



# NSE7\_EFW-6.2<sup>Q&As</sup>

Fortinet NSE 7 - Enterprise Firewall 6.2

## Pass Fortinet NSE7\_EFW-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[https://www.pass4itsure.com/nse7\\_efw-6-2.html](https://www.pass4itsure.com/nse7_efw-6-2.html)

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

View the global IPS configuration, and then answer the question below.

```
config ips global
  set fail-open disable
  set intelligent-mode disable
  set engine-count 0
  set algorithm engine-pick
end
```

Which of the following statements is true regarding this configuration?

- A. IPS will scan every byte in every session.
- B. FortiGate will spawn IPS engine instances based on the system load.
- C. New packets will be passed through without inspection if the IPS socket buffer runs out of memory.
- D. IPS will use the faster matching algorithm which is only available for units with more than 4 GB memory.

Correct Answer: A

---

**QUESTION 2**

Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated MAC address problem in the network.

What HA setting must be changed in one of the HA clusters to fix the problem?

- A. Group ID.
- B. Group name.
- C. Session pickup.
- D. Gratuitous ARPs.

Correct Answer: A

[https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA\\_failoverVMAC.htm](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm)

---

**QUESTION 3**

View the following FortiGate configuration.

```
config system global
    set snat-route-change disable
end
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 traffic to the Internet currently egresses from port1. The exhibit shows partial session information for Internet traffic from a user on the internal network:



```
# 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=57555/7/1 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
```

If the priority on route ID 1 were changed from 5 to 20, what would happen to traffic matching that user's session?

- A. The session would remain in the session table, and its traffic would still egress from port1.
- B. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
- C. The session would remain in the session table, and its traffic would start to egress from port2.
- D. The session would be deleted, so the client would need to start a new session.

Correct Answer: A

<http://kb.fortinet.com/kb/documentLink.do?externalID=FD40943>

#### QUESTION 4

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



```
# diagnose debug application urlfilter -1
# diagnose debug enable

msg="received a request /tmp/.ipsengine_498_0_0.url.socket, addr_len=37:
d=www.fortinet.com:80
id=83, vfname='root', vfid=0, profile='default', type=0, client=10.0.1.10,
url_source=1, url="/"
msg="Found it in cache. URL cat=52" IP cat=52user="N/A" src=10.0.1.10
sport=60348 dst=66.171.121.44 dport=80 service="http" hostname="
www.fortinet.com" url="/" matchType=prefix
action=10(ftgd-block) wf-act=3(BLOCK) user="N/A" src=10.0.1.10 sport=60348
dst=66.171.121.44
dport=80 service="http" cat=52 cat desc="Information Technology"
hostname="fortinet.com"
url="/"
```

Which of the following statements is true regarding this output? (Choose two.)

- A. This web request was inspected using the root web filter profile.
- B. FortiGate found the requested URL in its local cache.
- C. The requested URL belongs to category ID 52.
- D. The web request was allowed by FortiGate.

Correct Answer: BC

## QUESTION 5

Which two 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: AD

[https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager\\_Admin\\_Guide/1000\\_Device%20Manager/1200\\_install\\_to%20devices/0400\\_Install%20wizard-device%20settings.htm](https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/1200_install_to%20devices/0400_Install%20wizard-device%20settings.htm) There are 4 main wizards: Add Device: is used to add devices to central management and import their configurations. Install: is used to install configuration changes from Device Manager or Policies and Objects to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them. Import policy: is used to import interface mapping, policy database, and objects associated with the managed devices into a policy package under the Policy and Object tab. It runs with the Add Device wizard by default and may be run at any time from the





managed device list. Re-install policy: is used to perform a quick install of the policy package. It doesn't give the ability to preview the changes that will be installed to the managed device.

## QUESTION 6

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.

Correct Answer: B

## QUESTION 7

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



```
diagnose sys session list expectation
```

```
session info: proto=6 proto_state=00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=10.0.1.10/10.200.1.254
hook=pre dir-org act=dnat 10.171.121.38:0->10.200.1.1:60426(10.0.1.10:50365)
hook-pre dir-org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What statements are correct regarding the output? (Choose two.)

- A. This is an expected session created by a session helper.
- B. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.0.1.10.
- C. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.200.1.1.
- D. This is an expected session created by an application control profile.

Correct Answer: AC

## QUESTION 8

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 xxxxxxxx
  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.

Correct Answer: B

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516>

### QUESTION 9

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     -5     262432  0          846
64.26.151.35  10     46    -5     -5     329072  0          6806
66.117.56.37  10     75    -5     -5     71638   0          275
66.210.95.240 20     71    -8     -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      0      33728   0          120
80.85.69.41   71     226   1      1      33797   0          192
62.209.40.74  150    97    9      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 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.

Correct Answer: A

[http://docslegacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgtandfile=CLI\\_get\\_Commands.58.25.html](http://docslegacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgtandfile=CLI_get_Commands.58.25.html) The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACK remains in the table. The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACK remains in the table. The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in the table. A closed session remains in the session table for a few seconds more to allow any out-of- sequence packet.

---

#### QUESTION 11

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.

Correct Answer: CD

---

#### QUESTION 12

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



# diagnose webfilter fortiguard statistics list

Raring Statistics:

DNS failures	:	273
DNS lookups	:	280
Data send failures	:	0
Data read failures	:	0
Wrong package type	:	0
Hash table miss	:	0
Unknown server	:	0
Incorrect CRC	:	0
Proxy requests failures	:	0
Request timeout	:	1
Total requests	:	2409
Requests to FortiGuard servers	:	1182
Server errored responses	:	0
Relayed rating	:	0
Invalid profile	:	0
	:	
Allowed	:	1021
Blocked	:	3909
Logged	:	3927
Blocked Errors	:	565
Allowed Errors	:	0
Monitors	:	0
Authenticates	:	0
Warnings	:	18
Ovrd request timeout	:	0
Ovrd send failures	:	0
Ovrd read failures	:	0
Ovrd errored responses	:	0
...	:	

# diagnose webfilter fortiguard statistics list

Cache Statistics:

Maximum memory	:	0
Memory usage	:	0
	:	
Nodes	:	0
Leaves	:	0
Prefix nodes	:	0
Exact nodes	:	0
	:	
Requests	:	0
Misses	:	0
Hits	:	0
Prefix hits	:	0
Exact hits	:	0
	:	
No cache directives	:	0
Add after prefix	:	0
Invalid DB put	:	0
DB updates	:	0
	:	
Percent full	:	0%
Branches	:	0%
Leaves	:	0%
Prefix nodes	:	0%
Exact nodes	:	0%
	:	
Miss rate	:	0%
Hit rate	:	0%
Prefix hits	:	0%
Exact hits	:	0%

Which one of the following statements explains why the cache statistics are all zeros?

- A. The administrator has reallocated the cache memory to a separate process.
- B. There are no users making web requests.
- C. The FortiGuard web filter cache is disabled in the FortiGate's configuration.
- D. FortiGate is using a flow-based web filter and the cache applies only to proxy-based inspection.

Correct Answer: C

**QUESTION 13**



View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.

```
# 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=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 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=snst 10.0.1.10:65464->54.192.15.182:80 (10.200.1.1:65464
hook-pre dir=reply act=dnat 54.192.15.182:80->10.200.1.1:65464 (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 is correct regarding the output?

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

Correct Answer: B

#### QUESTION 14

Examine the output from the BGP real time debug shown in the exhibit, then answer the question below: Which statements are true regarding the output in the exhibit? (Choose two.)



```
# diagnose ip router bgp all enable
# diagnose ip router bgp level info
# diagnose debug enable
"BGP: 10.200.3.1-Outgoing [DECODE] KAlive: Received!"
"BGP: 10.200.3.1-Outgoing [FSM] State: OpenConfirm Event: 26"
"BGP: 10.200.3.1-Outgoing [DECODE] Msg-Hdr: type 2, length 56"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Byte
(37), msg_size (37)"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: NLRI Len(13)"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 27"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.4.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.3.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.0.2.0/24"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
"BGP: 10.200.3.1-Outgoing [ENCODE] Msg-Hdr: Type 2"
"BGP: 10.200.3.1-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 20"
"BGP: 10.200.3.1-Outgoing [ENCODE] Update: Msg #5 Size 55"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
```

- 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.

Correct Answer: AB

## QUESTION 15

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.

Correct Answer: AC

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).

[NSE7\\_EFW-6.2 VCE Dumps](#)

[NSE7\\_EFW-6.2 Practice Test](#)

[NSE7\\_EFW-6.2 Exam Questions](#)