



# Fortinet

NSE4\_FGT-5.6 Exam

**Fortinet NSE 4 – FortiOS 5.6 Exam**

Thank you for Downloading NSE4\_FGT-5.6 exam PDF Demo

You can Buy Latest NSE4\_FGT-5.6 Full Version Download

[https://www.certkillers.net/Exam/NSE4\\_FGT-5.6](https://www.certkillers.net/Exam/NSE4_FGT-5.6)

<https://www.certkillers.net>

## Version: 6.0

---

### Question: 1

---

View the routing table, then identify which route will be selected when trying to reach 10.20.30.254?

```
FGT1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

S*   0.0.0.0/0 [10/0] via 172.20.121.2, port1
C    172.20.121.0/24 is directly connected, port1
C    172.20.168.0/24 is directly connected, port2
C    172.20.167.0/24 is directly connected, port3
S    10.20.30.0/26 [10/0] via 172.20.168.254, port2
S    10.20.30.0/24 [10/0] via 172.20.167.254, port3
S    10.30.20.0/24 [10/0] via 172.20.121.2, port1
```

Response:

- A. 10.20.30.0/26 [10/0] via 172.20.168.254, port2
- B. 0.0.0.0/0 [10/0] via 172.20.121.2, port1
- C. 10.30.20.0/24 [10/0] via 172.20.121.2, port1
- D. 10.20.30.0/24 [10/0] via 172.20.167.254, port3

---

**Answer: D**

---

---

### Question: 2

---

Which of the following statements are true when using Web Proxy Auto-discovery Protocol (WPAD) with the DHCP discovery method?

(Choose two.)

Response:

- A. The browser sends a DHCPINFORM request to the DHCP server.
- B. The browser will need to be preconfigured with the DHCP server's IP address.
- C. The DHCP server provides the PAC file for download.
- D. If the DHCP method fails, browsers will try the DNS method.

---

**Answer: AD**

---

---

### Question: 3

---

Which of the following statements about the FSSO collector agent timers is true?

Response:

- A. The dead entry timeout interval is used to age out entries with an unverified status.
- B. The workstation verify interval is used to periodically check if a workstation is still a domain member.
- C. The user group cache expiry is used to age out the monitored groups.
- D. The IP address change verify interval monitors the server IP address where the collector agent is installed, and updates the collector agent configuration if it changes.

---

**Answer: A**

---

---

### Question: 4

---

Which of the following statements about NTLM authentication are correct?  
(Choose two.)

Response:

- A. It is useful when users log in to DCs that are not monitored by a collector agent.
- B. It takes over as the primary authentication method when configured alongside FSSO.
- C. Multi-domain environments require DC agents on every domain controller.
- D. NTLM-enabled web browsers are required.

---

**Answer: AD**

---

---

### Question: 5

---

How can you configure the explicit web proxy to block HTTP packets that request a specific HTTP method?

Response:

- A. Create an explicit proxy address that matches the HTTP method and apply it to an explicit proxy policy with the action Deny.
- B. Apply a web filter profile to an explicit proxy policy that blocks the HTTP method.
- C. Create a firewall service that matches the HTTP method and apply it to an explicit proxy policy with the action Deny.
- D. Create a DNS filter that matches the HTTP method and apply it to an explicit proxy policy with the action Deny.

---

**Answer: A**

---

---

### Question: 6

---

Firewall policies dictate whether a user or device can (or cannot) authenticate to a network. Which statements are true regarding firewall authentication?

(Choose two.)

Response:

- A. In order to authenticate a specific user, the firewall policy must include ..., both the IP address and the user as the source.
- B. Firewall policies can be configured to authenticate certificate users.
- C. Users are forced to actively authenticate when the following protocols are disabled in the firewall policy: HTTP, HTTPS, FTP, Telnet.
- D. The order of the firewall policies always determine whether a user's credentials are determined actively or passively.

**Answer: AB**

**Question: 7**

View the exhibit. You are trying to go to <http://www.dailymotion.com> (Dailymotion) from the computer behind the FortiGate. Which statement is correct regarding this application control profile?

Name	Category	Technology	Popularity	Risk	Behavior
Dailymotion	Video/Audio	Browser-Based	☆☆☆☆☆	★☆☆	Excessive-Bandwidth

**Categories**

<input type="checkbox"/> Botnet	<input type="checkbox"/> Game	<input type="checkbox"/> Proxy	<input type="checkbox"/> Video/Audio
<input type="checkbox"/> Business	<input type="checkbox"/> General Interest	<input type="checkbox"/> Remote Access	<input type="checkbox"/> VoIP
<input type="checkbox"/> Cloud IT	<input type="checkbox"/> Mobile	<input type="checkbox"/> Social Media	<input type="checkbox"/> Web Client
<input type="checkbox"/> Collaboration	<input type="checkbox"/> Network Service	<input type="checkbox"/> Storage Backup	<input checked="" type="checkbox"/> Unknown Applications
<input type="checkbox"/> Email	<input type="checkbox"/> P2P	<input type="checkbox"/> Update	

**Application Overrides**

+ Add Signatures   Edit Parameters   Delete

Application Signature	Category	Action
Dailymotion	Video/Audio	Monitor

**Filter Overrides**

+ Add Filter   Edit   Delete

Filter Details	Action
Behavior: Excessive-Bandwidth	Block

Response:

- A. Dailymotion will be blocked, as the Video/Audio category is blocked.
- B. Dailymotion will be allowed, based on application overrides.
- C. Dailymotion will be blocked, based on filter overrides.
- D. Dailymotion will be allowed only if the action for Dailymotion is set to authenticate in application overrides.

**Answer: B**

**Question: 8**

What statement describes what DNS64 does?

Response:

- A. Converts DNS A record lookups to AAAA record lookups.
- B. Translates the destination IPv6 address of the DNS traffic to an IPv4 address.
- C. Synthesizes DNS AAAA records from A records.
- D. Translates the destination IPv4 address of the DNS traffic to an IPv6 address.

---

**Answer:**

---

---

**Question: 9**

---

What information is flushed when the chunk-size value is changed in the config dlp settings?

Response:

- A. The database for DLP document fingerprinting
- B. The supported file types in the DLP filters
- C. The archived files and messages
- D. The file name patterns in the DLP filters

---

**Answer: A**

---

---

**Question: 10**

---

What step is required to configure an SSL VPN to access to an internal server using port forward mode?

Response:

- A. Configure the virtual IP addresses to be assigned to the SSL VPN users.
- B. Install FortiClient SSL VPN client
- C. Create a SSL VPN realm reserved for clients using port forward mode.
- D. Configure the client application to forward IP traffic to a Java applet proxy.

---

**Answer: D**

---

---

**Question: 11**

---

Examine the partial output from the diagnose sys session list CLI command. What does this output state?

Response:

- A. proto\_state=05 is the TCP state.
- B. proto\_state=05 is the UDP state.
- C. proto\_state=05 is the ICMP state.
- D. timeout=3600 reflects the maximum length of time a session can be opened.

---

**Answer: A**

---

---

**Question: 12**

---

Which statement about firewall policy NAT is true?

Response:

- A. DNAT is not supported.
- B. DNAT can automatically apply to multiple firewall policies, based on DNAT rules.
- C. You must configure SNAT for each firewall policy.
- D. SNAT can automatically apply to multiple firewall policies, based on SNAT rules.

---

**Answer: C**

---

---

**Question: 13**

---

Which statements are true regarding firewall policy NAT using the Outgoing Interface Address with Fixed Port disabled?

(Choose two.)

Response:

- A. Source IP is translated to outgoing interface IP
- B. Port address translation is not used
- C. This is known as many-to-one NAT.
- D. Connections are tracked using source port and source MAC address.

---

**Answer: AC**

---

---

**Question: 14**

---

Which statements are true regarding blocking botnet command and control traffic?

(Choose two.)

Response:

- A. DNS lookups are checked against the Botnet Command and Control database.
- B. The botnet command and control domains can be enabled on the web filter profile
- C. This service requires a FortiGuard web filtering license.
- D. The Botnet Command and Control database cannot be downloaded -it's only available on FortiGuard servers.

---

**Answer: AC**

---

---

**Question: 15**

---

What methods can be used to deliver the token code to a user who is configured to use two-factor

authentication?

(Choose three.)

Response:

- A. SMS text message
- B. Instant message app
- C. Voicemail message
- D. Email
- E. FortiToken

---

**Answer: ADE**

---

CertKillers.net

## Thank You for trying NSE4\_FGT-5.6 PDF Demo

To Buy Latest NSE4\_FGT-5.6 Full Version Download visit link below

[https://www.certkillers.net/Exam/NSE4\\_FGT-5.6](https://www.certkillers.net/Exam/NSE4_FGT-5.6)

## Start Your NSE4\_FGT-5.6 Preparation

**[Limited Time Offer]** Use Coupon “CKNET” for Further discount on your purchase. Test your NSE4\_FGT-5.6 preparation with actual exam questions.

<https://www.certkillers.net>