PassQueen
a.k.a dumpsqueen.com

FCP - FortiGate 7.4 Administrator

Fortinet FCP_FGT_AD-7.4

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	6
Topic 2, Firewall Policies and Authentication	10
Topic 3, VPN	1
Topic 4, Content Inspection	2
Topic 5, Routing	4
Total	23

QUESTION NO: 1

An administrator runs flow debug for a client connection and receives the message *Denied by forward policy check*.

What does this message indicate?

A. No matching firewall policy permits the forwarded traffic.

B. No route exists for the packet destination.

C. The IPsec Phase 1 security association has failed.

D. The FortiGuard web-filter rating server is unreachable.

ANSWER: A

Explanation:

The message indicates that FortiGate did not find a firewall policy that permits the forwarded traffic. The administrator should verify the source and destination interfaces, addresses, services, policy order, schedule, and other policy-match criteria.

This message is generated during firewall policy processing. It does not by itself indicate a routing failure, an IPsec Phase 1 failure, or a failed FortiGuard rating lookup.

QUESTION NO: 2

An administrator applies a deep-inspection SSL/SSH inspection profile to an HTTPS firewall policy. Users can reach the websites, but their browsers display certificate warnings for every inspected site. The websites use valid public certificates.

Which action resolves the certificate warnings while retaining deep inspection?

A. Install the FortiGate CA certificate as a trusted root certificate on the client devices.

B. Import each destination website certificate into the FortiGate.

C. Change the firewall policy action from accept to ssl-vpn.

D. Enable NAT on the HTTPS firewall policy.

ANSWER: A

Explanation:

The administrator must install the FortiGate CA certificate as a trusted root certificate on the client devices. During deep inspection, FortiGate decrypts the SSL/TLS session and generates a replacement certificate for the destination site, signed by the configured FortiGate CA certificate. Clients that do not trust this CA report a certificate warning. Certificate inspection would avoid replacement certificates, but it would not provide the same decrypted-content inspection.