

NSE7_EFW-6.4^{Q&As}

Fortinet NSE 7 - Enterprise Firewall 6.4

Pass Fortinet NSE7_EFW-6.4 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse7_efw-6-4.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 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 iS-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 2

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.

Correct Answer: AD

QUESTION 3

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

- A. Only the root FortiGate collects network information and forwards it to FortiAnalyzer.
- B. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.

- C. All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity.
- D. Branch FortiGate devices must be configured first.

Correct Answer: BC

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/327890/deploying-security-fabric>

QUESTION 4

Which statement is true regarding File description (FD) conserve mode?

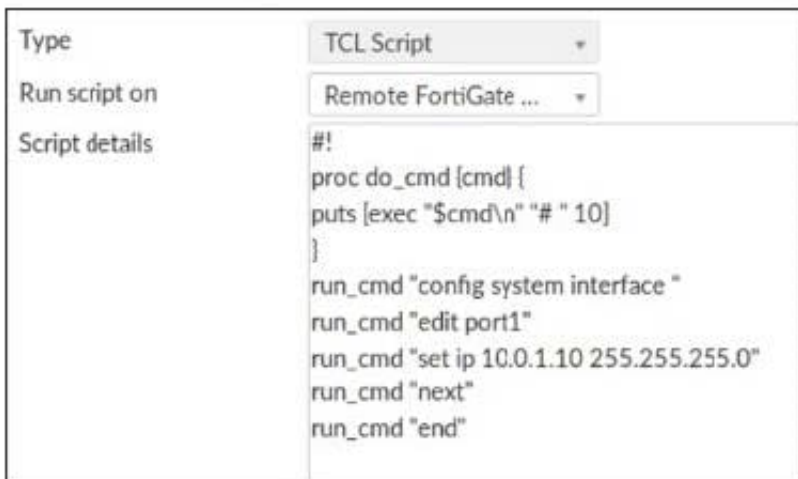
- A. IPS inspection is affected when FortiGate enters FD conserve mode.
- B. A FortiGate enters FD conserve mode when the amount of available description is less than 5%.
- C. FD conserve mode affects all daemons running on the device.
- D. Restarting the WAD process is required to leave FD conserve mode.

Correct Answer: B

QUESTION 5

Refer to the exhibit, which contains a TCL script configuration on FortiManager.

An administrator has configured the TCL script on FortiManager, but the TCL script failed to apply any changes to the managed device after being run.



Why did the TCL script fail to make any changes to the managed device?

- A. The TCL command run_cmd has not been created.
- B. The TCL script must start with tinclude .
- C. Incomplete commands are ignored in TCL scripts.

D. Changes to an interface configuration can be made only by a CLI script.

Correct Answer: A

QUESTION 6

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

Correct Answer: AC

QUESTION 7

Which two statements about OCVPN are true? (Choose two.)

- A. Only root vdom supports OCVPN.
- B. OCVPN supports static and dynamic IPs in WAN interface.
- C. OCVPN offers only Hub-Spoke VPNs.
- D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Correct Answer: AB

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/977344/one-click-vpn-ocvpn> <https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/496884/overlay-controller-vpn-ocvpn>

QUESTION 8

Examine the output of the ``get router info bgp summary`` command shown in the exhibit; then answer the question below.

```
Student# get router info bgp summary
BGP router identifier 10.200.1.1, local AS number 65500
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.200.3.1	4	65501	92	112	0	0	0	never	Connect

Total number of neighbors 1

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

- A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
- B. The TCP session for the BGP connection to 10.200.3.1 is down.
- C. The local peer has received the BGP prefixed from the remote peer.
- D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Correct Answer: B

<http://www.ciscopress.com/articles/article.asp?p=2756480andseqNum=4>

QUESTION 9

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

- A. Installing configuration changes to managed devices
- B. Importing interface mappings from managed devices
- C. Adding devices to FortiManager
- D. Previewing pending configuration changes for managed devices

Correct Answer: AD

Reference: <https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/668612/using-theinstall-wizard-to-install-device-settings-only>

QUESTION 10

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.

Correct Answer: C

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

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 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
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 13

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

```
ike 0:9268ab9dea63aa3/0000000000000000:591: responder: main mode get 1st message...
...
ike 0:9268ab9dea63aa3/0000000000000000:591: incoming proposal:
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 0:
ike 0:9268ab9dea63aa3/0000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:     trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:     encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id=0:
ike 0:9268ab9dea63aa3/0000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:     trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:     encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISA KMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: my proposal, gw VPN:
ike 0:9268ab9dea63aa3/0000000000000000:591:     proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:     trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:     encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:     protocol_id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:     trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591:     encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591:     protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:     trans_id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591:     encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591:     type= OAKLEY_ENCRYPT_ALG, val =AES-CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591:     type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
```

The administrator does not have access to the remote gateway. Based on the debug output, what configuration changes can the administrator make to the local gateway to resolve the phase 1 negotiation error?

- A. Change phase 1 encryption to 3DES and authentication to SHA128.
- B. Change phase 1 encryption to AES128 and authentication to SHA512.

C. Change phase 1 encryption to AESCBC and authentication to SHA2.

D. Change phase 1 encryption to AES256 and authentication to SHA256.

Correct Answer: D

QUESTION 14

Examine the output of the `get router info ospf neighbor` command shown in the exhibit; then answer the question below.

```
# get router info ospf neighbor
```

```
OSPF process 0:
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.0.69	1	Full/DR	00:00:32	10.126.0.69	wan1
0.0.0.117	1	Full/DROther	00:00:34	10.126.0.117	wan1
0.0.0.2	1	Full/ -	00:00:36	172.16.1.2	ToRemote

Refer to the exhibit, which shows the output of a debug command.

Which statement about the output is true?

A. The OSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wan1 network.

B. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.

C. The local FortiGate is the designated router for the wan1 network.

D. The interface ToRemote is a point-to-point OSPF network.

Correct Answer: D

<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html>

QUESTION 15

An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.

B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.

C. Sends a link failed signal to all connected devices.

D. Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

Correct Answer: A

[Latest NSE7_EFW-6.4 Dumps](#)

[NSE7_EFW-6.4 VCE Dumps](#)

[NSE7_EFW-6.4 Practice Test](#)