

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.leads4pass.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

Which statement is not correct regarding SSL VPN Tunnel mode?

- A. IP traffic is encapsulated over HTTPS.
- B. The standalone FortiClient SSL VPN client can be used to establish a Tunnel mode SSL VPN.
- C. A limited amount of IP applications are supported.
- D. The FortiGate device will dynamically assign an IP address to the SSL VPN network adapter.

Correct Answer: C

QUESTION 2

Which of the following items does NOT support the Logging feature?

- A. File Filter
- B. Application control
- C. Session timeouts
- D. Administrator activities
- E. Web URL filtering

Correct Answer: C

QUESTION 3

An issue could potentially occur when clicking Connect to start tunnel mode SSL VPN. The tunnel will start up for a few seconds, then shut down. Which of the following statements best describes how to resolve this issue?

- A. This user does not have permission to enable tunnel mode. Make sure that the tunnel mode widget has been added to that user's web portal.
- B. This FortiGate unit may have multiple Internet connections. To avoid this problem, use the appropriate CLI command to bind the SSL VPN connection to the original incoming interface.
- C. Check the SSL adaptor on the host machine. If necessary, uninstall and reinstall the adaptor from the tunnel mode portal.
- D. Make sure that only Internet Explorer is used. All other browsers are unsupported.

Correct Answer: B

QUESTION 4

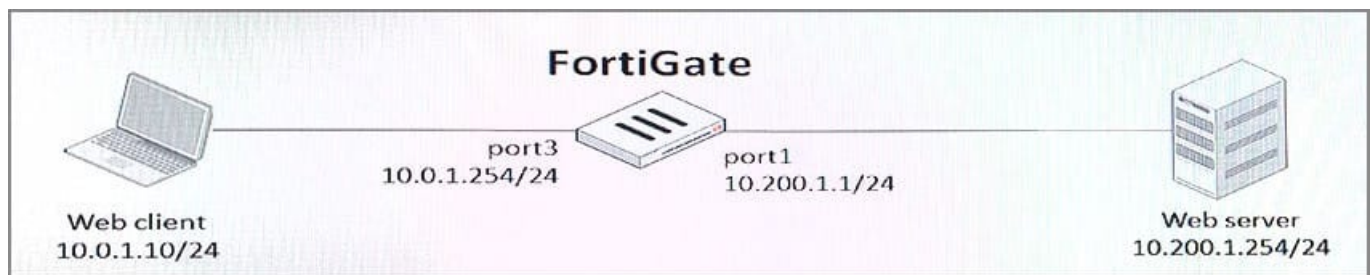
With FSSO, a domain user could authenticate either against the domain controller running the Collector Agent and Domain Controller Agent, or a domain controller running only the Domain Controller Agent. If you attempt to authenticate with the Secondary Domain Controller running only the Domain Controller Agent, which of the following statements are correct? (Select all that apply.)

- A. The login event is sent to the Collector Agent.
- B. The FortiGate unit receives the user information from the Domain Controller Agent of the Secondary Controller.
- C. The Collector Agent performs the DNS lookup for the authenticated client's IP address.
- D. The user cannot be authenticated with the FortiGate device in this manner because each Domain Controller Agent requires a dedicated Collector Agent.

Correct Answer: AC

QUESTION 5

View the exhibit.



The client cannot connect to the HTTP web server. The administrator run the FortiGate built-in sniffer and got the following output:

```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
14.755510 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 868017830
```

What should be done next to troubleshoot the problem?

- A. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10".
- B. Run a sniffer in the web server.
- C. Capture the traffic using an external sniffer connected to port1.
- D. Execute a debug flow.

Correct Answer: B

QUESTION 6

Which TCP states does the global setting `tcp-half-open-timer` applies to? (Choose two.)

- A. SYN SENT
- B. SYN and SYN/ACK
- C. FIN WAIT
- D. TIME WAIT

Correct Answer: AD

QUESTION 7

What information is synchronized between two FortiGate units that belong to the same HA cluster? (Choose three)

- A. IP addresses assigned to DHCP enabled interface.
- B. The master devices hostname.
- C. Routing configured and state.
- D. Reserved HA management interface IP configuration.
- E. Firewall policies and objects.

Correct Answer: ACE

QUESTION 8

A FortiGate 60 unit is configured for your small office. The DMZ interface is connected to a network containing a web server and email server. The Internal interface is connected to a network containing 10 user workstations and the WAN1

interface is connected to your ISP.

You want to configure firewall policies so that your users can send and receive email messages to the email server on the DMZ network. You also want the email server to be able to retrieve email messages from an email server hosted by your ISP using the POP3 protocol.

Which policies must be created for this communication? (Select all that apply.)

- A. Internal > DMZ
- B. DMZ > Internal
- C. Internal > WAN1

D. WAN1 > Internal

E. DMZ > WAN1

F. WAN1 > DMZ

Correct Answer: AE

QUESTION 9

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 10

Review the IPS sensor filter configuration shown in the exhibit

Pattern Based Signatures and Filters

+ Create New ✎ Edit 🗑 Delete				
Severity	Target	OS	Action	Packet Logging
Critical	Server	Linux	Block	

Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

A. It does not log attacks targeting Linux servers.

B. It matches all traffic to Linux servers.

C. Its action will block traffic matching these signatures.

D. It only takes effect when the sensor is applied to a policy.

Correct Answer: CD

QUESTION 11

You are the administrator in charge of a FortiGate unit which acts as a VPN gateway.

You have chosen to use Interface Mode when configuring the VPN tunnel and you want users from either side to be able to initiate new sessions.

There is only 1 subnet at either end and the FortiGate unit already has a default route.

Which of the following configuration steps are required to achieve these objectives? (Select all that apply.)

- A. Create one firewall policy.
- B. Create two firewall policies.
- C. Add a route for the remote subnet.
- D. Add a route for incoming traffic.
- E. Create a phase 1 definition.
- F. Create a phase 2 definition.

Correct Answer: BCEF

QUESTION 12

Which of the following products is designed to manage multiple FortiGate devices?

- A. FortiGate device
- B. FortiAnalyzer device
- C. FortiClient device
- D. FortiManager device
- E. FortiMail device
- F. FortiBridge device

Correct Answer: D

QUESTION 13

Which authentication scheme is not supported by the RADIUS implementation on FortiGate?

- A. CHAP
- B. MSCHAP2
- C. PAP

D. FSSO

Correct Answer: D

QUESTION 14

Which changes to IPS will reduce resource usage and improve performance? (Choose three)

- A. In custom signature, remove unnecessary keywords to reduce how far into the signature tree that FortiGate must compare in order to determine whether the packet matches.
- B. In IPS sensors, disable signatures and rate based statistics (anomaly detection) for protocols, applications and traffic directions that are not relevant.
- C. In IPS filters, switch from '\\Advanced\\' to '\\Basic\\' to apply only the most essential signatures.
- D. In firewall policies where IPS is not needed, disable IPS.
- E. In firewall policies where IPS is used, enable session start logs.

Correct Answer: ABD

QUESTION 15

Which of the following statements are true regarding traffic accelerated by an NP processor? (Choose two.)

- A. TCP SYN packets are always handled by the NP Processor
- B. The initial packets go to the NP Processor, where a decision is taken on if the session can be offloaded or not.
- C. Packets for a session termination are always handled by the CPU.
- D. The initial packets go to the CPU, where a decision is taken on if the session can be offloaded or not.

Correct Answer: AD

[Latest NSE4-5.4 Dumps](#)

[NSE4-5.4 VCE Dumps](#)

[NSE4-5.4 Exam Questions](#)