Vendor: Fortinet

Exam Code: FCNSP

Exam Name: Fortinet Certified Network Security Professional

Version: DEMO

QUESTION 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: AD

QUESTION 2
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.

Answer: AD

QUESTION 3
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.

Answer: AD

QUESTION 4
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the Exhibit below.

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.

Answer: AD

QUESTION 5
Review the IPsec diagnostics output of the command diag vpn tunnel list shown in the Exhibit below.

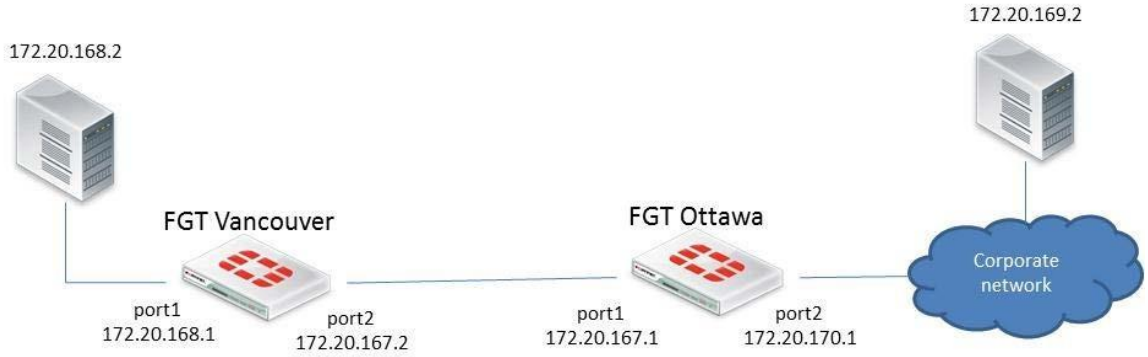
```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=FClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_inst bound_if=2
parent=FClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 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: AB

QUESTION 6
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.

Answer: B

QUESTION 7
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.

Answer: C

QUESTION 8
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.

Answer: B

QUESTION 9
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: AC

QUESTION 10
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