PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 4FortiOS 7.6 Administrator

Fortinet NSE4_FGT_AD-7.6

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, FortiGate Security	8
Topic 2, FortiGate Firewall Policies	7
Topic 3, FortiGate Authentication	1
Topic 4, FortiGate VPN	1
Topic 5, FortiGate Routing	3
Topic 6, FortiGate High Availability	3
Total	23

QUESTION NO: 1

An administrator enables central NAT on a FortiGate. Internet-bound traffic that previously used source NAT configured in an IPv4 firewall policy is no longer translated.

What must the administrator configure to restore source NAT for the traffic?

A. A matching central SNAT map for the outbound traffic.

B. A virtual IP that maps the internal subnet to the public address.

C. A firewall policy with the NAT option enabled.

D. A static route that uses the WAN interface as the gateway.

ANSWER: A

Explanation:

A matching central SNAT map is correct because, when central NAT is enabled, source NAT is controlled by central SNAT mappings rather than by the NAT setting in individual IPv4 firewall policies. The central SNAT map must match the relevant source, destination, outgoing interface, and service criteria.

Adding a VIP configures destination NAT, not source NAT for outbound sessions. Enabling a NAT option on the firewall policy does not replace the required central SNAT configuration when central NAT is in use. A static route determines forwarding but does not translate source addresses.

QUESTION NO: 2

An administrator configures a DoS policy to block sources that exceed a TCP SYN flood threshold. A source address is permitted by an IPv4 firewall policy, but its new connections are dropped after it exceeds the configured threshold.

Why does the allow firewall policy not permit the connections?

A. DoS policy processing occurs before regular firewall policy processing

B. The IPv4 firewall policy applies only to established TCP sessions

C. The DoS policy converts the source address into a blocked IP address object

D. The IPv4 firewall policy must use proxy-based inspection mode

ANSWER: A

Explanation:

DoS policy processing occurs before regular firewall policy processing is correct. When the configured anomaly threshold is exceeded, the DoS policy action is applied before traffic can be accepted by a matching IPv4 firewall policy.

The firewall policy permits normal traffic that reaches policy evaluation, but it does not override a matching DoS policy. Changing the policy order or enabling session logging does not bypass the SYN flood protection.