Vendor: Fortinet

Exam Code:NSE4

Exam Name: Fortinet Network Security Expert 4 Written Exam (400)

Version: Demo

QUESTION 1

Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

A. The source quick mode selector must be an IPv4 address.

B. The destination quick mode selector must be an IPv6 address.

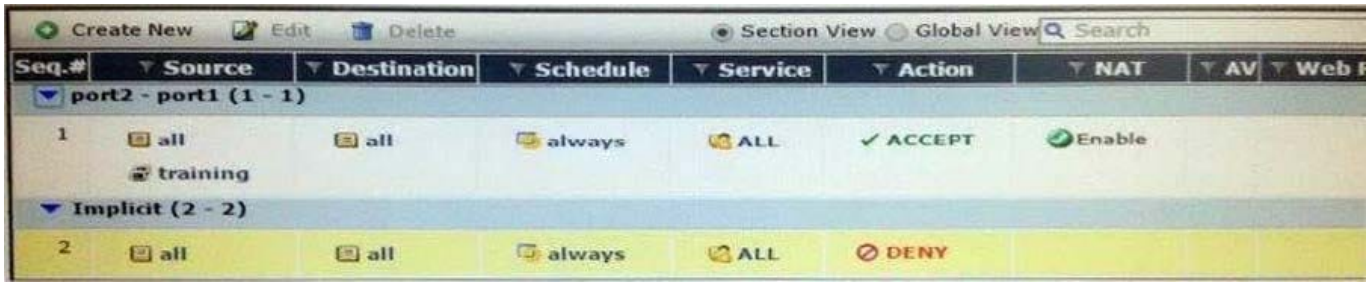
C. The Local Gateway IP must be an IPv4 address.

D. The remote gateway IP must be an IPv6 address.

Correct Answer: BC

QUESTION 2

The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.



Based on the firewall configuration illustrated in the exhibit, which statement is correct?

A. A user that has not authenticated can access the Internet using any protocol that does not trigger an authentication challenge.

B. A user that has not authenticated can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP.

C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access all Internet services.

D. DNS Internet access is always allowed, even for users that have not authenticated.

Correct Answer: D

QUESTION 3

Which best describe the mechanism of a TCP SYN flood?

A. The attacker keeps open many connections with slow data transmission so that other clients cannot start new connections.

B. The attacker sends a packet designed to "sync" with the FortiGate.

C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.

D. The attacker starts many connections, but never acknowledges to fully form them.

Correct Answer: D

QUESTION 4

Which of the following FSSO modes must be used for Novell eDirectory networks?

A. Agentless polling

B. LDAP agent

C. eDirectory agent

D. DC agent

Correct Answer: C

QUESTION 5

Which statement best describes what SSL.root is?

A. The name of the virtual network adapter required in each user\\'s PC for SSL VPN Tunnel mode.

B. The name of a virtual interface in the root VDOM where all the SSL VPN user traffic comes from.

C. A Firewall Address object that contains the IP addresses assigned to SSL VPN users.

D. The virtual interface in the root VDOM that the remote SSL VPN tunnels connect to.

Correct Answer: B

QUESTION 6

You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using routebased mode. Users from either side must be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate already has a default route.

Which two configuration steps are required to achieve these objectives? (Choose two.)

A. Create one firewall policy.

B. Create two firewall policies.

C. Add a route to the remote subnet.

D. Add two IPsec phases 2.

Correct Answer: BC

QUESTION 7

Which of the following statements are true regarding application control? (Choose two.)

A. Application control is based on TCP destination port numbers.

B. Application control is proxy based.

C. Encrypted traffic can be identified by application control.

D. Traffic shaping can be applied to the detected application traffic.

Correct Answer: CD

QUESTION 8

Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic.

What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

A. They are accelerated by hardware in the master unit.

B. They are not accelerated by hardware in the master unit.

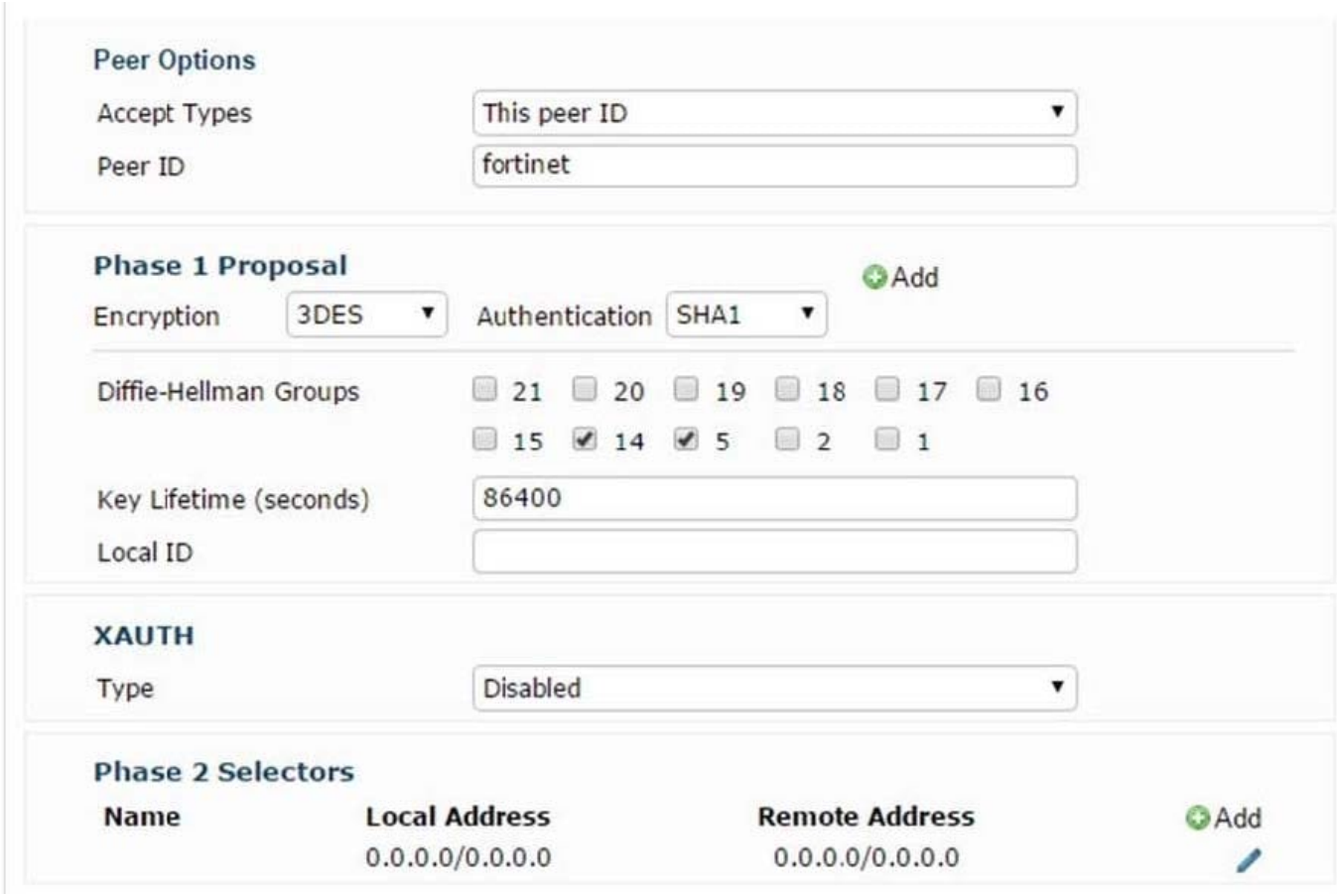
C. They are accelerated by hardware in the slave unit.

D. They are not accelerated by hardware in the slave unit.

Correct Answer: AD

QUESTION 9

Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)



A. The quick mode selector in the remote site must also be 0.0.0.0/0 for the source and destination addresses.

B. Only remote peers with the peer ID \\'fortinet\\' will be able to establish a VPN.

C. The FortiGate device will automatically add a static route to the source quick mode selector address received from each remote VPN peer.

D. The configuration will work only to establish FortiClient-to-FortiGate tunnels. A FortiGate tunnel requires a different configuration.

Correct Answer: CD

QUESTION 10

The exhibit shows a FortiGate routing table.

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default
O*E2  0.0.0.0/0 [110/10] via 192.168.11.254, wan1, 01:29:24
C        172.16.78.0/24 is directly connected, wan2
O        192.168.1.0/24 [110/200] via 192.168.11.59, internal, 01:30:28
C        192.168.3.0/24 is directly connected, dmz
C        192.168.11.0/24 is directly connected, internal
```

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

A. There is only one active default route.

B. The distance values for the route to 192.168.1.0/24 is 200

C. An IP address in the subnet 172.16.78.0/24 has been assigned to the dmz interface.

D. The FortiGate will route the traffic to 172.17.1.2 to next hop with the IP address 192.168.11.254

Correct Answer: AD

QUESTION 11

Which of the following statements are correct regarding logging to memory on a FortiGate unit?

A. When the system has reached its capacity for log messages, the FortiGate unit will stop logging to memory.

B. When the system has reached its capacity for log messages, the FortiGate unit overwrites the oldest messages.

C. If the FortiGate unit is reset or loses power, log entries captured to memory will be lost.

D. None of the above.

Correct Answer: BC

QUESTION 12

Which protocol can an Internet browser use to download the PAC file with the web proxy configuration?

A. HTTPS

B. FTP

C. TFTP

D. HTTP

Correct Answer: D