PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7 - Zero Trust Access 7.2

Fortinet NSE7_ZTA-7.2

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which two statements are true regarding certificate-based authentication for ZTNA deployment? (Choose two.)

A. FortiGate signs the client certificate submitted by FortiClient.

B. The default action for empty certificates is block

C. Certificate actions can be configured only on the FortiGate CLI

D. Client certificate configuration is a mandatory component for ZTNA

ANSWER: B D

Explanation:

For certificate-based authentication in a ZTNA access-proxy deployment, FortiGate must be configured to request and validate the client certificate presented by FortiClient. This client-certificate configuration establishes the trust relationship used to authenticate the endpoint during the mutual TLS connection, making it a required component when this authentication method is selected. The FortiGate configuration identifies the trusted certificate authority and defines how the access proxy handles client-certificate validation before allowing access to protected applications.

The default handling for an empty certificate is *block*. An empty certificate situation occurs when the client does not present a certificate after FortiGate requests one. Blocking by default supports the Zero Trust principle that an endpoint must provide the expected cryptographic identity before it can access a private application. Administrators can explicitly configure certificate-handling behavior where required, but the secure default prevents an unauthenticated client from gaining access merely because no certificate was supplied.

Fortinet's ZTNA documentation describes the access-proxy model and certificate-based endpoint validation in the FortiGate 7.2 Administration Guide. Additional ZTNA architecture and deployment context is available from Fortinet Zero Trust Access.

QUESTION NO: 2

A ZTNA access proxy virtual host uses a server pool with health monitoring enabled. All server-pool members are marked unhealthy. What is the expected result for a newly authorized client request?

A. FortiGate does not forward the request to an unhealthy pool member

B. FortiGate bypasses the access proxy and connects the client directly to the application

C. FortiGate ignores health status after the client is authorized

D. FortiGate assigns the client a registration VLAN

ANSWER: A

Explanation:

FortiGate does not select a server-pool member that is marked unhealthy. Although the client can satisfy the ZTNA authorization conditions, FortiGate has no eligible backend application server to which it can proxy the request. Changing the ZTNA rule would not restore service while all pool members remain unhealthy.