# Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

**https://www.2passeasy.com/dumps/NSE7_EFW-7.0/**

**NEW QUESTION 1**
When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filter web requests when the client browser does not provide the server name indication (SNI) extension?

A. FortiGate uses the requested URL from the user's web browser.
B. FortiGate uses the CN information from the Subject field in the server certificate.
C. FortiGate blocks the request without any further inspection.
D. FortiGate switches to the full SSL inspection method to decrypt the data.

**Answer:** B

**NEW QUESTION 2**
Refer to the exhibit, which shows the output of a debug command.

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
     Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
     Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
     Transmit Delay is 1 sec, State DROther, Priority 1
     Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
     Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
     Timer inervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
          Hello due in 00:00:05
     Neighbor Count is 4, Adjacent neighbor count is 2
     Crypt Sequence Number is 411
     Hello received 106 send 27, DD received 6 sent 3
     LS-Req received 2 sent 2, LS-Upd received 7 sent 17
     LS-Ack received 4 sent 3, Discarded 1
```

Which two statements about the output are true? (Choose two.)

A. The local FortiGate OSPF router ID is 0.0.0.4.
B. Port4 is connected to the OSPF backbone area.
C. In the network connected to port4, two OSPF routers are down.
D. The local FortiGate is the backup designated router.

**Answer:** AB

**Explanation:**
Area 0.0.0.0 is the backbone area.

**NEW QUESTION 3**
Refer to the exhibit, which contains partial outputs from two routing debug commands.

```
FortiGate # get router into routing-table database

S    0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S  *>0.0.0.0/0 [10/0] via 100.64.1.254, port1

FortiGate # get router info routing-table all

S*   0.0.0.0/0 [10/0] via 100.64.1.254, port1
```

Why is the port2 default route not in the second command's output?

A. It has a higher priority value than the default route using port1.
B. It is disabled in the FortiGate configuration.
C. It has a lower priority value than the default route using port1.
D. It has a higher distance than the default route using port1.

**Answer:** D

**NEW QUESTION 4**
Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

A. FortiGate limits the number of simultaneous sessions per explicit web proxy use
B. This limit CANNOT be modified by the administrator.
C. FortiGate limits the total number of simultaneous explicit web proxy users.
D. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator
E. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials.This limit CANNOT be modified by the administrator.

**Answer:** B

**Explanation:**
https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-WAN-opt-52/web_proxy.htm#Explicit2
The explicit proxy does not limit the number of active sessions for each user. As a result the actual explicit proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.

**NEW QUESTION 5**
Refer to the exhibit, which contains the output of get system ha status. Which two statements about the output are true? (Choose two.)

```
NGFW-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 2
Debug: 0
Cluster Uptime: 0 days 4:23:19
Cluster state change time: 2019-01-25 10:19:46
Master selected using:
  <2019/01/25 10:19:46> FGVM010000077649 is selected as the master because it has the largest value
of override priority.
  <2019/01/25 10:19:40> FGVM010000077649 is selected as the master because it's the only member in
the cluster.
ses_pickup: disable
override: enable
Configuration Status:
     FGVM010000077649 (updated 1 seconds ago): in-sync
     FGVM010000077650 (updated 0 seconds ago): out-of-sync
System Usage stats:
     FGVM010000077649 (updated 1 seconds ago):
          sessions=27, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=56%
     FGVM010000077650 (updated 0 seconds ago):
          sessions=2, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=57%
HBDEV stats:
     FGVM010000077649 (updated 1 seconds ago):
          port7: physical/10000full, up, rx-bytes/packets/dropped/errors=63817615/202024/0/0, tx=
71110281/121109/0/0
     FGVM010000077650 (updated 0 seconds ago):
          port7: physical/10000full, up, rx-bytes/packets/dropped/errors=79469596/122024/0/0, tx=
30877890/107878/0/0
Master: NGFW-1     , FGVM010000077649, cluster index = 1
Slave : NGFW-2     , FGVM010000077650, cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master: FGVM010000077649, operating cluster index = 0
Slave : FGVM010000077650, operating cluster index = 1
```

A. The slave configuration is synchronized with the master.
B. port7 is used as the HA heartbeat on all devices in the cluster.
C. Primary is selected based on the priority configured under config system ha.
D. The HA management IP is 169.254.0.2.

**Answer:** BC

**NEW QUESTION 6**
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.

**Answer:** AD

**Explanation:**
diagnose debug crashlog read
275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated276: 2014-08-05
13:03:53 proxy=acceptor service=ftp session fail mode=activated277: 2014-08-05 13:03:53 proxy=acceptor service=nntp session fail mode=activated278:
2014-08-06 11:05:47 service=kernel conserve=on free="45034 pages" red="45874 pages" msg="Kernel279: 2014-08-06 11:05:47 enters conserve mode"280:
2014-08-06 13:07:16 service=kernel conserve=exit free="86704 pages" green="68811 pages"281: 2014-08-06 13:07:16 msg="Kernel leaves conserve
mode"282: 2014-08-06
13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201283: 2014-08-06 13:07:16 marginexit=302

**NEW QUESTION 7**
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
   Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
   Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DROther, Priority 1
   Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:05
   Neighbor Count is 4, Adjacent neighbor count is 2
   Crypt Sequence Number is 411
   Hello received 106, sent 27, DD received 7 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

Which of the following statements about the exhibit are true? (Choose two.)

A. In the network on port4, two OSPF routers are down.
B. Port4 is connected to the OSPF backbone area.
C. The local FortiGate's OSPF router ID is 0.0.0.4
D. The local FortiGate has been elected as the OSPF backup designated router.

**Answer:** BC

**NEW QUESTION 8**
Which statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

A. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.
B. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.
C. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.
D. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

**Answer:** BD

**Explanation:**
CLI scripts can be run in three different ways:Device Database: By default, a script is executed on the device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard.
Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard.
Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don't need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

**NEW QUESTION 9**
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.

**Answer:** CDE

**Explanation:**
A configured static route only goes to routing table from routing database when all the following are met :
- The outgoing interface is up
- There is no other matching route with a lower distance
- The link health monitor (if configured) is successful
- The next-hop IP address belongs to one of the outgoing interface subnets

**NEW QUESTION 10**
A FortiGate has two default routes:

```
config router static
   edit 1
     set gateway 10.200.1.254
     set priority 5
     set device "port1"
   next
   edit2
     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 expire=7 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-
>10.200.1.1:64907(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. The session would be deleted, and the client would need to start a new session.
B. The session would remain in the session table, and its traffic would start to egress from port2.
C. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
D. The session would remain in the session table, and its traffic would still egress from port1.

**Answer:** D

**NEW QUESTION 10**
An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.
B. TCP half close.
C. TCP time wait.
D. TCP session time to live.

**Answer:** A

**Explanation:**
http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=CLI_get_Commands.58.25.html
The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACKremains in the table.
The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACKremains in the table.
The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in thetable. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.

**NEW QUESTION 14**
An administrator is running the following sniffer in a FortiGate: diagnose sniffer packet any "host 10.0.2.10" 2
What information is included in the output of the sniffer? (Choose two.)

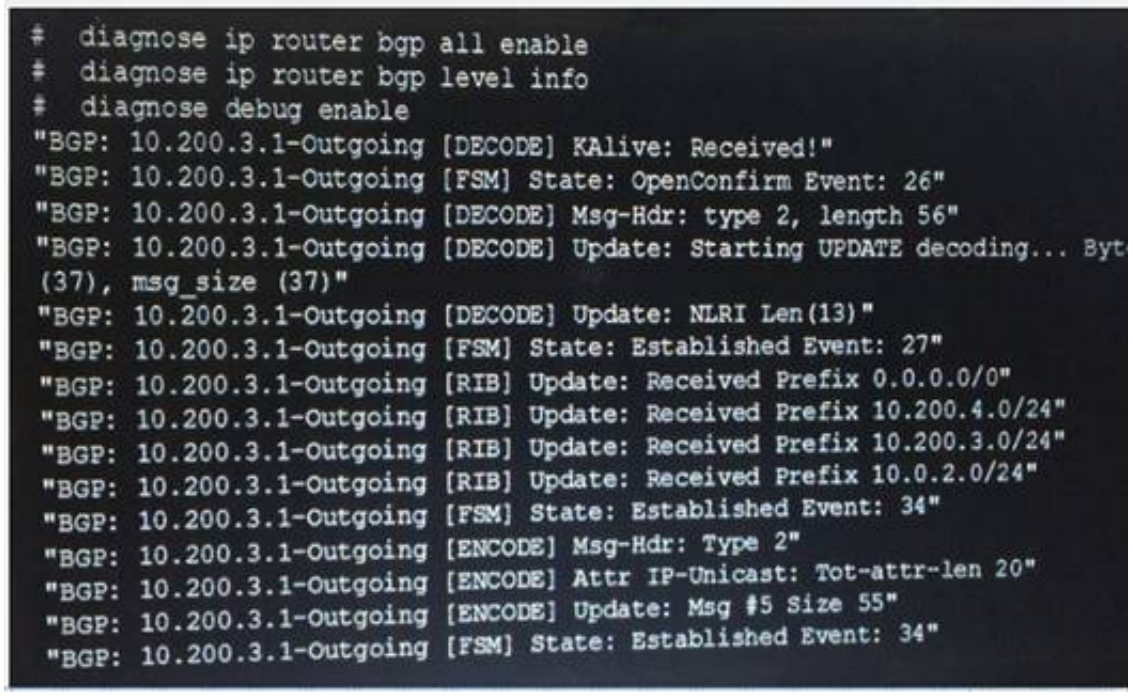
A. Ethernet headers.
B. IP payload.
C. IP headers.
D. Port names.

**Answer:** BC

**Explanation:**
https://kb.fortinet.com/kb/documentLink.do?externalID=11186

**NEW QUESTION 19**

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:




Which statements are true regarding the output in the exhibit? (Choose two.)

A. BGP peers have successfully interchanged Open and Keepalive messages.
B. Local BGP peer received a prefix for a default route.
C. The state of the remote BGP peer is OpenConfirm.
D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

**Answer:** AB

**NEW QUESTION 22**
Examine the following partial outputs from two routing debug commands; then answer the question below:

```
#get router info routing-table database
S      0.0.0.0/. [20/0] via 10.200.2.254, port2, [10/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
# get router info routing-table all
S*     0.0.0.0/0 [10/0] via 10.200.1.254, port1
```

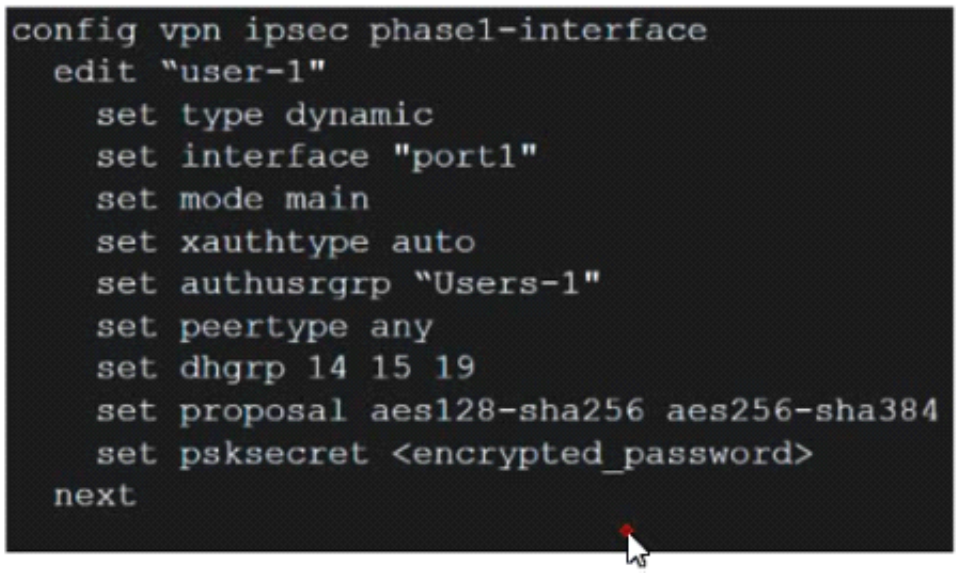
Why the default route using port2 is not displayed in the output of the second command?

A. It has a lower priority than the default route using port1.
B. It has a higher priority than the default route using port1.
C. It has a higher distance than the default route using port1.
D. It is disabled in the FortiGate configuration.

**Answer:** C

**Explanation:**
http://kb.fortinet.com/kb/viewContent.do?externalId=FD32103

**NEW QUESTION 27**
Refer to the exhibits.




Which contain the partial configurations of two VPNs on FortiGate.
An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovered that FortiGate is not matching the user-2 VPN for members of the Users-2 group.
Which two changes must administrator make to fix the issue? (Choose two.)

A. Use different pre-shared keys on both VPNs
B. Enable Mode Config on both VPNs.
C. Set up specific peer IDs on both VPNs.
D. Change to aggressive mode on both VPNs.

**Answer:** CD

**NEW QUESTION 29**
A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

A. Firewall monitor.
B. Policy monitor.
C. Logs.
D. Crashlogs.

**Answer:** CD

**NEW QUESTION 31**
Examine the following partial output from a sniffer command; then answer the question below.

```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
.....
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

What is the meaning of the packets dropped counter at the end of the sniffer?

A. Number of packets that didn't match the sniffer filter.
B. Number of total packets dropped by the FortiGate.
C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.
D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

**Answer:** D

**Explanation:**
https://kb.fortinet.com/kb/documentLink.do?externalID=11655

**NEW QUESTION 32**
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# diagnose hardware sysinfo conserve
memory conserve mode:                on
total RAM:                           3040 MB
memory used:                         2706 MB 89% of total RAM
Memory freeable:                      334 MB 11% of total RAM
memory used + freeable threshold extreme:    2887 MB 95% of total RAM
memory used threshold red:           2675 MB 88% of total RAM
memory used threshold green:         2492 MB 82% of total RAM
```

Which one of the following statements about this FortiGate is correct?

A. It is currently in system conserve mode because of high CPU usage.
B. It is currently in extreme conserve mode because of high memory usage.
C. It is currently in proxy conserve mode because of high memory usage.
D. It is currently in memory conserve mode because of high memory usage.

**Answer:** D

**NEW QUESTION 33**
An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created and inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

A. Router ID.
B. OSPF interface area.
C. OSPF interface cost.
D. OSPF interface MTU.
E. Interface subnet mask.

**Answer:** BDE

**NEW QUESTION 36**
A FortiGate device has the following LDAP configuration:

```
config user ldap
   edit "WindowsLDAP"
      set server "10.0.1.10"
      set cnid "cn"
      set dn "cn=Users, dc=trainingAD, dc=training, dc=lab"
      set type regular
      set username "dc=trainingAD, dc=training, dc=lab"
      set password xxxxxxx
   next
end
```

The administrator executed the 'dsquery' command in the Windows LDAp server 10.0.1.10, and got the following output:
>dsquery user –samid administrator
"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab" Based on the output, what FortiGate LDAP setting is configured incorrectly?

A. cnid.
B. username.
C. password.
D. dn.

**Answer:** B

**Explanation:**
https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516

**NEW QUESTION 38**
View the IPS exit log, and then answer the question below.
# diagnose test application ipsmonitor 3 ipsengine exit log"
pid = 93 (cfg), duration = 5605322 (s) at Wed Apr 19 09:57:26 2017 code = 11, reason: manual
What is the status of IPS on this FortiGate?

A. IPS engine memory consumption has exceeded the model-specific predefined value.
B. IPS daemon experienced a crash.
C. There are communication problems between the IPS engine and the management database.
D. All IPS-related features have been disabled in FortiGate's configuration.

**Answer:** D

**Explanation:**
The command diagnose test application ipsmonitor includes many options that are useful for troubleshooting purposes.Option 3 displays the log entries generated every time an IPS engine process stopped. There are various reasons why these logs are generated:Manual: Because of the configuration, IPS no longer needs to run (that is, all IPS-releated features have been disabled)

**NEW QUESTION 43**
Examine the output of the 'diagnose debug rating' command shown in the exhibit; then answer the question below.

```
# diagnose debug rating
Locale       : english
License      : Contract
Expiration   : Wed Mar 27 17:00:00 20xx
-=- Server List (Mon Apr 16 15:32:55 20xx) -=-
IP               Weight   RTT   Flags   TZ   Packets   Curr Lost   Total Lo
69.195.205.101   10       45            -5   262432    0           846
69.195.205.102   10       46            -5   329072    0           6806
209.222.147.43   10       75            -5   71638     0           275
96.45.33.65      20       71            -8   36875     0           92
208.91.112.196   20       103   DI      -8   34784     0           1070
208.91.112.198   20       107   D       -8   35170     0           1533
80.85.69.41      60       144           0    33728     0           120
62.209.40.73     71       226           1    33797     0           192
121.111.236.180  150      197           9    33754     0           145
69.195.205.103   45       44    F       -5   26410     26226       26227
```

Which statement are true regarding the output in the exhibit? (Choose two.)

A. There are three FortiGuard servers that are not responding to the queries sent by the FortiGate.
B. The TZ value represents the delta between each FortiGuard server's time zone and the FortiGate's time zone.
C. FortiGate will send the FortiGuard queries to the server with highest weight.
D. A server's round trip delay (RTT) is not used to calculate its weight.

**Answer:** BC

**NEW QUESTION 47**
Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.
B. SIP ALG supports SIP HA failover; SIP helper does not.
C. SIP ALG supports SIP over IPv6; SIP helper does not.
D. SIP ALG can create expected sessions for media traffic; SIP helper does not.

E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

**Answer:** BCD

**NEW QUESTION 51**
Examine the following partial outputs from two routing debug commands; then answer the question below.
# get router info kernel
tab=254 vf=0 scope=0type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254 dev=2(port1)
tab=254 vf=0 scope=0type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254 dev=3(port2)
tab=254 vf=0 scope=253type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0 dev=4(port3)
# get router info routing-table all s*0.0.0.0/0 [10/0] via 10.200.1.254, portl [10/0] via 10.200.2.254, port2, [10/0] dO.0.1.0/24 is directly connected, port3
dO.200.1.0/24 is directly connected, portl d0.200.2.0/24 is directly connected, port2
Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

A. port!
B. port2.
C. Both portl and port2.
D. port3.

**Answer:** B

**NEW QUESTION 55**
When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the user credentials yet.
B. The server requires more information from the user, such as the token code for two-factor authentication.
C. The user credentials are wrong.
D. The user account is not found in the server.

**Answer:** B

**NEW QUESTION 56**
Examine the partial output from two web filter debug commands; then answer the question below:

```
# diagnose test application urlfilter 3
Domain | IP    DB Ver   T URL
34000000| 34000000   16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
   34 Finance and Banking
   37 Search Engines and Portals
   43 General Organizations
   49 Business
   50 Information and Computer Security
   51 Government and Legal Organizations
   52 Information Technology
```

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

A. Finance and banking
B. General organization.
C. Business.
D. Information technology.

**Answer:** C

**NEW QUESTION 59**
Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

A. Neighbor range
B. Route reflector
C. Next-hop-self
D. Neighbor group

**Answer:** B

**Explanation:**
Route reflectors help to reduce the number of IBGP sessions inside an AS. A route reflector forwards the routers learned from one peer to the other peers. If you configure route reflectors, you dont' need to create a full mesh IBGP network. All clients in a cluster only talck to route reflector to get sync routing updates. Route reflectors pass the routing updates to other route reflectors and border routers within the AS.

**NEW QUESTION 64**
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.

**Answer:** C

**NEW QUESTION 68**
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.

**Answer:** A

**NEW QUESTION 70**
Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:H2S_0_1:1249: notify msg received: SHORTCUT-QUERY
ike 0:H2S_0_1:  recv shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000 100.64.3.1
10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 32 nat 0 ver 1 mode 0
ike 0:H2S_0: iif 13 10.1.1.254->10.1.2.254 route lookup oif 13
ike 0:H2S_0_0: forward shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 31 ver 1 mode 0, ext-ma
ike 0:H2S_0_0:1248: sent IKE msg (SHORTCUT-QUERY): 100.64.1.1:500->100.64.5.1:500, len=236,
id=e2beec89f13c7074/06a73dfb3a5d3b54:340a645c
ike 0: comes 100.64.5.1:500->100.64.1.1:500, ifindex=3. . .
ike 0: IKEv1 exchange=Informational id=e2beec89f13c7074/06a73dfb3a5d3b5d:26254ae9 len=236
ike 0:H2S_0_0:1248: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0 100.64.5.1
to 10.1.1.254 psk 64 ppk 0 ver 1 mode 0 ext-mapping 100.64.3.1:500
ike 0:H2S_0: iif 13.10.1.2.254->10.1.1.254 route lookup oif 13
ike 0:H2S 0 1: forward shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0
100.64.5.1 to 10.1.1.254 psk 64 ppk 0 ttl 31 ver 1 mode 0 ext-mapping 100.
```

Based on the debug output, which phase 1 setting is enabled in the configuration of this VPN?

A. auto-discovery-shortcut
B. auto-discovery-forwarder
C. auto-discovery-sender
D. auto-discovery-receiver

**Answer:** D

**NEW QUESTION 73**
Examine the output of the 'get router info ospf interface' command shown in the exhibit; then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
   Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
   Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DROther, Priority 1
   Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address
172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit
5
     Hello due in 00:00:05
   Neighbor Count is 4, Adjacent neighbor count is 2
   Crypt Sequence Number is 411
   Hello received 106, sent 27, DD received 7 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

Which statements are true regarding the above output? (Choose two.)

A. The port4 interface is connected to the OSPF backbone area.
B. The local FortiGate has been elected as the OSPF backup designated router.
C. There are at least 5 OSPF routers connected to the port4 network.
D. Two OSPF routers are down in the port4 network.

**Answer:** AC

**Explanation:**
on BROADCAST network there are 4 neighbors, among which 1*DR +1*BDR. So our FG has 4 neighbors, but create adjacency only with 2 (with DR and BDR). 2 neighbors DRother (not down).

**NEW QUESTION 74**
Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. FortiGate first checks the OSPF ID to elect a DR.
B. Non-DR and non-BDR routers will form full adjacencies to DR and BDR only.
C. BDR is responsible for forwarding link state information from one router to another.
D. Only the DR receives link state information from non-DR routers.

**Answer:** B

**NEW QUESTION 78**
In which two states is a given session categorized as ephemeral? (Choose two.)

A. A TCP session waiting to complete the three-way handshake.
B. A TCP session waiting for FIN ACK.
C. A UDP session with packets sent and received.
D. A UDP session with only one packet received.

**Answer:** AD

**NEW QUESTION 82**
View the exhibit, which contains a session entry, and then answer the question below.

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement is correct regarding this session?

A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

**Answer:** B

**NEW QUESTION 84**
What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

A. Reduce the session time to live.
B. Increase the TCP session timers.
C. Increase the FortiGuard cache time to live.
D. Reduce the maximum file size to inspect.

**Answer:** AD

**NEW QUESTION 86**
Which two statements about an auxiliary session are true? (Choose two.)

A. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.
B. With the auxiliary session setting enabled, two sessions will be created in case of routing change.
C. With the auxiliary session setting disabled, for each traffic path, FortiGate will use the same auxiliary session.
D. With the auxiliary session disabled, only auxiliary sessions will be offloaded.

**Answer:** CD

**NEW QUESTION 87**
View these partial outputs from two routing debug commands:

```
# get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254
dev=2(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0
dev=4(port3)
# get router info routing-table all
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
                  [10/0] via 10.200.2.254, port2, [10/0]
C       10.0.1.0/24 is directly connected, port3
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
```

Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

A. Both port1 and port2
B. port3
C. port1
D. port2

**Answer:** C

**NEW QUESTION 89**
Which two statements about FortiManager is true when it is deployed as a local FDS? (Choose two.)

A. It caches available firmware updates for unmanaged devices.
B. It can be configured as an update server, or a rating server, but not both.
C. It supports rating requests from both managed and unmanaged devices.
D. It provides VM license validation services.

**Answer:** CD

**NEW QUESTION 90**
Examine the output of the ‘get router info bgp summary’ command shown in the exhibit; then answer the question below.

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor     V     AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.125.0.60  4  65060     1698     1756     103    0     0  03:02:49             1
10.127.0.75  4  65075     2206     2250     102    0     0  02:45:55             1
10.200.3.1   4  65501      101      115       0    0     0  never              Active

Total number of neighbors 3
```

Which statements are true regarding the output in the exhibit? (Choose two.)

A. BGP state of the peer 10.125.0.60 is Established.
B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.
C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.
D. The local BGP peer has received a total of 3 BGP prefixes.

**Answer:** AC

**NEW QUESTION 92**
Refer to the exhibit, which contains the output of diagnose sys session list.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement about the output is true?

A. This session cannot be synced with the slave unit.
B. The inspection of this session has been offloaded to the slave unit.
C. The master unit is processing this traffic.
D. This session is for HA heartbeat traffic.

**Answer:** C

**NEW QUESTION 97**
Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. IPS failopen
B. mem failopen
C. AV failopen
D. UTM failopen

**Answer:** AC

**NEW QUESTION 98**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_EFW-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_EFW-7.0 Product From:

**https://www.2passeasy.com/dumps/NSE7_EFW-7.0/**

## Money Back Guarantee

## NSE7_EFW-7.0 Practice Exam Features:

* NSE7_EFW-7.0 Questions and Answers Updated Frequently

* NSE7_EFW-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_EFW-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_EFW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year