Fortinet NSE4_FGT-5.6 Exam

Volume: 114 Questions

Question: 1
Which remote device's logs can you display in the FortiGate GUI by configuring the log setting's GUI Preferences?

A. Disk

B. FortiAnalyzer

C. Syslog

D. FortiSIEM

Answer: B

Question: 2
Which of the following statements about the FortiGate application control database are true? (Choose two.)

A. The application control database uses TCP port 53 for downloads.

B. The application control database uses a hierarchical structure to organize application signatures.

C. The application control database is part of the IPS signatures database.

D. The application control database updates are included in the free FortiGuard service.

Answer: B,D

Question: 3
Which statements are true regarding active authentication? (Choose two.)

A. Active authentication prompts the user for login credentials.

B. Active authentication is always used before passive authentication.

C. The firewall policy must allow the HTTP, HTTPS, FTP, and/or Telnet protocols.

D. Enabling authentication on a policy always enforces active authentication.

Answer: A,C

Question: 4
Which of the following statements about application control profile mode are true? (Choose two.)

A. It can be configured in either flow-based profile-based or proxy-based FortiOS inspection mode.

B. It cannot be used in conjunction with IPS scanning.

C. It uses flow-based scanning techniques, regardless of the inspection mode used.

D. It can scan only unsecure protocols.

Answer: A,C

Question: 5
Examine the exhibit, which shows a FortiGate device with two VDOMs: VDOM1 and VDOM2. Both VDOMs are operating in NAT/route mode. The subnet 10.0.1.0/24 is connected to VDOM1.
The subnet 10.0.2.0/24 is connected to VDOM2. There is an inter-VDOM link between VDOM1 and VDOM2.
What is required in the FortiGate configuration to route traffic between both subnets through an inter-VDOM link?
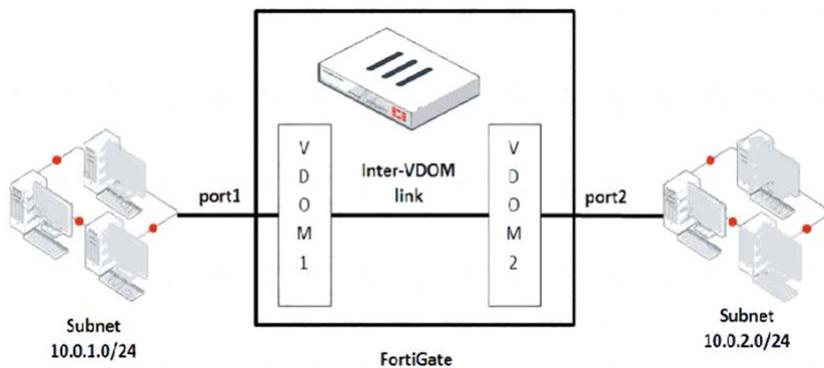
A. A firewall policy in VDOM1 to allow the traffic from 10.0.1.0/24 to 10.0.2.0/24 with port1 as the source interface and port2 as the destination interface.

B. A static route in VDOM1 for the destination subnet of 10.0.1.0/24.

C. A static route in VDOM2 with the destination subnet matching the subnet assigned to the

inter-VDOM link.

D. A static route in VDOM2 for the destination subnet 10.0.1.0/24.

Answer: D

Question: 6
What is Diffie Hellman?

A. An algorithm and agreement method for two peers to independently calculate a common private key after sharing only their public keys

B. An algorithm for generating a public and private key

C. An agreement method for authenticating two peers using a pre-shared key

D. An agreement method for negotiating an IKE security association (SA)

Answer: A

Question: 7
Which FortiGate feature sends real-time queries to the FortiGuard Distribution Network (FDN)?

A. Web filtering

B. VPN

C. Antivirus

D. IPS

Answer: A

Question: 8
Which of the following web filtering modes apply to full URL inspection? (Choose two.)

A. Proxy-based

B. DNS-based

C. Policy-based

D. Flow-based

E. IP-based

Answer: A,B

Question: 9
Which statements about FortiGate inspection modes are true? (Choose two.)

A. The default inspection mode is proxy based.

B. Switching from proxy-based mode to flow-based, then back to proxy-based mode, will not result in the original configuration.

C. Proxy-based inspection is not available in VDOMs operating in transparent mode.

D. Flow-based profiles must be manually converted to proxy-based profiles before changing the inspection mode from flow based to proxy based.

Answer: A,C

Question: 10
Which of the following statements are true about route-based IPsec VPNs? (Choose two.)

A. A virtual IPsec interface is automatically created after a phase 1 is added to the configuration

B. They require firewall policies with the Action set to IPsec

C. They support L2TP-over-IPsec tunnels

D. They can be created in transparent mode VDOMs

Answer: A,C

Question: 11
How does FortiGate verify the login credentials of a remote LDAP user?

A. FortiGate sends the user entered credentials to the LDAP server for authentication.

B. FortiGate re-generates the algorithm based on the login credentials and compares it against the algorithm stored on the LDAP server.

C. FortiGate queries its own database for credentials.

D. FortiGate queries the LDAP server for credentials.

Answer: A

Question: 12
An administrator has configured a route-based IPsec VPN between two FortiGates. Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.

B. This VPN cannot be used as part of a hub and spoke topology.

C. The IPsec firewall policies must be placed at the top of the list.

D. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.

Answer: D

Question: 13
Which statement about the firewall policy authentication timeout is true?

A. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this times expires.

B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this times expires.

C. It is an idle timeout. The FortiGate considers a user to be idle if it does not see any packets coming from the user's source MAC address.

D. It is an idle timeout. The FortiGate considers a user to be idle if it does not see any packets coming from the user's source IP.

Answer: D