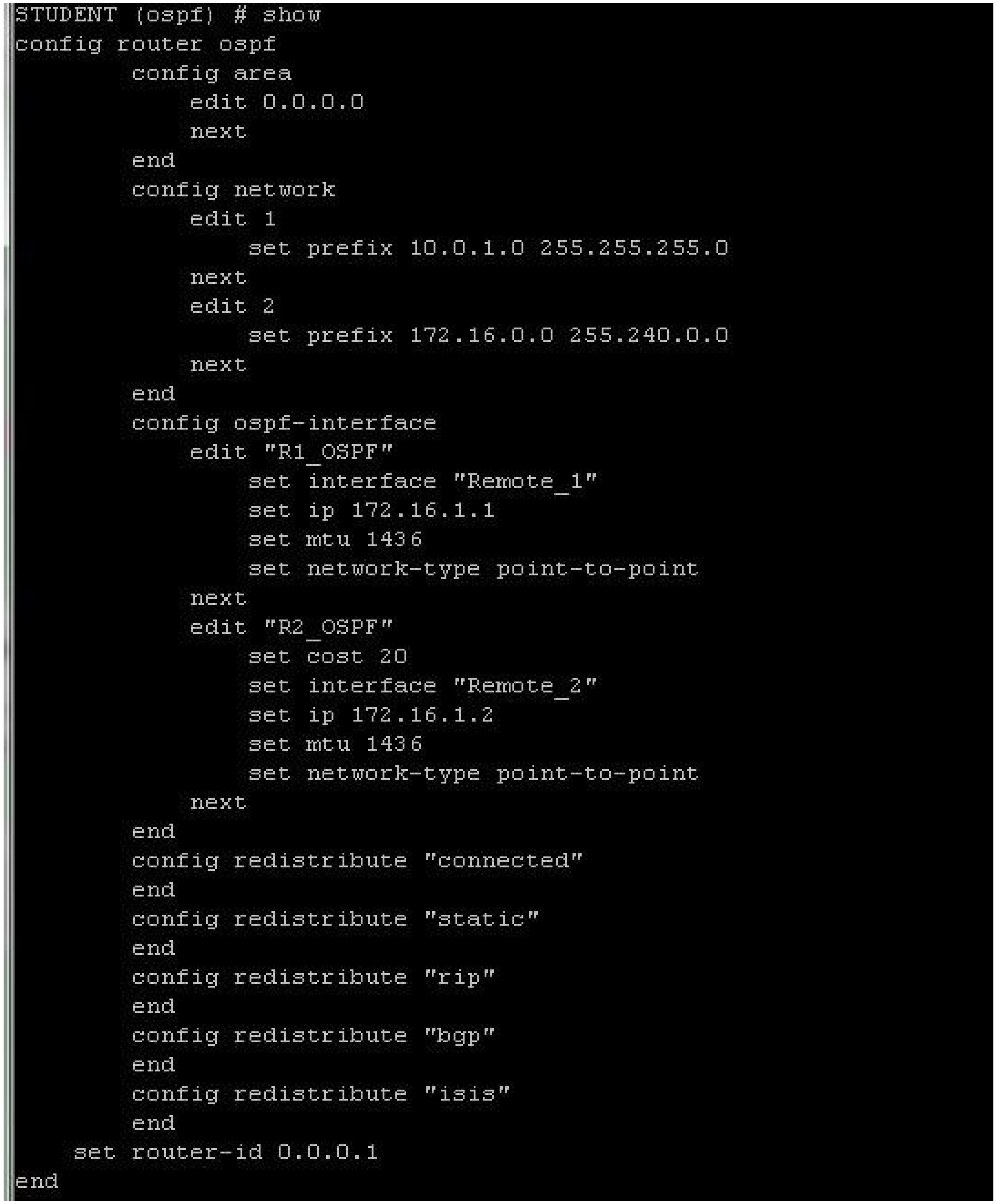
A. A block action prevents the transaction. A quarantine action blocks all future transactions, regardless of the protocol.

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: Volume A
Explanation

Explanation/Reference:

QUESTION 92
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
    set router-id 0.0.0.1
end
```

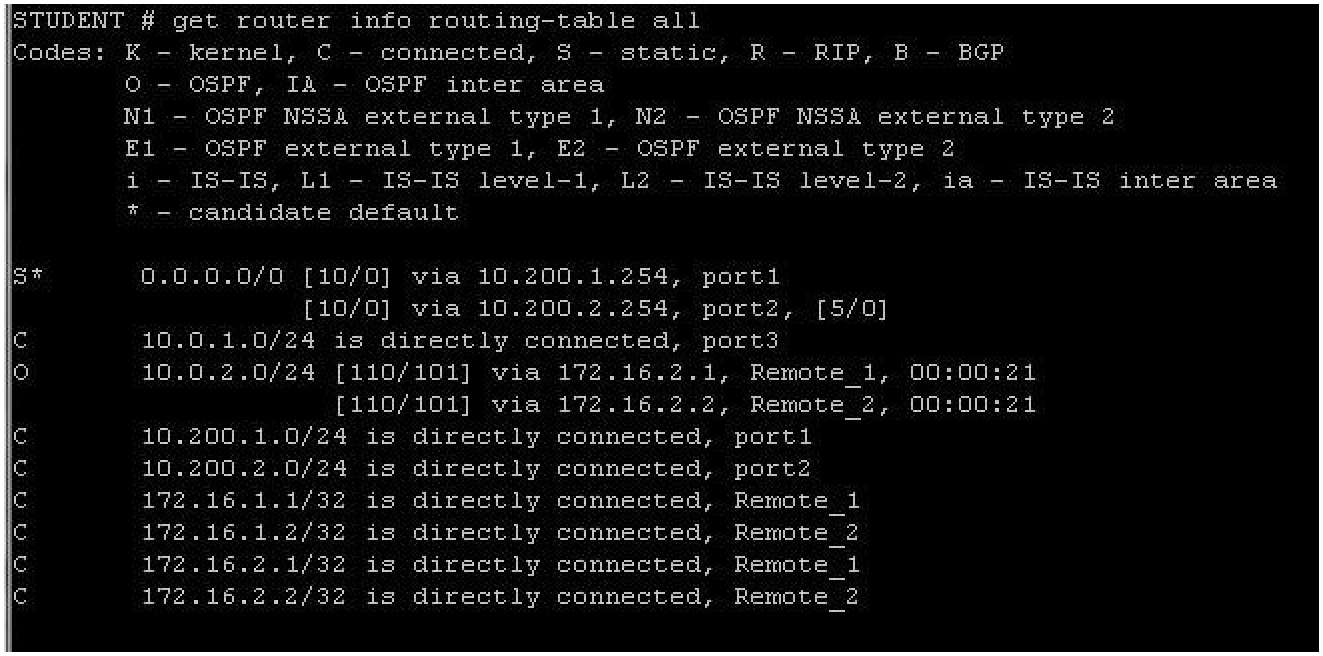
Which one of the following statements is correct regarding this output?

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: Volume A
Explanation

Explanation/Reference:

QUESTION 93
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: Volume A
Explanation

Explanation/Reference:

QUESTION 94
Which of the following statements correctly describe Transparent Mode operation? (Select all that apply.)

A. The FortiGate unit acts as transparent bridge and routes traffic using Layer-2 forwarding.
B. Ethernet packets are forwarded based on destination MAC addresses NOT IPs.
C. The device is transparent to network hosts.
D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.
E. All interfaces must be on different IP subnets.

Correct Answer: ABCD
Section: Volume A
Explanation

Explanation/Reference:
Modified.

QUESTION 95
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: Volume A
Explanation

Explanation/Reference:

QUESTION 96
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: Volume A
Explanation

Explanation/Reference:

QUESTION 97
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: Volume B
Explanation

Explanation/Reference:

QUESTION 98
An administrator logs into a FortiGate unit using an account which has been assigned a super_admin profile. Which of the following operations can this administrator perform?

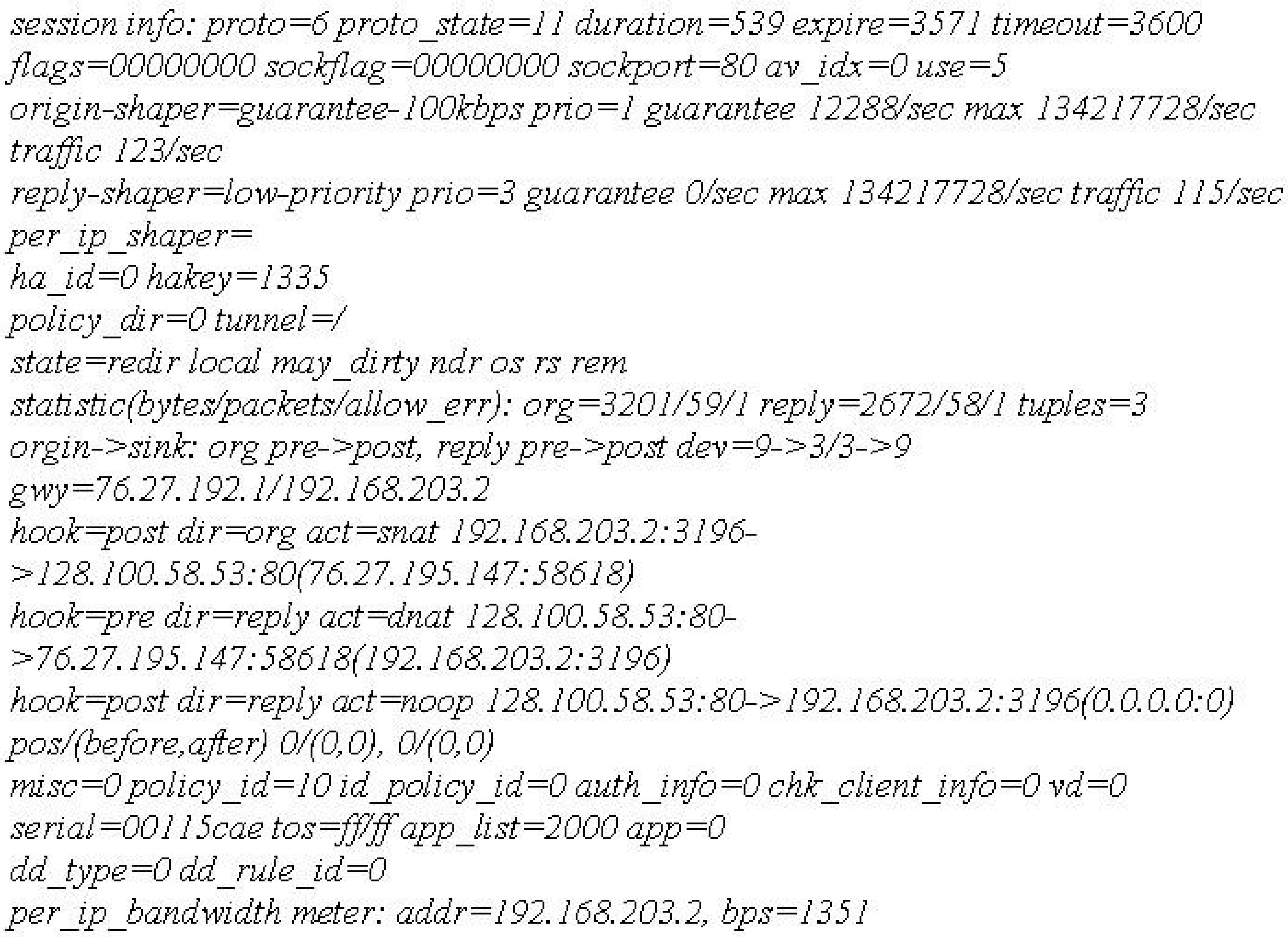
A. They can delete logged-in users who are also assigned the super_admin access profile.

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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 99
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: Volume B
Explanation

Explanation/Reference:

QUESTION 100
A FortiGate unit is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root.

Which of the following items would an administrator logging in using this account NOT be able to configure?

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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 101
What is the effect of using CLI "config system session-ttl" to set session_ttl to 1800 seconds?

A. Sessions can be idle for no 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 reauthenticate.
D. After a session has been open for 1800 seconds, the FortiGate unit will send a keepalive packet to both client and server.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 102
Which of the following statements is correct about how the FortiGate unit verifies username and password during user authentication?

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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 103
A FortiClient fails to establish a VPN tunnel with a FortiGate unit.

The following information is displayed in the FortiGate unit logs:

msg="Initiator: sent 192.168.11.101 main mode message #1 (OK)" msg="Initiator: sent 192.168.11.101 main mode message #2 (OK)" msg="Initiator: sent 192.168.11.101 main mode message #3 (OK)" msg="Initiator: parsed 192.168.11.101 main mode message #3 (DONE)" msg="Initiator: sent 192.168.11.101 quick mode message #1 (OK)" msg="Initiator: tunnel 192.168.1.1/192.168.11.101 install ipsec sa" msg="Initiator: sent 192.168.11.101 quick mode message #2 (DONE)" msg="Initiator: tunnel 192.168.11.101, transform=ESP_3DES, HMAC_MD5" msg="Failed to acquire an IP address

Which of the following statements is a possible cause for the failure to establish the VPN tunnel?

A. An IPSec DHCP server is not enabled on the external interface of the FortiGate unit.
B. There is no IPSec firewall policy configured for the policy-based VPN.
C. There is a mismatch between the FortiGate unit and the FortiClient IP addresses in the phase 2 settings.
D. The phase 1 configuration on the FortiGate unit uses Aggressive mode while FortiClient uses Main mode.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 104

An administrator sets up a new FTP server on TCP port 2121. A FortiGate unit is located between the FTP clients and the server. The administrator has created a policy for TCP port 2121.

Users have been complaining that when downloading data they receive a 200 Port command successful message followed by a 425 Cannot build data connection message.

Which of the following statements represents the best solution to this problem?

A. Create a new session helper for the FTP service monitoring port 2121.
B. Enable the ANY service in the firewall policies for both incoming and outgoing traffic.
C. Place the client and server interface in the same zone and enable intra-zone traffic.
D. Disable any protection profiles being applied to FTP traffic.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 105
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: Volume B
Explanation

Explanation/Reference:

QUESTION 106
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: Volume B
Explanation

Explanation/Reference:

QUESTION 107
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: Volume B
Explanation

Explanation/Reference:

QUESTION 108
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: Volume B
Explanation

Explanation/Reference:

QUESTION 109
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 CLI:

```
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 # 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 10.0.0.0/8 [10/0] is a summary, Null
C 10.0.1.0/25 is directly connected, vlan1
C 10.0.1.128/25 is directly connected, internal
```

```
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=277 msg="vd-root received a packet(proto=6, 10.0.1.130 :47922->10.0.1.1:443) from internal."
id=20085 trace_id=277 msg="allocate a new session-00000b21" id=20085 trace_id=277 msg="iprope_in_check() check failed, drop"
```

Based on the output from these commands, which of the following 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. There is no firewall policy allowing traffic from INTERNAL -> VLAN1.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 110
Which of the following statements are correct about the HA diag command diagnose sys ha reset-uptime? (Select all that apply.)

A. The device this command is executed on is likely to switch from master to slave status if master override is disabled.

B. The device this command is executed on is likely to switch from master to slave status if master override is enabled.

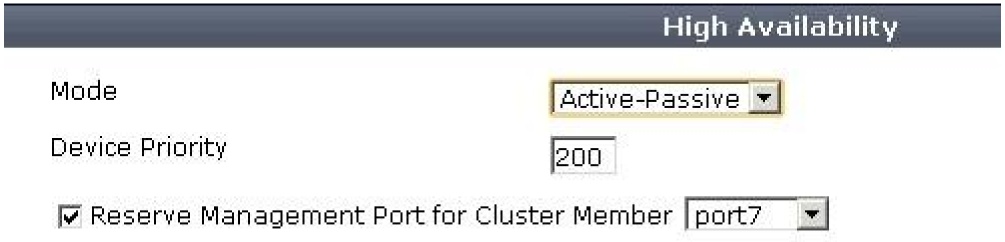
C. This command has no impact on the HA algorithm.

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: Volume A
Explanation

Explanation/Reference:

QUESTION 111
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the Exhibit below.



Mode Active-Passive

Device Priority 200

☑ Reserve Management Port for Cluster Member port7

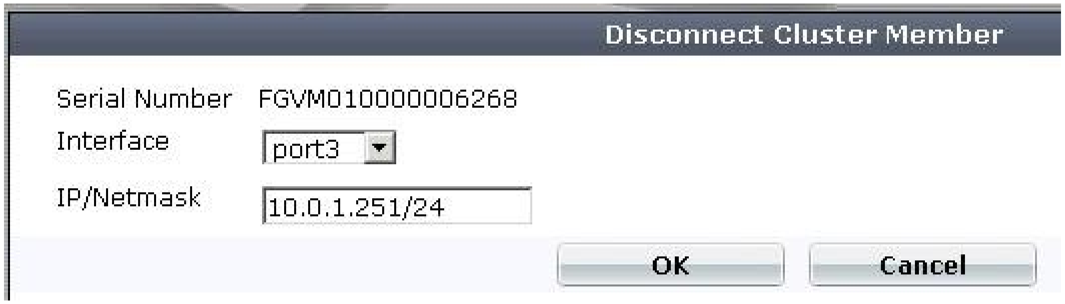
Which of the following statements are correct regarding this setting? (Select all that apply.)

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. Port7 appears in the routing table.
D. A gateway address may be configured for port7.
E. When connecting to port7 you always connect to the master device.

Correct Answer: AD
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 112
In HA, what is the effect of the Disconnect Cluster Member command as given in the Exhibit.



Serial Number FGVM010000006268

Interface port3

IP/Netmask 10.0.1.251/24

A. The HA mode changes to standalone.

B. Port3 is configured with an IP address for management access.
C. The Firewall rules are purged on the disconnected unit.
D. All other interface IP settings are maintained.

Correct Answer: AB
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 113
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: Volume B
Explanation

Explanation/Reference:

QUESTION 114
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: Volume B
Explanation

Explanation/Reference:

QUESTION 115

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.)

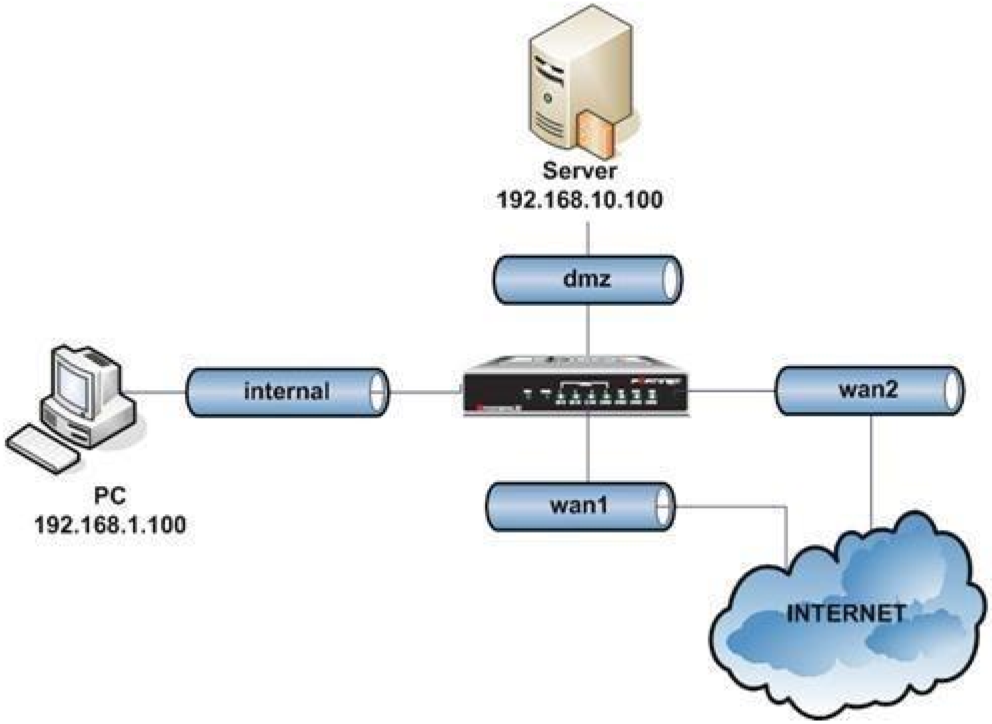
A. Create one firewall policy.
B. Create two firewall policies.
C. Add a route for the remote subnet.
D. Add a route for incoming traffic.
E. Create a phase 1 definition.
F. Create a phase 2 definition.

Correct Answer: BCEF
Section: Volume B
Explanation

Explanation/Reference:
It's appropriated.

QUESTION 116

An intermittent connectivity issue is noticed between two devices located behind the FortiGate dmz and internal interfaces. A continuous sniffer trace is run on the FortiGate unit that the administrator will convert into a .cap file for an off-line analysis with a sniffer application.



Given the high volume of global traffic on the network, which of the following CLI commands will best allow the administrator to perform this troubleshooting operation?

A. diagnose sniffer packet any
B. diagnose sniffer packet dmz "" 3
C. diagnose sniffer packet any "host 192.168.1.100 and host 192.168.10.100 " 3
D. diagnose sniffer packet any "host 192.168.1.100 and host 192.168.10.100 " 4

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 117
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: Volume B
Explanation

Explanation/Reference:

QUESTION 118
An administrator configures a VPN and selects the Enable IPSec Interface Mode option in the phase 1 settings.

Which of the following statements are correct regarding the IPSec VPN configuration?

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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 119
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: Volume B
Explanation

Explanation/Reference: