

NSE7_EFW-6.2^{Q&As}

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.pass2lead.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

What conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

- A. IP addresses are in the same subnet.
- B. Hello and dead intervals match.
- C. OSPF IP MTUs match.
- D. OSPF peer IDs match.
- E. OSPF costs match.

Correct Answer: ABC

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_OSPF/OSPF_Background_Concepts.htm#Adjacenc

QUESTION 2

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 filures           : 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 FortGuard 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
Ovr request timeout   : 0
Ovr send failures     : 0
Ovr read failures     : 0
Ovr 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 3

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
origin->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 4

What is the diagnose test application ipsmonitor 99 command used for?

- A. To enable IPS bypass mode
- B. To provide information regarding IPS sessions
- C. To disable the IPS engine
- D. To restart all IPS engines and monitors

Correct Answer: D

QUESTION 5

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.

Correct Answer: D

<https://kb.fortinet.com/kb/documentLink.do?externalID=11655>

QUESTION 6

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.

Correct Answer: D

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-related features have been disabled)

QUESTION 7

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

```
FGT # 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
100.64.3.1    4 65501    101      115     0       0     0    never          Active

Total number of neighbors 3
```

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

- A. The local router's BGP state is Established with the 10.125.0.60 peer.
- B. Since the counters were last reset, the 10.200.3.1 peer has never been down.
- C. The local router has received a total of three BGP prefixes from all peers.
- D. The local router has not established a TCP session with 100.64.3.1.

Correct Answer: AD

QUESTION 8

The logs in a FSSO collector agent (CA) are showing the following error: failed to connect to registry: PIKA1026 (192.168.12.232)

What can be the reason for this error?

- A. The CA cannot resolve the name of the workstation.
- B. The FortiGate cannot resolve the name of the workstation.
- C. The remote registry service is not running in the workstation 192.168.12.232.
- D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Correct Answer: C

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548>

QUESTION 9

View the exhibit, which contains a partial routing table, and then answer the question below.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C    10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C    10.1.0.0/24 is directly connected, port3
S    10.10.4.0/24 [10/0] via 10.1.0.100, port3
C    10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S    10.1.0.0/24 [10/0] via 10.72.3.254, port4
C    10.72.3.0/24 is directly connected, port4
S    192.168.2.0/24 [10/0] via 10.72.3.254, port4
...
```

Assuming all the appropriate firewall policies are configured, which of the following pings will FortiGate route? (Choose two.)

- A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.
- B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.
- C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.
- D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

Correct Answer: BC

QUESTION 10

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: CDE

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

QUESTION 11

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

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder: main mode get 1st message...
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:   trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:   encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 1:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:   trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:   encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278:
proposal chosen
...
```

Why didn't the tunnel come up?

- A. The pre-shared keys do not match.
- B. The remote gateway's phase 2 configuration does not match the local gateway's phase 2 configuration.
- C. The remote gateway's phase 1 configuration does not match the local gateway's phase 1 configuration.
- D. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Correct Answer: C

QUESTION 12

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

Correct Answer: B

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.

QUESTION 13

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 14

Examine the following traffic log; then answer the question below. date=20xx-02-01 time=19:52:01

```
devname=master device_id="xxxxxxx" log_id=0100020007 type=event subtype=system pri critical vd=root  
service=kemel status=failure msg="NAT port is exhausted."
```

What does the log mean?

- A. There is not enough available memory in the system to create a new entry in the NAT port table.
- B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.
- C. FortiGate does not have any available NAT port for a new connection.
- D. The limit for the maximum number of entries in the NAT port table has been reached.

Correct Answer: B

QUESTION 15

Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all  
*0.0.0.0/0 [10/0] via 10.200.1.254, port1  
C10.200.1.0/24 is directly connected, port1  
S192.168.0.0/16 [10/0] via 10.200.1.254, port1  
# show router bgp  
config router bgp  
set as 65500  
set router-id 10.200.1.1  
set network import check enable  
set ebgp-multipath disable  
config neighbor  
edit "10.200.3.1"  
set remote-as 65501  
next  
end  
config network  
edit1
```

The BGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

- A. Enable the redistribution of connected routers into BGP.
- B. Enable the redistribution of static routers into BGP.
- C. Disable the setting network-import-check.

D. Enable the setting ebgp-multipath.

Correct Answer: C

[NSE7_EFW-6.2 Practice Test](#)

[NSE7_EFW-6.2 Study Guide](#)

[NSE7_EFW-6.2 Braindumps](#)