



# NSE4\_FGT-5.6<sup>Q&As</sup>

Fortinet NSE 4 - FortiOS 5.6

## Pass Fortinet NSE4\_FGT-5.6 Exam with 100% Guarantee

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

[https://www.passapply.com/nse4\\_fgt-5-6.html](https://www.passapply.com/nse4_fgt-5-6.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

You have enabled a web filter security profile in a firewall policy to log all blocked websites. What options do you have to either actively or passively monitor these logs? (Choose two.)

Response: A. Alert Message console

B. FortiView menu

C. Alert email

D. Monitor menu

Correct Answer: AC

---

### QUESTION 2

You have configured the following log settings on the Log Settings page. Which configurations are now required to generate log messages on traffic coming through your network?

(Choose two.)

Response:

A. Enable Log Allowed Traffic on your firewall policy.

B. Enable Local Traffic Log on the Log Settings page.

C. Enable Historical FortiView on the Log Settings page.

D. Enable a security profile on your firewall policy.

E. Enable Capture Packets on your firewall policy.

Correct Answer: AB

---

### QUESTION 3

Which statements are true of public key infrastructure (PKI) users on FortiGate?

(Choose two.)

Response:

A. FortiGate must include the CA certificate that issued the PKI peer user certificate.

B. PKI users can belong to firewall user groups.

C. PKI users must authenticate with both a certificate and a password.



D. The first PKI user must be added to FortiGate through the GUI.

Correct Answer: AB

#### QUESTION 4

Under which circumstance is the IPsec ESP traffic encapsulated over UDP? Response:

- A. When using IKE version 2 (IKEv2)
- B. When the phase 1 is configured to use aggressive mode
- C. When the IPsec VPN is configured as dial-up
- D. When NAT-T detects there is a device between both IPsec peers doing NAT over the IPsec traffic

Correct Answer: D

#### QUESTION 5

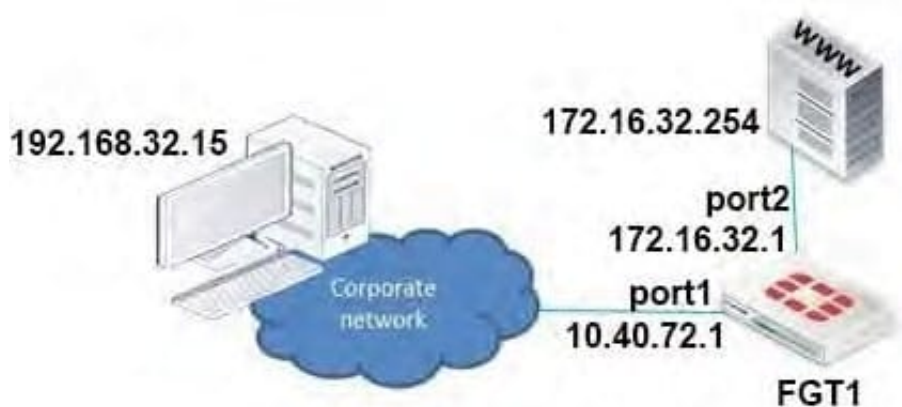
Which component of FortiOS performs application control inspection? Response:

- A. Kernel
- B. Antivirus engine
- C. IPS engine
- D. Application control engine

Correct Answer: C

#### QUESTION 6

View the exhibit.





In this scenario, FGT1 has the following routing table: S\*0. 0. 0. 0/0 [10/0] via 10. 40.

72. 2, port1 C172. 16. 32. 0/24 is directly connected, port2

C10. 40. 72. 0/30 is directly connected, port1

A user at 192.168.32.15 is trying to access the web server at 172.16.32.254. Which of the following statements best describe how the FortiGate will perform reverse path forwarding checks on this traffic?

(Choose two.)

Response:

- A. Strict RPF check will deny the traffic.
- B. Strict RPF check will allow the traffic.
- C. Loose RPF check will allow the traffic.
- D. Loose RPF check will deny the traffic.

Correct Answer: BD

---

#### QUESTION 7

When does the FortiGate enter into fail-open session mode? Response:

- A. When CPU usage goes above the red threshold.
- B. When a proxy (for proxy-based inspection) runs out of connections.
- C. When memory usage goes above the red threshold.
- D. When memory usage goes above the extreme threshold.

Correct Answer: B

---

#### QUESTION 8

Which statements about IP-based explicit proxy authentication are true?

(Choose two.)

Response:

- A. IP-based authentication is best suited to authenticating users behind a NAT device.
- B. Sessions from the same source address are treated as a single user.
- C. IP-based authentication consumes less FortiGate's memory than session-based authentication.
- D. FortiGate remembers authenticated sessions using browser cookies.

Correct Answer: BC

---

### QUESTION 9

Which ways can FortiGate deliver one-time passwords (OTPs) to two-factor authentication users in your network?

(Choose three.)

Response:

- A. Hardware FortiToken
- B. Web portal
- C. SMS
- D. USB FortiToken
- E. FortiToken Mobile

Correct Answer: ACE

---

### QUESTION 10

An administrator has configured a route-based IPsec VPN between two FortiGates. Which statement about this IPsec VPN configuration is true?

Response:

- A. A phase 2 configuration is not required.
- B. This VPN cannot be used as part of a hub and spoke topology.
- C. The IPsec firewall policies must be placed at the top of the list.
- D. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.

Correct Answer: D

---

### QUESTION 11

Which remote device's logs can you display in the FortiGate GUI by configuring the log setting's GUI Preferences?

Response:

- A. Disk
- B. FortiAnalyzer



C. Syslog

D. FortiSIEM

Correct Answer: B

---

#### QUESTION 12

An administrator needs to be able to view logs for application usage on your network. What configurations are required to ensure that FortiGate generates logs for application usage activity?

(Choose two.)

Response:

A. Enable a web filtering profile on the firewall policy.

B. Create an application control policy.

C. Enable logging on the firewall policy.

D. Enable an application control security profile on the firewall policy.

Correct Answer: CD

---

#### QUESTION 13

Which of the following statements are true about route-based IPsec VPNs?

(Choose two.)

Response:

A. A virtual IPsec interface is automatically created after a phase 1 is added to the configuration

B. They require firewall policies with the Action set to IPsec

C. They support L2TP-over-IPsec tunnels

D. They can be created in transparent mode VDOMs

Correct Answer: AC

---

#### QUESTION 14

Which statement about the firewall policy authentication timeout is true? Response:

A. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this times expires.



B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this times expires.

C. It is an idle timeout. The FortiGate considers a user to be idle if it does not see any packets coming from the user's source MAC address.

D. It is an idle timeout. The FortiGate considers a user to be idle if it does not see any packets coming from the user's source IP.

Correct Answer: D

## QUESTION 15

Examine the exhibit, which contains a virtual IP and a firewall policy configuration.

Virtual IP

Name

VIP

Comments

Network

Interface

WAN (port1)

Type

Static NAT

External IP Address/Range

10.200.1.10 - 10.200.1.10

Mapped IP Address/Range

10.0.1.10 - 10.0.1.10

Source Address Filter

☐

Port Forwarding

☐

OK

Cancel

Firewall Policies

Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT
LAN (port2) - WAN (port1) (1 - 1)							
1	Full_Access	all	all	always	ALL	ACCEPT	Enabled
WAN (port1) - LAN (port2) (2 - 2)							
2	WebServer	all	VIP	always	ALL	ACCEPT	Disabled

The WAN(port1) interface has the IP address 10.200.1.1/24. The LAN(port2) interface has the IP address 10.0.1.254/24. The top firewall policy has NAT enabled using outgoing interface address. The second firewall policy configured with a virtual IP (VIP) as the destination address. Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0.1.10/24?

Response:

A. 10.200.1.1

B. 10.0.1.254

C. Any available IP address in the WAN(port1) subnet 10.200.1.0/24



D. 10.200.1.10

Correct Answer: D

[NSE4\\_FGT-5.6 PDF Dumps](#) [NSE4\\_FGT-5.6 Study Guide](#)

[NSE4\\_FGT-5.6 Exam Questions](#)