DUMPSBOSS.

Fortinet NSE 7Enterprise Firewall 7.6 Administrator

Fortinet FCSS_EFW_AD-7.6

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Firewall Policies and Authentication	8
Topic 2, Routing	8
Topic 3, VPN	4
Topic 4, Content Inspection	1
Topic 5, High Availability	2
Total	23

QUESTION NO: 1

Refer to the exhibit, which shows the ADVPN network topology and partial BGP configuration.

Which two parameters must an administrator configure in the config neighbor range for spokes shown in the exhibit? (Choose two.)

A. set max-neighbor-num 2

B. set neighbor-group advpn

C. set route-reflector-client enable

D. set prefix 172.16.1.0 255.255.255.0

ANSWER: B D

Explanation:

`set neighbor-group advpn` is required to associate dynamically learned spoke peers with the predefined BGP neighbor-group. The neighbor-group supplies the common BGP peer settings that the hub must apply when a spoke whose address matches the dynamic range initiates a session. This is particularly important in ADVPN because the hub can accept multiple spoke peers without defining a separate static BGP neighbor entry for every spoke.

`set prefix 172.16.1.0 255.255.255.0` defines the address range from which the hub is permitted to accept those dynamic BGP neighbors. The individual spoke tunnel addresses shown are within that subnet, so the prefix matches the possible spoke BGP source addresses and enables the neighbor-range mechanism to select the `advpn` neighbor-group for them. Together, the prefix identifies eligible dynamic peers and the neighbor-group provides their shared BGP policy and session attributes. Fortinet documents neighbor ranges as the mechanism for dynamically matching BGP peers by prefix and applying a specified neighbor group; see the FortiOS 7.6 CLI reference and the FortiOS 7.6 Administration Guide.

QUESTION NO: 2

Refer to the exhibit, which shows a corporate network and a new remote office network.

An administrator must integrate the new remote office network with the corporate enterprise network.

What must the administrator do to allow routing between the two networks?

A. The administrator must implement BGP to inject the new remote office network into the corporate FortiGate device

B. The administrator must configure a static route to the subnet 192.168.l.0/24 on the corporate FortiGate device.

C. The administrator must configure virtual links on both FortiGate devices.

D. The administrator must implement OSPF over IPsec on both FortiGate devices.

ANSWER: D

Explanation:

The administrator must implement OSPF over IPsec on both FortiGate devices. An IPsec VPN provides the protected Layer-3 transport required to carry traffic and routing-protocol packets across the public Internet between the corporate site and the remote office. With a route-based IPsec tunnel in place, each FortiGate can use the tunnel interface as an OSPF-enabled interface and form an OSPF adjacency with its peer.

Once the adjacency reaches the established state, OSPF exchanges link-state information and installs the learned routes in each FortiGate routing table. The remote office subnet, including 192.168.1.0/24 when it is included in the remote FortiGate OSPF configuration, is then advertised dynamically to the corporate network. Likewise, routes from the corporate OSPF domain can be propagated to the remote office. This approach retains OSPF's automatic route learning and reconvergence behavior while IPsec encrypts the intersite traffic in transit.

FortiGate supports dynamic routing over IPsec tunnel interfaces, and OSPF configuration is applied to the relevant tunnel and local interfaces as part of the routing design. See the FortiGate 7.6 Administration Guide and Fortinet's OSPF over IPsec configuration guidance.