Fortinet FCP_FGT_AD-7.4 Exam Questions

Total Questions: 250+
Demo Questions: 35
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: FCP_FGT_AD-7.4 Exam Dumps by Cert Empire

Question: 1

Which three methods are used by the collector agent for AD polling? (Choose three.)

A. WMI

B. Novell API

C. WinSecLog

D. NetAPI

E. FortiGate polling

Answer:

A, C, D

Explanation:

The Fortinet Single Sign-On (FSSO) Collector Agent uses three primary methods to poll Active Directory Domain Controllers (DCs) for user logon information. These methods are:
1. WinSecLog: The Collector Agent polls the security event logs on each DC for specific logon event IDs (e.g., 4624, 4768, 4769) to identify user authentications.
2. WMI (Windows Management Instrumentation): The agent uses WMI to query management data and operations on the DCs to gather user logon session information.
3. NetAPI: The agent can use the NetAPI function to poll DCs for active user session information.
These methods enable the Collector Agent to build and maintain a real-time database of user-to-IP address mappings for identity-based policies.

Why Incorrect Options are Wrong:

B. Novell API: This API is for Novell eDirectory, a different directory service, and is not used for polling Microsoft Active Directory.
E. FortiGate polling: This refers to a separate agentless FSSO mode where the FortiGate unit polls DCs directly, not a method used by the Collector Agent itself.

References:

1. Fortinet FortiOS 7.0.0 Administration Guide, Fortinet Single Sign-On FSSO polling modes, Page 1891. The guide states, "The Collector agent polls each DC for user logon events. There are several methods that can be used to poll the DC: WinSecLog, WMI, and NetAPI."
2. Fortinet Single Sign-On 5.0 Administration Guide, Collector agent polling modes Polling the DC, Page 23. This document details the three polling methods: "The Collector agent can poll the security event log of each DC for logon events (WinSecLog).", "The Collector agent can poll user logon session information from the DCs by using WMI.", and "The Collector agent can poll user logon session information from the DCs by using the NetAPI function."

Question: 2

If the Services field is configured in a Virtual IP (VIP), which of the following statements is true when central NAT is used?

A. The Services field removes the requirement of creating multiple VIPs for different services.

B. The Services field is used when several VIPs need to be bundled into VIP groups.

C. The Services field does not allow source NAT and destination NAT to be combined in the same policy.

D. The Services field does not allow multiple sources of traffic, to use multiple services, to connect to a
single computer.

Answer:

A

Explanation:

A Virtual IP (VIP) object in FortiOS is used to perform Destination NAT (DNAT). Within a single VIP object, the port forwarding feature (referred to as the Services field in some contexts) allows an administrator to define multiple port mapping rules. Each rule maps a specific external port and protocol to a corresponding internal port. This functionality consolidates configuration by allowing a single VIP object to handle various services (e.g., HTTP, HTTPS, RDP) destined for the same internal server, thereby eliminating the need to create a separate VIP object for each individual service.

Why Incorrect Options are Wrong:

B. VIP groups are used to bundle multiple, separate VIP objects together, typically for load balancing or policy simplification, not for bundling services within a single VIP.
C. The Services field within a VIP object defines the DNAT port translation; it does not impose any restrictions on whether Source NAT (SNAT) can be applied in the same policy.
D. The Services field explicitly enables traffic for multiple defined services from various sources (as defined in the firewall policy) to connect to a single mapped server.

References:

1. Fortinet FortiOS 7.4.0 Administration Guide:
Section: Firewall objects Virtual IPs Static NAT VIPs
Content: The guide explains the configuration of a VIP with port forwarding enabled. It states, "You can add multiple port forwarding entries to a VIP." This directly confirms that a single VIP can handle multiple services, supporting the correct answer (A). The guide also describes VIP Groups

as collections of VIP objects, which invalidates option B.
2. Fortinet FortiOS 7.4.0 Administration Guide:
Section: Central NAT DNAT & SNAT policies
Content: This section details how to create central NAT policies. It shows that a VIP object is used as the Destination Address for DNAT. The policy configuration allows for a separate IP Pool to be configured for SNAT within the same rule, demonstrating that DNAT and SNAT can be combined, which invalidates option C. The function of the VIP's internal service mapping is independent of this policy structure.

Question: 3

An administrator needs to increase network bandwidth and provide redundancy. What interface type must the administrator select to bind multiple FortiGate interfaces?

A. VLAN interface

B. Software Switch interface

C. Aggregate interface

D. Redundant interface

Answer:

C

Explanation:

An aggregate interface, also known as a Link Aggregation Group (LAG), combines multiple physical FortiGate interfaces into a single logical interface. This configuration uses the Link Aggregation Control Protocol (LACP, IEEE 802.3ad) to load balance traffic across the member interfaces, which effectively increases the total available bandwidth. It also provides redundancy because if one of the physical links in the aggregation fails, traffic is automatically redistributed among the remaining active links, ensuring continuous network connectivity. This interface type is the only option that meets both requirements of increasing bandwidth and providing redundancy simultaneously.

Why Incorrect Options are Wrong:

A. VLAN interface: This is a logical interface for segmenting a network on a single physical port; it does not bind multiple interfaces for bandwidth or redundancy.
B. Software Switch interface: This groups multiple interfaces into a single broadcast domain, functioning like a Layer 2 switch, but it does not aggregate their bandwidth.
D. Redundant interface: This provides link redundancy using an active-standby model. Only one interface is active at a time, so it does not increase bandwidth.

References:

1. Fortinet FortiOS 7.4.0 Administration Guide, "Interfaces Link aggregation (LAG)". Page 299: "A link aggregation group (LAG) combines two or more physical interfaces to work together as a single interface. This increases the bandwidth and provides link redundancy."
2. Fortinet FortiOS 7.4.0 Administration Guide, "Interfaces Redundant interfaces". Page 303: "A redundant interface is a virtual interface that consists of two or more physical interfaces. Only one interface is active at a time... This provides link redundancy, but does not increase the bandwidth."
3. Fortinet FortiOS 7.4.0 Administration Guide, "Interfaces Software switches". Page 305: "A

software switch is a virtual switch that consists of two or more interfaces. All interfaces in the software switch are in the same broadcast domain and can be managed as a single interface."
4. Fortinet FortiOS 7.4.0 Administration Guide, "Interfaces VLANs". Page 296: "A virtual LAN (VLAN) is a logical network that can span across multiple physical LANs. VLANs allow you to segment your network into smaller, more manageable broadcast domains."

Question: 4

Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

A. FG-traffic VDOM

B. Root VDOM

C. Customer VDOM

D. Global VDOM

Answer:

B

Explanation:

When a FortiGate is configured in split-task VDOM mode, its virtual domains are separated into management and traffic-processing roles. By default, the root VDOM is designated as the management VDOM, responsible for all administrative tasks. Joining the Security Fabric is a management-plane function that establishes a trusted connection between a downstream FortiGate and the root of the Fabric. Therefore, the downstream FortiGate must use its designated management VDOM, which is the root VDOM in a split-task configuration, to initiate and maintain the Security Fabric connection.

Why Incorrect Options are Wrong:

A. FG-traffic VDOM: This is a traffic-processing VDOM by design in split-task mode and is not responsible for management functions like joining the Security Fabric.
C. Customer VDOM: This is a generic name for a traffic-processing VDOM, which is isolated from management tasks and cannot be used to join the Fabric.
D. Global VDOM: This is not a standard VDOM type. While global settings can apply to all VDOMs, a specific management VDOM handles the Fabric connection itself.

References:

1. Fortinet FortiOS 7.4.0 Administration Guide, VDOMs Split VDOM mode, p. 1019: "In split VDOM mode, one VDOM is used for management, and the other VDOMs are used for traffic... By default, the root VDOM is the management VDOM." This establishes the root VDOM's role.
2. Fortinet FortiOS 7.4.0 Administration Guide, Security Fabric Security Fabric with VDOMs, p. 111: "When VDOMs are enabled on the downstream FortiGate, the management VDOM is used to join the Security Fabric." This directly links the management VDOM to the Fabric joining process.
3. Fortinet FortiOS 7.2.0 Administration Guide, Security Fabric Security Fabric with VDOMs, p.

109: "The management VDOM is used to join the Security Fabric. The management VDOM must have an IP address, and be able to connect to the upstream FortiGate." This confirms the requirement for the management VDOM to handle the connection.

Question: 5

Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

A. Denial of Service

B. Web application firewall

C. Antivirus

D. Application control

Answer:

B

Explanation:

The FortiGate Web Application Firewall (WAF) is the security feature specifically designed to protect web servers from application-layer attacks. It inspects HTTP and HTTPS traffic for threats targeting web applications, such as SQL injections, cross-site scripting (XSS), and other OWASP Top 10 vulnerabilities. By applying signatures and constraints to web traffic destined for internal servers, the WAF can identify and block malicious requests before they reach the application.

Why Incorrect Options are Wrong:

A. Denial of Service: This feature protects against traffic floods and resource exhaustion attacks, not application-layer code injection attacks like SQL injection.
C. Antivirus: This scans files for known malware signatures. It is not designed to analyze and block malicious code embedded within web application requests.
D. Application control: This feature identifies and manages the use of specific applications on the network but does not inspect the content of allowed traffic for attacks.

References:

1. Fortinet FortiOS 7.0.0 Administration Guide, Security Profiles Web Application Firewall, Page 1218: "The FortiGate web application firewall (WAF) feature examines HTTP and HTTPS traffic for web-based attacks, such as SQL injection and cross-site scripting."
2. Fortinet Cookbook, WAF profile for common web vulnerabilities (5.6), Document Version 1.0: "A WAF profile can be used to protect your web servers from sophisticated attacks, such as... SQL injection, Cross-site scripting, and Generic attacks."
3. Fortinet Product Matrix, FortiGate-FortiWiFi 70F Series Datasheet, Page 2: The datasheet lists "Web Application Firewall" as a core security service provided by the FortiGate platform to protect against web application attacks.

Question: 6

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.

B. By default, the SSL VPN portal requires the installation of a client's certificate.

C. By default, split tunneling is enabled.

D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer:

D

Explanation:

By default, a FortiGate device configures both the SSL VPN portal and the administrative management GUI to listen on the same TCP port, which is 443 for HTTPS. The FortiGate appliance differentiates between administrative access and SSL VPN user access based on the URL path requested by the client's browser. This shared port configuration simplifies firewall policy creation and external access setup, as only a single port needs to be opened for both services on the external-facing interface.

Why Incorrect Options are Wrong:

A. By default, FortiGate does not use WINS servers for name resolution for SSL VPN clients. It uses the DNS servers configured in the FortiGate's system settings.
B. Requiring a client certificate for SSL VPN authentication is a security enhancement that is disabled by default. The default authentication method relies on user credentials.
C. By default, split tunneling is disabled for the full-access portal. This ensures all traffic from the remote client is routed through the FortiGate for complete security inspection.

References:

1. Fortinet FortiOS 7.4 Administration Guide, SSL VPN, Section: SSL VPN settings.
"By default, the SSL VPN daemon runs on port 443. This may conflict with administrative access to the FortiGate on the same port. It is recommended to change the port to 10443 or 4433, or change the administrative access port." This statement confirms that by default, both services use port 443.
2. Fortinet FortiOS 7.4 CLI Reference, vpn ssl settings.
The documentation for the config vpn ssl settings command shows the default value for port is 443 and the default for client-cert is disable.
3. Fortinet FortiOS 7.4 SSL VPN Guide, Portals, Section: Configuring a portal.
The guide details the configuration of SSL VPN portals. The default full-access portal has split-tunneling disabled. The CLI default for set split-tunneling within a portal configuration is

disable.

Question: 7

Consider the topology: Application on a Windows machine --SSL VPN --FGT-- Telnet to Linux server. An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout. The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN. What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

A. Set the maximum session TTL value for the TELNET service object.

B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen
after 90 minutes.

C. Create a new service object for TELNET and set the maximum session TTL.

D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic,
and set the new TELNET service object in the policy.

Answer:

C, D

Explanation:

The most precise and recommended method to resolve this issue without affecting other services is to isolate the configuration change to only the specific traffic flow. This is achieved by creating a new, custom service object specifically for the Telnet traffic that requires a longer session timeout. Then, a new, dedicated firewall policy is created for this specific traffic (SSL VPN users to the Linux server via Telnet) using the new custom service object. By placing this new policy above the existing, more general SSL VPN policy, FortiGate will match the specific Telnet traffic first and apply the longer session timeout, while all other traffic falls through to the original policy with its default settings.

Why Incorrect Options are Wrong:

A. Modifying the predefined TELNET service object is a global change that would affect all firewall policies using this service, violating the requirement not to impact other services.
B. Setting the session TTL on the entire SSL VPN policy would apply the longer timeout to all traffic matching that policy (e.g., HTTP, DNS), not just Telnet, which is an unnecessarily broad change.

References:

1. FortiOS 7.0.1 Administration Guide, Page 448 (Firewall policies): "FortiGate matches traffic to the first policy in the list that meets the criteria. Once a match is found, no other policies are checked. For this reason, you should place more specific policies at the top of the policy list." This supports the strategy in option D of creating a more specific policy and placing it first.
2. FortiOS 7.0.0 CLI Reference, Page 1018 (config firewall service custom): This section details the commands for creating a custom firewall service. Within this configuration context, the set session-ttl command is available. This confirms that a custom service object can be created with a specific session TTL, as described in option C.
3. Fortinet Cookbook (KB), "Changing the session TTL" (FD30062): This document explains the different methods for modifying session TTL. It states, "The session TTL value can be configured globally, per VDOM, in a firewall policy, or in a firewall service." It implicitly supports the best practice of using the most granular method (a custom service within a specific policy) to avoid unintended consequences on other traffic.

Question: 8

Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

A. Subject Key Identifier value

B. SMMIE Capabilities value

C. Subject value

D. Subject Alternative Name value

Answer:

A

Explanation:

FortiGate, like other systems implementing Public Key Infrastructure (PKI), builds and validates certificate chains by linking a certificate to its issuer. This is primarily achieved using the Authority Key Identifier (AKI) and Subject Key Identifier (SKI) extensions. The AKI extension within a signed certificate contains a value that matches the SKI value of the issuing Certificate Authority's (CA) certificate. This direct correspondence allows FortiGate to unambiguously identify the specific issuer certificate and key used for signing, which is essential for constructing the correct chain of trust.

Why Incorrect Options are Wrong:

B. S/MIME Capabilities value: This extension is specific to the S/MIME standard and describes the cryptographic capabilities of an email client, not the issuer-subject relationship in a certificate chain.
C. Subject value: The Subject field identifies the entity to whom the certificate is issued. While the Issuer field of this certificate must match the Subject field of the CA's certificate, the SKI provides a more precise link to the specific key used.
D. Subject Alternative Name value: This extension lists additional identities (like hostnames or IP addresses) for the certificate's subject, but it does not provide any information about the certificate's issuer.

References:

1. Fortinet FortiOS 7.0.1 Handbook - Public Key Infrastructure: In the "Certificate verification" section, it states, "The Authority Key Identifier (AKI) extension in a certificate points to the Subject Key Identifier (SKI) of the certificate that signed it. This allows the FortiGate to build the certificate chain of trust." (p. 21).
2. IETF RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile:

Section 4.2.1.1, "Authority Key Identifier," explains that this extension identifies the public key used to sign a certificate, typically by referencing the issuer's Subject Key Identifier.
Section 4.2.1.2, "Subject Key Identifier," defines this extension as a means of identifying certificates that contain a particular public key, which is then referenced by the AKI of certificates it issues.

Question: 9

Which two statements are true about the Security Fabric rating? (Choose two.)

A. The Security Fabric rating is a free service that comes bundled with all FortiGate devices.

B. Many of the security issues can be fixed immediately by clicking Apply where available.

C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.

D. It provides executive summaries of the four largest areas of security focus.

Answer:

B, C

Explanation:

The Security Fabric rating is a tool designed to assess the security posture and configuration of the entire Security Fabric. This assessment must be initiated from the root FortiGate, as it has the necessary visibility and control over all downstream devices in the fabric. The rating report provides actionable recommendations to improve security. For many of these recommendations, the FortiOS GUI includes an "Apply" button, which allows administrators to implement the suggested fix directly from the report interface, simplifying and accelerating the remediation process.

Why Incorrect Options are Wrong:

A. The Security Fabric rating is a subscription-based service linked to FortiGuard services; it is not a free service that is automatically included with all FortiGate devices. D. The Security Fabric rating provides a summary based on three main pillars: Security Posture, Fabric Coverage, and Optimization, not four distinct areas of security focus.

References:

1. Fortinet FortiOS 7.0.1 Administration Guide, Page 101, "Security Fabric Security Rating": "The Security Rating feature is available on the root FortiGate in the Security Fabric." This supports option C.
2. Fortinet FortiOS 7.0.1 Administration Guide, Page 101, "Security Fabric Security Rating": "The Security Fabric rating is a subscription service that checks your FortiGate for security vulnerabilities and provides recommendations for improvement." This refutes option A.
3. Fortinet FortiOS 7.0.1 Administration Guide, Page 103, "Security Fabric Security Rating Running a report": "For failed checks, you can select Apply to immediately implement the recommended changes." This supports option B.
4. Fortinet FortiOS 7.0.1 Administration Guide, Page 102, "Security Fabric Security Rating": The guide details the scoring breakdown into three categories: "Security Posture", "Fabric Coverage", and "Optimization". This refutes option D.

Question: 10

Which of the following statements correctly describes FortiGates route lookup behavior when searching for a suitable gateway? (Choose two)

A. Lookup is done on the first packet from the session originator

B. Lookup is done on the last packet sent from the responder

C. Lookup is done on every packet, regardless of direction

D. Lookup is done on the first reply packet from the responder

Answer:

A, D

Explanation:

FortiGate is a stateful firewall that establishes a session for new connections. A route lookup is performed on the first packet from the session originator to determine the egress interface and next-hop gateway for the forward path. This information is then stored in a new session table entry. Subsequently, when the first reply packet is received from the responder, a second route lookup is performed for the original source IP address (which is the destination for the reply packet). This confirms the return path and fully populates the session table. All subsequent packets for that session are processed quickly using the established session information, without requiring additional route lookups.

Why Incorrect Options are Wrong:

B. A route lookup is not performed on the last packet; forwarding is based on the already established session table entry.
C. This describes stateless behavior. FortiGate is stateful and uses a session table to avoid resource-intensive lookups for every packet.

References:

1. Fortinet. (2024). FortiGate / FortiOS 7.0.12 / Administration Guide. Fortinet Document Library. In the "Firewall" chapter, section "Life of a packet", the "New session" subsection states: "The FortiGate then does a route lookup to determine the egress interface that it can use to forward the packet to its destination." This directly supports the lookup on the first packet from the originator.
2. Fortinet. (2021). FortiOS Handbook - Firewall for FortiOS 7.0.0. Fortinet Document Library. On page 10, under "Packet flow and session management", the text confirms the process for the initial packet: "When the first packet of a new session arrives...the FortiGate performs a route lookup for the destination address to find the egress interface."
3. The route lookup on the first reply packet is a fundamental aspect of establishing the bidirectional session state. The FortiGate must determine the return path to the originator. This

principle is a core component of the official Fortinet Certified Professional (FCP) curriculum, which explains that the session table stores information for both directions of traffic, and this information is populated by lookups on the initial and reply packets.

Question: 11

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?

A. The administrator can register the same FortiToken on more than one FortiGate.

B. The administrator must use a FortiAuthenticator device.

C. The administrator can use a third-party radius OTP server.

D. The administrator must use the user self-registration server.

Answer:

B

Explanation:

A single FortiToken is associated with a unique seed that can only be registered and synchronized with one authentication server at a time. Therefore, it cannot be registered directly on multiple FortiGate devices simultaneously. To use the same FortiToken across multiple sites, a centralized authentication server is mandatory. FortiAuthenticator is the designated Fortinet solution for this purpose. It acts as a central RADIUS server, manages the FortiToken seeds, and validates OTPs for authentication requests from multiple FortiGate devices, enabling a seamless user experience across different VPN gateways.

Why Incorrect Options are Wrong:

A. A FortiToken's unique seed can only be registered and synchronized with a single FortiGate or central authentication server at a time.
C. While a third-party server could centralize authentication, FortiAuthenticator is the specific, officially supported Fortinet solution for managing FortiTokens across multiple devices.
D. User self-registration is a mechanism for user onboarding and provisioning, not for centralizing the authentication validation process for an existing token.

References:

1. FortiAuthenticator 6.5 Administration Guide, Page 10, "FortiAuthenticator overview": "FortiAuthenticator is the gatekeeper of the Fortinet Security Fabric, providing centralized identity and access management... It is the single point of contact for authenticating users on the network." This establishes its role as a central authentication point.
2. FortiAuthenticator 6.5 Cookbook, "Using FortiAuthenticator as a RADIUS and FortiToken server for FortiGate", Introduction: "This recipe shows how to configure FortiAuthenticator to act as a RADIUS server for remote user authentication, and to provide two-factor authentication using FortiTokens. This allows you to offload authentication from the FortiGate to a central server, which

is useful in a network with multiple FortiGates." This document directly addresses the scenario in the question.
3. FortiOS 7.0 Administration Guide, Page 2198, "RADIUS Servers": This section details how a FortiGate is configured as a RADIUS client to forward authentication requests to an external server, such as a FortiAuthenticator, which would manage the FortiTokens centrally.

Question: 12

Which three statements about security associations (SA) in IPsec are correct? (Choose three.) 136/219

A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.

B. An SA never expires.

C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.

D. Phase 2 SA expiration can be time-based, volume-based, or both.

E. Both the phase 1 SA and phase 2 SA are bidirectional.

Answer:

A, C, D

Explanation:

In an IPsec VPN, the Internet Key Exchange (IKE) protocol establishes Security Associations (SAs). The Phase 1 SA (IKE SA) is a single, bidirectional channel created to authenticate the peers and secure the negotiation of the Phase 2 SAs. The Phase 2 SAs (IPsec SAs) are unidirectional and are used to apply security services, such as encryption and authentication via ESP or AH, to the actual data traffic flowing through the tunnel. To ensure security, Phase 2 SAs have a finite lifetime, which can be configured to expire based on a set time duration, a specific volume of processed data, or whichever of these two limits is reached first.

Why Incorrect Options are Wrong:

B. An SA never expires.
This is incorrect. All SAs have a defined lifetime (time or volume-based) to force re-keying, which is a critical security practice to limit the impact of a compromised key.
E. Both the phase 1 SA and phase 2 SA are bidirectional.
This is incorrect. The Phase 1 (IKE) SA is bidirectional, but the Phase 2 (IPsec) SAs are unidirectional. Two Phase 2 SAs are required for bidirectional data communication.

References:

1. Fortinet FortiOS 7.0 Administration Guide:
In the "IPsec VPN concepts IKE and IPsec Phase 1 and Phase 2" section, it states: "The IKE SA is a bidirectional secure channel... The purpose of IKE phase 2 is to negotiate IPsec SAs to set up the IPsec tunnel. The IPsec SAs are unidirectional... The IPsec SAs handle the encryption and decryption of traffic in the IPsec tunnel." This supports options A and C.
In the "IPsec VPN concepts IKE and IPsec Phase 2 settings" section, it details lifetime settings: "You can define the SA lifetime in seconds, in kilobytes of data processed, or both. The SA

expires when one of these values is reached." This supports option D and refutes B.
2. RFC 4301, Security Architecture for the Internet Protocol:
Section 4.1, "Security Associations": "An SA is unidirectional. That is, it is a security relationship that applies to traffic in one direction... For peer-to-peer communication, two SAs are required, one in each direction." This confirms the unidirectional nature of IPsec (Phase 2) SAs, supporting option C and refuting E.
3. RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2):
Section 1.2, "The IKESA": "An IKESA is a bidirectional entity that is created as the result of an IKESAINIT exchange... All IKE messages are protected by an IKESA." This confirms the bidirectional nature of the IKE (Phase 1) SA, supporting option C.

Question: 13

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.

B. Only secondary FortiGate devices are rebooted.

C. Uninterruptable upgrade is enabled by default.

D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer:

C, D

Explanation:

When upgrading the firmware on a FortiGate active-active (A-A) High Availability (HA) cluster, the process is designed to minimize traffic disruption. The uninterruptible-upgrade feature, which is enabled by default, facilitates this. During the upgrade, the secondary unit is upgraded and rebooted first. While this occurs, the A-A cluster temporarily suspends load balancing and directs all traffic to the primary unit, effectively operating in an active-passive mode. Once the secondary unit is back online, a failover occurs, making it the new primary. The original primary unit is then upgraded. This sequential process ensures that at least one unit is always available to process traffic, but the load balancing function is inactive until the entire cluster has been successfully upgraded and stabilized.

Why Incorrect Options are Wrong:

A. The firmware image is uploaded only to the primary FortiGate, which then automatically synchronizes the image to all secondary units in the cluster.
B. Both the primary and secondary units are rebooted during the upgrade process, but this happens sequentially to prevent a complete service outage.

References:

1. FortiOS Administration Guide 7.0.0, High Availability Upgrading the cluster firmware, Page 193: "You can upgrade the firmware of a FortiGate HA cluster in the same way as upgrading the firmware of a standalone FortiGate. You connect to the primary FortiGate and upload the new firmware image. The firmware is first upgraded on the secondary FortiGate, which reboots. Then the firmware is upgraded on the primary FortiGate, which reboots." This confirms that the upload is only to the primary (invalidating A) and that both units reboot (invalidating B).
2. FortiOS Administration Guide 7.0.0, High Availability Uninterruptible upgrade, Page 194: "By default, uninterruptible upgrade is enabled. When it is enabled, the secondary FortiGate is upgraded first. After it is upgraded and rebooted, a failover occurs and the new primary FortiGate

(old secondary) takes over traffic processing." This confirms that uninterruptible upgrade is enabled by default (validating C).
3. FortiOS CLI Reference 7.0.0, config system ha, Page 1832: The default setting for uninterruptible-upgrade is shown as enable.
4. Fortinet Certified Professional - Network Security Study Guide for FortiOS 7.0, Chapter 11: High Availability, Section: Upgrading the Cluster Firmware: "During the upgrade of an active-active cluster, load balancing is temporarily suspended. All traffic is processed by the primary unit while the subordinate units are being upgraded." This directly confirms that load balancing is temporarily disabled (validating D).

Question: 14

Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

A. Shut down/reboot a downstream FortiGate device.

B. Disable FortiAnalyzer logging for a downstream FortiGate device.

C. Log in to a downstream FortiSwitch device.

D. Ban or unban compromised hosts.

Answer:

A, D

Explanation:

The root FortiGate in a Security Fabric acts as the central management and orchestration point. Two key functions exclusive to the root device are direct administrative control over fabric members and centralized threat response. From the Security Fabric topology on the root FortiGate, an administrator can reboot or shut down a downstream FortiGate. Furthermore, the root FortiGate is responsible for managing the fabric-wide compromised host list, allowing an administrator to ban or unban an IP address across the entire Security Fabric. This centralized command and control is a core aspect of the root FortiGate's role.

Why Incorrect Options are Wrong:

B. Disabling FortiAnalyzer logging is a local configuration on the downstream device itself. You can log in to the downstream FortiGate to change this setting.
C. A FortiSwitch is managed by the FortiGate it is directly connected to via FortiLink. This managing FortiGate could be a downstream device, not necessarily the root.

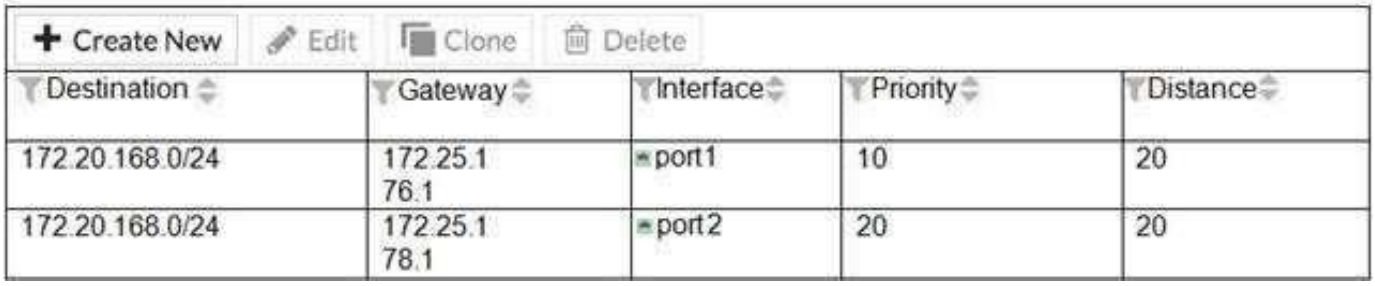
References:

1. FortiOS Administration Guide 7.0.0, Page 1011, "Security Fabric topology": "From the root FortiGate, you can right-click a device in the topology to perform actions, such as logging in to the device, upgrading the firmware, or rebooting the device." This directly supports option A.
2. FortiOS Administration Guide 7.0.0, Page 1043, "Banning an IP address": "When a compromised host is detected, the FortiGate can ban the host's IP address from accessing the network. In the Security Fabric, the root FortiGate shares the banned IP address with the other FortiGates in the Security Fabric." This confirms that managing the banned IP list is a root FortiGate function, supporting option D.
3. FortiOS Administration Guide 7.0.0, Page 833, "Log Settings": This section details that log settings are configured on a per-device basis under the Log & Report menu, demonstrating that this is not an action exclusive to the root FortiGate. This refutes option B.

4. FortiOS Administration Guide 7.0.0, Page 487, "FortiSwitch Manager": The documentation explains that FortiSwitch devices are managed from the FortiGate they are connected to. This management is not exclusive to the root FortiGate in a multi-FortiGate fabric. This refutes option C.

Question: 15

Examine the two static routes shown in the exhibit, then answer the following question.



Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

A. FortiGate will load balance all traffic across both routes.

B. FortiGate will use the port1 route as the primary candidate.

C. FortiGate will route twice as much traffic to the port2 route

D. FortiGate will only actuate the port1 route in the routing table

Answer:

B

Explanation:

FortiGate determines the best path to a destination by evaluating routing protocol attributes in a specific order. It first compares the administrative distance (AD) of all routes to a destination. If multiple routes share the same lowest AD, FortiGate then compares their priority values. A lower priority value is considered more preferable.
In this scenario, both static routes to the 10.0.1.0/24 network have an identical administrative distance of 10. Therefore, the priority value is used as the tie-breaker. The route via port1 has a priority of 100, which is lower than the port2 route's priority of 200. As a result, FortiGate selects the port1 route as the primary and active route.

Why Incorrect Options are Wrong:

A. FortiGate performs Equal-Cost Multi-Path (ECMP) load balancing only when multiple routes to the same destination have identical administrative distance and priority values.
C. This describes unequal cost load balancing, which is not the default behavior. The port2 route is less preferred due to its higher priority and will not be used while the primary is active.
D. While it is true that only the port1 route will be active in the routing table, option B is more precise because it correctly identifies the reason-it is the primary candidate due to its lower priority.

References:

1. Fortinet FortiOS 7.4.1 Administration Guide:
Page 1012, Section "Routing Routing concepts Route selection": "FortiOS builds a routing table from all the active routes from all the routing protocols, and selects the best route to a destination. The best route is the one with the lowest administrative distance. If there are two routes to the same destination with the same administrative distance, the route with the lower priority is selected."
Page 1018, Section "Static routing Advanced static route options Priority": "If two routes have the same distance, the route with the lower priority is chosen. Priority is a number from 0 to 4294967295. The default is 0." This confirms that the lower numerical value for priority is preferred.

Question: 16

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

A. FortiGuard web filter cache

B. FortiGate hostname

C. NTP

D. DNS

Answer:

C, D

Explanation:

In a FortiGate High Availability (HA) cluster, the primary unit synchronizes most of its configuration to all subordinate units to ensure the cluster operates as a single logical device. System-level network services, such as NTP (Network Time Protocol) and DNS (Domain Name System) server settings, are part of this synchronized configuration. This ensures that all cluster members have consistent time and name resolution capabilities, which are critical for logging, updates, and policy enforcement.

Why Incorrect Options are Wrong:

A. FortiGuard web filter cache: This is dynamic runtime data, not a configuration setting. Caches are built independently on each unit as they process traffic and are not synchronized between cluster members.
B. FortiGate hostname: The hostname is a device-specific setting used to uniquely identify each member of the cluster for management purposes. It is explicitly excluded from configuration synchronization.

References:

1. Fortinet FortiOS 7.4.0 Administration Guide, High Availability Configuration synchronization: "The primary unit synchronizes its configuration with all subordinate units... However, some settings are not synchronized because they are specific to the FortiGate, such as the HA priority or the hostname." This confirms that the hostname is not synchronized.
2. Fortinet FortiOS 7.4.0 Administration Guide, High Availability Information synchronized in an HA cluster: "The FortiGuard web filter and spam filter caches are not synchronized." This confirms that the web filter cache is not synchronized.
3. Fortinet FortiOS 7.4.0 Administration Guide, High Availability Configuration synchronization: The guide explains that the running configuration is synchronized, with only specific exceptions listed. config system ntp and config system dns are part of the general system configuration and

are not listed as exceptions, therefore they are synchronized by default.

Question: 17

Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.

B. It is available only on a proxy-based firewall policy.

C. It inspects video files hosted on file sharing services.

D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Answer:

B

Explanation:

Video filtering on a FortiGate requires the firewall to buffer and inspect traffic to identify and categorize video content. This level of inspection is only possible in proxy-based inspection mode. Flow-based inspection, which processes packets as they arrive without significant buffering, does not support the advanced content analysis needed for video filtering. Therefore, to use the video filtering security profile, the corresponding firewall policy must be set to proxy-based inspection mode.

Why Incorrect Options are Wrong:

A. Full SSL Inspection is not required.
This is incorrect because to inspect encrypted video traffic (like YouTube), at least certificate inspection is required. For more granular control, such as by channel ID, full (deep) SSL inspection is mandatory.
C. It inspects video files hosted on file sharing services.
This is incorrect. The FortiGuard video filtering service is designed specifically for major streaming platforms like YouTube, Vimeo, and Dailymotion, not for generic video files on file-sharing sites.
D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.
This is incorrect. Video filtering and web filtering use separate and distinct sets of categories provided by FortiGuard. Video categories are specific to video content (e.g., "Comedy," "Education"), not web page types.

References:

1. Fortinet FortiOS 7.4.0 Administration Guide, Security Profiles Video Filter, Page 1388.
"Video filtering is only available in proxy-based firewall policies." This directly supports the correct answer (B).
"To filter HTTPS traffic, you must also apply a certificate inspection or deep inspection SSL/SSH inspection profile to the policy." This refutes option A, as some form of SSL inspection is always required for HTTPS video.

2. Fortinet FortiOS 7.4.0 Administration Guide, Security Profiles Video Filter FortiGuard categories, Page 1389.
This section lists the specific categories for video filtering, such as "Arts & Culture," "Cars & Vehicles," and "Comedy." A comparison with the Web Filter categories in the same guide (page 1298) shows they are distinct, refuting option D.
3. Fortinet FortiOS 7.4.0 Administration Guide, Security Profiles Video Filter Configuration, Page 1388.
The guide specifies the supported platforms: "FortiGate can use FortiGuard Video Filtering Service to filter videos from YouTube, Vimeo, and Dailymotion." This confirms that the feature is not for general file-sharing services, refuting option C.

Question: 18

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status

B. diagnose sys top

C. get system performance status

D. get system arp

Answer:

D

Explanation:

The get system arp command is used to display the FortiGate's Address Resolution Protocol (ARP) table. The ARP table maps Layer 3 (IP) addresses to their corresponding Layer 2 (MAC) addresses. An IP address conflict occurs when two or more devices on the same network segment are assigned the same IP address. This conflict can be identified by examining the ARP table, where a single IP address might be associated with multiple or flapping MAC addresses. Therefore, this command is a primary tool for troubleshooting such Layer 2 issues.

Why Incorrect Options are Wrong:

A. get system status: This command provides general system information like firmware version, serial number, and license status, not specific Layer 2 networking data.
B. diagnose sys top: This command displays real-time system process and resource utilization (CPU, memory), used for performance troubleshooting, not Layer 2 issues.
C. get system performance status: This command shows a summary of performance statistics, such as active sessions and resource usage, not the ARP table.

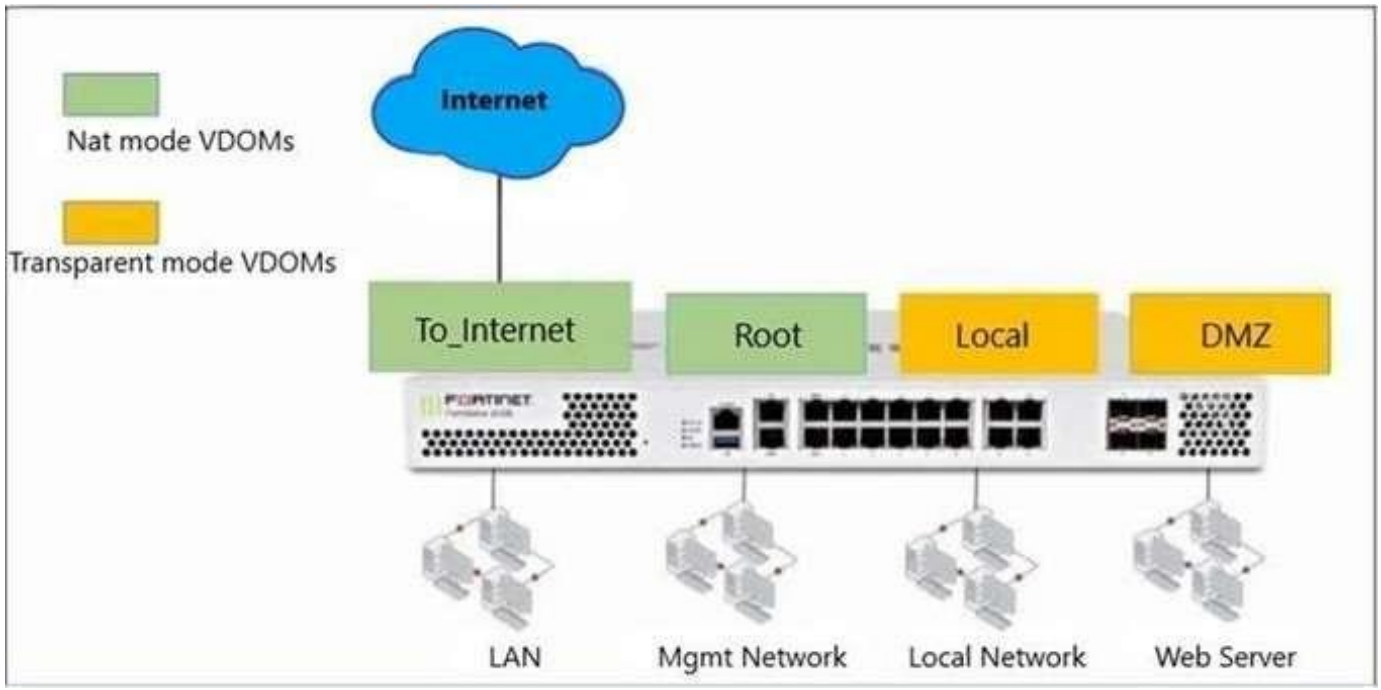
References:

1. Fortinet FortiOS 7.0.1 CLI Reference:
Page 1910, get system arp: The documentation explicitly states this command is used to "Display the system ARP table." The ARP table is fundamental for diagnosing Layer 2 to Layer 3 mapping issues like IP conflicts.
Page 2011, get system status: Described as "Display system status," confirming its use for general information.
Page 1018, diagnose sys top: Described as "Display real-time process information," confirming its use for system performance monitoring.
Page 1986, get system performance status: Described as "Display system performance statistics," confirming its use for high-level performance metrics.

2. Fortinet FortiOS Handbook 7.0.0 - Troubleshooting:
Section: Troubleshooting tools, Page 13: In the context of network troubleshooting, the guide explains, "An IP conflict occurs when two devices on a network are assigned the same IP address... You can use the ARP table on the FortiGate to help identify the conflicting devices." This directly links the troubleshooting of IP conflicts to the use of the ARP table, which is accessed via get system arp.

Question: 19

141/219 Refer to the exhibit.



The Root and ToInternet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode. The Root VDOM is the management VDOM. The ToInternet VDOM allows LAN users to access the internet. The ToInternet VDOM is the only VDOM with internet access and is directly connected to ISP modem. With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.

B. A default static route is not required on the ToInternet VDOM to allow LAN users to access the internet.

C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.

D. Inter-VDOM links are not required between the Root and ToInternet VDOMs because the Root VDOM is used only as a management VDOM.

Answer:

C

Explanation:

Virtual Domains (VDOMs) on a FortiGate are completely separate virtual firewall instances. By design, they are isolated from one another. To permit traffic to flow between any two VDOMs, regardless of their operational mode (NAT or Transparent), an inter-VDOM link must be explicitly configured. This link creates a pair of virtual interfaces, one in each VDOM, effectively creating a

virtual point-to-point connection. Firewall policies can then be applied to these interfaces to control the traffic between the Local and DMZ VDOMs.

Why Incorrect Options are Wrong:

A. An inter-VDOM link is only required if traffic must flow between the Local and Root VDOMs; the scenario does not state this is a requirement.
B. A VDOM in NAT mode, like ToInternet, requires a default static route (0.0.0.0/0) to forward traffic to the internet for destinations not in its routing table.
D. The management VDOM (Root) often requires internet access for services like FortiGuard updates or DNS, which would necessitate an inter-VDOM link to the ToInternet VDOM.

References:

1. Fortinet FortiOS 7.4.0 Administration Guide, Page 1011, Section: Inter-VDOM routing.
The documentation states: "Inter-VDOM routing adds one or more virtual interfaces, called VDOM links, to each VDOM that you want to route between. VDOM links are virtual interfaces that connect VDOMs." This confirms that to pass traffic between any two VDOMs, such as Local and DMZ, these links are the required mechanism.
2. Fortinet FortiOS 7.4.0 Networking Guide, Page 10, Section: Static routing.
The guide explains: "A default route is a type of static route with the destination 0.0.0.0/0.0.0.0. A default route is used when there is no other known route to a destination." This refutes option B, as the ToInternet VDOM needs this to reach the internet.

3. Fortinet FortiOS 7.4.0 Administration Guide, Page 999, Section: Management VDOM.
The guide notes: "The management VDOM is the only VDOM that can communicate with FortiGuard." If the Root VDOM is the management VDOM, it needs a path to the internet to contact FortiGuard, which would require an inter-VDOM link to the ToInternet VDOM, thus invalidating option D.

Question: 20

Which two statements are true when FortiGate is in transparent mode? (Choose two.)

A. By default, all interfaces are part of the same broadcast domain.

B. The existing network IP schema must be changed when installing a transparent mode FortiGate in
the network.

C. Static routes are required to allow traffic to the next hop.

D. FortiGate forwards frames without changing the MAC address.

Answer:

A, D

Explanation:

When a FortiGate is configured in transparent mode, it functions as a Layer 2 bridge or switch. By default, all physical interfaces are placed into a single virtual switch, effectively making them part of the same broadcast domain. In this mode, the FortiGate inspects and forwards Ethernet frames based on their destination MAC address. It does not modify the source or destination MAC addresses of the original frames as they pass through, making its presence on the network "transparent" to other devices. This allows the FortiGate to be inserted into an existing network without requiring any changes to the IP addressing scheme.

Why Incorrect Options are Wrong:

B. The primary advantage of transparent mode is that it can be deployed without altering the existing network's IP address schema, making this statement false.
C. Transparent mode operates at Layer 2, forwarding frames based on a MAC address table. Static routes, a Layer 3 concept, are not required for traffic forwarding through the device.

References:

1. FortiOS Administration Guide 7.0.0, System Operation Mode Transparent mode, Page 218: "In Transparent mode, the FortiGate is installed between the internal network and the router. In this mode, the FortiGate acts as a transparent bridge, forwarding frames without modifying the MAC addresses." This directly supports option D.
2. FortiOS Administration Guide 7.0.0, System Operation Mode Transparent mode, Page 218: "When you install a FortiGate in Transparent mode, you do not have to change the IP addresses of the computers on the private network." This directly refutes option B.
3. FortiOS Administration Guide 7.0.0, System Operation Mode Example: Transparent mode, Page 220: "When you change the operating mode to Transparent, the FortiGate configuration is reset and the FortiGate restarts. All physical interfaces are now part of the default virtual switch,

root." This supports option A, as a virtual switch groups interfaces into a single broadcast domain.
4. FortiOS Administration Guide 7.0.0, System Operation Mode Transparent mode, Page 218: "The FortiGate unit functions like a bridge, and traffic is not routed." This refutes the premise of option C, which implies Layer 3 routing is the primary forwarding mechanism.

Question: 21

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

A. To detect intermediary NAT devices in the tunnel path.

B. To dynamically change phase 1 negotiation mode aggressive mode.

C. To encapsulation ESP packets in UDP packets using port 4500.

D. To force a new DH exchange with each phase 2 rekey

Answer:

A, C

Explanation:

NAT Traversal (NAT-T) in IPsec serves two primary functions as defined in RFC 3947 and RFC 3948. First, it detects the presence of any Network Address Translation (NAT) devices along the path between the two IPsec peers. This is accomplished during the IKE Phase 1 negotiation by exchanging NAT-Discovery (NAT-D) payloads. If a NAT device is detected, the second function is triggered: the IPsec peers switch their communication from UDP port 500 to UDP port 4500. All subsequent ESP packets are then encapsulated within UDP packets. This UDP encapsulation allows the IPsec traffic, which would otherwise be blocked, to traverse the NAT device successfully.

Why Incorrect Options are Wrong:

B. NAT-T is compatible with both main and aggressive modes for Phase 1 negotiation; it does not force a change between them.
D. Forcing a new Diffie-Hellman (DH) exchange during Phase 2 rekeying is a feature known as Perfect Forward Secrecy (PFS), which is independent of NAT traversal.

References:

1. Fortinet FortiOS 7.2.0 Administration Guide:
Section: IPsec VPN NAT traversal
Content: "During IKE negotiation, NAT-T is enabled if both peers support it. The peers detect if there is a NAT device between them. If there is, then after IKE Phase 1 is complete, all further IPsec traffic is encapsulated in UDP on port 4500." This statement directly supports answers A and C.
2. RFC 3947: Negotiation of NAT-Traversal in the IKE:
Section 2.1, Paragraph 1: "The first part of NAT-T is to detect if both IKE peers implement this specification and to detect if NAT is being used between the peers. This is done by exchanging vendor ID payloads and by exchanging NAT-Discovery (NAT-D) payloads." This reference validates option A.

3. RFC 3948: UDP Encapsulation of IPsec ESP Packets:
Abstract: "This document describes a method for encapsulating IPsec ESP packets in UDP. This allows IPsec packets to pass through Network Address Translators (NATs)." This reference validates the core mechanism described in option C.

Question: 22

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.What is the default behavior when the local disk is full?

A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of
95%.

B. No new log is recorded until you manually clear logs from the local disk.

C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of
75%.

D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of
95%.

Answer:

C

Explanation:

By default, when the local disk on a FortiGate device becomes full, it is configured to overwrite the oldest log files to make space for new ones. This behavior is controlled by the diskfull setting, which defaults to overwrite. Additionally, FortiGate is configured to generate a warning event log when the disk usage reaches a specific threshold. The default value for this warning threshold (log-disk-warning-level) is 75%. Therefore, the first warning is issued when usage reaches 75%, and logs continue to be written by overwriting the oldest entries.

Why Incorrect Options are Wrong:

A. The default warning threshold is 75%, not 95%.
B. The default behavior is to overwrite the oldest logs, not to stop recording new logs.
D. Logging does not stop by default, and the warning threshold is 75%, not 95%.

References:

1. FortiOS 7.2.0 Administration Guide, Log settings Disk logging, Page 102:
"Configure the behavior of the FortiGate when the log disk is full. The default is overwrite, which overwrites the oldest logs."
"Configure the log disk warning level. An event log is created when the configured percentage of the disk is used for logs. The default is 75%."
2. FortiOS 7.2.8 CLI Reference, config log disk setting, Page 1581:

Under set diskfull overwrite nolog, the documentation specifies Default: overwrite.
Under set log-disk-warning-level , the documentation specifies Default: 75.

Question: 23

If the Issuer and Subject values are the same in a digital certificate, to which type of entity was the certificate issued?

A. A subordinate CA

B. A root CA

C. A user

D. A CRL

Answer:

B

Explanation:

A digital certificate in which the 'Issuer' and 'Subject' fields contain the same distinguished name is known as a self-signed certificate. In a standard Public Key Infrastructure (PKI) hierarchy, the root Certificate Authority (CA) serves as the ultimate trust anchor. To establish this trust, the root CA authenticates itself by creating and signing its own certificate. This act of self-signing is what results in the Issuer and Subject fields being identical, a defining characteristic of a root CA certificate.

Why Incorrect Options are Wrong:

A. A subordinate CA: A subordinate CA's certificate is issued and signed by a higher-level authority (like a root CA), so its 'Issuer' and 'Subject' fields are different.
C. A user: A user's certificate is issued by a CA. Therefore, the 'Issuer' field contains the CA's name, and the 'Subject' field contains the user's name.
D. A CRL: A Certificate Revocation List (CRL) is a signed list of revoked certificates; it is not a certificate issued to an entity and does not have this structure.

References:

1. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
Section 3.2.7, "Self-Issued Certificate": "A self-issued certificate is a certificate where the issuer and subject are the same entity... A certificate is self-signed if the digital signature can be verified by the public key contained in the certificate." Root CA certificates are self-issued and typically self-signed.
2. Fortinet Documentation, FortiOS 7.0.0 Administration Guide.
Page 610, "Certificates": The guide explains the role of Certificate Authorities (CAs) and the certificates they issue. It describes the FortiGate's ability to act as a CA, which involves creating a

root CA certificate that, by definition, is self-signed with matching Issuer and Subject fields to establish a trust chain.

3. NIST Special Publication 800-32, "Introduction to Public Key Technology and the Federal PKI Infrastructure."

Section 2.1.3, "Certificate Path": "The CA that is at the top of a hierarchy is referred to as the root CA. The root CA issues a certificate for itself; this is called a self-signed certificate." This explicitly states that the root CA's certificate has the same issuer and subject.

Question: 24

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

A. Configure Source IP Pools

B. Configure different SSL VPN realms

C. Configure host check

D. Configure split tunneling in tunnel mode

Answer:

C

Explanation:

Host check is a security feature that enhances SSL VPN access by verifying the security posture of the connecting endpoint. After successful user authentication (including two-factor authentication), FortiGate can check the client device for specific security requirements, such as a running antivirus, a specific OS version, or the presence of a firewall. If the client fails the host check, access is denied. This adds a critical layer of device-level security, ensuring that only compliant and secure devices can connect to the network, thereby strengthening the overall security of the VPN solution.

Why Incorrect Options are Wrong:

A. Configure Source IP Pools: This is a fundamental configuration step required for SSL VPN to function; it assigns IP addresses to clients and is not considered an additional security best practice.
B. Configure different SSL VPN realms: Realms provide customized login portals and access policies for different user groups. While useful for management and segmentation, they do not inherently strengthen the security of the connection itself.
D. Configure split tunneling in tunnel mode: This determines traffic routing. Disabling split tunneling (full tunnel) is often the security best practice, as it forces all client traffic through the FortiGate for inspection. The option is ambiguous and not universally a strengthening measure.

References:

1. Fortinet Training Institute, FortiGate Infrastructure 7.0 Study Guide, "SSL VPN" chapter, "Host Check" section (p. 269): "You can use host check to enhance security. With host check, FortiGate checks the remote client's integrity before allowing the SSL VPN tunnel connection."
2. Fortinet Document Library, FortiOS 7.0.1 Administration Guide, "SSL VPN" chapter, "Host check" section: "You can configure the SSL VPN to perform a host check on a client to ensure it meets certain criteria before the user can log in... This ensures that the client computer has a

minimum level of security."
3. Fortinet Document Library, FortiOS 7.0.0 Security Best Practices, "Endpoint Security" section: Recommends ensuring endpoints connecting to the network are secure. Host check is a primary mechanism for enforcing this for VPN clients. "Use host checking to ensure that remote devices connecting over VPN have antivirus software and a firewall enabled."

Question: 25

Which two statements correctly describe auto discovery VPN (ADVPN)? (Choose two.)

A. IPSec tunnels are negotiated dynamically between spokes.

B. ADVPN is supported only with IKEv2.

C. It recommends the use of dynamic routing protocols, so that spokes can learn the routes to other
spokes.

D. Every spoke requires a static tunnel to be configured to other spokes, so that phase 1 and phase 2
proposals are defined in advance.

Answer:

A, C

Explanation:

Auto-Discovery VPN (ADVPN) is a Fortinet technology that enhances a standard hub-and-spoke IPsec VPN topology. Its primary function is to allow spokes to dynamically establish direct, on-demand IPsec tunnels, known as shortcuts, between each other. This prevents the need for spoke-to-spoke traffic to traverse the hub, thus reducing latency and hub workload. For this "auto-discovery" to function, a dynamic routing protocol (BGP is recommended, but OSPF is also supported) must be running over the VPN. The routing protocol allows spokes to learn the routes to subnets behind other spokes via the hub, which then triggers the ADVPN shortcut negotiation process when traffic is initiated.

Why Incorrect Options are Wrong:

B. ADVPN is supported with both IKEv1 and IKEv2. While IKEv2 is generally recommended for modern deployments, the feature is not exclusively limited to it.
D. This describes a static full-mesh VPN topology. The core benefit of ADVPN is to eliminate the need for pre-configuring static tunnels between all spokes.

References:

1. Fortinet FortiOS 7.0.0 Administration Guide, VPN IPsec VPN Auto-Discovery VPN (ADVPN), Page 1189.
"ADVPN is a technology that allows a traditional hub-and-spoke VPN to dynamically establish tunnels between the spokes... These dynamically-created tunnels are called shortcuts." (Supports Answer A)
"A dynamic routing protocol, such as BGP or OSPF, must be configured between the hub and the spokes." (Supports Answer C)

2. Fortinet FortiOS 7.0.0 CLI Reference, config vpn ipsec phase1-interface, Page 2589.
The set ike-version command under the phase 1 interface configuration allows for a value of 1 or 2, indicating that both versions are available for configuration, including on interfaces where ADVPN is enabled. (Refutes Answer B)
3. Fortinet Certified Professional - Network Security 7.0 Study Guide, Chapter 10: IPsec VPN ADVPN, Page 318.
"ADVPN allows spokes to create dynamic, on-demand tunnels between each other called shortcuts." (Supports Answer A)
"ADVPN requires a dynamic routing protocol running between the hub and spokes." (Supports Answer C)
"The main problem that ADVPN solves is the need to configure a full mesh of tunnels between spokes." (Refutes Answer D)

Question: 26

Which of the following SD-WAN load -balancing method use interface weight value to distribute traffic? (Choose two.)

A. Source IP

B. Spillover

C. Volume

D. Session

Answer:

C, D

Explanation:

In FortiGate SD-WAN, the load-balancing algorithm determines how traffic is distributed across member interfaces. The Volume algorithm distributes traffic based on a weighted round-robin mechanism, where interfaces with a higher weight value receive a proportionally larger volume of traffic (measured in bytes/packets). Similarly, the Session algorithm distributes new network sessions across member interfaces based on their configured weights, meaning an interface with a higher weight is assigned a proportionally greater number of new sessions. Both methods directly use the configured interface weight to influence traffic distribution.

Why Incorrect Options are Wrong:

A. Source IP: This is a hashing algorithm that sends all traffic from a specific source IP address to the same interface to ensure session persistence, not a weighted distribution method.
B. Spillover: This method directs all traffic to a primary interface until a specified bandwidth threshold is exceeded, at which point excess traffic "spills over" to the next interface. It is threshold-based, not weight-based.

References:

1. Fortinet. (2023). FortiOS 7.4.0 SD-WAN Administration Guide. Fortinet Document Library. pp. 43-44, Section: "Load balancing algorithms".
Session: "Distributes new sessions on a round-robin basis among all available member interfaces. The number of sessions for each interface is based on the interface weight."
Volume: "Distributes traffic among all available member interfaces based on the interface weight. More traffic is sent to the interface with the higher weight."
Spillover: "Sends all traffic to the first member interface until the traffic volume exceeds the spill-over threshold..."
Source IP: "All traffic from a source IP address is sent to the same interface."
2. Fortinet. (2022). FortiOS 7.2.0 Administration Guide. Fortinet Document Library. p. 1119,

Section: "SD-WAN rules".
This guide provides equivalent descriptions for the load balancing algorithms, confirming that Session and Volume are the methods that utilize interface weights for traffic distribution.

Question: 27

Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

A. Web filter in flow-based inspection

B. Antivirus in flow-based inspection

C. DNS filter

D. Web application firewall

E. Application control

Answer:

A, B, E

Explanation:

The FortiOS Intrusion Prevention System (IPS) engine is a core component that performs pattern matching and protocol decoding for multiple security functions, especially in flow-based inspection mode. Application control is fundamentally built on the IPS engine, using its decoders and signature-matching capabilities to identify application traffic. Similarly, when operating in flow-based mode, both the web filter and antivirus features leverage the high-performance IPS engine to scan traffic content for threats and policy violations without the need for full proxying, enabling faster throughput.

Why Incorrect Options are Wrong:

C. DNS filter: This feature is primarily handled by a dedicated daemon (dnsfilterd) and process, which is distinct from the core IPS engine used for general signature matching.
D. Web application firewall: The WAF feature on a FortiGate uses its own specialized engine for deep inspection of HTTP/S traffic and protection against web application attacks, separate from the IPS engine.

References:

1. Fortinet FortiOS 7.0.0 Administration Guide: In the "Security Profiles" section, under "Application Control," it is stated that "Application control uses IPS protocol decoders and signatures to identify the applications that generate network traffic." (p. 689).
2. Fortinet FortiOS 7.0.0 Handbook - Architecture: The "Life of a Packet" chapter details the packet flow. In the flow-based inspection path, the diagram and accompanying text show that the ipsengine is responsible for processing IPS, Application Control, flow-based Web Filtering, and flow-based Antivirus. (Section: "Flow-based inspection").
3. Fortinet FortiOS 7.0.0 Handbook - Security Profiles: The "Antivirus" chapter explains, "In

flow-based inspection, the FortiGate uses the IPS engine to scan content as it passes through the FortiGate without any buffering." This same principle is described for flow-based Web Filtering. (Section: "Inspection modes").

Question: 28

Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

A. This is known as many-to-one NAT.

B. Source IP is translated to the outgoing interface IP.

C. Connections are tracked using source port and source MAC address.

D. Port address translation is not used.

Answer:

A, B

Explanation:

When a FortiGate firewall policy is configured to use the outgoing interface IP address for NAT with the fixed port option disabled, it performs Source NAT (SNAT) overload. This configuration translates the source IP addresses of multiple internal devices into the single IP address of the FortiGate's egress interface. This is a classic many-to-one NAT scenario. To keep track of the individual connections, FortiGate also translates the source port number, a process known as Port Address Translation (PAT). Disabling the fixed port setting allows FortiGate the flexibility to change the source port to avoid conflicts, which is the essence of PAT.

Why Incorrect Options are Wrong:

C. Connections are tracked using source port and source MAC address. Connections are tracked using the Layer 3/4 tuple (IP addresses, ports, protocol), not the Layer 2 MAC address, which changes at each hop. D. Port address translation is not used. This is incorrect. Disabling the 'fixed port' setting explicitly enables Port Address Translation (PAT), allowing FortiGate to modify source ports to manage multiple sessions.

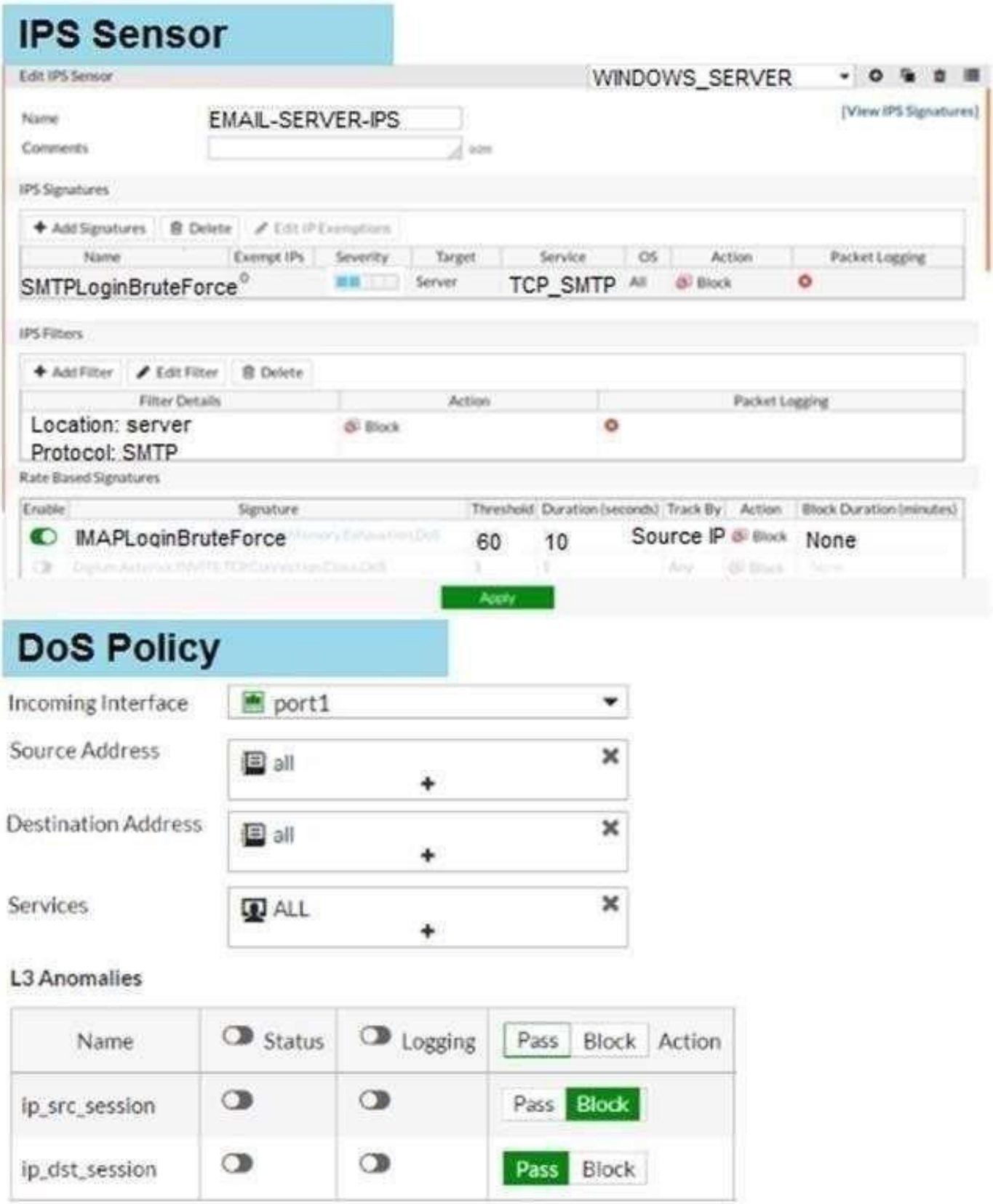
References:

1. Fortinet FortiOS 7.0.1 Administration Guide, Page 539, "NAT" section: "When you configure SNAT in a firewall policy, you can select to use the outgoing interface address... This is also known as overload NAT. Overload NAT maps multiple private IP addresses to a single public IP address by using different source ports." This statement directly supports answers A and B.
2. Fortinet FortiOS 7.0.1 Networking Guide, Page 478, "config firewall policy" section, under the fixedport setting: "Enable/disable changing the source port number in NATed traffic... When disabled (the default), FortiOS finds a free port from the translated port range... This is port address translation (PAT)." This confirms that PAT is used when fixed port is disabled, making option D incorrect.
3. Fortinet Cookbook, "Outgoing firewall policy with NAT enabled" recipe: This common

configuration example demonstrates that enabling NAT on an outgoing policy translates the source address of internal clients to the IP address of the WAN (outgoing) interface, allowing many users to share one public IP. This practically illustrates the concepts in options A and B. (Reference: Fortinet Cookbook for FortiOS 7.0, "Internet Access for a private network" section).

Question: 29

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below. 149/219



When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

A. SMTP.Login.Brute.Force

B. IMAP.Login.brute.Force

C. ipsrcsession

D. Location: server Protocol: SMTP

Answer:

C

Explanation:

According to the FortiOS packet processing order, also known as the "Life of a Packet," Denial of Service (DoS) policy checks are performed at the very beginning of the packet flow. This happens immediately after the packet is received on the ingress interface and before a session is created. Intrusion Prevention System (IPS) scanning, which evaluates signatures and filters, occurs much later in the process, after a firewall policy has accepted the traffic and a session has been established. Therefore, the ipsrcsession anomaly defined in the DoS policy is the first item to be evaluated by FortiGate.

Why Incorrect Options are Wrong:

A. SMTP.Login.Brute.Force: This is an IPS signature, which is evaluated by the IPS engine after the DoS policy check and session establishment. B. IMAP.Login.brute.Force: This is an IPS signature, which is processed later in the packet flow by the IPS engine, not before the DoS policy. D. Location: server Protocol: SMTP: This is an IPS filter used to apply specific signatures. It is part of the IPS engine's logic, which runs after the DoS policy.

References:

1. Fortinet FortiOS 7.4.0 Administration Guide, Packet flow and security profiles Life of a packet, Page 1031. The packet flow diagram and description clearly show that the dos-policy check occurs at the ingress stage, well before session setup and the application of security profiles like IPS (ipsscan).
2. Fortinet FortiOS 7.4.0 Administration Guide, Security Profiles DoS Protection, Page 568. This section explains that DoS policies are designed to "protect the FortiGate unit from denial of service attacks" by inspecting traffic before it is processed by the CPU, confirming its early position in the packet flow.

Question: 30

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy- based inspection mode? (Choose two.)

A. Warning

B. Exempt

C. Allow

D. Learn

Answer:

A, C

Explanation:

In a FortiGate web filter profile configured for proxy-based inspection, the FortiGuard category-based filter provides several actions to control web traffic. The Allow action explicitly permits users to access websites within a specific category. The Warning action, a feature available in proxy-based mode, presents a notification page to the user, who can then choose to proceed to the website. This provides a layer of user awareness without strictly blocking access. Both are valid and distinct actions available in the web filter profile user interface.

Why Incorrect Options are Wrong:

B. Exempt: This is not a primary action for a web category. Exemption is typically used to bypass inspection entirely for specific sources, destinations, or services, not as a per-category action.
D. Learn: The "Learn" action is not a valid option for FortiGuard web filter categories. This action type is associated with other security features, such as Data Leak Prevention (DLP), to build a profile of normal activity.

References:

1. Fortinet FortiOS 7.2.0 Administration Guide:
In the "Web Filter" chapter, under the "FortiGuard category based filter" section, the guide details the available actions. For proxy-based mode, it explicitly lists Allow, Monitor, Block, Warning, and Authenticate. This confirms that 'Allow' and 'Warning' are valid actions.
Reference: FortiOS 7.2.0 Administration Guide, Page 1234, "FortiGuard category based filter" section.
2. Fortinet FortiOS 7.4.0 Administration Guide:
The "Security Profiles Web Filter" chapter describes the configuration of FortiGuard category filters. The table of available actions for proxy-based inspection includes 'Allow' and 'Warning', while 'Exempt' and 'Learn' are not listed as valid actions for this specific feature.
Reference: FortiOS 7.4.0 Administration Guide, "Web Filter" chapter, "Actions" subsection.

Question: 31

Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

A. hard-timeout

B. auth-on-demand

C. soft-timeout

D. new-session

E. Idle-timeout

Answer:

A, D, E

Explanation:

FortiGate provides three distinct methods for managing user authentication session timeouts. The hard-timeout de-authenticates a user after a fixed period, regardless of their activity. The idle-timeout, which is the default, de-authenticates a user only after a specified period of inactivity; the timer resets whenever new traffic is detected. The new-session type requires the user to re-authenticate for every new TCP session they initiate, effectively creating a per-session authentication context rather than a time-based one. These settings are configured globally under config user setting in the CLI.

Why Incorrect Options are Wrong:

B. auth-on-demand: This is a separate setting that controls when the authentication prompt is triggered, not a type of session timeout.
C. soft-timeout: This term is not an official FortiGate configuration option; the correct term for an activity-based timeout is idle-timeout.

References:

1. FortiOS 7.2 Administration Guide, Firewall Firewall authentication Timeouts, Page 1010: "The FortiGate unit can be configured for three types of authentication timeouts: hard timeout, idle timeout, and new session." The guide proceeds to define each of the three correct options.
2. FortiOS 7.2.4 CLI Reference, config user setting, Page 2281: The auth-timeout-type attribute lists the available options: set auth-timeout-type hard-timeout idle-timeout new-session.
3. Fortinet Certified Professional - Security Operations Study Guide for FortiOS 7.2, Chapter 2: User Authentication, Section: Authentication Timeouts, Page 42: "FortiGate supports three authentication timeout types: Hard timeout, Idle timeout, and New session."

Question: 32

Which scanning technique on FortiGate can be enabled only on the CLI?

A. Machine learning (AI) scan

B. Trojan scan

C. Antivirus scan

D. Ransomware scan

Answer:

A

Explanation:

The global command to enable or disable the machine learning (AI) detection engine on a FortiGate device is exclusively available through the Command Line Interface (CLI). An administrator must use the commands config antivirus settings followed by set machine-learning-detection enable disable. While individual antivirus profiles can have AI-based scanning toggled on or off within the GUI, this master switch for the entire engine is not exposed in the graphical interface and must be managed via the CLI.

Why Incorrect Options are Wrong:

B. Trojan scan: Trojan scanning is an integral part of the standard antivirus engine and its configuration is managed through the antivirus security profile in the GUI. C. Antivirus scan: Antivirus scanning is a core security feature with comprehensive configuration options available directly within the FortiGate GUI under Security Profiles. D. Ransomware scan: Ransomware protection is implemented through features within the antivirus profile and FortiSandbox integration, both of which are fully configurable in the GUI.

References:

1. Fortinet FortiOS 7.4.2 CLI Reference: This official document lists the configuration options for the antivirus engine. Under the config antivirus settings section, the machine-learning-detection command is detailed as the method to enable or disable the machine learning engine. There is no corresponding global toggle mentioned for the GUI.
Source: FortiOS 7.4.2 CLI Reference, Page 221, config antivirus settings table.
2. Fortinet FortiOS 7.4.0 Administration Guide: This guide details the GUI configuration for security profiles. In the AntiVirus section, it shows how to enable "AI-based Scan" on a per-profile basis. However, it does not document a global GUI option to enable or disable the underlying machine learning engine itself, confirming this master switch is a CLI-only function.
Source: FortiOS 7.4.0 Administration Guide, "AntiVirus" chapter, "Create a new AntiVirus profile" section.

Question: 33

Examine this FortiGate configuration:

```
config system global
     set av-failopen pass
end
```

Examine the output of the following debug command:

```
# diagnose hardware sysinfo conserve
memory conserve mode: on
total RAM: 3040 MB
memory used: 2948 MB 97% of total RAM
memory freeable: 92 MB 3% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red: 2675 MB 88% of total RAM
memory used threshold green: 2492 MB 82% of total RAM
```

Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

A. It is allowed, but with no inspection

B. It is allowed and inspected as long as the inspection is flow based

C. It is dropped.

D. It is allowed and inspected, as long as the only inspection required is antivirus.

Answer:

A

Explanation:

The provided configuration set av-failopen pass explicitly instructs the FortiGate to allow traffic to pass without inspection if the antivirus scanning daemon (scand) fails. The debug output for scand confirms two key points: the scand daemon state is stopped, and the av-failopen mode is pass. Therefore, any new session that matches a firewall policy requiring antivirus inspection will be allowed to proceed without being scanned. While the IPS engine is also down and would block

traffic, option A accurately describes the direct consequence of the specific, non-default configuration provided in the exhibit.

Why Incorrect Options are Wrong:

B. It is allowed and inspected as long as the inspection is flow based: This is incorrect because the relevant inspection daemons (scand, ipsmonitor) are stopped, meaning no inspection of any kind can occur.
C. It is dropped: This is not universally true. While traffic requiring IPS inspection would be dropped, traffic requiring only antivirus inspection is explicitly allowed due to the av-failopen pass setting.
D. It is allowed and inspected, as long as the only inspection required is antivirus: This is incorrect because the traffic is allowed but it is not inspected. The purpose of the fail-open mechanism is to bypass inspection when the service is unavailable.

References:

1. FortiOS Administration Guide 7.4.1, Page 1018, "Fail-open behavior": "By default, when a daemon fails, traffic that is supposed to be processed by that daemon is blocked. This is fail-close behavior. You can configure fail-open behavior to allow traffic to pass through without being processed when the daemon fails." This document confirms the principle of fail-open.
2. FortiOS CLI Reference 7.4.1, Page 103, config system global: The set av-failopen pass command is documented here. It enables traffic to pass when the AV service is unavailable, which is the scenario shown in the debug output.
3. FortiOS Handbook - Security Profiles for FortiOS 7.4.0, Page 21, "Fail-open configuration": "You can configure fail-open to allow traffic to pass through the FortiGate unit without being scanned if the IPS or antivirus scanner fails." This directly supports that av-failopen pass allows traffic when the antivirus scanner has failed.

Question: 34

Which three statements are true regarding session-based authentication? (Choose three.)

A. HTTP sessions are treated as a single user.

B. IP sessions from the same source IP address are treated as a single user.

C. It can differentiate among multiple clients behind the same source IP address.

D. It requires more resources.

E. It is not recommended if multiple users are behind the source NAT

Answer:

A, C, D

Explanation:

Session-based authentication in FortiOS uses browser cookies to track and authenticate individual user web sessions. This method ties the authentication to a specific HTTP session, treating each as a unique user. Its primary advantage is the ability to distinguish between multiple users who share a single source IP address, such as those behind a Network Address Translation (NAT) device. However, because the FortiGate must manage and track each individual session state via cookies, this method is more resource-intensive (CPU and memory) compared to the simpler IP-based authentication scheme.

Why Incorrect Options are Wrong:

B. This statement describes IP-based authentication, where all traffic from a single source IP is treated as belonging to one authenticated user, not session-based authentication.
E. Session-based authentication is specifically recommended for environments where multiple users are behind a source NAT, as it is the primary method to differentiate and apply policies to them individually.

References:

1. Fortinet FortiOS 7.0.1 Administration Guide, Page 1013, "Firewall authentication" section. "Session-based authentication uses cookies to track users. This allows multiple users to authenticate from behind a NAT device, as each user's browser has a separate cookie. This method is more resource intensive than IP-based authentication."
This single section directly supports answers A (by explaining cookie-based tracking of user sessions), C (differentiating users behind NAT), and D (more resource-intensive). It also implicitly refutes E.
2. Fortinet FortiOS 7.0.1 Cookbook, "User Authentication" chapter, "Firewall Authentication" section.

"Session-based authentication uses cookies to identify the user. This is useful when multiple users are on a network behind a NAT device with a single public IP address."
This confirms that session-based authentication is the appropriate method for users behind NAT (refuting E) and that it can differentiate them (supporting C).
3. Fortinet FortiOS 7.0.1 Firewall Handbook, Page 41, "Authentication" section.
"IP-based authentication authenticates the user's source IP address. All traffic from that IP address is considered to be from the authenticated user."
This reference explicitly defines the behavior described in option B as IP-based authentication, confirming it is incorrect for session-based authentication.

Question: 35

In which two ways can RPF checking be disabled? (Choose two.)

A. Enable anti-replay in firewall policy.

B. Enable asymmetric routing.

C. Disable strict-src-check under system settings.

D. Disable the RPF check at the FortiGate interface level for the source check.

Answer:

C, D

Explanation:

Reverse Path Forwarding (RPF) is a security feature that verifies that the source IP address of an incoming packet is reachable through the interface on which it arrived. FortiOS provides two primary methods to disable this check:
1. Per-Interface: The RPF check can be disabled on individual interfaces. This is the most granular and common method, typically used when a known asymmetric routing path exists for a specific network segment. This corresponds to option D.
2. Globally: Option C refers to disabling the strict source check at a global level. While strict-src-check is not a literal CLI command, it represents the concept of disabling the system-wide strict RPF policy, contrasting with the per-interface method.

Why Incorrect Options are Wrong:

A. Enable anti-replay in firewall policy.
Anti-replay is a security feature, primarily for IPsec VPNs, that prevents the re-transmission of captured packets. It is unrelated to the RPF source address verification mechanism.
B. Enable asymmetric routing.
Enabling asymmetric routing (set asymroute enable) disables a stateful inspection check for reply packets, but it does not disable the initial RPF check on the first packet of a session.

References:

1. FortiOS 7.0 CLI Reference, FortiGate. (2021). Fortinet.
Page 1731, config system interface table: The src-check attribute is defined with options enable or disable. The description states, "Enable/disable source IP check for reverse path. Packets found with invalid source IP address are dropped." This directly supports option D.
2. FortiGate Infrastructure 7.0 Study Guide, Fortinet. (2021).
Page 217, "Reverse Path Forwarding (RPF) Check" section: "You can disable the RPF check on a per-interface basis. You might need to do this, for example, if you have asymmetric routing in your network." This confirms the per-interface method (Option D) is a standard procedure.

3. Fortinet Knowledge Base, Article ID: FD32528, "Troubleshooting RPF (Reverse Path Forwarding) failures".
This article outlines solutions for RPF failures. It clearly distinguishes between disabling src-check on an interface and enabling asymroute (config system settings - set asymroute enable). This distinction supports the reasoning that enabling asymmetric routing (Option B) is a different function from disabling the RPF check itself.