PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7 - Enterprise Firewall 6.0

Fortinet NSE7_EFW-6.0

Version Demo

Total Demo Questions: 5

Total Premium Questions: 50

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, System Configuration	7
Topic 2, Firewall Policies	11
Topic 3, VPN	5
Topic 4, High Availability	2
Topic 5, Advanced Routing	16
Topic 6, Diagnostics	9
Total	50

QUESTION NO: 1

When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filler web requests when the client browser does not provide the server name indication (SNI) extension ?

A. FortiGate switches to the full SSL inspection method to decrypt the data.

B. FortiGate blocks the request without any further inspection.

C. FortiGate uses the Issued To: field in the server's certificate.

D. FortiGate uses the requested URL from the user's web browser.

ANSWER: C

Explanation:

FortiGate uses the Issued To: field in the server's certificate. Certificate inspection does not decrypt the HTTPS payload; instead, it uses TLS handshake information and the presented server certificate to identify the destination and apply relevant web-filtering decisions. Normally, the Server Name Indication extension in the client hello provides the hostname requested by the browser before the encrypted session is established. When that extension is absent, FortiGate can obtain the hostname from the identity information presented by the server certificate, commonly represented as the certificate subject's Common Name and shown by certificate viewers as the "Issued To" value. This permits FortiGate to continue making domain-based inspection and policy decisions without performing full SSL deep inspection. The certificate-based identity is available during the TLS negotiation, so it is suitable for the certificate-inspection workflow even though the HTTP request contents remain encrypted. Fortinet documents certificate inspection as an SSL/SSH inspection mode that examines certificate and handshake information rather than decrypted application data. See the FortiGate SSL/SSH inspection documentation and Fortinet's technical guidance on identifying HTTPS traffic with SSL inspection.

QUESTION NO: 2

What configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. mem-failopen

B. ips-failopen

C. utm-failopen

D. av-failopen

ANSWER: B D

Explanation:

`ips-failopen` and `av-failopen` are the global FortiGate settings that control the handling of traffic requiring IPS and antivirus content inspection when the firewall enters conserve mode because of memory pressure. Conserve mode protects FortiGate stability by reducing memory consumption, but administrators can explicitly determine whether these inspection engines fail closed, pass traffic without the respective inspection, or use the one-shot behavior when resources are constrained. The `ips-failopen` setting applies that behavior to IPS processing, while `av-failopen` applies it to antivirus processing. These settings are therefore directly relevant to content-inspected sessions during conserve mode and allow an administrator to make an intentional availability-versus-inspection decision for each engine. Fortinet documents conserve mode as a memory-protection mechanism and identifies the related fail-open controls as global configuration settings. For additional operational context, see Fortinet's conserve mode technical tip and the official FortiOS 6.0 documentation.

QUESTION NO: 3

Which statements are correct when SSL deep inspection is applied to HTTPS traffic? (Choose two.)

A. FortiGate presents a substitute certificate to the client.

B. Clients must trust the inspection CA certificate to avoid certificate warnings.

C. FortiGate forwards the server certificate unchanged to the client.

D. HTTPS content remains encrypted and unavailable to security profiles.

E. Deep inspection can be used only with explicit proxy policies.

ANSWER: A B

Explanation:

SSL deep inspection acts as an intermediary between the client and the HTTPS server. FortiGate establishes a separate TLS session to the server and presents the client with a substitute certificate signed by the configured inspection CA certificate.

For client browsers to trust the substituted certificate without certificate warnings, the issuing FortiGate CA certificate must be installed as a trusted CA on the client devices. Deep inspection enables inspection of decrypted content by security profiles, unlike certificate inspection, which examines TLS handshake and certificate information without decrypting the payload. Fortinet describes these inspection modes in the SSL/SSH inspection documentation.

QUESTION NO: 4

An administrator enables central NAT on a FortiGate VDOM. How is source NAT configured for IPv4 firewall policies in that VDOM?

A. Source NAT is configured with central SNAT maps.

B. Source NAT is configured only by enabling NAT in each firewall policy.

C. Source NAT is configured by creating a VIP for every internal client.

D. Source NAT is automatically disabled for all traffic.

ANSWER: A

Explanation:

When central NAT is enabled, source NAT is configured using central SNAT maps instead of the NAT settings in individual IPv4 firewall policies. A central SNAT map can match traffic based on source address, destination address, outgoing interface, and service, and then apply the required source translation. This separates NAT configuration from security-policy configuration.

Fortinet documents central NAT and central SNAT maps in the FortiOS 6.0 Handbook.

QUESTION NO: 5

What is the purpose of an internal segmentation firewall (ISFW)?

A. It is the first line of defense at the network perimeter.

B. It inspects incoming traffic to protect services in the corporate DMZ.

C. It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.

D. It splits the network into multiple security segments to minimize the impact of breaches.

ANSWER: D

Explanation:

An internal segmentation firewall (ISFW) divides an organization's internal network into separate security zones and enforces security policies on traffic moving between those zones. Its primary purpose is to provide segmentation and control east-west traffic, such as communications between user networks, application servers, databases, and other internal resources. By requiring traffic to pass through the ISFW and be evaluated against firewall policies and security inspection profiles, an organization can apply least-privilege access controls between network areas.

This segmentation reduces an attacker's ability to move laterally after gaining an initial foothold. Rather than allowing a compromise in one part of the network to reach all systems freely, the ISFW confines access to only the resources explicitly permitted by policy. This helps minimize the scope and operational impact of a breach, while also improving visibility into internal traffic flows. Fortinet describes internal segmentation as a key component of a Security-Driven Networking architecture for reducing attack surfaces and limiting lateral movement. See Fortinet's Internal Segmentation Firewall overview and its network segmentation guidance.