

NSE4_FGT-6.2^{Q&As}

Fortinet NSE 4 - FortiOS 6.2

Pass Fortinet NSE4_FGT-6.2 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse4_fgt-6-2.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

How can you block or allow to Twitter using a firewall policy?

- A. Configure the Destination field as Internet Service objects for Twitter.
- B. Configure the Action field as Learn and select Twitter.
- C. Configure the Service field as Internet Service objects for Twitter.
- D. Configure the Source field as Internet Service objects for Twitter.

Correct Answer: A

QUESTION 2

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

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

Correct Answer: BC

Reference: <https://www.fortinetguru.com/2016/07/configuring-authenticated-access/12/>

QUESTION 3

Which statement about the IP authentication header (AH) used by IPsec is true?

- A. AH does not provide any data integrity or encryption.
- B. AH does not support perfect forward secrecy.
- C. AH provides data integrity but no encryption.
- D. AH provides strong data integrity but weak encryption.

Correct Answer: C

QUESTION 4

What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

- A. Traffic to botnetservers

- B. Traffic to inappropriate web sites
- C. Server information disclosure attacks
- D. Credit card data leaks
- E. SQL injection attacks

Correct Answer: ACE

QUESTION 5

An administrator needs to strengthen the security for SSL VPN access. Which of the following statements are best practices to do so? (Choose three.)

- A. Configure split tunneling for content inspection.
- B. Configure host restrictions by IP or MAC address.
- C. Configure two-factor authentication using security certificates.
- D. Configure SSL offloading to a content processor (FortiASIC).
- E. Configure a client integrity check (host-check).

Correct Answer: CDE

QUESTION 6

An administrator needs to create an SSL-VPN connection for accessing an internal server using the bookmark Port Forward. What step is required for this configuration?

- A. Configure an SSL VPN realm for clients to use the port forward bookmark.
- B. Configure the client application to forward IP traffic through FortiClient.
- C. Configure the virtual IP address to be assigned to the SSL VPN users.
- D. Configure the client application to forward IP traffic to a Java applet proxy.

Correct Answer: D

QUESTION 7

View the exhibit.

Destination ⓘ Subnet Named Address Internet Service 172.13.24.0/255.255.255.0 Interface TunnelB Administrative Distance ⓘ 5 Comments <small>0/255</small> Status ➕ Enabled ➖ Disabled Advanced Options Priority ⓘ 30	Destination ⓘ Subnet Named Address Internet Service 172.13.24.0/255.255.255.0 Interface TunnelA Administrative Distance ⓘ 10 Comments <small>0/255</small> Status ➕ Enabled ➖ Disabled Advanced Options Priority ⓘ 0
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
- D. This is a redundant IPsec setup.

Correct Answer: CD

QUESTION 8

NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

- A. Web filtering
- B. Antivirus
- C. Web proxy
- D. Application control

Correct Answer: B

QUESTION 9

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scope of application control to the browser-based technology category only.
- B. It limits the scope of application control to scan application traffic based on application category only.
- C. It limits the scope of application control to scan application traffic using parent signatures only.

D. It limits the scope of application control to scan application traffic on DNS protocol only.

Correct Answer: B

QUESTION 10

Examine this FortiGate configuration: How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D

QUESTION 11

Which statements about antivirus scanning mode are true? (Choose two.)

- A. In proxy-based inspection mode antivirus buffers the whole file for scanning before sending it to the client.
- B. In flow-based inspection mode, you can use the CLI to configure antivirus profiles to use protocol option profiles.
- C. In proxy-based inspection mode, if a virus is detected, a replacement message may not be displayed immediately.
- D. In quick scan mode, you can configure antivirus profiles to use any of the available signature data bases.

Correct Answer: AB

QUESTION 12

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager
- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

Correct Answer: B

QUESTION 13

Which statement about DLP on FortiGate is true?

- A. It can archive files and messages.
- B. It can be applied to a firewall policy in a flow-based VDOM
- C. Traffic shaping can be applied to DLP sensors.
- D. Files can be sent to FortiSandbox for detecting DLP threats.

Correct Answer: A

QUESTION 14

When using SD-WAN, how do you configure the next-hop gateway address for a member interface so that FortiGate can forward Internet traffic?

- A. It must be configured in a static route using the sdwan virtual interface.
- B. It must be provided in the SD-WAN member interface configuration.
- C. It must be configured in a policy-route using the sdwan virtual interface.
- D. It must be learned automatically through a dynamic routing protocol.

Correct Answer: A

QUESTION 15

Which statements about a One-to-One IP pool are true? (Choose two.)

- A. It is used for destination NAT.
- B. It allows the fixed mapping of an internal address range to an external address range.
- C. It does not use port address translation.
- D. It allows the configuration of ARP replies.

Correct Answer: CD

[Latest NSE4_FGT-6.2 Dumps](#)

[NSE4_FGT-6.2 VCE Dumps](#)

[NSE4_FGT-6.2 Exam Questions](#)