Vendor: Fortinet

Exam Code:NSE7_EFW

Exam Name:NSE7 Enterprise Firewall - FortiOS 5.4

Version: Demo

QUESTION 1

View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7....

ike 0: IKEv1 exchange=Aggressive id=baf47d0988e9237f/2f405ef3952f6fda len=430

ike 0: in

BAF47D0988E9237F2F405EF3952F6FDA0110040000000000000001AE0400003C000000010000000100

0000300101000

ike 0:RemoteSite:4: initiator: aggressive mode get 1st response... ike 0:RemoteSite:4: VID RFC 3947 4A131c81070358455C5728F20E95452F ike 0:RemoteSite:4: VID DPD AFCAD71368A1F1C96B8696FC77570100

ike 0:RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7

ike 0:RemoteSite:4: peer is FortiGate/Fortios (v5 b727)

ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3

ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000

ike 0:RemoteSite:4: received peer identifier FQDN `remore\\'

ike 0:RemoteSite:4: negotiation result

ike 0:RemoteSite:4: proposal id = 1:

ike 0:RemoteSite:4: protocol id = ISAKMP:

ike 0:RemoteSite:4: trans_id = KEY_IKE.

ike 0:RemoteSite:4: encapsulation = IKE/none

ike 0:RemoteSite:4: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key ?en=128 ike 0:RemoteSite:4:

type=OAKLEY_HASH_ALG, val=SHA.

ike 0:RemoteSite:4: type-AUTH_METHOD, val=PRESHARED_KEY.

ike 0:RemoteSite:4: type=OAKLEY_GROUP, val=MODP1024.

ike 0:RemoteSite:4: ISAKMP SA lifetime=86400

ike 0:RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key 16:

B25B6C9384D8BDB24E3DA3DC90CF5E73

ike 0:RemoteSite:4: PSK authentication succeeded

ike 0:RemoteSite:4: authentication OK

ike 0:RemoteSite:4: add INITIAL-CONTACT

ike 0:RemoteSite:4: enc

BAF47D0988E9237F405EF3952F6FDA08100401000000000000000080140000181F2E48BFD8E9D603F

ike 0:RemoteSite:4: out
BAF47D0988E9237F405EF3952F6FDA08100401000000000000000008C2E3FC9BA061816A396F009A12 ike 0:RemoteSite:4: sent IKE msg (agg_i2send): 10.0.0.1:500-10.0.0.2:500, len=140,

id=baf47d0988e9237f/2 ike 0:RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda Which statements about this debug output are correct? (Choose two.)

A. The remote gateway IP address is 10.0.0.1.

B. It shows a phase 1 negotiation.

C. The negotiation is using AES128 encryption with CBC hash.

D. The initiator has provided remote as its IPsec peer ID.

Correct Answer: BD

QUESTION 2

A FortiGate\\'s portl is connected to a private network. Its port2 is connected to the Internet. Explicit web proxy is enabled in port1 and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP. Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)

A. Both session have the local flag on.

B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate\\'s interfaces.

C. One session has the proxy flag on, the other one does not.

D. One of the sessions has the IP address of port2 as the source IP address.

Correct Answer: AD

QUESTION 3

Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

A. The next-hop IP address is up.

B. There is no other route, to the same destination, with a higher distance.

C. The link health monitor (if configured) is up.

D. The next-hop IP address belongs to one of the outgoing interface subnets.

E. The outgoing interface is up.

Correct Answer: ABE

QUESTION 4

View the exhibit, which contains the output of a diagnose command, and the answer the question below.

```
# diagnose debug rating
Locale       : English
License      : Contract
Expiration   : Thu Sep 28 17:00:00 20XX
-=- Server List (Thu APR 19 10:41:32 20XX) -=-
IP               Weight   RTT   Flags   TZ   Packets  Curr Lost  Total Lost
64.26.151.37     10       45            -5    262432  0           846
64.26.151.35     10       46            -5    329072  0           6806
66.117.56.37     10       75            -5    71638   0           275
66.210.95.240    20       71            -8    36875   0           92
209.222.147.36   20       103    DI     -8    34784   0           1070
208.91.112.194   20       107    D      -8    35170   0           1533
96.45.33.65      60       144           0     33728   0           120
80.85.69.41      71       226           1     33797   0           192
62.209.40.74     150      97            9     33754   0           145
121.111.236.179  45       44     F      -5    26410   26226       26227
```

Which statements are true regarding the Weight value?

A. Its initial value is calculated based on the round trip delay (RTT).

B. Its initial value is statically set to 10.

C. Its value is incremented with each packet lost.

D. It determines which FortiGuard server is used for license validation.

Correct Answer: C

QUESTION 5

Four FortiGate devices configured for OSPF connected to the same broadcast domain. The first unit is elected as the designated router The second unit is elected as the backup designated router Under normal operation, how many OSPF full adjacencies are formed to each of the other two units?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B

QUESTION 6

View the central management configuration shown in the exhibit, and then answer the question below.

```
Config system central-management
   set type forimanager
   set fmg "10.0.1.242"
   config server-list
      edit 1
         set server-type rating
         set server-address 10.0.1.240
      next
      edit 2
          set server-type update
          set server-address 10.0.1.243
      next
      edit 3
          set server-type rating
          set server-address 10.0.1.244
      next
     end
     set include-default-servers enable
end
```

Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

A. 10.0.1.240

B. One of the public FortiGuard distribution servers

C. 10.0.1.244

D. 10.0.1.242

Correct Answer: B

QUESTION 7

A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the `diagnose debug authd fsso list\\' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

A. The user student must not be listed in the CA\\'s ignore user list.

B. The user student must belong to one or more of the monitored user groups.

C. The student workstation\\'s IP subnet must be listed in the CA\\'s trusted list.

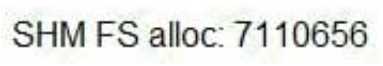
D. At least one of the student\\'s user groups must be allowed by a FortiGate firewall policy.

Correct Answer: BD

QUESTION 8

Examine the following partial output from two system debug commands; then answer the question below.

```
# diagnose hardware sysinfo memory
MemTotal: 3092728 kB
MemFree: 1954204 kB
MemShared: 0 kB
Buffers: 284 kB
Cached: 143004 kB
SwapCached: 0 kB
Active: 34092 kB
Inactive: 109256 kB
HighTotal: 117948 kB
HighFree: 853516 kB
LowTotal: 1913080 kB
LowFree: 1100688 kB
SwapTotal: 0 kB
SwapFree: 0 kB
# diagnose hardware sysinfo shm
SHM counter: 285
SHM allocated: 6823936
SHM total: 623452160
concervemode: 0
shm last entered: n/a
SHM FS total: 639725568
SHM FS free: 632614912
```



Which of the following statements are true regarding the above outputs? (Choose two.)

A. The unit is running a 32-bit FortiOS

B. The unit is in kernel conserve mode

C. The Cached value is always the Active value plus the Inactive value

D. Kernel indirectly accesses the low memory (LowTotal) through memory paging

Correct Answer: AC

QUESTION 9

Which of the following tasks are automated using the Install Wizard on FortiManager? (Choose two.)

A. Preview pending configuration changes for managed devices.

B. Add devices to FortiManager.

C. Import policy packages from managed devices.

D. Install configuration changes to managed devices.

E. Import interface mappings from managed devices.

Correct Answer: BD

QUESTION 10

What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

A. A process crash.

B. Configuration changes.

C. Changes in the status of any of the FortiGuard licenses.

D. System entering to and leaving from the proxy conserve mode.

Correct Answer: AD

QUESTION 11

Examine the output of the `diagnose ips anomaly list\\' command shown in the exhibit; then answer the question below.

```
# diagnose ips anomaly list

list nids meter:
id=ip_dst_session      ip=192.168.1.10     dos_id=2    exp=3646    pps=0    freq=0
id=udp_dst_session     ip=192.168.1.10     dos_id=2    exp=3646    pps=0    freq=0
id=udp_scan            ip=192.168.1.110    dos_id=1    exp=649     pps=0    freq=0
id=udp_flood           ip=192.168.1.110    dos_id=2    exp=653     pps=0    freq=0
id=tcp_src_session     ip=192.168.1.110    dos_id=1    exp=5175    pps=0    freq=8
id=tcp_port_scan       ip=192.168.1.110    dos_id=1    exp=175     pps=0    freq=0
id=ip_src_session      ip=192.168.1.110    dos_id=1    exp=5649    pps=0    freq=30
id=udp_src_session     ip=192.168.1.110    dos_id=1    exp=5649    pps=0    freq=22
```

Which IP addresses are included in the output of this command?

A. Those whose traffic matches a DoS policy.

B. Those whose traffic matches an IPS sensor.

C. Those whose traffic exceeded a threshold of a matching DoS policy.

D. Those whose traffic was detected as an anomaly by an IPS sensor.

Correct Answer: A

QUESTION 12

A FortiGate has two default routes:

```
config router static
   edit 1
     set gateway 10.200.1.254
     set priority 5
     set device "port1"
   next
   edit 2
     set gateway 10.200.2.254
     set priority 10
     set device "port2"
   next
end
```

All Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:

```
# diagnose sys session list
Session info: proto=6 proto_state=01 duration=17 expire7 timeout=3600
flags= 00000000 sockflag=00000000 sockport=0 av idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic (bytes/packets/allow_err): org=575/7/1 reply=23367/19/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907-
>54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80-
>10.200.1.1:67907(10.0.1.10:64907)
pos/(before, after) 0/(0,0),0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

A. Session would remain in the session table and its traffic would keep using port1 as the outgoing interface.

B. Session would remain in the session table and its traffic would start using port2 as the outgoing interface.

C. Session would be deleted, so the client would need to start a new session.

D. Session would remain in the session table and its traffic would be shared between port1 and port2.

Correct Answer: A