



## **Fortinet**

### **Exam Questions NSE4\_FGT-6.4**

Fortinet NSE 4 - FortiOS 6.4

#### NEW QUESTION 1

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.

**Answer: C**

#### NEW QUESTION 2

Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

- A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
- B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
- C. Virtual IP addresses are used to distinguish between cluster members.
- D. The primary device in the cluster is always assigned IP address 169.254.0.1.

**Answer: AB**

#### NEW QUESTION 3

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

- A. To delete intermediary NAT devices in the tunnel path.
- B. To dynamically change phase 1 negotiation mode aggressive mode.
- C. To encapsulation ESP packets in UDP packets using port 4500.
- D. To force a new DH exchange with each phase 2 rekey.

**Answer: AC**

#### NEW QUESTION 4

Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

- A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
- B. An SA never expires.
- C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
- D. Phase 2 SA expiration can be time-based, volume-based, or both.
- E. Both the phase 1 SA and phase 2 SA are bidirectional.

**Answer: BCD**

#### NEW QUESTION 5

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

**Answer: C**

#### NEW QUESTION 6

Examine this FortiGate configuration:

Examine the output of the following debug command:

Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

- A. It is allowed, but with no inspection
- B. It is allowed and inspected as long as the inspection is flow based
- C. It is dropped.
- D. It is allowed and inspected, as long as the only inspection required is antivirus.

**Answer: C**

#### NEW QUESTION 7

Which of the following statements correctly describes FortiGate's route lookup behavior when searching for a suitable gateway? (Choose two)

- A. Lookup is done on the first packet from the session originator
- B. Lookup is done on the last packet sent from the responder
- C. Lookup is done on every packet, regardless of direction
- D. Lookup is done on the trust reply packet from the responder

**Answer: AD**

#### NEW QUESTION 8

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

**Answer:** A

#### NEW QUESTION 9

Which of the following statements is true about SSL VPN web mode?

- A. The tunnel is up while the client is connected.
- B. It supports a limited number of protocols.
- C. The external network application sends data through the VPN.
- D. It assigns a virtual IP address to the client.

**Answer:** C

#### NEW QUESTION 10

Refer to the exhibit.

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

- A. Custom permission for Network
- B. Read/Write permission for Log & Report
- C. CLI diagnostics commands permission
- D. Read/Write permission for Firewall

**Answer:** A

#### NEW QUESTION 10

Refer to the exhibit showing a debug flow output.

Which two statements about the debug flow output are correct? (Choose two.)

- A. The debug flow is of ICMP traffic.
- B. A firewall policy allowed the connection.
- C. A new traffic session is created.
- D. The default route is required to receive a reply.

**Answer:** B

#### NEW QUESTION 13

Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

- A. The public key of the web server certificate must be installed on the browser.
- B. The web-server certificate must be installed on the browser.
- C. The CA certificate that signed the web-server certificate must be installed on the browser.
- D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

**Answer:** C

#### NEW QUESTION 16

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check.

**Answer:** D

#### NEW QUESTION 17

An administrator is running the following sniffer command:

Which three pieces of information will be included in the sniffer output? (Choose three.)

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

**Answer:**

BCE

#### NEW QUESTION 21

Refer to the exhibit.

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack.
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

**Answer: C**

#### NEW QUESTION 25

Examine the following web filtering log.

Which statement about the log message is true?

- A. The action for the category Games is set to block.
- B. The usage quota for the IP address 10.0.1.10 has expired
- C. The name of the applied web filter profile is default.
- D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

**Answer: C**

#### NEW QUESTION 30

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. The collector agent uses a Windows API to query DCs for user logins.
- B. NetAPI polling can increase bandwidth usage in large networks.
- C. The collector agent must search security event logs.
- D. The NetSessionEnum function is used to track user logouts.

**Answer: A**

#### NEW QUESTION 33

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

- A. The Services field prevents SNAT and DNAT from being combined in the same policy.
- B. The Services field is used when you need to bundle several VIPs into VIP groups.
- C. The Services field removes the requirement to create multiple VIPs for different services.
- D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

**Answer: C**

#### NEW QUESTION 37

Refer to the exhibits.

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook.

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

- A. The SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

**Answer: A**

#### NEW QUESTION 40

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuard update servers
- C. Operating mode
- D. NGFW mode

**Answer:** AD

#### NEW QUESTION 44

Examine the two static routes shown in the exhibit, then answer the following question.

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

- A. FortiGate will load balance all traffic across both routes.
- B. FortiGate will use the port1 route as the primary candidate.
- C. FortiGate will route twice as much traffic to the port2 route
- D. FortiGate will only activate the port1 route in the routing table

**Answer:** B

#### Explanation:

"If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path."

#### NEW QUESTION 47

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE4\_FGT-6.4 Practice Exam Features:

- \* NSE4\_FGT-6.4 Questions and Answers Updated Frequently
- \* NSE4\_FGT-6.4 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE4\_FGT-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE4\_FGT-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
[Order The NSE4\\_FGT-6.4 Practice Test Here](#)