PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7 - Enterprise Firewall 7.2

Fortinet NSE7_EFW-7.2

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Deployment and System Configuration	1
Topic 2, Firewall Policies and Authentication	6
Topic 3, Routing	4
Topic 4, Virtual Private Networks	3
Topic 5, Content Inspection	4
Topic 6, High Availability	2
Topic 7, Diagnostics and Troubleshooting	2
Topic 8, Mix Questions	1
Total	23

QUESTION NO: 1

A FortiGate administrator enables central NAT. An IPv4 firewall policy permits traffic from the internal network to the Internet, but the policy does not provide a source NAT option.

Which configuration must the administrator use to translate the internal source addresses?

A. A central SNAT map matching the internal traffic and egress interface

B. A VIP mapping the internal subnet to the Internet interface address

C. A local-in policy permitting traffic on the Internet interface

D. An IPsec phase 2 selector for the internal subnet

ANSWER: A

Explanation:

When central NAT is enabled, source NAT is configured using central SNAT maps rather than the NAT setting in an IPv4 firewall policy. The central SNAT map must match the relevant source, destination, outgoing interface, and service criteria, and define the required translated address or IP pool. A VIP is used primarily for destination NAT and does not replace a central SNAT map for outbound source translation.

QUESTION NO: 2

A route-based IPsec VPN passes through a NAT device between the FortiGate and the remote peer.

Which two statements about NAT traversal are true? (Choose two.)

A. IKE peers use NAT detection payloads during negotiation.

B. ESP traffic can be encapsulated in UDP port 4500 when NAT is detected.

C. IPsec data traffic is encapsulated in TCP port 443 when NAT is detected.

D. NAT traversal requires ESP to remain unencapsulated as IP protocol 50.

E. NAT traversal can be used only with policy-based IPsec VPNs.

ANSWER: A B

Explanation:

IKE peers use NAT detection payloads during IKE negotiation to determine whether a NAT device exists in the path. When NAT is detected and NAT traversal is used, ESP traffic is encapsulated in UDP port 4500 so that the NAT device can maintain the translation. NAT traversal does not use TCP, and native ESP is not retained across a detected NAT device when UDP encapsulation is required.