



# NSE7\_EFW-7.0<sup>Q&As</sup>

Fortinet NSE 7 - Enterprise Firewall 7.0

## Pass Fortinet NSE7\_EFW-7.0 Exam with 100% Guarantee

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

[https://www.pass4itsure.com/nse7\\_efw-7-0.html](https://www.pass4itsure.com/nse7_efw-7-0.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**

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 2**

Which two statements about an auxiliary session are true? (Choose two.)

- A. With the auxiliary session setting disabled, only auxiliary sessions are offloaded.
- B. With the auxiliary session setting enabled, two sessions are created in case of routing change.
- C. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.
- D. With the auxiliary session setting disabled, for each traffic path, FortiGate uses the same auxiliary session.

Correct Answer: BC

Reference: <https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/14295/controlling-return-path-with-auxiliary-session> NSE7 Study Guide Chapter 4 , slide "ECMP Accelerated with Auxiliary session"

**QUESTION 3**

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 4**

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 5**

Refer to the exhibit, which shows a central management configuration.

```
config system central-management
  set type fortimanager
  set fmg "10.0.1.242"
  config server-list
    edit 1
      set server-type rating
      set addr-type ipv4
      set server-address 10.0.1.240
    next
    edit 2
      set server-type update
      set addr-type ipv4
      set server-address 10.0.1.243
    next
    edit 3
      set server-type rating
      set addr-type ipv4
      set server-address 10.0.1.244
    next
  end
  set include-default-servers enable
end
```

Which server will FortiGate choose for web filter rating requests, if 10.0.1.240 is experiencing an outage?

- A. Public FortiGuard servers
- B. 10.0.1.243
- C. 10.0.1.242
- D. 10.0.1.244

Correct Answer: D



Explanation: by default, ( include-default-servers ) enabled .this allows fortigate to communicate with the public fortiguard servers , if the fortimanger devices (configured in server-list) are unavailable .

[NSE7\\_EFW-7.0 Practice Test](#)

[NSE7\\_EFW-7.0 Study Guide](#)

[NSE7\\_EFW-7.0 Braindumps](#)