Vendor: Fortinet

Exam Code: FCNSP.v5

Exam Name: Fortinet Certified Network Security Professional (FCNSP.v5)

Version: Demo

QUESTION 1
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

QUESTION 2
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

QUESTION 3
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

QUESTION 4
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

QUESTION 5
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

QUESTION 6
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

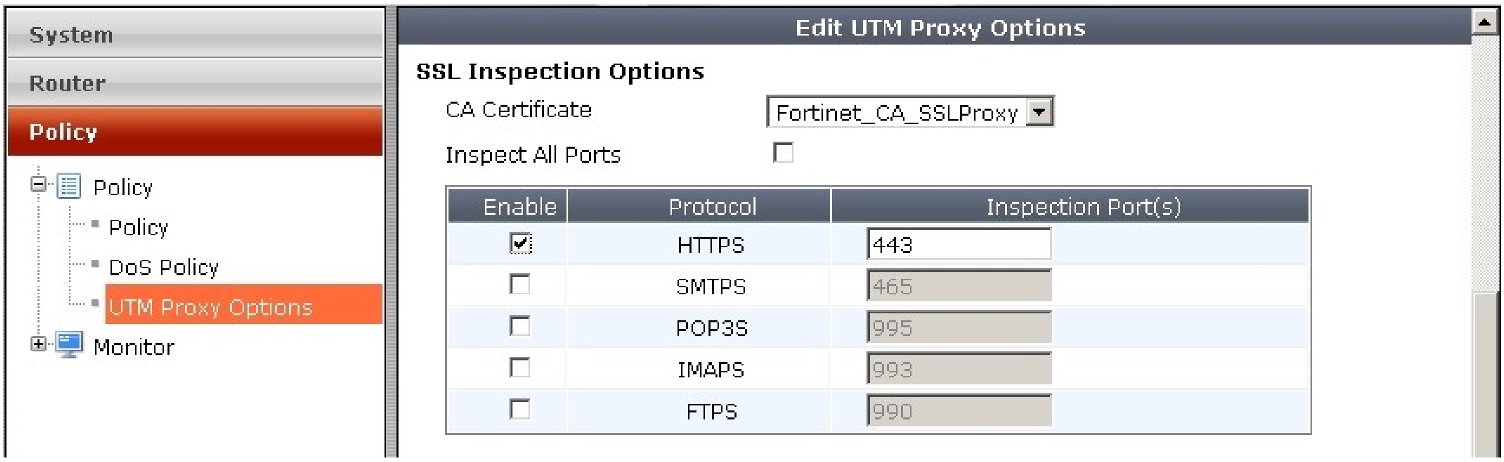
Correct Answer: CDE

QUESTION 7
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

QUESTION 8
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

QUESTION 9
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

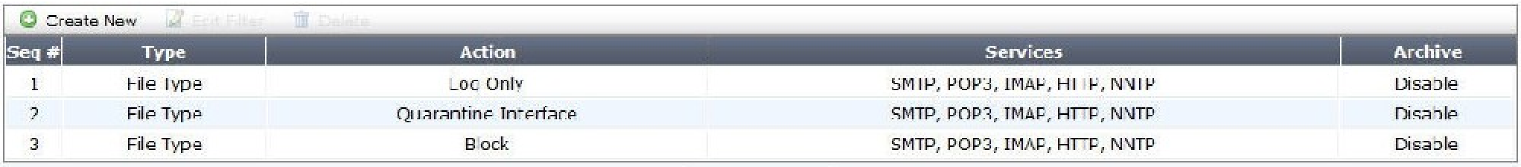
QUESTION 10
How can DLP file filters be configured to detect Office 2010 files? (Select all that apply.)

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

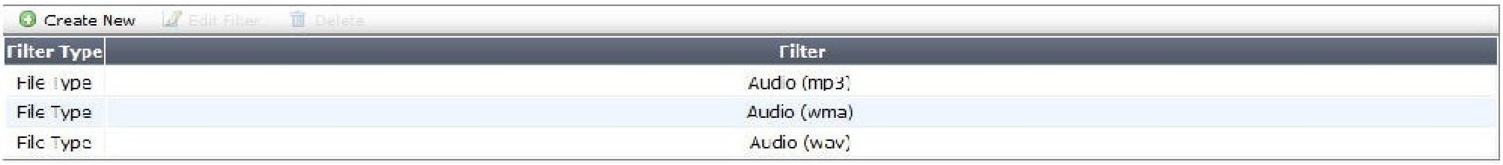
QUESTION 11
Examine the Exhibits shown below, then answer the question that follows.

Review the following DLP Sensor (Exhibit 1):



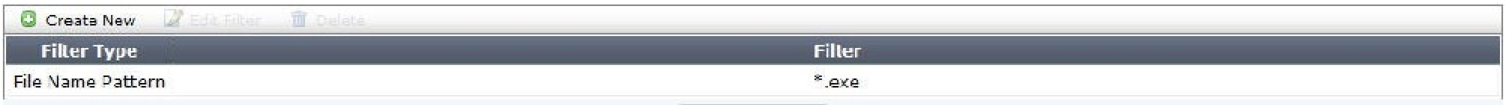
Seq #	Type	Action	Services	Archive
1	File Type	Log Only	SMTP, POP3, IMAP, HTTP, NNTP	Disable
2	File Type	Quarantine Interface	SMTP, POP3, IMAP, HTTP, NNTP	Disable
3	File Type	Block	SMTP, POP3, IMAP, HTTP, NNTP	Disable

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



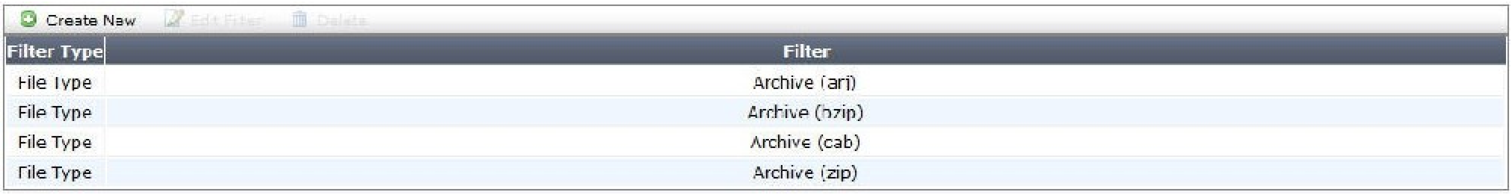
Filter Type	Filter
File Type	Audio (mp3)
File Type	Audio (wma)
File Type	Audio (wav)

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?

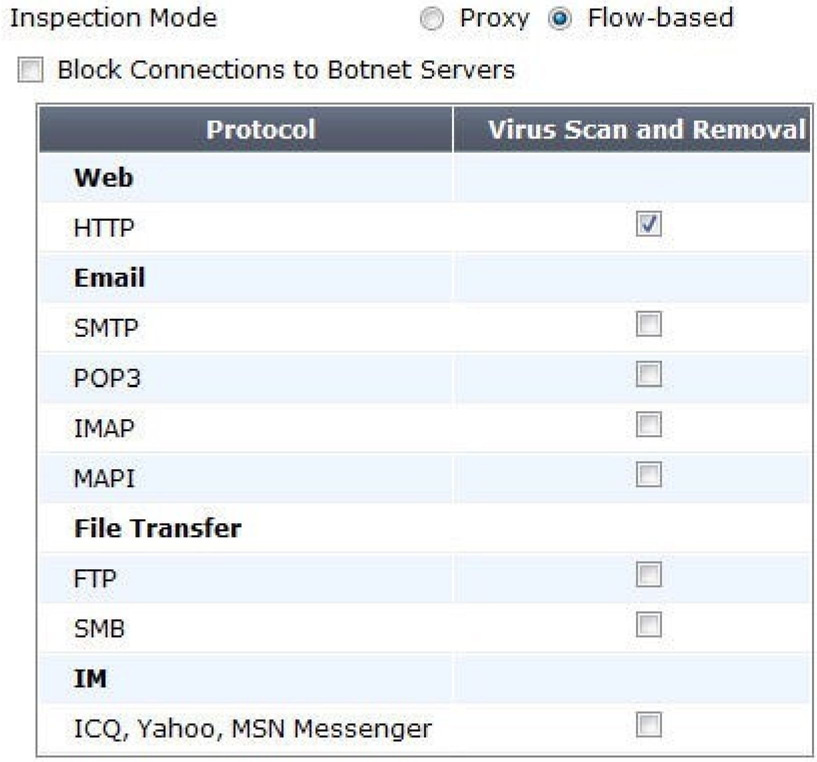
A. The file will be detected by rule #1 as an `Audio (mp3)', a log entry will be created and it will be allowed to pass through.
B. The file will be detected by rule #2 as a "*.exe", a log entry will be created and the interface that received the traffic will be brought down.
C. The file will be detected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

QUESTION 12

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:

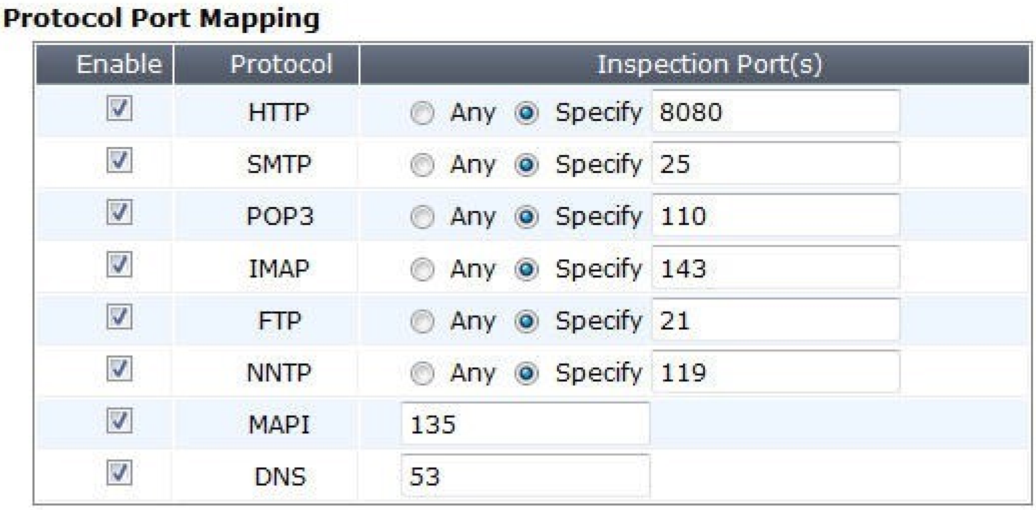


Inspection Mode ○ Proxy ● Flow-based

□ 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	□

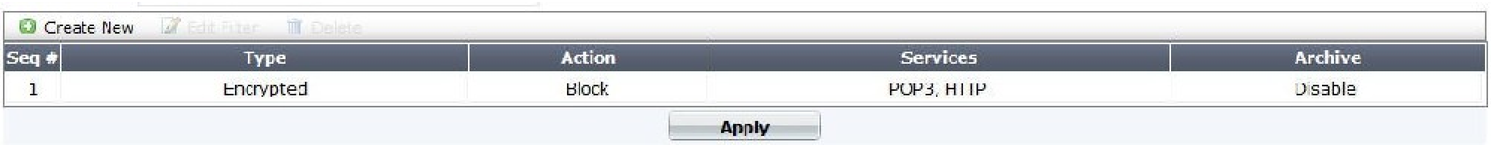
Exhibit B Non-default UTM Proxy Options Profile:



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

QUESTION 13
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

QUESTION 14
What are the requirements for a cluster to maintain TCP connections after device or link failover? (Select all that apply.)

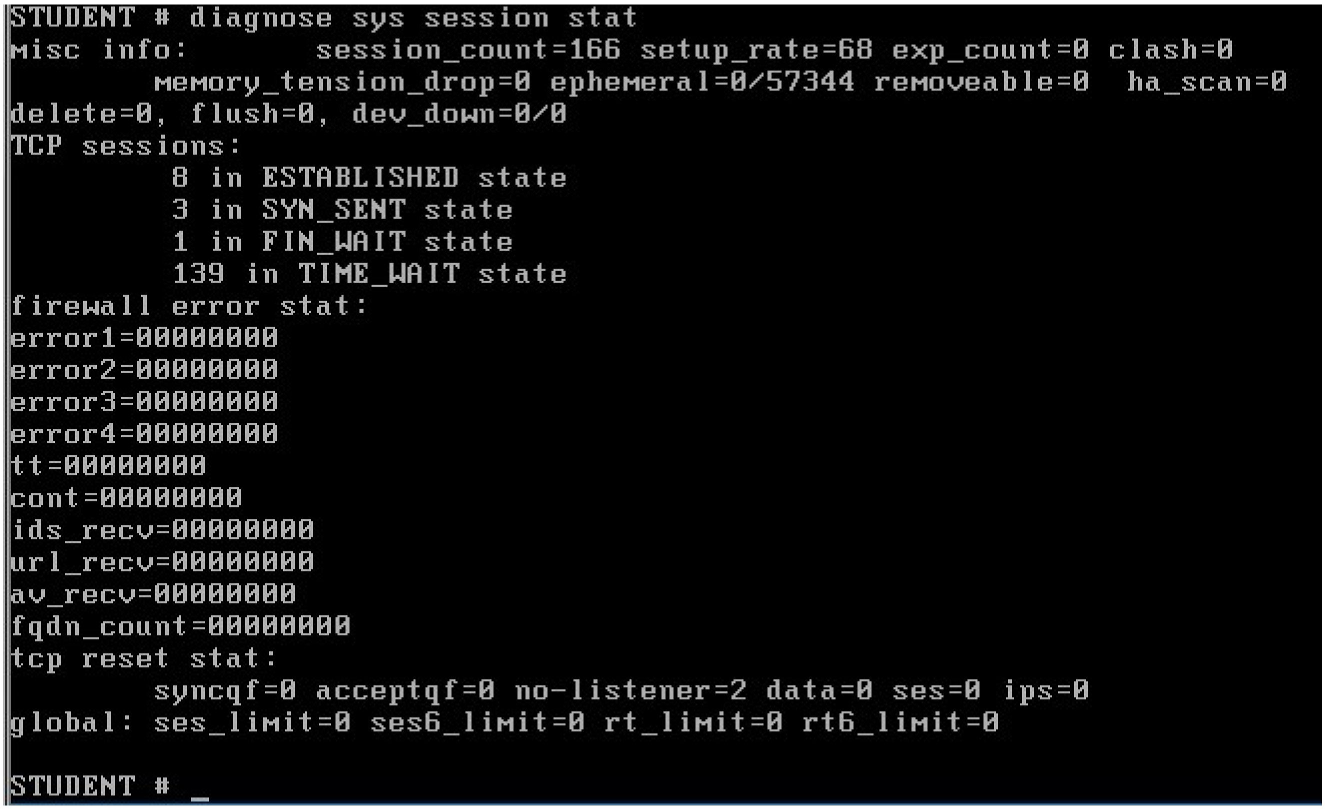
A. Enable session pick-up.

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

QUESTION 15
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.

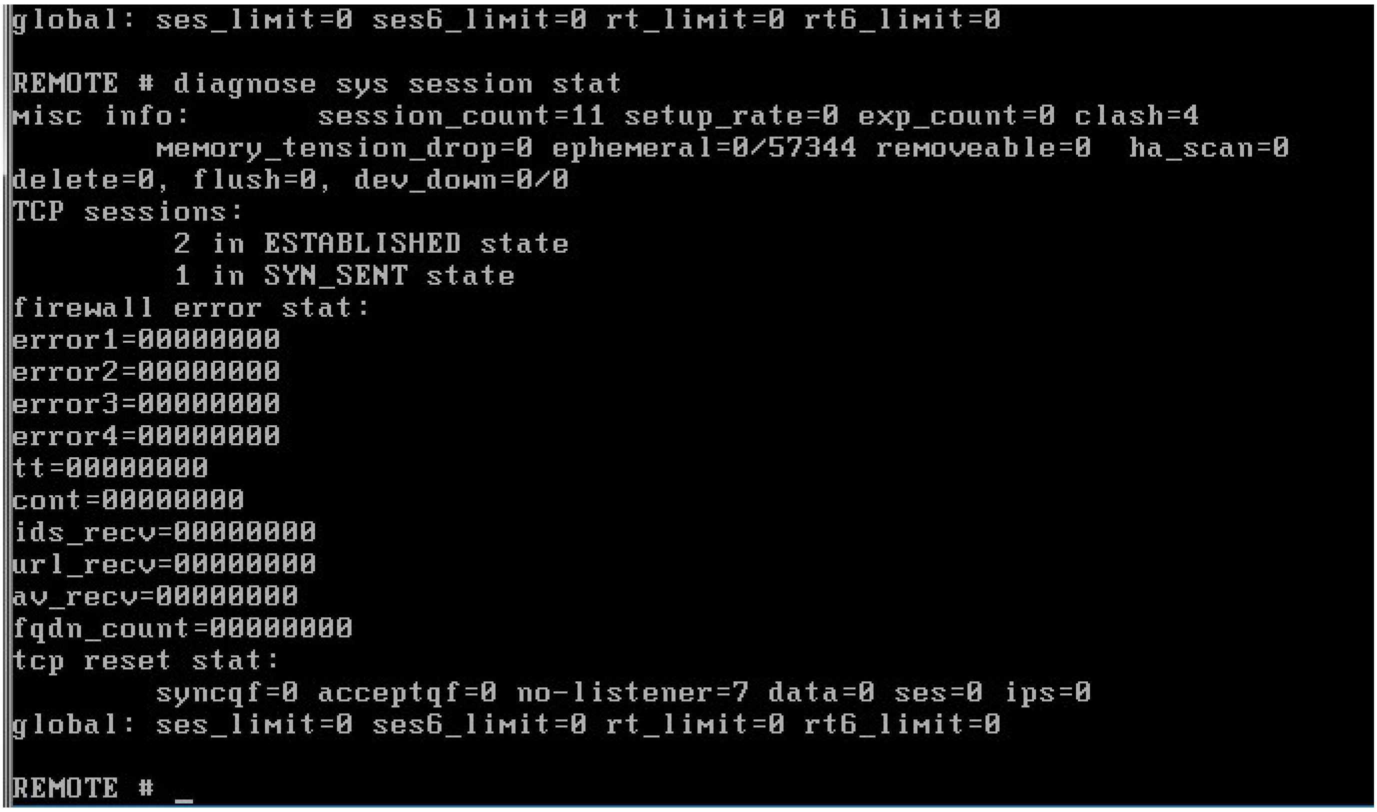
Exhibit A:



```
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.

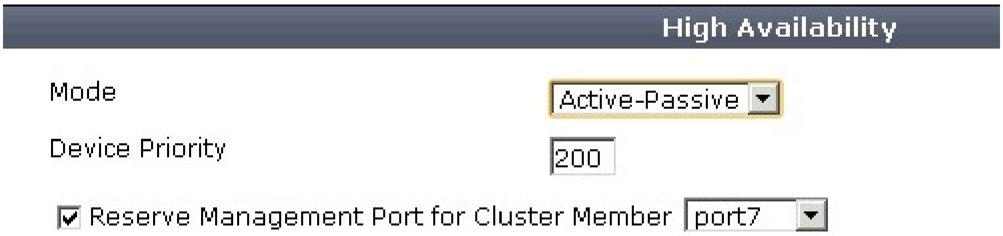
Correct Answer: AD

QUESTION 16
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

QUESTION 17
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the Exhibit below.



High Availability

Mode: Active-Passive

Device Priority: 200

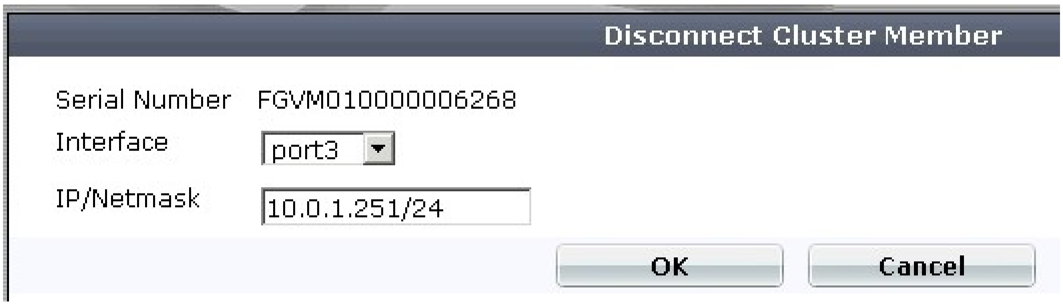
☑ Reserve Management Port for Cluster Member: port7

Which 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

QUESTION 18
In HA, what is the effect of the Disconnect Cluster Member command as given in the Exhibit.



Disconnect Cluster Member

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

QUESTION 19
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: