



NSE4-5.4^{Q&As}

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Pass Fortinet NSE4-5.4 Exam with 100% Guarantee

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

<https://www.passapply.com/nse4-5-4.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

By default, the Intrusion Protection System (IPS) on a FortiGate unit is set to perform which action?

- A. Block all network attacks.
- B. Block the most common network attacks.
- C. Allows all traffic
- D. Allow and log all traffic

Correct Answer: C

QUESTION 2

An administrator sets up a new FTP server on TCP port 2121. A FortiGate unit is located between the FTP clients and the server. The administrator has created a policy for TCP port 2121. Users have been complaining that when

downloading data they receive a 200 Port command successful message followed by a 425 Cannot build data connection message.

Which of the following statements represents the best solution to this problem?

- A. Create a new session helper for the FTP service monitoring port 2121.
- B. Enable the ANY service in the firewall policies for both incoming and outgoing traffic.
- C. Place the client and server interface in the same zone and enable intra-zone traffic.
- D. Disable any protection profiles being applied to FTP traffic.

Correct Answer: A

QUESTION 3

Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (Choose three)

- A. Irix
- B. QNIX
- C. Linux
- D. Mac OS
- E. BSD

Correct Answer: CDE



QUESTION 4

Which of the following are possible actions for static URL filtering? (Choose three.)

- A. Allow
- B. Block
- C. Exempt
- D. Warning
- E. Shape

Correct Answer: ABC

QUESTION 5

Which FSSO agents are required for a FSSO agent-based polling mode solution?

- A. Collector agent and DC agents
- B. Polling agent only
- C. Collector agent only
- D. DC agents only

Correct Answer: A

QUESTION 6

Examine the exhibit shown below then answer the question that follows it.

The screenshot shows the FortiGate configuration interface for 'Edit UTM Proxy Options'. The left sidebar shows the navigation tree with 'Policy' selected. The main area displays 'SSL Inspection Options' with a dropdown menu for 'CA Certificate' set to 'Fortinet_CA_SSLProxy' and an unchecked checkbox for 'Inspect All Ports'. Below this is a table with columns 'Enable', 'Protocol', and 'Inspection Port(s)'. The table contains five rows for different protocols: HTTPS (checked, port 443), SMTPS (unchecked, port 465), POP3S (unchecked, port 995), IMAPS (unchecked, port 993), and FTPS (unchecked, port 990).

Enable	Protocol	Inspection Port(s)
<input checked="" type="checkbox"/>	HTTPS	443
<input type="checkbox"/>	SMTPS	465
<input type="checkbox"/>	POP3S	995
<input type="checkbox"/>	IMAPS	993
<input type="checkbox"/>	FTPS	990

Within the UTM Proxy Options, the CA certificate Fortinet_CA_SSLProxy defines which of the following:

- A. FortiGate unit's encryption certificate used by the SSL proxy.



- B. FortiGate unit's signing certificate used by the SSL proxy.
- C. FortiGuard's signing certificate used by the SSL proxy.
- D. FortiGuard's encryption certificate used by the SSL proxy.

Correct Answer: A

QUESTION 7

What FortiGate configuration is required to actively prompt users for credentials?

- A. You must enable one or more protocols that support active authentication on a firewall policy.
- B. You must assign users to a group for active authentication.
- C. You must place the firewall policy for active authentication before a firewall policy for passive authentication.
- D. You must enable the Authentication setting on the firewall policy.

Correct Answer: B

QUESTION 8

Identify the statement which correctly describes the output of the following command:

```
diagnose ips anomaly list
```

- A. Lists the configured DoS policy.
- B. List the real-time counters for the configured DoS policy.
- C. Lists the errors captured when compiling the DoS policy.
- D. Lists the IPS signature matches.

Correct Answer: B

QUESTION 9

A network administrator needs to implement dynamic route redundancy between a FortiGate unit located in a remote office and a FortiGate unit located in the central office.

The remote office accesses central resources using IPSec VPN tunnels through two different Internet providers.

What is the best method for allowing the remote office access to the resources through the FortiGate unit used at the central office?

- A. Use two or more route-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
- B. Use two or more policy-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.



- C. Use route-based VPNs on the central office FortiGate unit to advertise routes with a dynamic routing protocol and use a policy-based VPN on the remote office with two or more static default routes.
- D. Dynamic routing protocols cannot be used over IPSec VPN tunnels.

Correct Answer: A

QUESTION 10

What configuration objects are automatically added when using the FortiGate's FortiClient VPN Configurations Wizard?(Choose two)

- A. Static route
- B. Phase 1
- C. Users group
- D. Phase 2

Correct Answer: BD

QUESTION 11

An administrator has created a custom IPS signature. Where does the custom IPS signature have to be applied?

- A. In an IPS sensor
- B. In an interface.
- C. In a DoS policy.
- D. In an application control profile.

Correct Answer: A

QUESTION 12

What actions are possible with Application Control? (Choose three.)

- A. Warn
- B. Allow
- C. Block
- D. Traffic Shaping
- E. Quarantine

Correct Answer: BCD



QUESTION 13

Review the output of the command `get router info routing-table all` shown in the Exhibit below; then answer the question following it.

```
STUDENT # 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 10.200.1.254, port1
      [10/0] via 10.200.2.254, port2, [5/0]
C    10.0.1.0/24 is directly connected, port3
O    10.0.2.0/24 [110/101] via 172.16.2.1, Remote_1, 00:00:21
      [110/101] via 172.16.2.2, Remote_2, 00:00:21
C    10.200.1.0/24 is directly connected, port1
C    10.200.2.0/24 is directly connected, port2
C    172.16.1.1/32 is directly connected, Remote_1
C    172.16.1.2/32 is directly connected, Remote_2
C    172.16.2.1/32 is directly connected, Remote_1
C    172.16.2.2/32 is directly connected, Remote_2
```

Which one of the following statements correctly describes this output?

- A. The two routes to the 10.0.2.0/24 subnet are ECMP routes and traffic will be load balanced based on the configured ECMP settings.
- B. The route to the 10.0.2.0/24 subnet via interface Remote_1 is the active and the route via Remote_2 is the backup.
- C. OSPF does not support ECMP therefore only the first route to subnet 10.0.1.0/24 is used.
- D. 172.16.2.1 is the preferred gateway for subnet 10.0.2.0/24.

Correct Answer: A

QUESTION 14

Which of the following features could be used by an administrator to block FTP uploads while still allowing FTP downloads?

- A. Anti-Virus File-Type Blocking
- B. Data Leak Prevention
- C. Network Admission Control
- D. FortiClient Check

Correct Answer: B

**QUESTION 15**

The exhibit shows a FortiGate routing table. Which of the following statements are correct? (Choose two)

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default
O*E2  0.0.0.0/0 [110/10] via 192.168.11.254, wan1, 01:29:24
C      172.16.78.0/24 is directly connected, wan2
O      192.168.1.0/24 [110/200] via 192.168.11.59, internal, 01:30:28
C      192.168.3.0/24 is directly connected, dmz
C      192.168.11.0/24 is directly connected, internal
```

- A. There is only one active default route.
- B. The distance values for the route to 192.168.1.0/24 is 200
- C. An IP address in the subnet 172.16.78.0/24 has been assigned to the dmz interface.
- D. The FortiGate will route the traffic to 172.17.1.2 to next hop with the IP address 192.168.11.254

Correct Answer: AD

[Latest NSE4-5.4 Dumps](#)

[NSE4-5.4 VCE Dumps](#)

[NSE4-5.4 Braindumps](#)