

NSE4_FGT-6.4^{Q&As}

Fortinet NSE 4 - FortiOS 6.4





Pass Fortinet NSE4_FGT-6.4 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse4_fgt-6-4.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

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.

Correct Answer: B

QUESTION 2

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

- A. IP address
- B. Once Internet Service is selected, no other object can be added
- C. User or User Group
- D. FQDN address

Correct Answer: B

Reference: <https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-inpolicy>

QUESTION 3

Refer to the exhibit.

The diagram shows two FortiGate devices connected via the Internet. HQ-FortiGate (left) has port1 with IP 10.10.100.10. Remote-FortiGate (right) has port2 with IP 10.10.200.10. Below are screenshots of their IPsec configurations.

HQ-FortiGate Configuration

Network
 IP Version: IPv4
 Remote Gateway: Static IP Address
 IP Address: 10.10.200.10
 Interface: port1
 Local Gateway:
 Mode Config:
 NAT Traversal: Enable
 Keepalive Frequency: 10
 Dead Peer Detection: Disable On Idle
 Forward Error Correction: Egress Ingress

Authentication
 Method: Pre-shared Key
 Pre-shared Key: [REDACTED]

IKE
 Version: 1 2
 Mode: Aggressive Main (ID protection)

Peer Options
 Accept Types: Any peer ID

Phase 1 Proposal
 Add
 Encryption: AES128 Authentication: SHA1
 Encryption: AES256 Authentication: SHA256
 Diffie-Hellman Group: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1
 Key Lifetime (seconds): 86400
 Local ID: [REDACTED]

Remote-FortiGate Configuration

Network
 IP Version: IPv4
 Remote Gateway: Static IP Address
 IP Address: 10.10.100.10
 Interface: port1
 Local Gateway:
 Mode Config:
 NAT Traversal: Enable
 Keepalive Frequency: 10
 Dead Peer Detection: Disable On Idle On Demand
 Forward Error Correction: Egress Ingress

Authentication
 Method: Pre-shared Key
 Pre-shared Key: [REDACTED]

IKE
 Version: 1 2
 Mode: Aggressive Main (ID protection)

Phase 1 Proposal
 Add
 Encryption: AES256 Authentication: SHA256
 Diffie-Hellman Group: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1
 Key Lifetime (seconds): 86400
 Local ID: [REDACTED]

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the preshared key on both FortiGate devices to make sure they match.

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to Main (ID protection).
- B. On both FortiGate devices, set Dead Peer Detection to On Demand.
- C. On HQ-FortiGate, disable Diffie-Helman group 2.
- D. On Remote-FortiGate, set port2 as Interface.

Correct Answer: AD

QUESTION 4

An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value.

Which timeout option should be configured on FortiGate?

- A. auth-on-demand
- B. soft-timeout
- C. idle-timeout
- D. new-session
- E. hard-timeout

Correct Answer: E

QUESTION 5

Refer to the exhibits.



The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

- A. Change the SSL VPN port on the client.
- B. Change the Server IP address.
- C. Change the idle-timeout.
- D. Change the SSL VPN portal to the tunnel.

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494>

[Latest NSE4_FGT-6.4 Dumps](#)

[NSE4_FGT-6.4 PDF Dumps](#)

[NSE4_FGT-6.4 Practice Test](#)