FCNSP.V5$^{Q\&As}$

Fortinet Certified Network Security Professional (FCNSP.v5)

QUESTION 1

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

QUESTION 2

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

QUESTION 3

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

QUESTION 4

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.

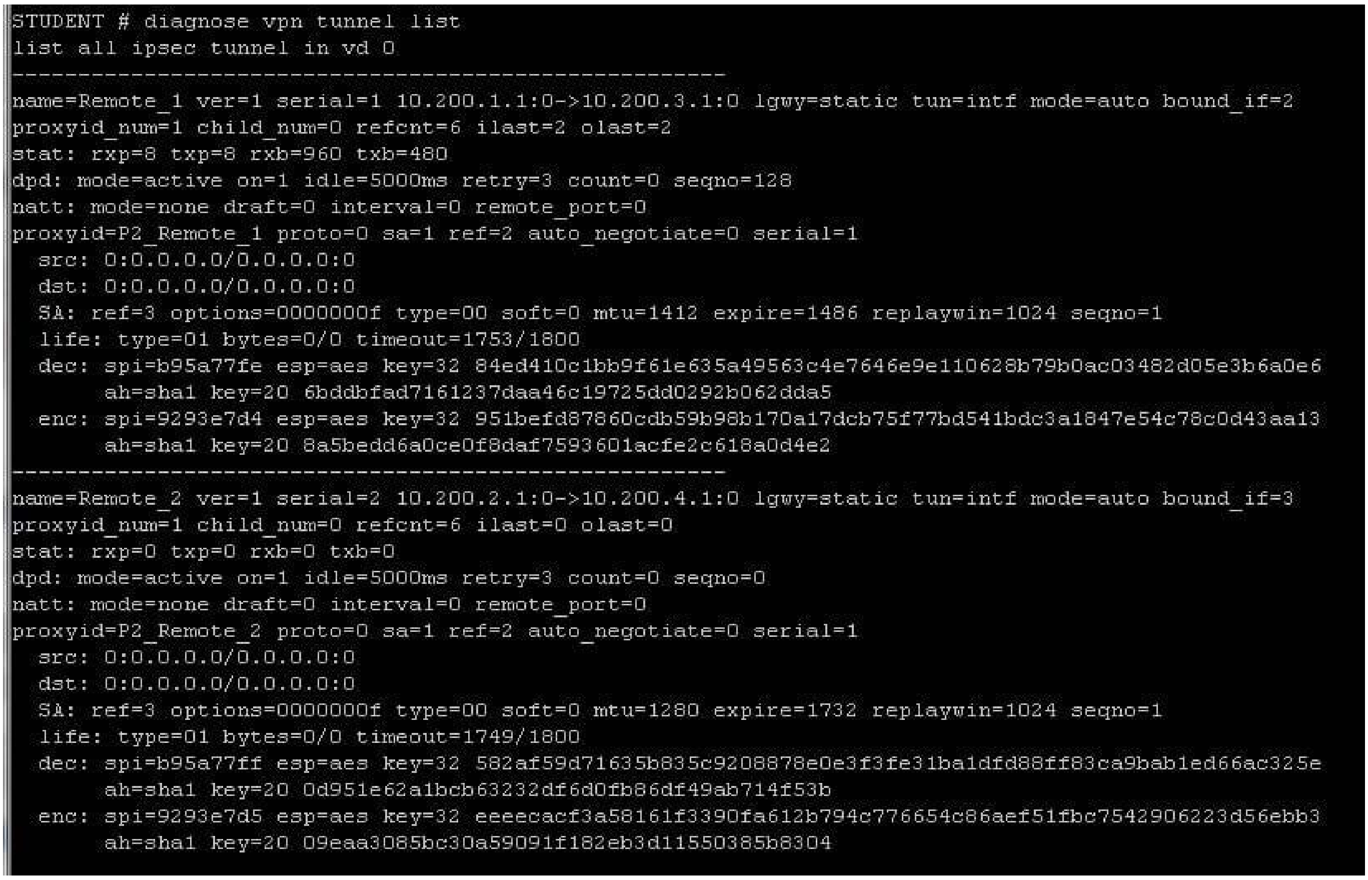
C. The traffic matching the DLP rule will bypass antivirus scanning.

D. The client IP address will be added to a white list.

Correct Answer: A

QUESTION 5

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 eeeecacf3a58161f3390fa612b794c776654c86aef51fbc754290 6223d56ebb3
       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

QUESTION 6

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

QUESTION 7

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.

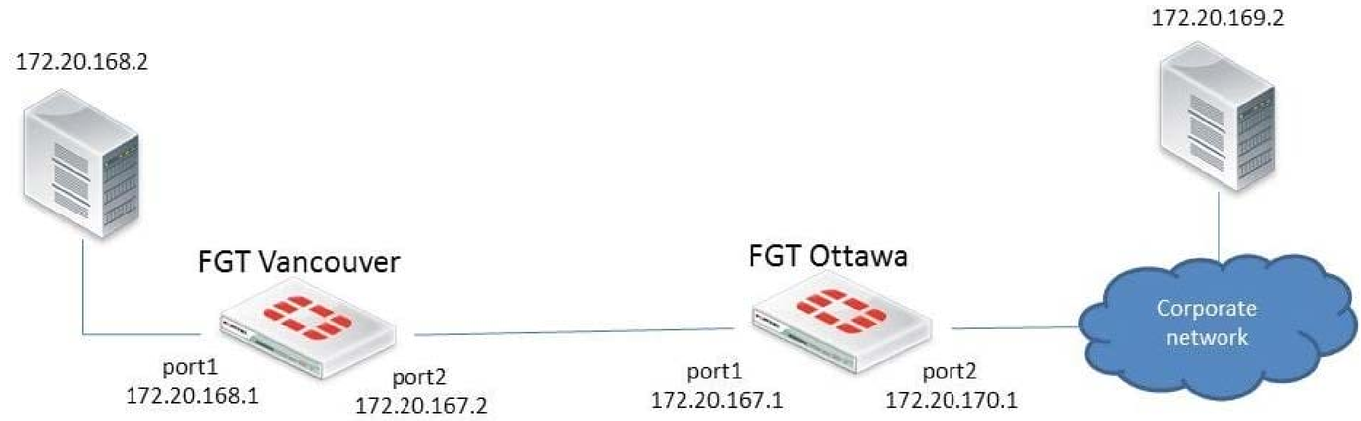
C. NAC quarantine allows administrators to isolate clients whose network activity poses a security risk.

D. If you chose the quarantine action, you must decide whether the quarantine type is NAC quarantine or File quarantine.

Correct Answer: C

QUESTION 8

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.

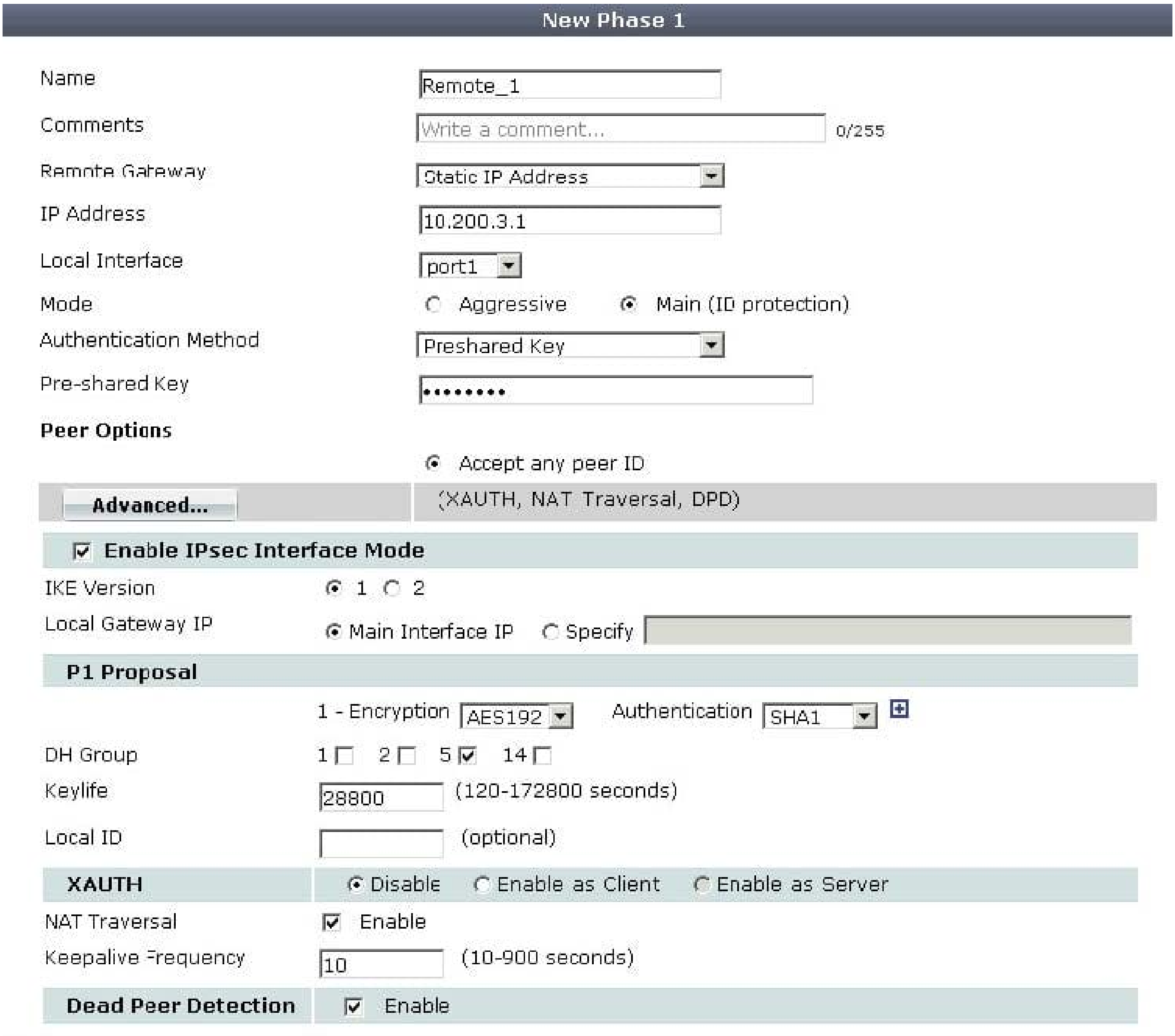
C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate unit\\'s routing table.

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

QUESTION 9

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

QUESTION 10

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.

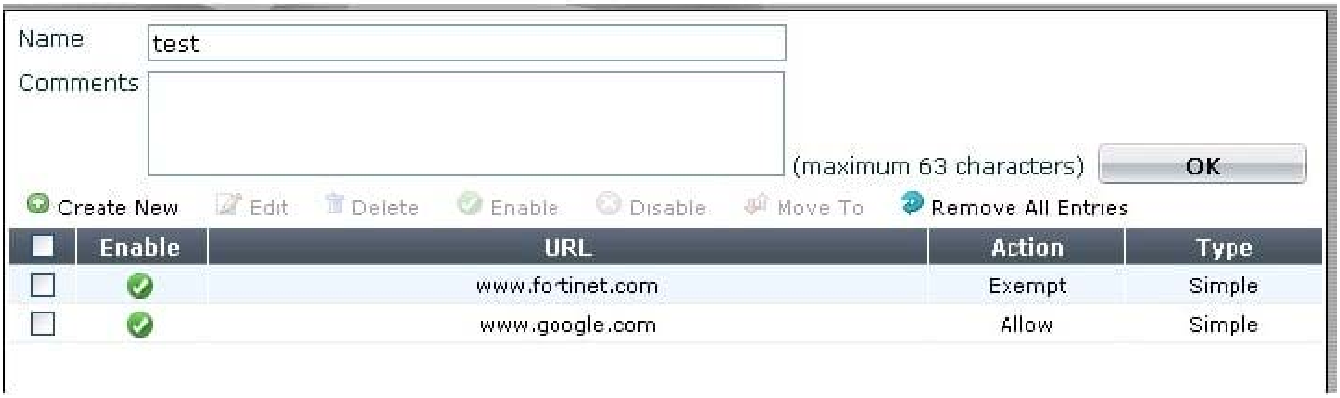
D. The dmz interface is in PPPoE or DHCP mode.

E. Reassigning an interface to a different VDOM can only be done through the CLI.

Correct Answer: A

QUESTION 11

Based on the web filtering configuration illustrated in the exhibit,



Name: test

Comments:

□	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

QUESTION 12

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 13

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

QUESTION 14

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

QUESTION 15

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