

# NSE4\_FGT-6.4<sup>Q&As</sup>

Fortinet NSE 4 - FortiOS 6.4

## Pass Fortinet NSE4\_FGT-6.4 Exam with 100% Guarantee

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

[https://www.pass2lead.com/nse4\\_fgt-6-4.html](https://www.pass2lead.com/nse4_fgt-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**

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

- A. The keyUsage extension must be set to keyCertSign.
- B. The common name on the subject field must use a wildcard name.
- C. The issuer must be a public CA.
- D. The CA extension must be set to TRUE.

Correct Answer: AD

---

**QUESTION 2**

Which two VDOMs are the default VDOMs created when FortiGate is set up in split VDOM mode? (Choose two.)

- A. FG-traffic
- B. Mgmt
- C. FG-Mgmt
- D. Root

Correct Answer: AD

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/758820/split-task-ldom-mode>

---

**QUESTION 3**

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

- A. FortiGuard web filter cache
- B. FortiGate hostname
- C. NTP
- D. DNS

Correct Answer: CD

---

**QUESTION 4**

Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

- A. DNS
- B. ping
- C. udp-echo
- D. TWAMP

Correct Answer: CD

---

### QUESTION 5

Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

- A. The next-hop IP address is unreachable.
- B. It failed the RPF check.
- C. It matched an explicitly configured firewall policy with the action DENY.
- D. It matched the default implicit firewall policy.

Correct Answer: D

<https://kb.fortinet.com/kb/documentLink.do?externalID=13900>

---

### QUESTION 6

Refer to the exhibit to view the application control profile.

### Edit Application Sensor

Categories

<input type="button" value="Business (143, ☁6)"/>	<input checked="" type="button" value="Cloud.IT (47, ☁1)"/>
<input checked="" type="button" value="Collaboration (255, ☁10)"/>	<input checked="" type="button" value="Email (78, ☁12)"/>
<input type="button" value="Game (84)"/>	<input checked="" type="button" value="General.Interest (229, ☁7)"/>
<input type="button" value="Mobile (3)"/>	<input checked="" type="button" value="Network.Service (330)"/>
<input type="button" value="P2P (56)"/>	<input type="button" value="Proxy (168)"/>
<input type="button" value="Remote.Access (84)"/>	<input type="button" value="Social.Media (116, ☁31)"/>
<input checked="" type="button" value="Storage.Backup (162, ☁16)"/>	<input checked="" type="button" value="Update (49)"/>
<input type="button" value="Video/Audio (154, ☁14)"/>	<input type="button" value="VoIP (24)"/>
<input type="button" value="Web.Client (24)"/>	<input type="button" value="Unknown Applications"/>

Network Protocol Enforcement

#### Application and Filter Overrides

Priority	Details	Type	Action
1	<b>BHVR</b> Excessive-Bandwidth	Filter	<input type="button" value="Block"/>
2	<b>VEND</b> Apple	Filter	<input type="button" value="Monitor"/>

Users who use Apple FaceTime video conferences are unable to set up meetings. In this scenario, which statement is true?

- A. Apple FaceTime belongs to the custom monitored filter.
- B. The category of Apple FaceTime is being monitored.
- C. Apple FaceTime belongs to the custom blocked filter.
- D. The category of Apple FaceTime is being blocked.

Correct Answer: C

### QUESTION 7

A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.

What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

- A. Static IP Address
- B. Dialup User
- C. Dynamic DNS
- D. Pre-shared Key

Correct Answer: B

---

### QUESTION 8

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.

What order must FortiGate use when the web filter profile has features enabled, such as safe search?

- A. DNS-based web filter and proxy-based web filter
- B. Static URL filter, FortiGuard category filter, and advanced filters
- C. Static domain filter, SSL inspection filter, and external connectors filters
- D. FortiGuard category filter and rating filter

Correct Answer: B

Reference: [https://fortinet121.rssing.com/chan-67705148/all\\_p1.html](https://fortinet121.rssing.com/chan-67705148/all_p1.html)

---

### QUESTION 9

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

- A. Log ID
- B. Universally Unique Identifier
- C. Policy ID
- D. Sequence ID

Correct Answer: B

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies>

---

**QUESTION 10**

Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

- A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
- B. An SA never expires.
- C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
- D. Phase 2 SA expiration can be time-based, volume-based, or both.
- E. Both the phase 1 SA and phase 2 SA are bidirectional.

Correct Answer: ACD

**QUESTION 11**

Refer to the exhibit.

```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000 4500 003c 2f8f 0000 8001 f020 0a00 0102 E.</.....
0x0010 0808 0808 0800 4d5a 0001 0001 6162 6364 .....MZ....abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000 4500 003c 2f8f 0000 7f01 0106 0a38 f0e4 E.</.....8..
0x0010 0808 0808 0800 6159 ec01 0001 6162 6364 .....aY....abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000 4500 003c 0000 0000 7501 3a95 0808 0808 E.<.....u:.....
0x0010 0a38 f0e4 0000 6959 ec01 0001 6162 6364 .8....iY....abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000 4500 003c 0000 0000 7401 2bb0 0808 0808 E.<....t.+.....
0x0010 0a00 0102 0000 555a 0001 0001 6162 6364 .....UZ....abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.

Which three pieces of information are included in the sniffer output? (Choose three.)

- A. Interface name
- B. Ethernet header



- C. IP header
- D. Application header
- E. Packet payload

Correct Answer: ACE

FortiGate\_Infrastructure\_6.4 page 58

**QUESTION 12**

Refer to the exhibit.

Name	Type	IP/Netmask	VLAN ID
<b>Physical Interface 14</b>			
port1	Physical Interface	10.200.1.1/255.255.255.0	
• port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
• port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
port10	Physical Interface	10.0.11.1/255.255.255.0	
port2	Physical Interface	10.200.2.1/255.255.255.0	
• port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
• port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

- A. Traffic between port2 and port2-vlan1 is allowed by default.
- B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- C. port1 is a native VLAN.
- D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Correct Answer: CD

**QUESTION 13**

How does FortiGate act when using SSL VPN in web mode?

- A. FortiGate acts as an FDS server.
- B. FortiGate acts as an HTTP reverse proxy.

- C. FortiGate acts as DNS server.
- D. FortiGate acts as router.

Correct Answer: B

Reference: [https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate\\_v4.0MR3/fortigatesslvpn-40-mr3.pdf](https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigatesslvpn-40-mr3.pdf)

#### QUESTION 14

Refer to the exhibit.



Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

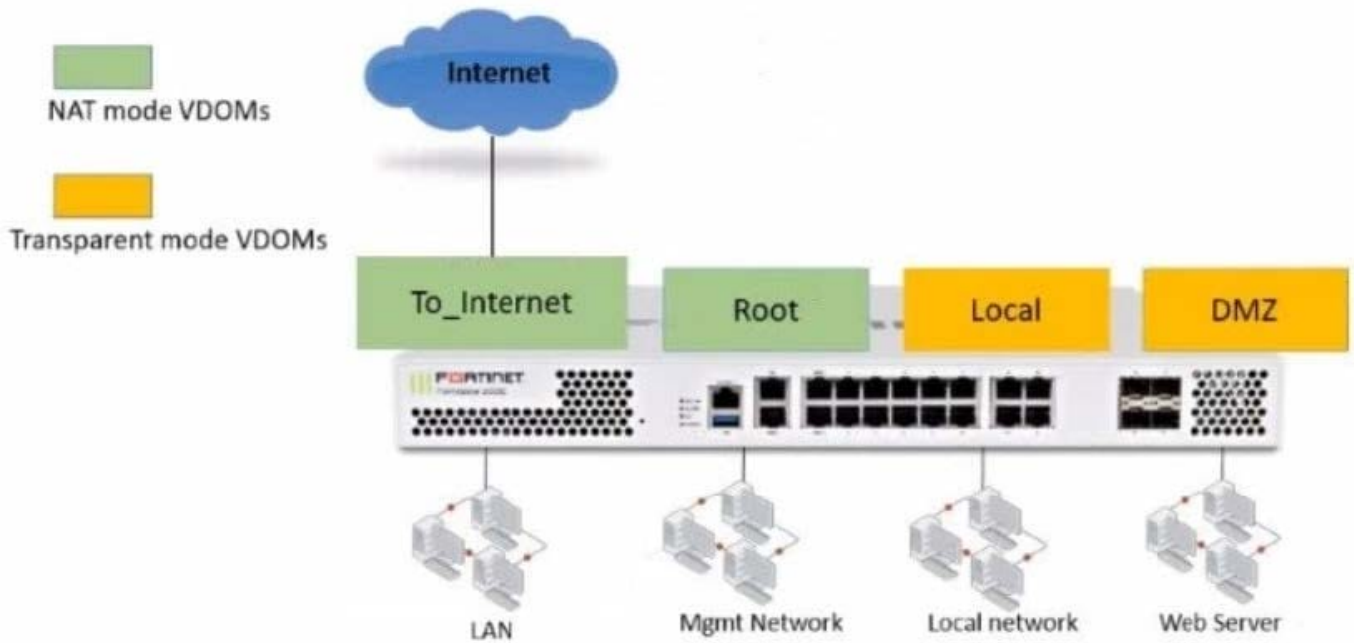
- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.

Correct Answer: D

#### QUESTION 15

Refer to the exhibit.





The Root and To\_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.

The Root VDOM is the management VDOM. The To\_Internet VDOM allows LAN users to access the Internet. The To\_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.

Which two statements are true? (Choose two.)

- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
- B. A static route is required on the To\_Internet VDOM to allow LAN users to access the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
- D. Inter-VDOM links are not required between the Root and To\_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Correct Answer: AD

[NSE4\\_FGT-6.4 PDF Dumps](#) [NSE4\\_FGT-6.4 Study Guide](#) [NSE4\\_FGT-6.4 Braindumps](#)