

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

NSE7 Enterprise Firewall - FortiOS 5.4

**Pass Fortinet NSE7\_EFW Exam with 100% Guarantee**

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

[https://www.pass2lead.com/nse7\\_efw.html](https://www.pass2lead.com/nse7_efw.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 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

---

### QUESTION 2

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: B

---

### QUESTION 3

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

#### QUESTION 4

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: A

#### QUESTION 5

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 directive : 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: D