



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.geekcert.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

An administrator cannot connect to the GUI of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

```
# diagnose debug flow filter port 80
# diagnose debug flow trace start 5
# diagnose debug enable

id=20085 trace_id=5 msg="vd-root received a packet(proto=6,
10.0.1.10:57459->10.0.1.254:80) from port3. flag [S], seq 3190430861, ack
0, win 8192"
id=20085 trace_id=5 msg="allocate a new session-0000008c"
id=20085 trace_id=5 msg="iprope_in_check() check failed on policy 0, drop"
```

Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

- A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
- B. Redirection of HTTP to HTTPS administrative access is disabled.
- C. HTTP administrative access is configured with a port number different than 80.
- D. The packet is denied because of reverse path forwarding check.

Correct Answer: AC

QUESTION 2

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



```
#dia hardware sysinfo shm
SHM counter:          150
SHM allocated:       0
SHM total:           625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total:        641236992
SHM FS free:         641208320
SHM FS avail:        641208320
SHM FS alloc:         28672
```

What statement is correct about this FortiGate?

- A. It is currently in system conserve mode because of high CPU usage.
- B. It is currently in FD conserve mode.
- C. It is currently in kernel conserve mode because of high memory usage.
- D. It is currently in system conserve mode because of high memory usage.

Correct Answer: D

QUESTION 3

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 4



```
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
```

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

- 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.

Correct Answer: BC

QUESTION 5

Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

Why didn't the tunnel come up?

- A. IKE mode configuration is not enabled in the remote IPsec gateway.



- 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. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Correct Answer: C

[Latest NSE7_EFW-6.4 Dumps](#)

[NSE7_EFW-6.4 VCE Dumps](#)

[NSE7_EFW-6.4 Exam Questions](#)