Fortinet

Exam NSE4

Fortinet Network Security Expert 4 Written Exam (400)

Version: 10.0

[Total Questions: 274]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	43
Topic 2: Volume B	77
Topic 3: Volume C	154

Topic 1, Volume A

Question No : 1 - (Topic 1)

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.

Answer: A,C

Question No : 2 - (Topic 1)

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.

Answer: A,D

Question No : 3 - (Topic 1)

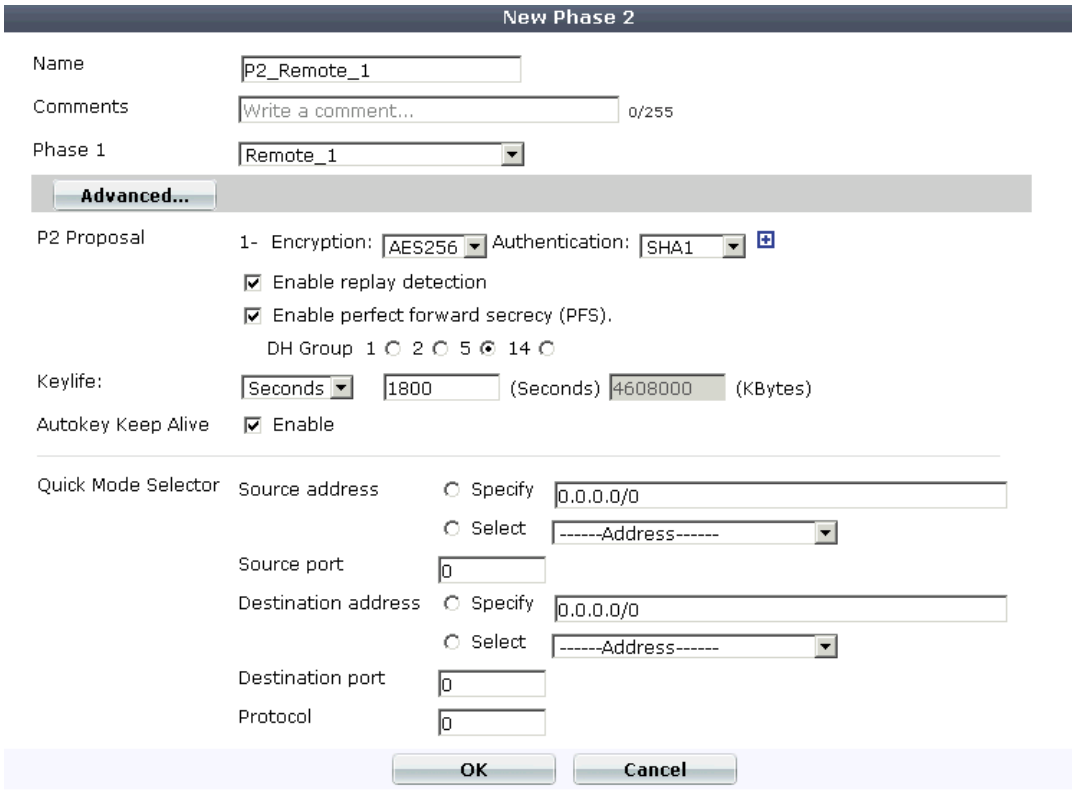
For Data Leak Prevention, which of the following describes the difference between the block and quarantine actions?

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.

Answer: A

Question No : 4 - (Topic 1)

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



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.

Answer: A,B

Question No : 5 - (Topic 1)

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.

Answer: A,C

Question No : 6 - (Topic 1)

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 No : 7 - (Topic 1)

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
------------------------------------------------------
```

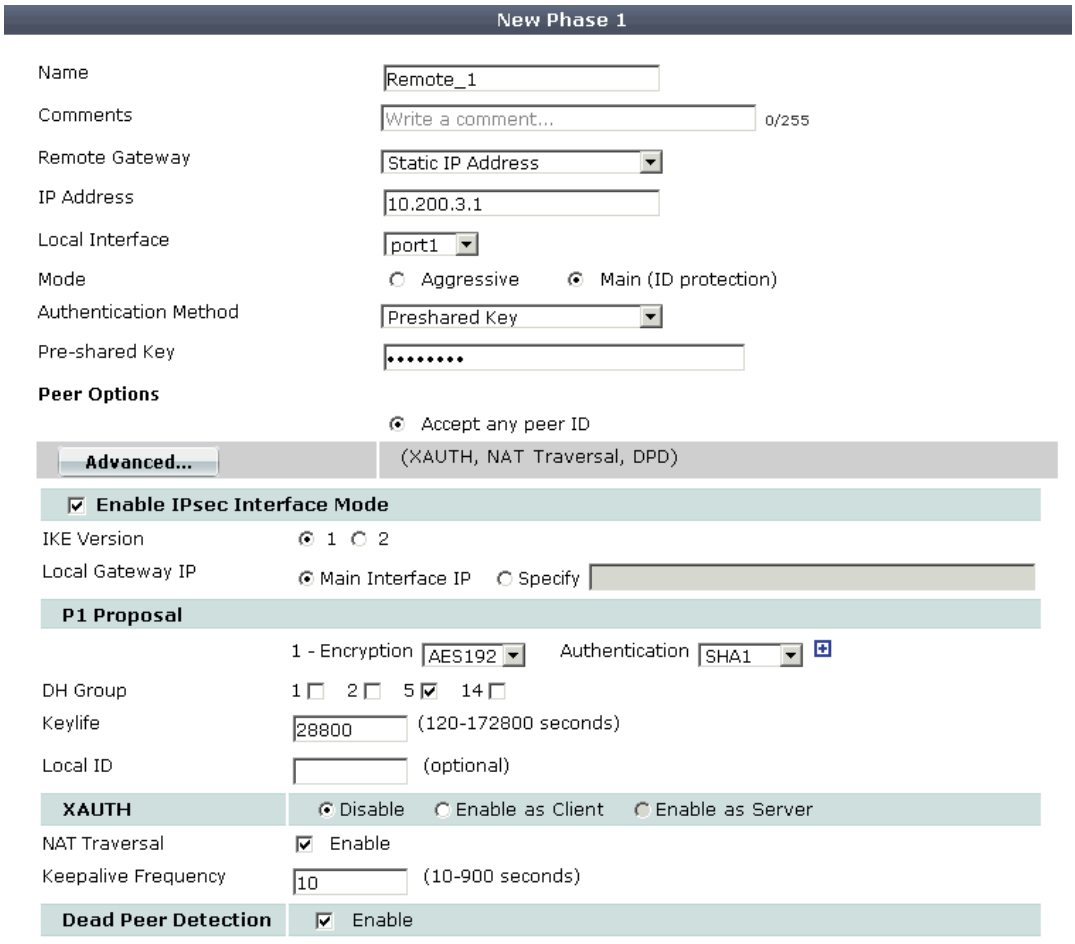
Which of the following statements are correct regarding this output? (Select all that apply.)

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.

Answer: A,B

Question No : 8 - (Topic 1)

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



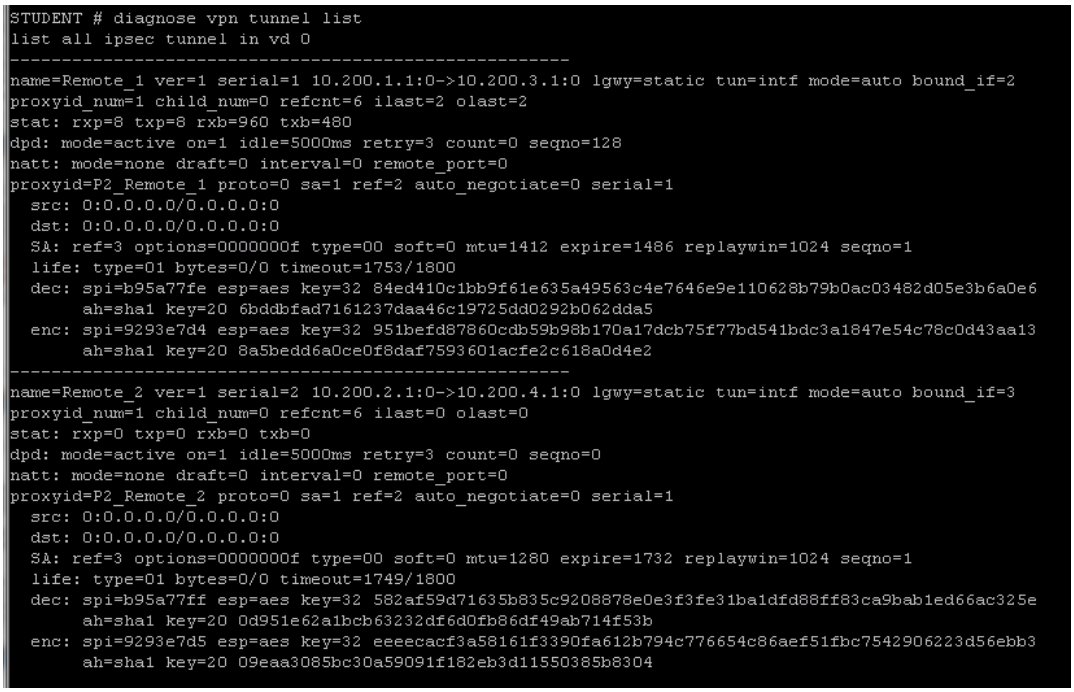
Which of the following statements are correct regarding this configuration? (Select all that apply).

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.

Answer: A,C

Question No : 9 - (Topic 1)

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

Answer: C

Question No : 10 - (Topic 1)

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.

Answer: B,D

Question No : 11 - (Topic 1)

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.

Answer: B,D

Question No : 12 - (Topic 1)

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.

Answer: B

Question No : 13 - (Topic 1)

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.

Answer: A,B,C,D

Question No : 14 - (Topic 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"

Answer: B,E

Question No : 15 - (Topic 1)

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