ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices.

Which three approaches can the company take to successfully deploy advanced initial configurations on remote branches? (Choose three.)

A. Use metadata variables to dynamically assign values according to each FortiGate device.

B. Use provisioning templates and install configuration settings at the device layer.

C. Use the Global ADOM to deploy global object configurations to each FortiGate device.

D. Apply Jinja in the FortiManager scripts for large-scale and advanced deployments.

E. Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices.

Answer: A, B, E

Explanation:

Use metadata variables to dynamically assign values according to each FortiGate device:

Metadata variables in FortiManager allow device-specific configurations to be dynamically assigned without manually configuring each FortiGate. This is especially useful when deploying multiple devices with similar base configurations.

Use provisioning templates and install configuration settings at the device layer:

Provisioning templates in FortiManager provide a structured way to configure FortiGate devices.

These templates can define interfaces, policies, and settings, ensuring that each device is correctly configured upon deployment.

Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices:

Zero-Touch Provisioning (ZTP) and Local Touch Provisioning (LTP) help automate the deployment of FortiGate devices. By adding devices as model devices in FortiManager, configurations can be pushed automatically when devices connect for the first time, reducing manual effort.

Question: 2

An administrator is checking an enterprise network and sees a suspicious packet with the MAC address e0:23:ff:fc:00:86.

What two conclusions can the administrator draw? (Choose two.)

A. The suspicious packet is related to a cluster that has VDOMs enabled.

B. The network includes FortiGate devices configured with the FGSP protocol.

C. The suspicious packet is related to a cluster with a group-id value lower than 255.

D. The suspicious packet corresponds to port 7 on a FortiGate device.

Answer: A, D

Explanation:

According to the FortiOS 7.6 Infrastructure study guide and High Availability (HA) documentation, FortiGate units in an HA cluster use a virtual MAC address to ensure seamless failover. The structure of this virtual MAC address is strictly defined by the Fortinet HA protocol.

For a standard HA cluster, the virtual MAC address format is 00:09:0f:09:<group- id_hex>:<vcluster_port_hex>. However, when VDOMs are enabled, the virtual MAC address prefix changes to e0:23:ff to accommodate the additional complexity of multiple virtual domains. Therefore, the prefix e0:23:ff in the suspicious MAC address e0:23:ff:fc:00:86 confirms that the packet originated from a cluster with VDOMs enabled (Option A).

Regarding the interface identification, the last byte (86) is calculated as follows:

The 0x80 bit indicates virtual-cluster 2 (vcluster 2). Since $0x86 = 0x80 + 0x06$, we know the packet is from vcluster 2.

The remaining value 0x06 represents the interface index. In FortiOS, the index starts at 0 (port1 = 0, port2 = 1, port3 = 2, port4 = 3, port5 = 4, port6 = 5, port7 = 6). Therefore, the index 6 corresponds

exactly to port 7 (Option D).

The fourth byte (fc) represents the HA Group ID (252 in decimal). While this is indeed lower than 255, the specific logic of the virtual MAC composition in a VDOM-enabled environment points specifically to the port identification and vcluster status as the primary diagnostic conclusions.

Question: 3

A company's guest internet policy, operating in proxy mode, blocks access to Artificial Intelligence Technology sites using FortiGuard. However, a guest user accessed a page in this category using port 8443.

Which configuration changes are required for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443 when full SSL inspection is active in the guest policy?

A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.

B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.

C. To analyze nonstandard ports in web filter profiles, use TLSv1.3 in the SSL/SSH Inspection Profile.

D. Administrators can block traffic on nonstandard ports by enabling the SNI check in the SSL/SSH Inspection Profile.

Answer: B

Explanation:

When FortiGate is operating in proxy mode with full SSL inspection enabled, it inspects encrypted HTTPS traffic by default on port 443. However, some websites may use non-standard HTTPS ports (such as 8443), which FortiGate does not inspect unless explicitly configured.

To ensure that FortiGate inspects HTTPS traffic on port 8443, administrators must manually add port 8443 in the Protocol Port Mapping section of the SSL/SSH Inspection Profile. This allows FortiGate to treat HTTPS traffic on port 8443 the same as traffic on port 443, enabling proper inspection and enforcement of FortiGuard category-based web filtering.

Question: 4

An administrator needs to install an IPS profile without triggering false positives that can impact applications and cause problems with the user's normal traffic flow.

Which action can the administrator take to prevent false positives on IPS analysis?

A. Use the IPS profile extension to select an operating system, protocol, and application for all the network internal services and users to prevent false positives.

B. Enable Scan Outgoing Connections to avoid clicking suspicious links or attachments that can deliver botnet malware and create false positives.

C. Use an IPS profile with action monitor, however, the administrator must be aware that this can compromise network integrity.

D. Install missing or expired SSUTLS certificates on the client PC to prevent expected false positives.

Answer: A

Explanation:

False positives in Intrusion Prevention System (IPS) analysis can disrupt legitimate traffic and negatively impact user experience. To reduce false positives while maintaining security, administrators can:

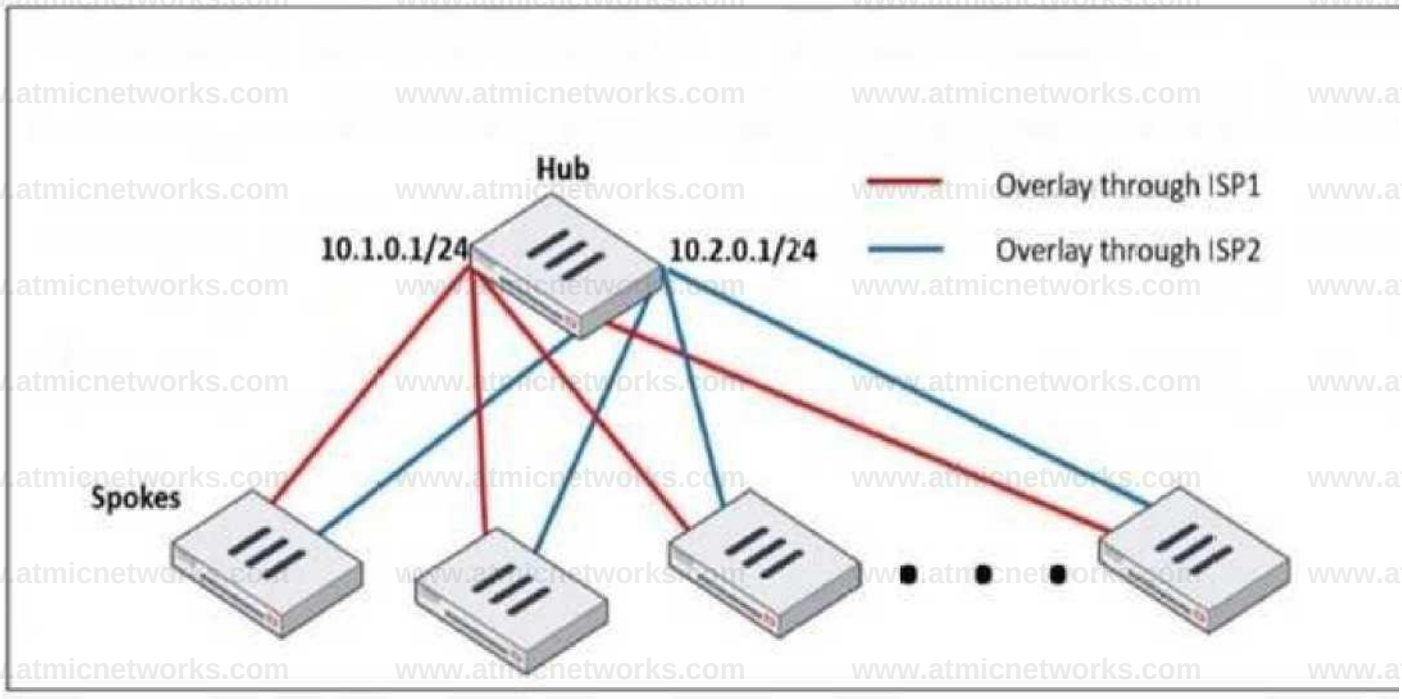
- Use IPS profile extensions to fine-tune the settings based on the organization's environment.
- Select the correct operating system, protocol, and application types to ensure that IPS signatures match the network's actual traffic

patterns, reducing false positives.

- Customize signature selection based on the network's specific services, filtering out unnecessary or irrelevant signatures.

Question: 5

Refer to the exhibit, which shows a hub and spokes deployment.



An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub.

Which two commands allow the administrator to minimize the configuration? (Choose two.)

A. neighbor-group

B. route-reflector-client

C. neighbor-range

D. ibgp-enforce-multihop

Answer: A, C

Explanation:

neighbor-group:

- This command is used to group multiple BGP neighbors with the same configuration, reducing redundant configuration.
- Instead of defining individual BGP settings for each spoke, the administrator can create a neighbor-group and apply the same policies, reducing manual work.

neighbor-range:

- This command allows the configuration of a range of neighbor IPs dynamically, reducing the need to manually define each spoke neighbor.
- It automatically adds BGP neighbors that match a given prefix, simplifying deployment.

Question: 6

Why does the ISDB block layers 3 and 4 of the OSI model when applying content filtering? (Choose two.)

A. FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard.

B. The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard.

C. The ISDB works in proxy mode, allowing the analysis of packets in layers 3 and 4 of the OSI model.

D. The ISDB limits access by URL and domain.

Answer: A, B

Explanation:

The Internet Service Database (ISDB) in FortiGate is used to enforce content filtering at Layer 3 (Network Layer) and Layer 4 (Transport Layer) of the OSI model by identifying applications based on their predefined IP addresses and ports.

FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard:

- FortiGate retrieves and updates a predefined list of IPs and ports for different internet services from FortiGuard.
- This allows FortiGate to block specific services at Layer 3 and Layer 4 without requiring deep packet inspection.

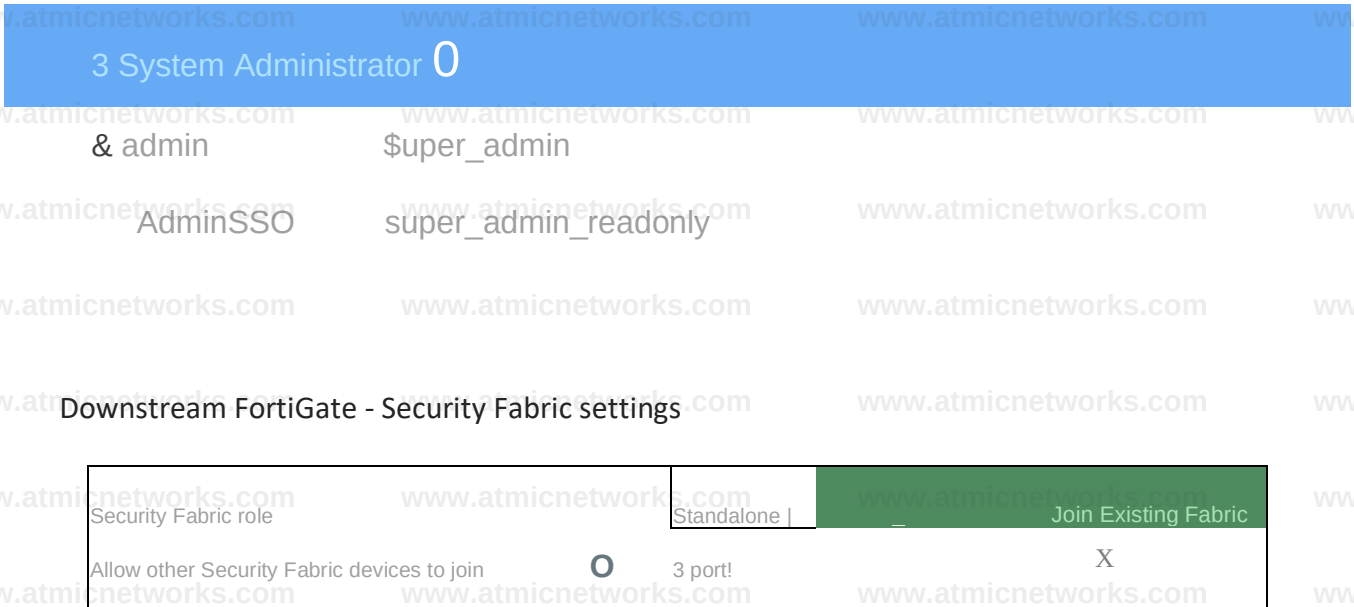
The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard:

- ISDB works by matching traffic to known IP addresses and ports of categorized services.
- When an application or service is blocked, FortiGate prevents communication by denying traffic based on its destination IP and port number.

Question: 7

Refer to the exhibits.

Root FortiGate - System Administrator configuration



Downstream FortiGate - Security Fabric settings

The Administrators section of a root FortiGate device and the Security Fabric Settings section of a downstream FortiGate device are shown.

When prompted to sign in with Security Fabric in the downstream FortiGate device, a user enters the AdminSSO credentials.

What is the next status for the user?

A. The user is prompted to create an SSO administrator account for AdminSSO.

B. The user receives an authentication failure message.

C. The user accesses the downstream FortiGate with super_admin_readonly privileges.

D. The user accesses the downstream FortiGate with super_admin privileges.

Answer: C

Explanation:

From the Root FortiGate - System Administrator Configuration exhibit:

- The AdminSSO account has the super_admin_readonly role.

From the Downstream FortiGate - Security Fabric Settings exhibit:

- The Security Fabric role is set to Join Existing Fabric, meaning it will authenticate with the root FortiGate.
- SAML Single Sign-On (SSO) is enabled, and the default admin profile is set to super_admin_readonly.

When the AdminSSO user logs into the downstream FortiGate using SSO, the authentication request is sent to the root FortiGate, where AdminSSO has super_admin_readonly permissions. Since the downstream FortiGate inherits this permission through the Security Fabric configuration, the user will be granted super_admin_readonly access.

Question: 8

A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on the policy.

How can an administrator ensure that FortiGate can analyze encrypted HTTPS traffic on a website?

A. The administrator must enable reputable websites to allow only SSL/TLS websites rated by FortiGuard web filter.

B. The administrator must enable URL extraction from SNI on the SSL certificate inspection to ensure the TLS three-way handshake is correctly analyzed by FortiGate.

C. The administrator must enable DNS over TLS to protect against fake Server Name Indication (SNI) that cannot be analyzed in common DNS requests on HTTPS websites.

D. The administrator must enable full SSL inspection in the SSL/SSH Inspection Profile to decrypt packets and ensure they are analyzed as expected.

Answer: D

Explanation:

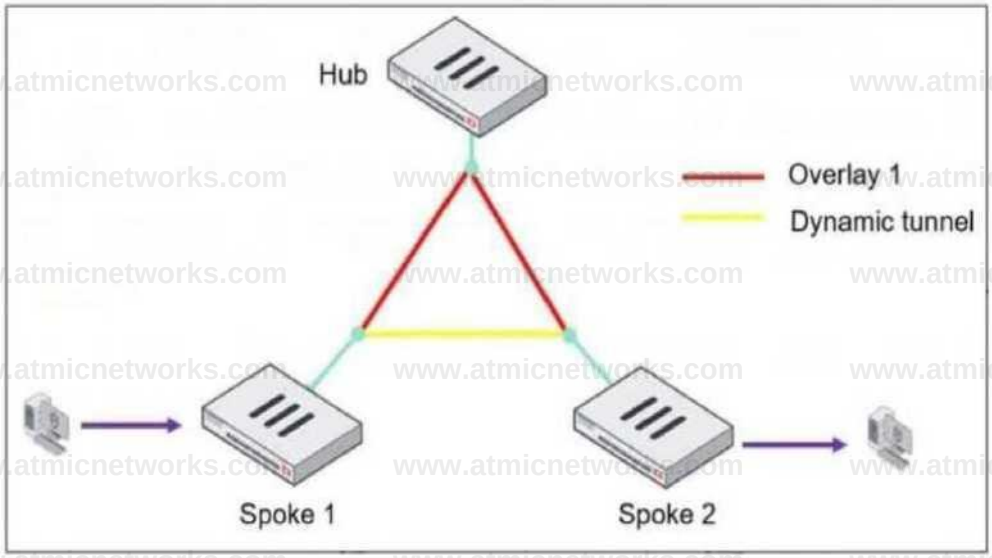
FortiGate, like other security appliances, cannot analyze encrypted HTTPS traffic unless it decrypts it first. If only certificate inspection is enabled, FortiGate can see the certificate details (such as the domain and issuer) but cannot inspect the actual web content.

To fully analyze the traffic and detect potential malware threats:

- Full SSL inspection (Deep Packet Inspection) must be enabled in the SSL/SSH Inspection Profile.
- This allows FortiGate to decrypt the HTTPS traffic, inspect the content, and then re-encrypt it before forwarding it to the user.
- Without full SSL inspection, threats embedded in encrypted traffic may go undetected.

Question: 9

Refer to the exhibit, which shows an ADVPN network.



The client behind Spoke-1 generates traffic to the device located behind Spoke-2.

What is the first message that the hub sends to Spoke-1 to bring up the dynamic tunnel?

A. Shortcut query

B. Shortcut offer

C. Shortcut reply

D. Shortcut forward

Answer: B

Explanation:

In an ADVPN (Auto-Discovery VPN) network, a dynamic VPN tunnel is established on-demand between spokes to optimize traffic flow and reduce latency.

Process:

1. Traffic Initiation:

■ A client behind Spoke-1 sends traffic to a device behind Spoke-2.

■ The traffic initially flows through the hub, following the pre-established overlay tunnel.

2. Hub Detection:

■ The hub detects that Spoke-1 is communicating with Spoke-2 and determines that a direct shortcut tunnel between the spokes can optimize the connection.

3. Shortcut Offer:

The hub sends a "Shortcut Offer" message to Spoke-1, informing it that a direct dynamic tunnel to Spoke-2 is possible.

4. Tunnel Establishment:

Spoke-1 and Spoke-2 then negotiate and establish a direct IPsec tunnel for communication.

Question: 10

What is the initial step performed by FortiGate when handling the first packets of a session?

A. Installation of the session key in the network processor (NP)

B. Data encryption and decryption

C. Security inspections such as ACL, HPE, and IP integrity header checking

D. Ofloading the packets directly to the content processor (CP)

Answer: C

Explanation:

When FortiGate processes the first packets of a session, it follows a sequence of steps to determine how the traffic should be handled before establishing a session. The initial step involves:

- Access Control List (ACL) checks: Determines if the traffic should be allowed or blocked based on predefined security rules.
- Hardware Packet Engine (HPE) inspections: Ensures that packet headers are valid and comply with protocol standards.
- IP Integrity Header Checking: Verifies if the IP headers are intact and not malformed or spoofed.

Once these security inspections are completed and the session is validated, FortiGate then installs the session in hardware (if ofloading is enabled) or processes it in software.

Question: 11

An administrator applied a block-all IPS profile for client and server targets to secure the server, but the database team reported the application stopped working immediately after.

How can an administrator apply IPS in a way that ensures it does not disrupt existing applications in the network?

A. Use an IPS profile with all signatures in monitor mode and verify patterns before blocking.

B. Limit the IPS profile to server targets only to avoid blocking connections from the server to clients.

C. Select flow mode in the IPS profile to accurately analyze application patterns.

D. Set the IPS profile signature action to default to discard all possible false positives.

Answer: A

Explanation:

Applying an aggressive IPS profile without prior testing can disrupt legitimate applications by incorrectly identifying normal traffic as malicious. To prevent disruptions while still monitoring for threats:

- Enable IPS in "Monitor Mode" first:
  - This allows FortiGate to log and analyze potential threats without actively blocking traffic.
  - Administrators can review logs and fine-tune IPS signatures to minimize false positives before switching to blocking mode.

- Verify and adjust signature patterns:
    - Some signatures might trigger unnecessary blocks for legitimate application traffic.
        - By analyzing logs, administrators can disable or modify specific rules causing false positives.

Question: 12

An administrator is extensively using VXLAN on FortiGate.

Which specialized acceleration hardware does FortiGate need to improve its performance?

A. NP7

B. SP5

C. CP9

D. NTurbo

Answer: A

Explanation:

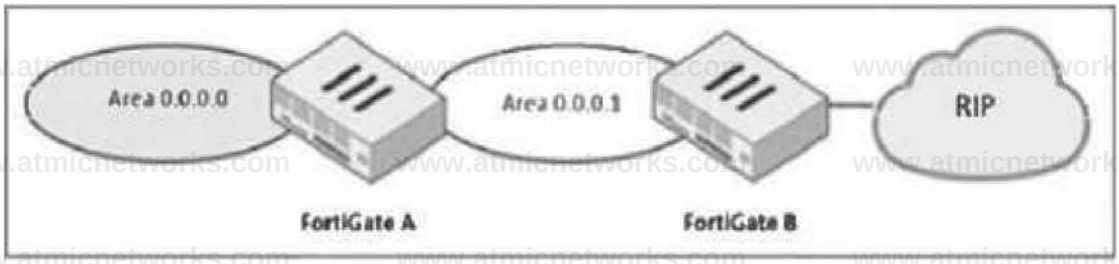
VXLAN (Virtual Extensible LAN) is an overlay network technology that extends Layer 2 networks over Layer 3 infrastructure. When VXLAN is used extensively on FortiGate, hardware acceleration is crucial for maintaining performance.

- NP7 (Network Processor 7) is Fortinet's latest network processor designed to accelerate high- performance networking features, including:
    - VXLAN encapsulation/decapsulation
        - IPsec VPN ofloading
        - Firewall policy enforcement
        - Advanced threat protection at wire speed

NP7 significantly reduces latency and improves throughput when handling VXLAN traffic, making it the best choice for large-scale VXLAN deployments.

Question: 13

Refer to the exhibit, which shows a partial enterprise network.



An administrator would like the area 0.0.0.0 to detect the external network.

What must the administrator configure?

A. Enable RIP redistribution on FortiGate B.

B. Configure a distribute-route-map-in on FortiGate B.

C. Configure a virtual link between FortiGate A and B.

D. Set the area 0.0.0.l type to stub on FortiGate A and B.

Answer: A

Explanation:

The diagram shows a multi-area OSPF network where:

- FortiGate A is in OSPF Area 0 (Backbone area).
- FortiGate B is in OSPF Area 0.0.0.1 and is connected to an RIP network.

To ensure that OSPF Area 0 (0.0.0.0) learns routes from the external RIP network, FortiGate B must redistribute RIP routes into OSPF.

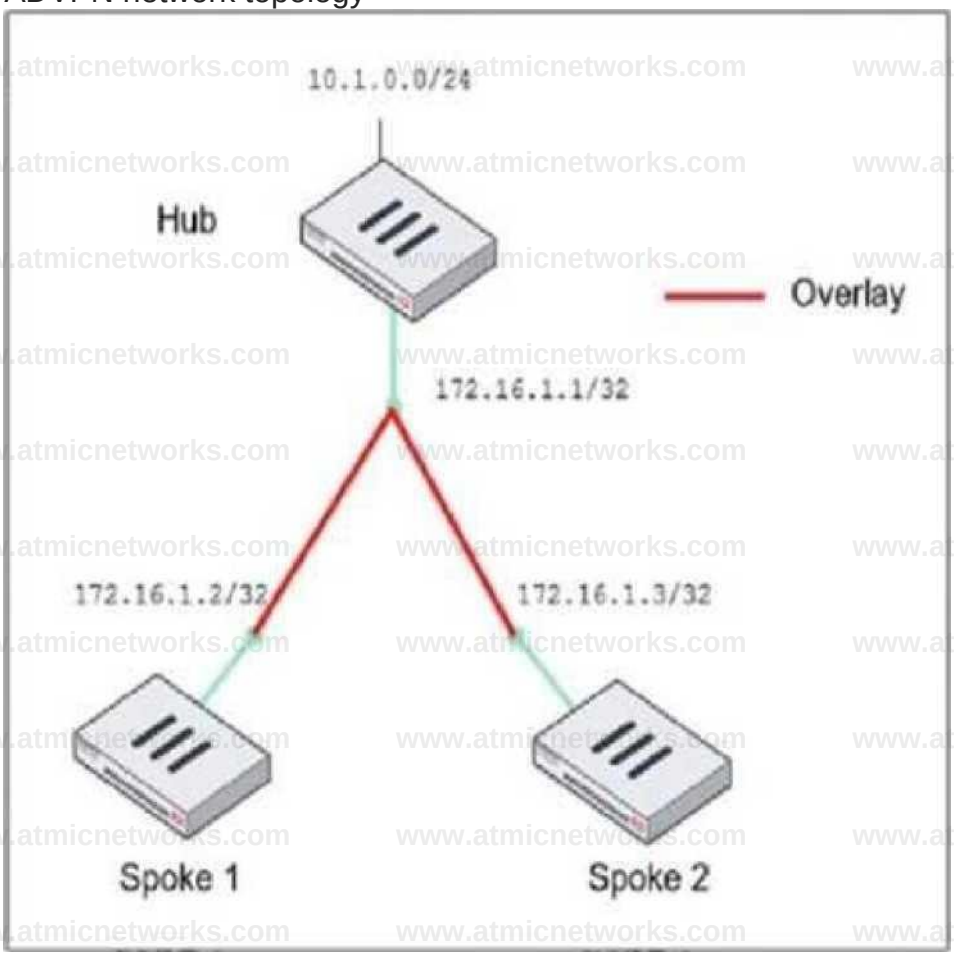
Steps to achieve this:

1. Enable route redistribution on FortiGate B to inject RIP-learned routes into OSPF.
2. This allows OSPF Area 0.0.0.1 to forward RIP routes to OSPF Area 0 (0.0.0.0), making the external network visible.

Question: 14

Refer to the exhibit, which shows the ADVPN network topology and partial BGP configuration.

ADVPN network topology



Partial BGP configuration

```
Hub I config router bgp set as 65100 set router-id 172.16.1.1 config
neighbor-group edit "advpn" set remote-as 65100 end config neighbor-
range edit 1 end config network • * end
```

Which two parameters must an administrator configure in the config neighbor range for spokes shown in the exhibit? (Choose two.)

A. set max-neighbor-num 2

B. set neighbor-group advpn

C. set route-reflector-client enable

D. set prefix 172.16.1.0 255.255.255.0

Answer: B, D

Explanation:

In the given ADVPN (Auto-Discovery VPN) topology, BGP is being used to dynamically establish routes between spokes. The neighbor-range configuration is crucial for simplifying BGP peer setup by automatically assigning neighbors based on their IP range.

set neighbor-group advpn

- The neighbor-group parameter is used to apply pre-defined settings (such as AS number) to dynamically discovered BGP neighbors.
- The advpn neighbor-group is already defined in the configuration, and assigning it to the neighborrange ensures consistent BGP settings for all spoke neighbors.

set prefix 172.16.1.0 255.255.255.0

- This command allows dynamic BGP peer discovery by defining a range of potential neighbor IPs (172.16.1.1 - 172.16.1.255).
- Since each spoke has a unique /32 IP within this subnet, this ensures that any spoke within the

172.16.1.0/24 range can automatically establish a BGP session with the hub.

Question: 15

Which two statements about IKEv2 are true if an administrator decides to implement IKEv2 in the VPN topology? (Choose two.)

A. It includes stronger Diffie-Hellman (DH) groups, such as Elliptic Curve (ECP) groups.

B. It supports interoperability with devices using IKEv1.

C. It exchanges a minimum of two messages to establish a secure tunnel.

D. It supports the extensible authentication protocol (EAP).

Answer: A, D

Explanation:

IKEv2 (Internet Key Exchange version 2) is an improvement over IKEv1, offering enhanced security, efficiency, and flexibility in VPN configurations.

It includes stronger Diffie-Hellman (DH) groups, such as Elliptic Curve (ECP) groups.

IKEv2 supports stronger cryptographic algorithms, including Elliptic Curve Diffie-Hellman (ECDH) groups such as ECP256 and ECP384, providing improved security compared to IKEv1.

It supports the extensible authentication protocol (EAP).

IKEv2 natively supports EAP authentication, which allows integration with external authentication mechanisms such as RADIUS, certificates, and smart cards. This is particularly useful for remote access VPNs where user authentication must be flexible and secure.

Question: 16

An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection.

The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best available connection.

How can this automatic detection and optimal link utilization between spokes be achieved?

A. Set up OSPF routing over static VPN tunnels between spokes.

B. Utilize ADVPN 2.0 to facilitate dynamic direct tunnels and automatic link optimization.

C. Establish static VPN tunnels between spokes with predefined backup routes.

D. Implement SD-WAN policies at the hub to manage spoke link quality.

Answer: B

Explanation:

ADVPN (Auto-Discovery VPN) 2.0 is the optimal solution for enabling direct spoke-to-spoke communication without passing through the hub, while also allowing automatic link selection based on quality metrics.

- Dynamic Direct Tunnels:
  - ADVPN 2.0 allows spokes to establish direct IPsec tunnels dynamically based on traffic patterns, reducing latency and improving performance.
  - Unlike static VPNs, spokes do not need to pre-configure tunnels for each other.
- Automatic Link Optimization:
  - ADVPN 2.0 monitors the quality of multiple internet connections on each spoke.
  - It automatically switches to the best available connection when the primary link degrades or fails.
  - This is achieved by dynamically adjusting BGP-based routing or leveraging SD-WAN integration.

Question: 17

What does the command set forward-domain <domain_ID> in a transparent VDOM interface do?

A. It configures the interface to prioritize traffic based on the domain ID, enhancing quality of service for specified VLANs.

B. It isolates traffic within a specific VLAN by assigning a broadcast domain to an interface based on the VLAN ID.

C. It restricts the interface to managing traffic only from the specified VLAN, effectively segregating network traffic.

D. It assigns a unique domain ID to the interface, allowing it to operate across multiple VLANs within the same VDOM.

Answer: B

Explanation:

In a transparent mode Virtual Domain (VDOM) configuration, FortiGate operates as a Layer 2 bridge rather than

performing Layer 3 routing. The set forward-domain <domain_ID> command is used to control how traffic is forwarded between interfaces within the same transparent VDOM.

A forward-domain acts as a broadcast domain, meaning only interfaces with the same forwarddomain ID can exchange traffic. This setting is commonly used to separate different VLANs or network segments within the transparent VDOM while still allowing FortiGate to apply security policies.

Question: 18

Refer to the exhibit, which shows a physical topology and a traffic log.

The administrator is checking on FortiAnalyzer traffic from the device with IP address 10.1.10.1,

located behind the FortiGate ISFW device.

The firewall policy in on the ISFW device does not have UTM enabled and the administrator is surprised to see a log with the action Malware, as shown in the exhibit.

What are the two reasons FortiAnalyzer would display this log? (Choose two.)

A. Security rating is enabled in ISFW.

B. ISFW is in a Security Fabric environment.

C. ISFW is not connected to FortiAnalyzer and must go through NGFW-1.

D. The firewall policy in NGFW-1 has UTM enabled.

Answer: B, D

Explanation:

From the exhibit, ISFW is part of a Security Fabric environment with NGFW-1 as the Fabric Root. In this architecture, FortiGate devices share security intelligence, including logs and detected threats.

ISFW is in a Security Fabric environment:

- Security Fabric allows devices like ISFW to receive threat intelligence from NGFW-1, even if UTM is not enabled locally.
- If NGFW-1 detects malware from IP 10.1.10.1 to 89.238.73.97, this information can be propagated to ISFW and FortiAnalyzer.

The firewall policy in NGFW-1 has UTM enabled:

- Even though ISFW does not have UTM enabled, NGFW-1 (which sits between ISFW and the external network) does have UTM enabled and is scanning traffic.
- Since NGFW-1 detects malware in the session, it logs the event, which is then sent to FortiAnalyzer.

Question: 19

Refer to the exhibit, which contains a partial VPN configuration.

```
config vpn ipsec phasel-interface edit tunnel set type dynamic
set interface "portl*
set ike-version 2 set keylife 22800 set peertype any set net-device
disable set proposal aesl28-sha25€ aes256-sha256 set dpd on-idle
set add-route enable set psksecret fortinet next
end
```

What can you conclude from this VPN IPsec phase 1 configuration?

A. This configuration is the best for networks with regular traffic intervals, providing a balance between connectivity assurance and resource utilization.

B. Peer IDs are unencrypted and exposed, creating a security risk.

C. FortiGate will not add a route to its routing or forwarding information base when the dynamic tunnel is negotiated.

D. A separate interface is created for each dial-up tunnel, which can be slower and more resource intensive, especially in large networks.

Answer: A

Explanation:

This IPsec Phase 1 configuration defines a dynamic VPN tunnel that can accept connections from multiple peers. The settings chosen here suggest a configuration optimized for networks with intermittent traffic patterns while ensuring resources are used efficiently.

Key configurations and their impact:

- set type dynamic ^ This allows multiple peers to establish connections dynamically without needing predefined IP addresses.
- set ike-version 2 → Uses IKEv2, which is more efficient and supports features like EAP authentication and reduced rekeying overhead.
- set dpd on-idle → Dead Peer Detection (DPD) is triggered only when the tunnel is idle, reducing unnecessary keep-alive packets and improving resource utilization.
- set add-route enable → FortiGate automatically adds the route to the routing table when the tunnel is established, ensuring connectivity when needed.
- set proposal aes128-sha256 aes256-sha256 → Uses strong encryption and hashing algorithms, ensuring a secure connection.
- set keylife 28800 → Sets a longer key lifetime (8 hours), reducing the frequency of rekeying, which is beneficial for stable connections.

Because DPD is set to on-idle, the tunnel will not constantly send keep-alive messages but will still ensure connectivity when traffic is detected. This makes the configuration ideal for networks with regular but non-continuous traffic, balancing security and resource efficiency.

Question: 20

A company's users on an IPsec VPN between FortiGate A and B have experienced intermittent issues since implementing VXLAN. The administrator suspects that packets exceeding the 1500-byte default MTU are causing the problems.

In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that

add extra headers to IP packets?

A. Adjust the MTU on interfaces only if FortiGate has the FortiGuard enterprise bundle, which allows MTU modification.

B. Adjust the MTU on interfaces in all FortiGate devices that support the latest family of Fortinet SPUs: NP7, CP9 and SP5.

C. Adjust the MTU on interfaces in controlled environments where all devices along the path allow MTU interface changes.

D. Adjust the MTU on interfaces only in wired connections like PPPoE, optic fiber, and ethernet cable.

Answer: C

Explanation:

When using IPsec VPNs and VXLAN, additional headers are added to packets, which can exceed the default 1500-byte MTU. This can lead to fragmentation issues, dropped packets, or degraded performance.

To resolve this, the MTU (Maximum Transmission Unit) should be adjusted only if all devices in the network path support it. Otherwise, some devices may still drop or fragment packets, leading to continued issues.

Why adjusting MTU helps:

- VXLAN adds a 50-byte overhead to packets.
- IPsec adds additional encapsulation (ESP, GRE, etc.), increasing the packet size.
- If packets exceed the MTU, they may be fragmented or dropped, causing intermittent connectivity issues.
- Lowering the MTU on interfaces ensures packets stay within the supported size limit across all network devices.

Question: 21

Refer to the exhibit, which shows a command output.

E FortiGate B # get system session list | grep icmp

FortiGateB #

FortiGate_A and FortiGate_B are members of an FGSP cluster in an enterprise network.

While testing the cluster using the ping command, the administrator monitors packet loss and found that the session output on FortiGate_B is as shown in the exhibit.

What could be the cause of this output on FortiGate_B?

A. The session synchronization is encrypted.

B. session-pickup-connectionless is set to disable on FortiGate_B.

C. FortiGate_B is configured in passive mode.

D. FortiGate_A and FortiGate_B have the same standalone-group-id value.

Answer: B

Explanation:

The Fortinet FGSP (FortiGate Session Life Support Protocol) cluster allows session synchronization between two FortiGate devices to provide seamless failover. However, ICMP (ping) is a connectionless protocol, and by default, FortiGate does not synchronize connectionless sessions unless explicitly enabled.

In the exhibit:

- The command get system session list | grep icmp on FortiGate_B returns no output, meaning that ICMP sessions are not being synchronized from FortiGate_A.
- If session-pickup-connectionless is disabled, FortiGate_B will not receive ICMP sessions, causing packet loss during failover.

Question: 22

Refer to the exhibit, which shows a partial troubleshooting command output.

FortiGate # diagnose vpn tunnel list name Hub2Spokel

list ipsec tunnel by names in vd 0

. ..

npu flag=2O npu_rgwy=10.10.2.2 npu_lgwy=10.10.1.1 npu selid=l

An administrator is extensively using IPsec on FortiGate. Many tunnels show information similar to the output shown in the exhibit.

What can the administrator conclude?

A. IPsec SAs cannot be ofloaded.

B. The two IPsec SAs, inbound and outbound, are copied to the NPU.

C. Only the outbound IPsec SA is copied to the NPU.

D. Only the inbound IPsec SA is copied to the NPU.

Answer: A

Explanation:

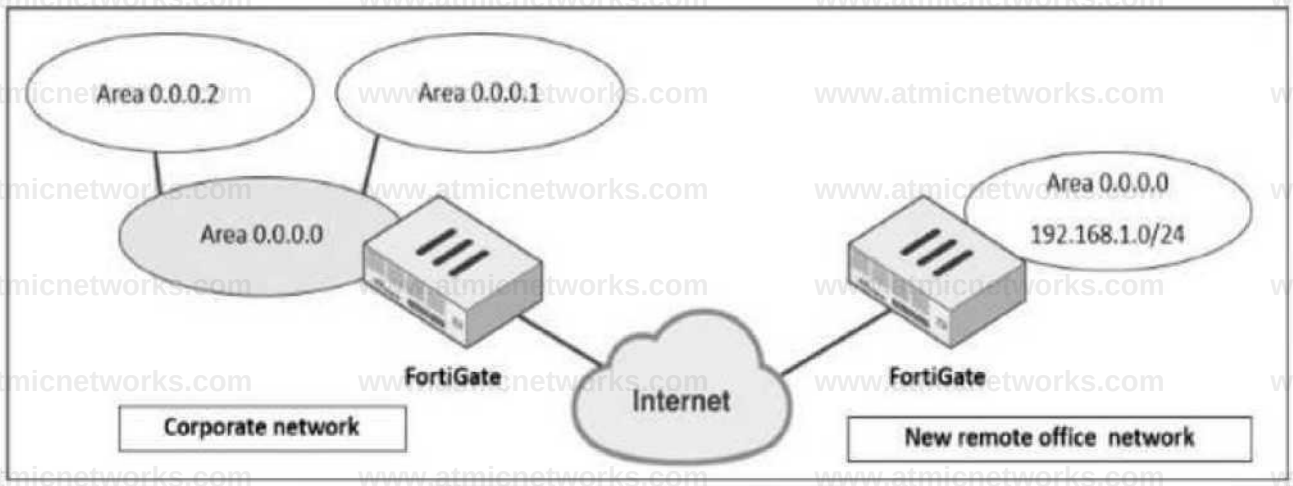
Based on the FortiGate Infrastructure 7.6 study guide and the Hardware Acceleration technical documentation, the diagnose vpn tunnel list command provides the status of IPsec tunnel ofloading to the Network Processor (NPU).

In the provided exhibit, the specific value npu_flag=20 (which corresponds to 0x20 in hexadecimal) indicates that the IPsec Security Association (SA) cannot be ofloaded to the NPU. While the NPU may have visibility of the gateway IPs (npu_rgwy and npu_lgwy), the flag itself serves as a diagnostic indicator that the traffic must be processed by the system CPU rather than the hardware accelerator.

This lack of ofloading typically occurs when the tunnel configuration uses a cipher (encryption algorithm) or an HMAC (authentication algorithm) that is not supported by the specific NPU model installed in the FortiGate. For example, if a tunnel is configured with a legacy or highly complex algorithm that the NP6 or NP7 chip is not designed to process in hardware, the FortiOS kernel handles the encryption and decryption, resulting in the npu_flag=20 status. Therefore, despite the presence of NPU-related fields, the specific flag value confirms that hardware acceleration is not active for these SAs.

Question: 23

Refer to the exhibit, which shows a corporate network and a new remote office network.



An administrator must integrate the new remote office network with the corporate enterprise network.

What must the administrator do to allow routing between the two networks?

A. The administrator must implement BGP to inject the new remote office network into the corporate FortiGate device

B. The administrator must configure a static route to the subnet 192.168.l.0/24 on the corporate FortiGate device.

C. The administrator must configure virtual links on both FortiGate devices.

D. The administrator must implement OSPF over IPsec on both FortiGate devices.

Answer: D

Explanation:

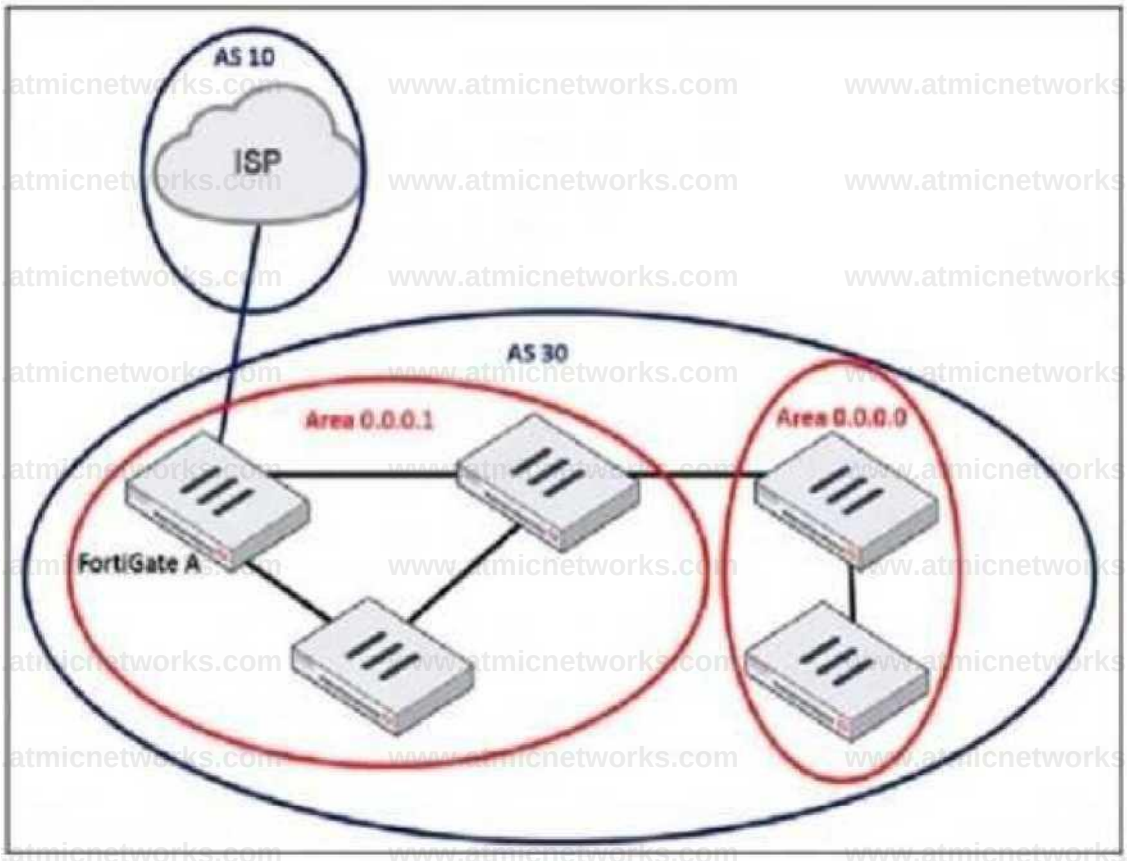
In this scenario, the corporate network and the new remote office network need to communicate over the Internet, which requires a secure and dynamic routing method. Since both networks are using OSPF (Open Shortest Path First) as the routing protocol, the best approach is to establish an OSPF over IPsec VPN to ensure secure and dynamic route propagation.

OSPF is already running on the corporate network, and extending it over an IPsec tunnel allows dynamic route exchange between the corporate FortiGate and the remote office FortiGate. IPsec provides encryption for traffic over the Internet, ensuring secure communication. OSPF over IPsec eliminates the need for manual static routes, allowing automatic route updates if networks change.

The new remote office's 192.168.1.0/24 subnet will be advertised dynamically to the corporate network without additional configuration.

Question: 24

Refer to the exhibit, which shows an enterprise network connected to an internet service provider.



The administrator must configure the BGP section of FortiGate A to give internet access to the enterprise network.

Which command must the administrator use to establish a connection with the internet service provider?

A. config neighbor

B. config redistribute bgp

C. config router route-map

D. config redistribute ospf

Answer: A

Explanation:

In BGP (Border Gateway Protocol), a neighbor (peer) configuration is required to establish a connection between two BGP routers. Since FortiGate A is connecting to the ISP (Autonomous System 10) from AS 30, the administrator must define the ISP's BGP router as a neighbor.

The config neighbor command is used to:

- Define the ISP's IP address as a BGP peer
- Specify the remote AS (AS 10 in this case)
- Allow BGP route exchanges between FortiGate A and the ISP

Question: 25

Refer to the exhibit, which shows the FortiGuard Distribution Network of a FortiGate device.

FortiGuard Distribution Network on FortiGate

0 License Infor (ration

Entitlement	Status	
0 Advanced Malware Protection	0 Licensed (Expiration Date; 2025/11/101	
D Attack Surface Security Rating	6 KensedlFxptrabort Date 2025/1110)	
loT Deter tlon Definitions	© Ver skxiC.00000	0 Upgrade Database
Outbreak Package DeftnitiorK	© Version 5 00036	
Security Rating & CIS Compliance	© Licensed (Expiration Date 2025/IV10)	
D Data Loss Prevention (DIP!	A Not licensed	
[X P Signatures	© Version 0,00000	
S Intrusion Prevention	0 Licensed (Expiration Dale 2025/1 V10|	
IPS Definitions	© Ver slon 28.00821	1 Actions'
IPS Ermine	© Version 7.00539	
Malicious URLs	© Version 1.00001	
Botnet IPs	© Version 7,03758	9 View Ust
Botnet Domains	© Version 100647	9 View Litt
G Operational Technology (OTI Security Sc	Tvice 0 Licensed 1 Expiration Date; 2025/11'10]	
S Wed Filtering	© Licensed (Expiration Date 2C25/11/1O!	
locked Certificates	© Version 100487	
DNS Filtering	© licensed (ExpirationDate 2025/11/10]	
Video Filter Ing	© Licenced (Expiration Date 2025/1110!	
SD WAN Network Monitor	A Not Licensed	1 Purchase •
SD-WAN Overlay as a Service	A Not Licensed	1 Purchase'

An administrator is trying to find the web filter database signature on FortiGate to resolve issues with websites not being filtered correctly in a flow-mode web filter profile.

Why is the web filter database version not visible on the GUI, such as with IPS definitions?

A. The web filter database is stored locally, but the administrator must run over CLI diagnose autoupdate versions.

B. The web filter database is stored locally on FortiGate, but it is hidden behind the GUI. It requires enabling debug mode to make it visible.

C. The web filter database is not hosted on FortiGate: FortiGate queries FortiGuard or FortiManager for web filter ratings on demand.

D. The web filter database is only accessible after manual syncing with a valid FDS server using diagnose test update info.

Answer: C

Explanation:

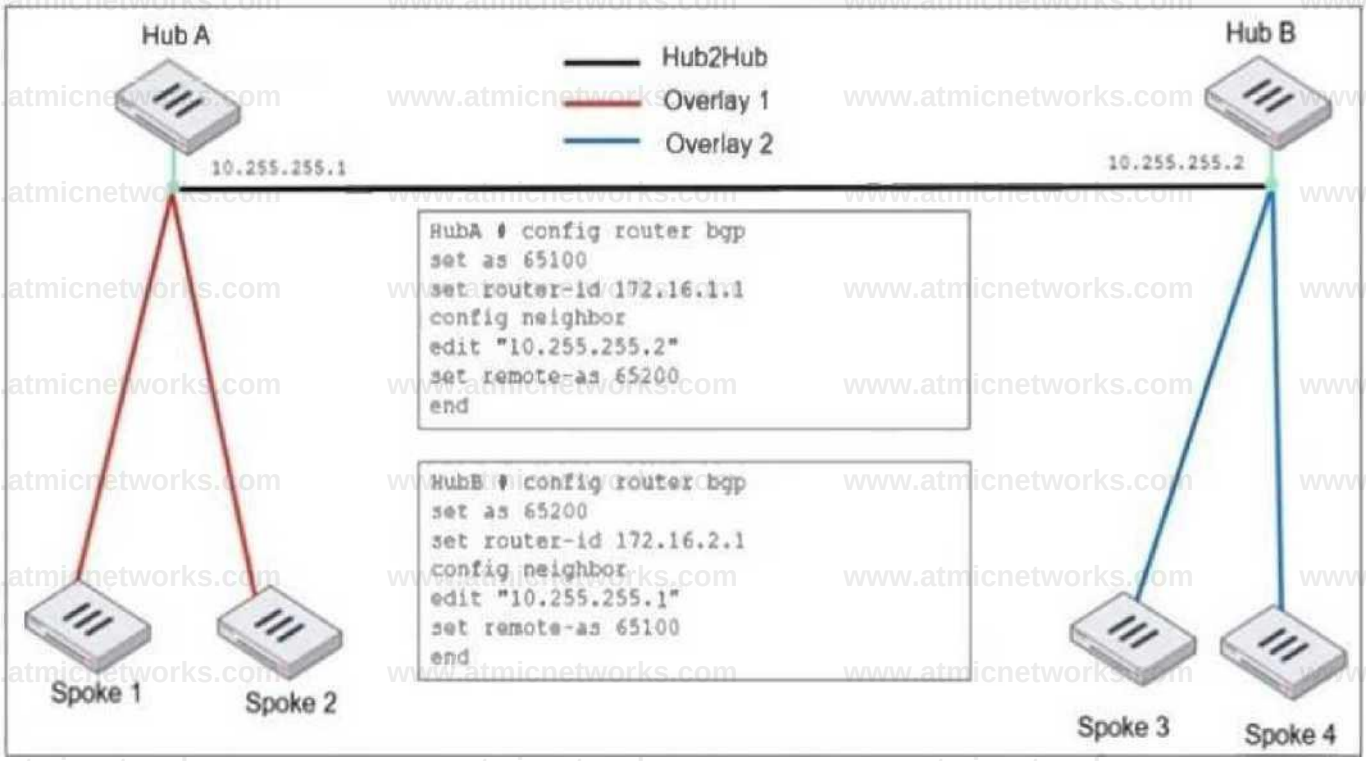
Unlike IPS or antivirus databases, FortiGate does not store a full web filter database locally. Instead, FortiGate queries FortiGuard (or FortiManager, if configured) dynamically to classify and filter web content in real time.

Key points:

- Web filtering works on a cloud-based model:
  - When a user requests a website, FortiGate queries FortiGuard servers to check its category and reputation.
  - The response is then cached locally for faster lookups on repeated requests.
- No local web filter database version:
  - Unlike IPS and antivirus, which download and store signature updates locally, web filtering relies on cloud-based queries.
  - This is why no database version appears in the GUI.
- Flow mode vs Proxy mode:
  - In proxy mode, FortiGate can cache some web filter data, improving performance.
  - In flow mode, all queries happen dynamically, with no locally stored database.

Question: 26

Refer to the exhibit, which shows an ADVPN network



An administrator must configure an ADVPN using IBGP and EBGP to connect overlay network 1 with 2.

What two options must the administrator configure in BGP? (Choose two.)

A. set ebgp-enforce-multrhop enable

B. set next-hop-self enable

C. set ibgp-enforce-multihop advpn

D. set attribute-unchanged next-hop

Answer: A, B

Explanation:

In this ADVPN (Auto-Discovery VPN) network, there are two hubs (Hub A and Hub B) connected via EBGP, while IBGP is used within each overlay. To ensure proper BGP routing between the overlays, the administrator must configure specific BGP options..

set ebgp-enforce-multihop enable

By default, EBGP requires directly connected neighbors. Since Hub A and Hub B are not directly connected but reach each other over an IPsec tunnel, multihop must be enabled for EBGP sessions to work.

set next-hop-self enable

In IBGP, the next-hop attribute does not change by default. When an IBGP route is advertised from a spoke to another hub or spoke, the next-hop needs to be updated to ensure proper reachability. Enabling next-hop-self forces the BGP speaker to advertise itself as the next-hop, ensuring that all spokes properly reach routes across the overlays.

Question: 27

Refer to the exhibit.

A pre-run CLI template that is used in zero-touch provisioning (ZTP) and low-touch provisioning (LTP) with FortiManager is shown.

The template is not assigned even though the configuration has already been installed on FortiGate.
What is true about this scenario?

A. The administrator did not assign the template correctly when adding the model device because pre-CLI templates remain permanently assigned to the firewall

B. Pre-run CLI templates are automatically unassigned after their initial installation

C. Pre-run CLI templates for ZTP and LTP must be unassigned manually after the first installation to avoid conflicting error objects when importing a policy package

D. The administrator must use post-run CLI templates that are designed for ZTP and LTP

Answer: B

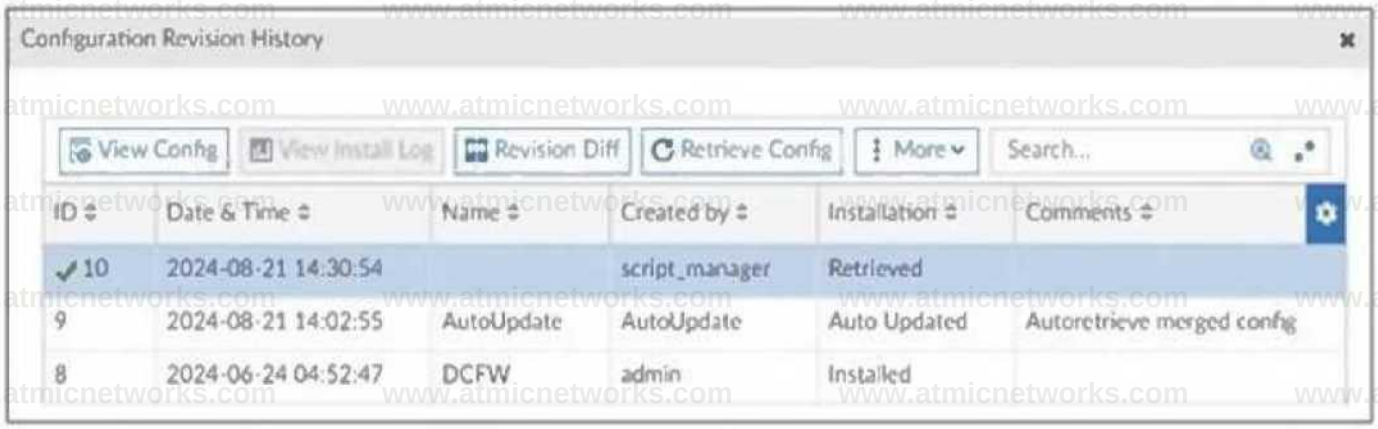
Explanation:

In FortiManager, pre-run CLI templates are used in Zero-Touch Provisioning (ZTP) and Low-Touch Provisioning (LTP) to configure a FortiGate device before it is fully managed by FortiManager.

These templates apply configurations when a device is initially provisioned. Once the pre-run CLI template is executed, FortiManager automatically unassigns it from the device because it is not meant to persist like other policy configurations. This prevents conflicts and ensures that the FortiGate configuration is not repeatedly applied after the initial setup.

Question: 28

Refer to the exhibit, which shows a revision history window in the FortiManager device layer.



The IT team is trying to identify the administrator responsible for the most recent update in the

FortiGate device database.

Which conclusion can you draw about this scenario?

A. This retrieved process was automatically triggered by a Remote FortiGate Directly (via CLI) script.

B. The user script_manager is an API user from the Fortinet Developer Network (FDN) retrieving a configuration.

C. To identify the user who created the event, check it on the Configuration and Installation widget on FortiGate within the FortiManager device layer.

D. Find the user in the FortiManager system logs and use the type=script command to find the administrator user in the user field.

Answer: D

Explanation:

The Configuration Revision History window in FortiManager shows that the most recent configuration change (ID 10) was created by script_manager with the action Retrieved.

Since script_manager is a system-level script execution user, the IT team needs to find who actually triggered this script.

This can be done by:

- Checking the FortiManager system logs for script execution events.
- Using the type=script filter to locate the administrator associated with the script execution.

Question: 29

Refer to the exhibit, which contains the partial output of an OSPF command.

```
FortiGate # get router info ospf status
Routing Process "ospf 0" with ID 0.0.0.5
Process uptime is 0 minute
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is enabled
Supports only single TOS(TOSO) routes
Supports opaque LSA
Do not support Restarting
This router is an ABR
```

An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.

What two conclusions can the administrator draw? (Choose two.)

A. The FortiGate device is a backup designated router

B. The FortiGate device is connected to multiple areas

C. The FortiGate device injects external routing information

D. The FortiGate device has OSPF ECMP enabled

Answer: B, C

Explanation:

The output of the get router info ospf status command provides key information about the OSPF (Open Shortest Path First) configuration on the FortiGate device.

The FortiGate device is connected to multiple areas

- The output states: "This router is an ABR"
- ABR (Area Border Router) means the device is connected to multiple OSPF areas and maintains routing information between them.
- This confirms that the FortiGate is not just in one area, but at least one backbone area (Area 0) and another OSPF area.

The FortiGate device injects external routing information

- The output states: "Supports opaque LSA"
- Opaque LSAs (Type 9, 10, and 11) are used in OSPF extensions, including those that support external route injection.
- Typically, ABRs or ASBRs (Autonomous System Boundary Routers) inject external routes, allowing routes from other routing protocols (such as BGP or static routes) to be advertised into OSPF.

Question: 30

Refer to the exhibit, which contains a partial command output.

FortiGate « get router info bgp neighbors

```
VRF 0 neighbor table:
BGP neighbor is 100.65.4.1, remote AS 65300, local AS 65200, external link
 BGP version 4, remote router ID 0.0.0.0
 BGP state = Idle
 Not directly connected EBGP
 Last read , hold time is 180, keepalive interval is 60 seconds
 Configured hold time is 180, keepalive interval is 60 seconds
 Received 0 messages, 0 notifications, 0 in queue
 Sent 0 messages, 0 notifications, 0 In queue
 Route refresh request: received 0, sent 0
 NLRI treated as withdraw: 0
 Minimum time between advertisement runs is 30 seconds
 Update source is Loopback
```

The administrator has configured BGP on FortiGate. The status of this new BGP configuration is shown in the exhibit.

What configuration must the administrator consider next?

A. Configure a static route to 100.65.4.1.

B. Configure the local AS to 65300.

C. Contact the remote peer administrator to enable BGP

D. Enable ebgp-enforce-multihop.

Answer: D

Explanation:

From the BGP neighbor status output, the key issue is that BGP is stuck in the "Idle" state, meaning the FortiGate is unable to establish a BGP session with its peer 100.65.4.1 (Remote AS 65300).

The output also shows:

- "Not directly connected EBGP" → This means the BGP peer is not on the same subnet, requiring multihop BGP.
- "Update source is Loopback" → Since a loopback interface is used, FortiGate must be configured to allow BGP neighbors over multiple hops.

To resolve this issue, the administrator must enable ebgp-enforce-multihop, which allows BGP sessions to be established even when the neighbors are not directly connected.

Question: 31

Refer to the exhibit, which shows the packet capture output of a three-way handshake between FortiGate and FortiManager Cloud.

Packet capture output of three-way handshake between a FortiGate and a FortiManager Cloud

```
Frame 35: 1034 byte* an wire (8272 bits), 10)4 bytes captured (8272 bits) co interface *, id 0
* Ethernet II, Src: 50:e5:d5:          (50:e5:d5:          ), Dst: Fortlnet_          (e«:23:ff:          )
Internet Protocol Version 4, Src; 192.168.2.66, Dst: 154.52.4.164
Transmission Control Protocol, Src Port: 16304, Ost Port: 541, Seq: 1, Ack: 1, ten: 980
* Transport layer Security v TLSvl.3 Record Layer: Handshake Protocols Client Hello Content Type: Handshake (22)
version: TlS 1.8 (0x0301) length: 975
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1) length; 971
        Version: TLS 1.2 (0x0303) Random: al4f«c4b«f9313bf Session ID Length: 32 session ID; aWe426e96e83a5
        Cipher Suites Length: 34 Cipher Suites (17 suites) Compression Methods Length: 1 Compression Methods (1
        method) Extensions Length: 864
      * Extension; servername (len^AS) name-9398,support.fortinet-ca2.fortlnet.com Type: server_name (0) Length:
          45
        * Server Name Indication extension
            Server Name list length: 43
            Server Name Type: host_name (0)
            Server Hane length: 40
            Server Name: 939S.suppcrt.fortinet-ca2.fortlnet.com
        Extension: ecj»lnt_fcrmats (len-4) > Extension: supportedjjro_ups (len-22)
        Extension: session_tlcket (lenng)
        Extension: encrypt_then_mac (len«0)
        Extension: extendedmastersecret (len«0)
        Extension; signature algorithm (len-48)
        Extension: supported_versiQns (len«9) TLS 1.3, TLS 1.2, TLS 1.1, TLS 10
> Extension; psk key exchange_modes (len-2)
```

What two conclusions can you draw from the exhibit? (Choose two.)

A. FortiGate will receive a certificate that supports multiple domains because FortiManager operates in a cloud computing environment.

B. FortiGate is connecting to the same IP server and will receive an independent certificate for its connection between FortiGate and FortiManager Cloud.

C. If the TLS handshake contains 17 cipher suites it means the TLS version must be 1.0 on this threeway handshake.

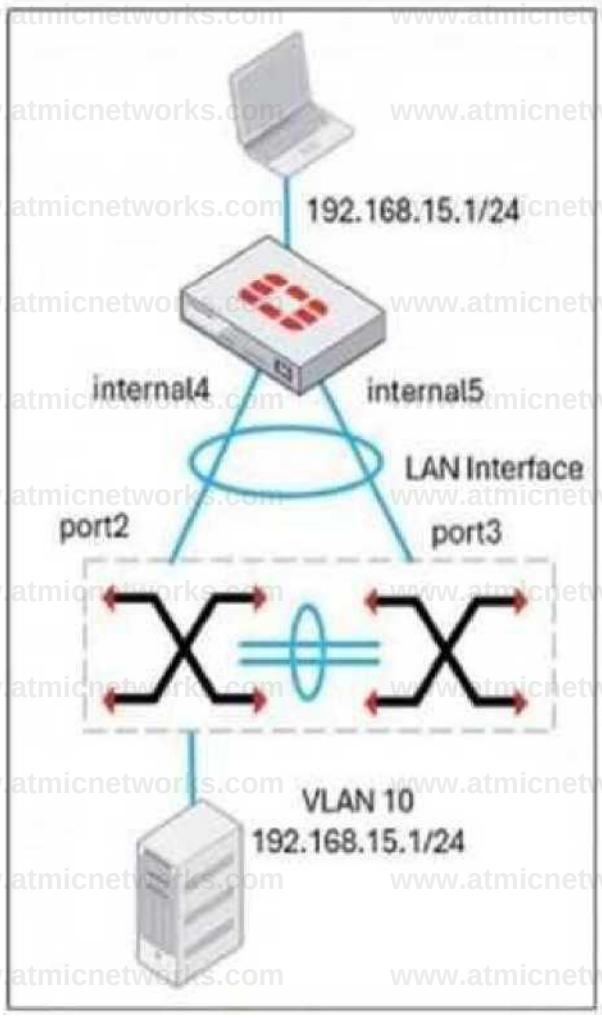
D. The wildcard for the domain *.fortinet-ca2.support.fortinet.com must be supported by FortiManager Cloud.

Answer: AD

Explanation:

Question: 32

Refer to the exhibit, which shows a LAN interface connected from FortiGate to two FortiSwitch devices.



What two conclusions can you draw from the corresponding LAN interface? (Choose two.)

A. You must enable STP or RSTP on FortiGate and FortiSwitch to avoid layer 2 loopbacks.

B. The LAN interface must use a 802.3ad type interface.

C. This connection is using a FortiLInk to manage VLANs on FortiGate.

D. FortiGate is using an SD-WAN-type interface to connect to a FortiSwitch device with MCLAG.

Answer: B, C

Explanation:

The diagram shows a FortiGate connected to two FortiSwitches, which suggests the use of FortiLink, Fortinet's protocol for managing switches directly from a FortiGate. Since multiple connections are being used, the LAN interface must be set to 802.3ad (LAG) mode to aggregate the links for redundancy and load balancing.

This setup allows FortiGate to handle VLAN assignments dynamically, as seen with VLAN 10 (192.168.15.1/24). FortiLink ensures seamless integration between FortiGate and FortiSwitches, making STP unnecessary because Fortinet's MCLAG prevents loops at Layer 2. SD-WAN, on the other hand, is used for WAN interfaces and does not apply to switch connectivity in this scenario.

Question: 33

Refer to the exhibit, which shows the HA status of an active-passive cluster.

Status	Priority	Hostname	Virtual Domains	Role	System Uptime
□ Virtual duster 1 ©					
© Synchronized	150	FortiGate.A	ft Corel ft root	Primary	4h52m
© Synchronized	100	FortiGate.B	ft Corel ft root	Secondary	4h 52m
0 Virtual duster? ©					
© Synchronized	150	FortiGate.A	ft Core?	Primary	
© Synchronized	128	FortiGate.B	ft Core?	Secondary	

An administrator wants FortiGate_B to handle the Core2 VDOM traffic.

Which modification must the administrator apply to achieve this?

A. The administrator must disable override on FortiGate_A.

B. The administrator must change the priority from 100 to 160 for FortiGate_B.

C. The administrator must change the load balancing method on FortiGate_B.

D. The administrator must change the priority from 128 to 200 for FortiGate_B.

Answer: D

Explanation:

The exhibit shows an active-passive HA (high availability) cluster with two virtual clusters, where FortiGate_A is the primary device for both Core1 and Core2. If the goal is to have FortiGate_B take over Core2 traffic, its priority must be higher than FortiGate_A for Virtual Cluster 2.

Currently, FortiGate_A has a priority of 150 for Core2, while FortiGate_B has 128. Increasing FortiGate_B's priority to 200 ensures it becomes the primary for Virtual Cluster 2, taking over the Core2 VDOM traffic while keeping Core1 traffic on FortiGate_A.

Disabling override would prevent forced failovers but wouldn't change the role distribution.

Adjusting the load-balancing method is irrelevant in an active-passive setup, as it only applies to active-active configurations.

Question: 34

During the maintenance window, an administrator must sniff all the traffic going through a specific firewall policy, which is handled by NP6 interfaces. The output of the sniffer trace provides just a few packets.

Why is the output of sniffer trace limited?

A. The traffic corresponding to the firewall policy is encrypted.

B. auto-asic-off load is set to enable in the firewall policy,

C. inspection-mode is set to proxy in the firewall policy.

D. The option npudbg is not added in the diagnose sniff packet command.

Answer: B

Explanation:

FortiGate devices with NP6 (Network Processor 6) acceleration ofload traffic directly to hardware, bypassing the CPU for improved performance. When auto-asic-ofload is enabled in a firewall policy, most of the traffic does not reach the CPU, which means it won't be captured by the standard sniffer trace command.

Since NP6-accelerated traffic is handled entirely in hardware, only a small portion of initial packets (such as session setup

packets or exceptions) might be seen in the sniffer output. To capture all packets, the administrator must disable hardware ofloading using:

config firewall policy

edit <policy_ID>

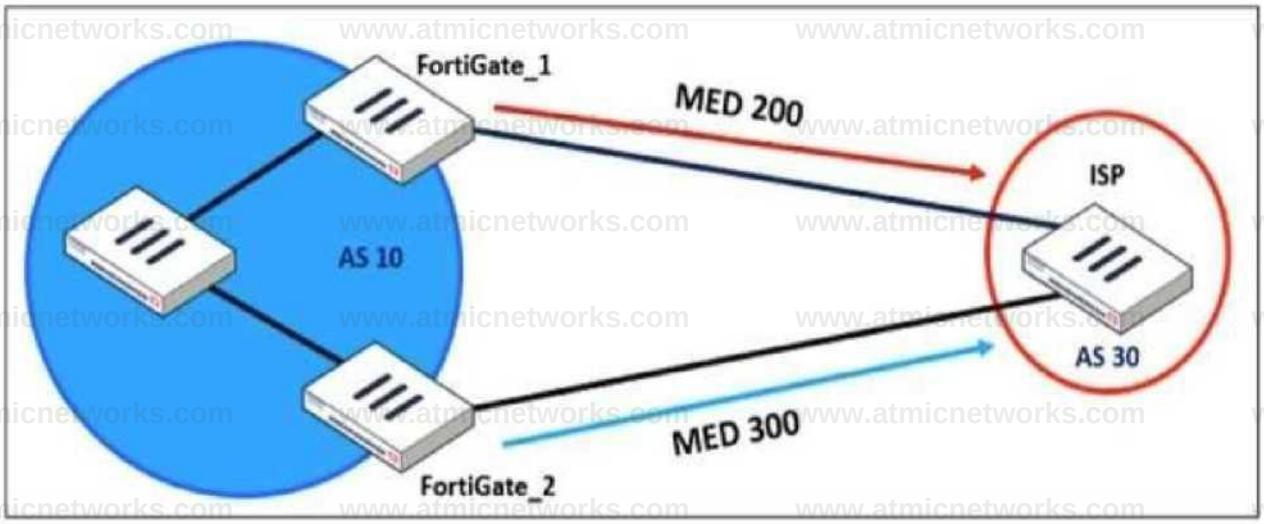
set auto-asic-ofload disable

end

Disabling ASIC ofload forces traffic to be processed by the CPU, allowing the sniffer tool to capture all packets.

Question: 35

Refer to the exhibit, which shows a network diagram.



An administrator would like to modify the MED value advertised from FortiGate_1 to a BGP neighbor in the autonomous system 30.

What must the administrator configure on FortiGate_1 to implement this?

A. route-map-out

B. network-import-check

C. prefix-list-out

D. distribute-list-out

Answer: A

Explanation:

The Multi-Exit Discriminator (MED) is a BGP attribute used to influence the preferred path for incoming traffic from an external autonomous system (AS). The diagram shows that FortiGate_1 advertises MED 200, while FortiGate_2 advertises MED 300, meaning the ISP will prefer the route through FortiGate_1 because a lower MED is preferred in BGP.

To modify the MED value on FortiGate_1 for routes advertised to AS 30, the administrator must configure a route-map-out. A route map can match specific routes and set the MED value before sending them to the BGP neighbor.

Question: 36

An administrator received a FortiAnalyzer alert that a 1 TB disk filled up in a day. Upon investigation, they found thousands of unusual DNS log requests, such as JHCMQK.website.com, with no answers. They later discovered that DNS exfiltration was occurring through both UDP and TLS.

How can the administrator prevent this data theft technique?

A. Create an inline-CASB to protect against DNS exfiltration.

B. Configure a File Filter profile to prevent DNS exfiltration.

C. Enable DNS Filter to protect against DNS exfiltration.

D. Use an IPS profile and DNS exfiltration-related signatures.

Answer: D

Explanation:

The excessive DNS log requests with random subdomains suggest a DNS exfiltration attack, where attackers encode and transmit data via DNS queries. Since this technique can use both UDP and TLS (DoH - DNS over HTTPS), a comprehensive security approach is needed.

Using an IPS profile with DNS exfiltration-specific signatures allows FortiGate to:

- Detect and block abnormal DNS query patterns often used in exfiltration.
- Inspect encrypted DNS (DoH, DoT) traffic if SSL inspection is enabled.
- Identify known exfiltration domains and techniques based on FortiGuard threat intelligence.

Question: 37

An administrator configured the FortiGate devices in an enterprise network to join the Fortinet Security Fabric. The administrator has a list of IP addresses that must be blocked by the data center firewall. This list is updated daily.

How can the administrator automate a firewall policy with the daily updated list?

A. With FortiNAC

B. With FortiAnalyzer

C. With a Security Fabric automation

D. With an external connector from Threat Feeds

Answer: D

Explanation:

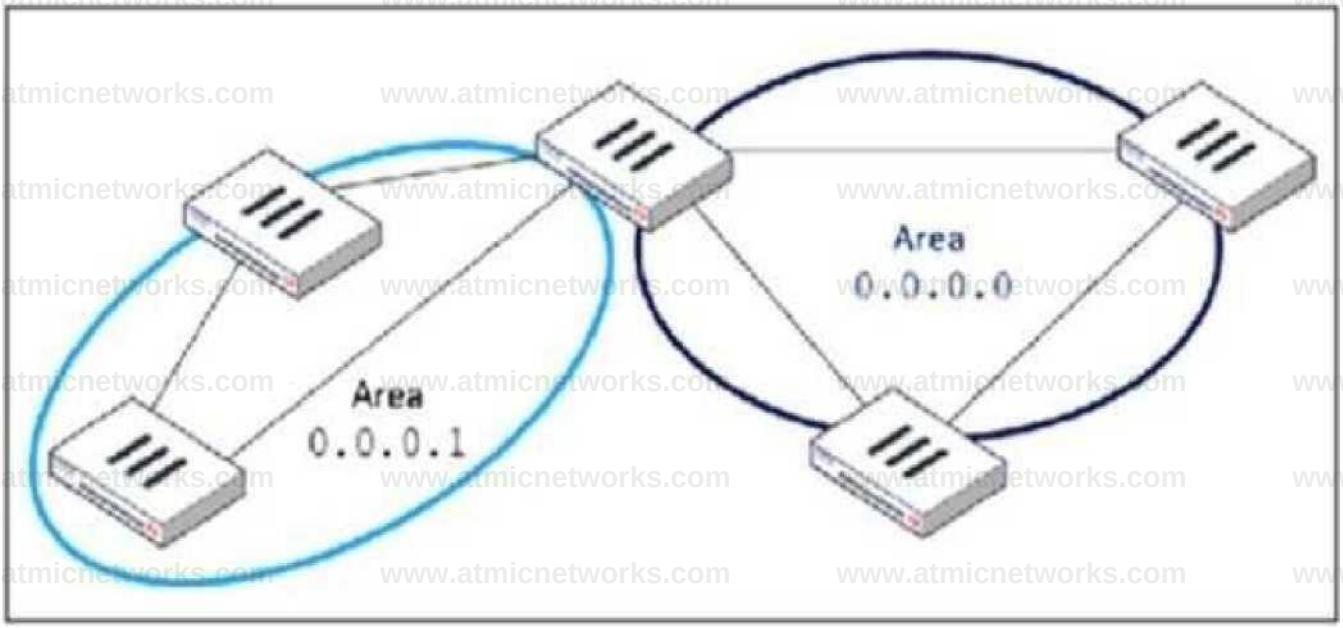
The best way to automate a firewall policy using a daily updated list of IP addresses is by using an external connector from Threat Feeds. This allows FortiGate to dynamically retrieve real-time threat intelligence from external sources and apply it directly to security policies.

By configuring Threat Feeds, the administrator can:

- Automatically update firewall policies with the latest malicious IPs daily.
- Block traffic from those IPs in real-time without manual intervention.
- Integrate with FortiGuard, third-party threat intelligence sources, or custom feeds (CSV, STIX/TAXII, etc.).

Question: 38

Refer to the exhibit, which shows an OSPF network.



Which configuration must the administrator apply to optimize the OSPF database?

A. Set a route map in the AS boundary FortiGate.

B. Set the area 0.0.0.1 to the type STUB in the area border FortiGate.

C. Set an access list in the AS boundary FortiGate.

D. Set the area 0.0.0.1 to the type NSSA in the area border FortiGate.

Answer: B

Explanation:

The OSPF database optimization is necessary to reduce unnecessary routing information and improve network performance. In the given topology, Area 0.0.0.1 is a non-backbone area connected to Area 0.0.0.0 (the backbone area) through an Area Border Router (ABR).

To optimize OSPF in this scenario, configuring Area 0.0.0.1 as a Stub Area will:

- Reduce the size of the OSPF database by preventing external routes (from outside OSPF) from being injected into Area 0.0.0.1.
- Allow only intra-area and inter-area routes, meaning routers in Area 0.0.0.1 will rely on a default route for external destinations.

- Improve convergence time and reduce router processing load since fewer LSAs (Link-State Advertisements) are exchanged.

Question: 39

The IT department discovered during the last network migration that all zero phase selectors in phase 2 IPsec configurations impacted network operations.

What are two valid approaches to prevent this during future migrations? (Choose two.)

A. Use routing protocols to specify allowed subnets over the tunnel.

B. Configure an IPsec-aggregate to create redundancy between each firewall peer.

C. Clearly indicate to the VPN which segments will be encrypted in the phase two selectors.

D. Configure an IP address on the IPsec interface of each firewall to establish unique peer connections and avoid impacting network operations.

Answer: A, C

Explanation:

Zero phase selectors in IPsec Phase 2 mean that no specific traffic selectors (subnets) are defined, allowing any traffic to be encrypted through the VPN tunnel. This can cause unintended traffic forwarding issues and disrupt network operations.

To prevent this from happening during future migrations:

- Using routing protocols ensures that only specific subnets are advertised over the tunnel. Dynamic routing (such as OSPF or BGP) helps define which networks should use the tunnel, preventing unintended traffic from being encrypted.
- Clearly defining phase 2 selectors avoids the problem of encrypting all traffic by explicitly stating the allowed source and destination subnets. This prevents the tunnel from affecting unrelated network traffic.

Question: 40

How will configuring set tcp-mss-sender and set tcp-mss-receiver in a firewall policy affect the size and handling of TCP packets in the network?

A. The maximum segment size permitted in the firewall policy determines whether TCP packets are allowed or denied.

B. Applying commands in a firewall policy determines the largest payload a device can handle in a single TCP segment.

C. The administrator must consider the payload size of the packet and the size of the IP header to configure a correct value in the firewall policy.

D. The TCP packet modifies the packet size only if the size of the packet is less than the one the administrator configured in the firewall policy.

Answer: B

Explanation:

The set tcp-mss-sender and set tcp-mss-receiver commands in a firewall policy allow an administrator to adjust the Maximum Segment Size (MSS) of TCP packets.

This setting controls the largest payload size that a device can handle in a single TCP segment, ensuring that packets do not exceed the allowed MTU (Maximum Transmission Unit) along the network path.

- set tcp-mss-sender adjusts the MSS value for outgoing TCP traffic.
- set tcp-mss-receiver adjusts the MSS value for incoming TCP traffic.

This helps prevent issues with fragmentation and MTU mismatches, improving network performance and avoiding retransmissions.

Question: 41

A vulnerability scan report has revealed that a user has generated traffic to the website example.com (10.10.10.(10) using a weak SSL/TLS version supported by the HTTPS web server.

What can the firewall administrator do to block all outdated SSL/TLS versions on any HTTPS web server to prevent possible attacks on user traffic?

A. Configure the unsupported SSL version and set the minimum allowed SSL version in the HTTPS settings of the SSL/SSH inspection profile.

B. Enable auto-detection of outdated SSL/TLS versions in the SSL/SSH inspection profile to block vulnerable websites.

C. Install the required certificate in the client's browser or use Active Directory policies to block specific websites as defined in the SSL/SSH inspection profile.

D. Use the latest certificate, Fortinet_SSL_ECDSA256, and replace the CA certificate in the SSL/SSH inspection profile.

Answer: A

Explanation:

The best way to block outdated SSL/TLS versions is to configure the SSL/SSH inspection profile to enforce a minimum SSL/TLS version and disable weak SSL versions.

By setting the minimum allowed SSL version in the HTTPS settings of the SSL/SSH inspection profile, FortiGate will:

- Block any connection using outdated SSL/TLS versions (such as SSLv3, TLS 1.0, or TLS 1.1).
- Enforce secure communication using only strong SSL/TLS versions (such as TLS 1.2 or TLS 1.3).
- Protect users from man-in-the-middle (MITM) and downgrade attacks that exploit weak encryption.

Question: 42

Refer to the exhibit, which contains the partial output of an OSPF command.

```
FortiGate # get router info ospf status
Routing Process "ospf 0" with ID 0.0.0.5
Process uptime is 0 minute
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is enabled
Supports only single TOS(TOSO) routes
Supports opaque LSA
Do not support Restarting
This router is an ASBR
```

An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.

Which statement on this FortiGate device is correct?

A. The FortiGate device can inject external routing information.

B. The FortiGate device is in the area 0.0.0.5.

C. The FortiGate device does not support OSPF ECMP.

D. The FortiGate device is a backup designated router.

Answer: A

Explanation:

From the OSPF status output, the key information is:

- "This router is an ASBR" → This means the FortiGate is acting as an Autonomous System Boundary Router (ASBR).
- An ASBR is responsible for injecting external routing information into OSPF from another routing protocol (such as BGP, static routes, or connected networks).

Question: 43

An administrator is setting up an ADVPN configuration and wants to ensure that peer IDs are not exposed during VPN establishment.

Which protocol can the administrator use to enhance security?

A. Use IKEv2, which encrypts peer IDs and prevents exposure.

B. Opt for SSL VPN web mode because it does not use peer IDs at all.

C. Choose IKEv1 aggressive mode because it simplifies peer identification.

D. Stick with IKEv1 main mode because it offers better performance.

Answer: A

Explanation:

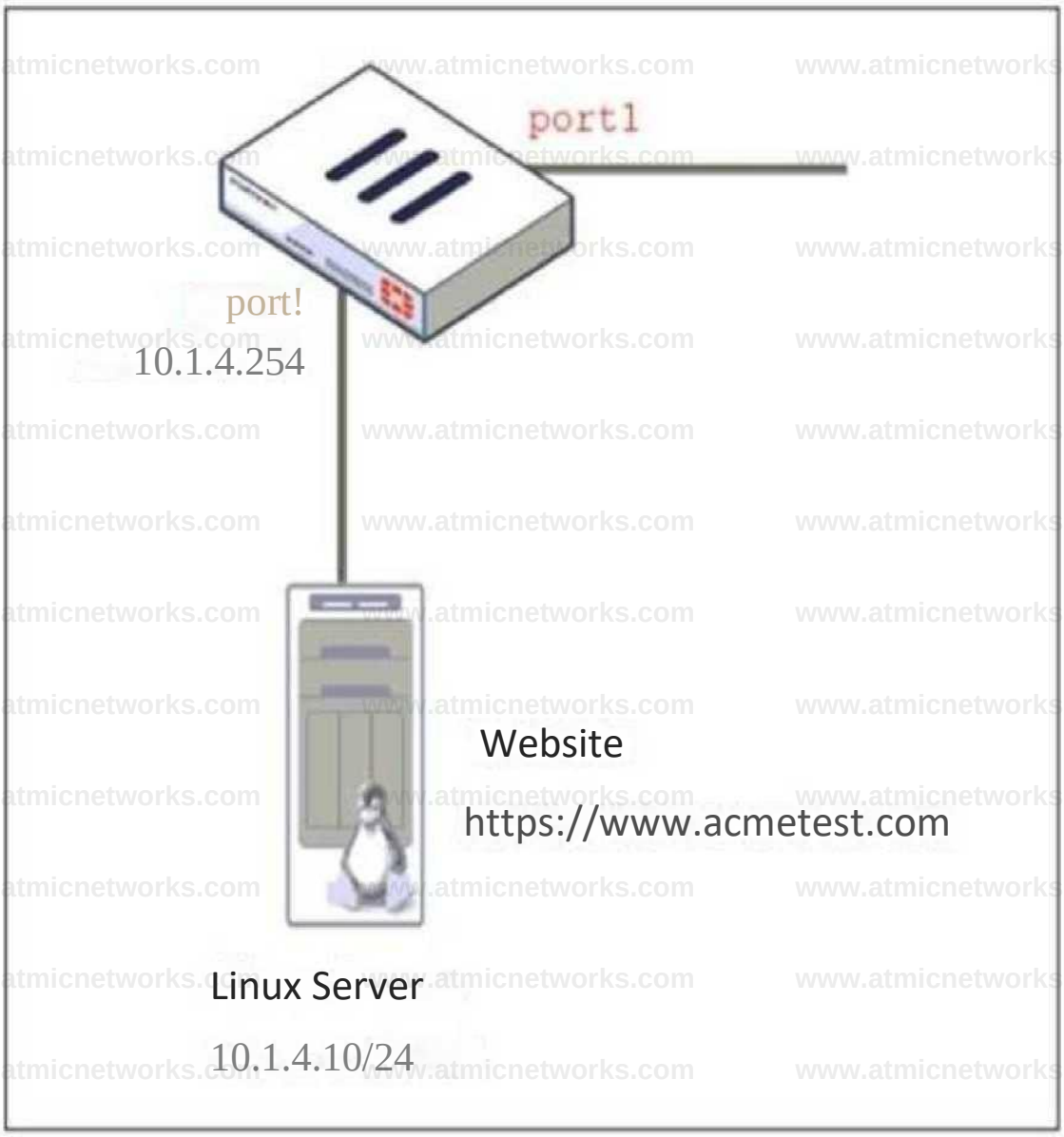
In ADVPN (Auto-Discovery VPN) configurations, security concerns include protecting peer IDs during VPN establishment. Peer IDs are exchanged in the IKE (Internet Key Exchange) negotiation phase, and their exposure could lead to privacy risks or targeted attacks.

- IKEv2 encrypts peer IDs, making it more secure compared to IKEvl, where peer IDs can be exposed in plaintext in aggressive mode.
- IKEv2 also provides better performance and flexibility while supporting dynamic tunnel establishment in ADVPN.

Question: 44

Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

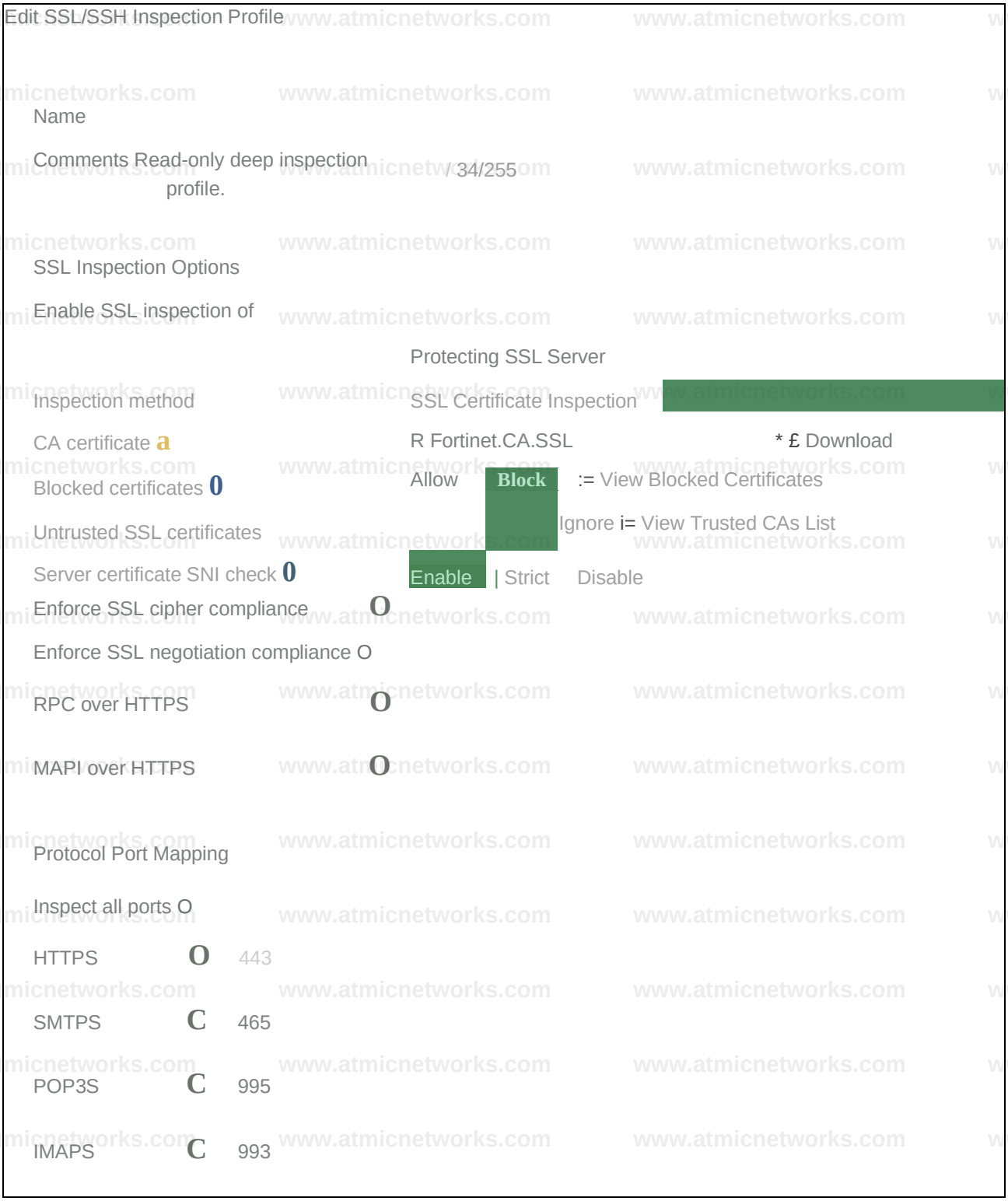
Network Topology



Firewall policy on FortiGate

```
DCFW I sh firewall policy 3 config firewall policy edit 3 set
tyane "To Linux Servers" set uuid bf77d59e-5513-51ef-147d-
e35066c267e9 set srcintf "portl" set dstintf "port3" set
action accept set srcaddr "all" set dstaddr "10.1.4." set
schedule "always" set service "ALL" set utm-status enable set
inspection-node proxy set ssl-ssh-prcfile "deep-inspection*
set ips-sensor "IPS Monitor" set logtraffic all next end
```

SSL/SSH inspection profile



Why is FortiGate unable to detect HTTPS attacks on firewall policy ID 3 targeting the Linux server?

A. The administrator must set the policy to inspection mode to analyze the HTTPS packets as expected.

B. The administrator must enable HTTPS in the protocol port mapping of the deep- inspection SSL/SSH inspection

profile.

C. The administrator must enable SSL inspection of the SSL server and upload the certificate of the Linux server website to the SSL/SSH inspection profile.

D. The administrator must enable cipher suites in the SSL/SSH inspection profile to decrypt the message.

Answer: C

Explanation:

The FortiGate SSL/SSH inspection profile is configured for Full SSL Inspection, which is necessary to analyze encrypted HTTPS traffic. However, the firewall policy is protecting an SSL server (the Linux server hosting the website), and currently, the SSL/SSH profile only applies to client-side SSL inspection.

To detect HTTPS-based attacks targeting the Linux server:

- FortiGate must act as an SSL intermediary to inspect encrypted traffic destined for the web server.
- The administrator must upload the SSL certificate of the Linux web server to FortiGate so that the server-side SSL inspection can decrypt incoming HTTPS traffic before analyzing it.

Question: 45

An administrator must minimize CPU and RAM use on a FortiGate firewall while also enabling essential security features, such as web filtering and application control for HTTPS traffic.

Which SSL inspection setting helps reduce system load while also enabling security features, such as web filtering and application control for encrypted HTTPS traffic?

A. Use full SSL inspection to thoroughly inspect encrypted payloads.

B. Disable SSL inspection entirely to conserve resources.

C. Configure SSL inspection to handle HTTPS traffic efficiently.

D. Enable SSL certificate inspection mode to perform basic checks without decrypting traffic.

Answer: D

Explanation:

To minimize CPU and RAM usage while still enforcing security features like web filtering and application control, SSL certificate inspection mode is the best choice.

- SSL certificate inspection allows FortiGate to inspect only the SSL/TLS handshake, including the Server Name Indication (SNI) and certificate details, without decrypting the full encrypted payload.

- This enables features like web filtering and application control because FortiGate can determine the destination website or application based on SNI and certificate information.
- It significantly reduces system load compared to full SSL inspection, which requires full decryption and re-encryption of traffic.

Question: 46

An administrator must standardize the deployment of FortiGate devices across branches with consistent interface roles and policy packages using FortiManager.

What is the recommended best practice for interface assignment in this scenario?

A. Enable metadata variables to use dynamic configurations in the standard interfaces of FortiManager.

B. Use the Install On feature in the policy package to automatically assign different interfaces based on the branch.

C. Create interfaces using device database scripts to use them on the same policy package of FortiGate devices.

D. Create normalized interface types per-platform to automatically recognize device layer interfaces based on the FortiGate model and interface name.

Answer: A

Explanation:

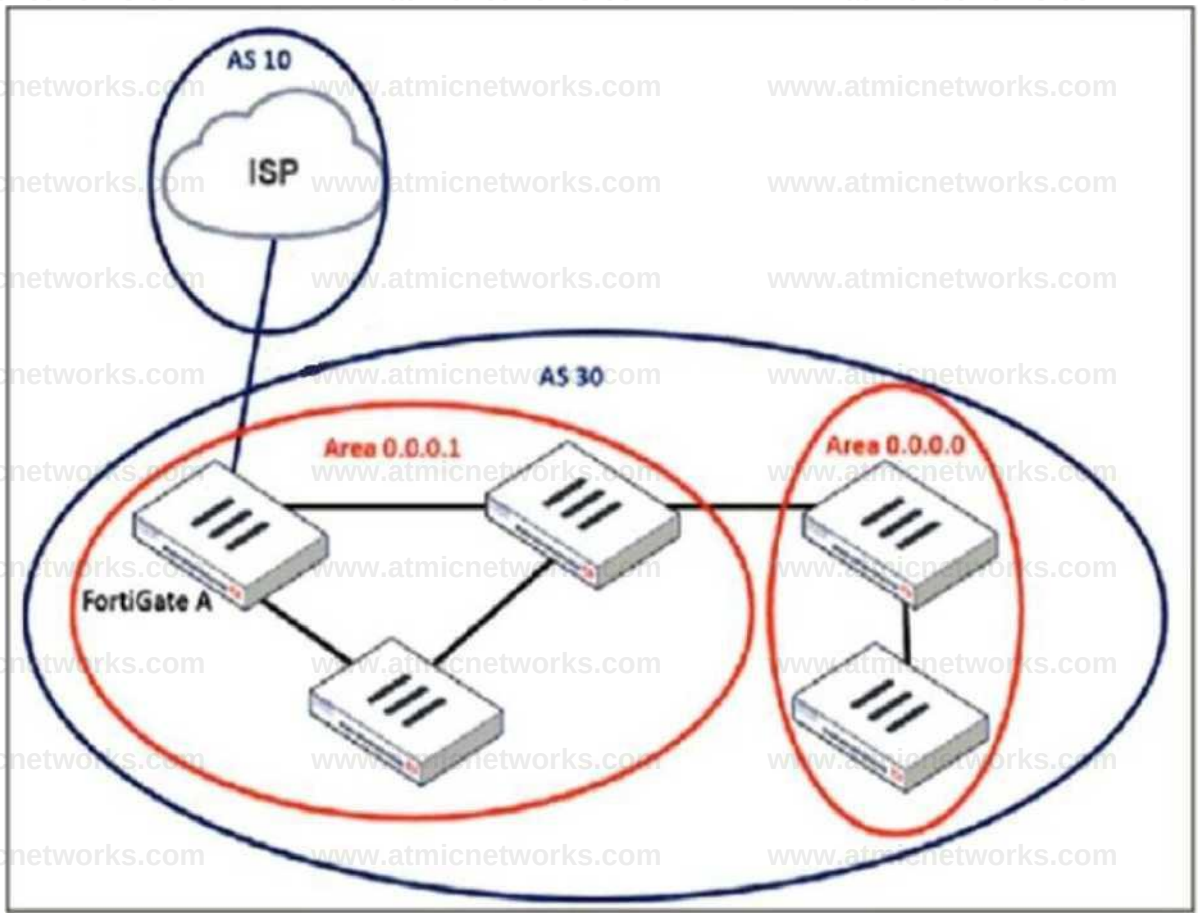
When standardizing the deployment of FortiGate devices across branches using FortiManager, the best practice is to use metadata variables. This allows for dynamic interface configuration while maintaining a single, consistent policy package for all branches.

- Metadata variables in FortiManager enable interface roles and configurations to be dynamically assigned based on the specific FortiGate device.
- This ensures scalability and consistent security policy enforcement across all branches without manually adjusting interface settings for each device.

- When a new branch FortiGate is deployed, metadata variables automatically map to the correct physical interfaces, reducing manual configuration errors.

Question: 47

Refer to the exhibit, which shows an enterprise network connected to an internet service provider.



An administrator must configure a loopback as a BGP source to connect to the ISP.

Which two commands are required to establish the connection? (Choose two.)

A. ebgp-enforce-multihop

B. update-source

C. ibgp-enforce-multihop

D. recursive-next-hop

Answer: A, B

Explanation:

When configuring a loopback interface as the BGP source for connecting to an ISP, two important settings must be applied:

1. Enable EBGP Multihop (ebgp-enforce-multihop)

BGP normally expects directly connected neighbors, but since the ISP and FortiGate A are using loopback interfaces, packets will not be sent directly between their physical interfaces.

The ebgp-enforce-multihop command allows BGP to form an eBGP peering over multiple hops.

2. Set the Update Source (update-source)

Since FortiGate is using a loopback interface as the source, the update-source command ensures that BGP updates originate from the loopback interface rather than a physical interface.

This is essential because BGP peers must match the source IP with the configured neighbor address.

Question: 48

What action can be taken on a FortiGate to block traffic using IPS protocol decoders, focusing on network transmission patterns and application signatures?

A. Use the DNS filter to block application signatures and protocol decoders.

B. Use application control to limit non-URL-based software handling.

C. Enable application detection-based SD-WAN rules.

D. Configure a web filter profile in flow mode.

Answer: B

Explanation:

FortiGate's IPS protocol decoders analyze network transmission patterns and application signatures to identify and block malicious traffic. Application Control is the feature that allows FortiGate to detect, classify, and block applications based on their behavior and signatures, even when they do not rely on traditional URLs.

- Application Control works alongside IPS protocol decoders to inspect packet payloads and enforce security policies based on recognized application behaviors.
- It enables granular control over non-URL-based applications such as P2P traffic, VoIP, messaging apps, and other non-web-based protocols that IPS can identify through protocol decoders.

- IPS and Application Control together can detect evasive or encrypted applications that might bypass traditional firewall rules.

Question: 49

An administrator is designing an ADVPN network for a large enterprise with spokes that have varying numbers of internet links. They want to avoid a high number of routes and peer connections at the hub.

Which method should be used to simplify routing and peer management?

A. Deploy a full-mesh VPN topology to eliminate hub dependency.

B. Implement static routing over IPsec interfaces for each spoke.

C. Use a dynamic routing protocol using loopback interfaces to streamline peers and routes.

D. Establish a traditional hub-and-spoke VPN topology with policy routes.

Answer: C

Explanation:

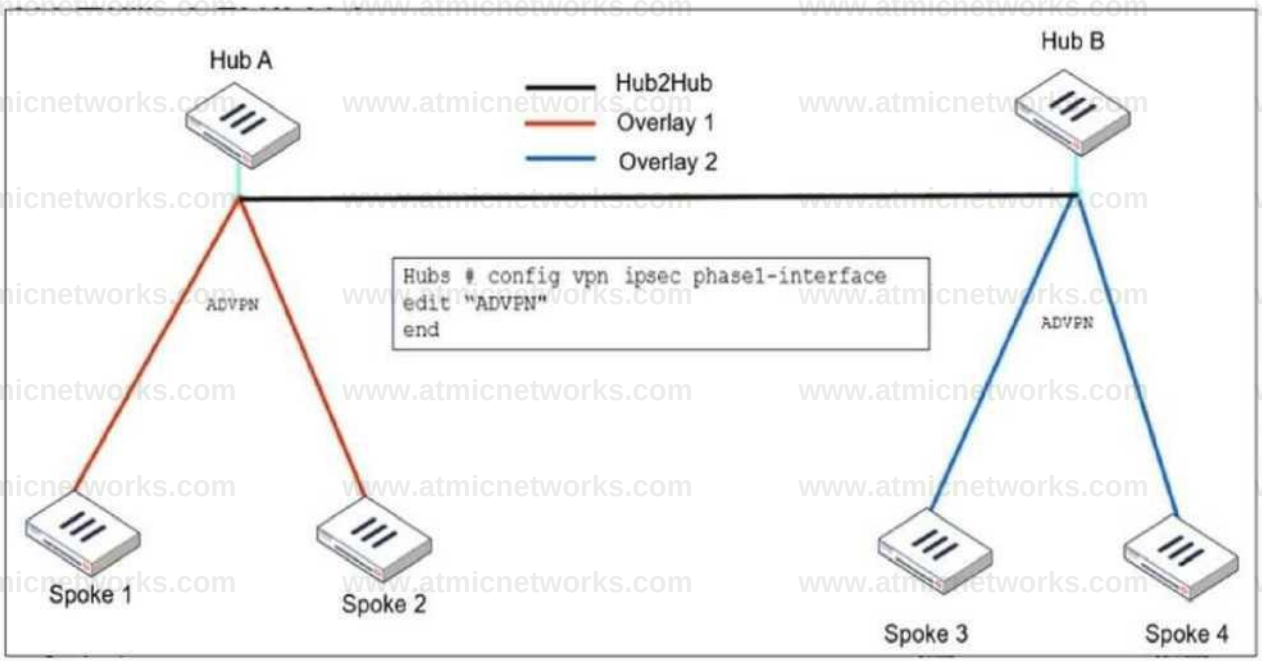
When designing an ADVPN (Auto-Discovery VPN) network for a large enterprise with spokes that have varying numbers of internet links, the main challenge is to minimize the number of peer connections and routes at the hub while maintaining scalability and efficiency.

Using a dynamic routing protocol (such as BGP or OSPF) with loopback interfaces helps in several ways:

- Reduces the number of peer connections at the hub by using a single loopback address per spoke instead of individual physical interfaces.
- Enables simplified route advertisement by dynamically learning and propagating routes instead of manually configuring static routes.
- Supports multiple internet links per spoke efficiently, as dynamic routing can automatically adjust to the best available path.
- Allows seamless failover if a spoke's internet link fails, ensuring continuous connectivity.

Question: 50

Refer to the exhibit, which shows the ADVPN IPsec interface representing the VPN IPsec phase 1 from Hub A to Spoke 1 and Spoke 2, and from Hub B to Spoke 3 and Spoke 4.



An administrator must configure an ADVPN using IBGP and EBGP to connect overlay network 1 with 2.

What must the administrator configure in the phase 1 VPN IPsec configuration of the ADVPN tunnels?

A. set auto-discovery-sender enable and set network-id x

B. set auto-discovery-forwarder enable and set remote-as x

C. set auto-discovery-crossover enable and set enforce-multihop enable

D. set auto-discovery-receiver enable and set npu-ofload enable

Answer: C

Explanation:

When configuring ADVPN (Auto-Discovery VPN) to connect overlay networks across different hubs using IBGP and EBGP, special configurations are required to allow spokes from different overlay networks to dynamically establish tunnels.

- set auto-discovery-crossover enable
  - This allows cross-hub tunnel discovery in an ADVPN deployment where multiple hubs are used.
  - Since Hub A and Hub B belong to different overlays, enabling crossover discovery ensures that spokes from one overlay can dynamically create direct tunnels to spokes in the other overlay when needed.
- set enforce-multihop enable

- This setting ensures that BGP peers using loopback interfaces can establish connectivity even if they are not directly connected.
- Multihop BGP sessions are required when using loopback addresses as BGP peer sources because the connection might need to traverse multiple routers before reaching the BGP neighbor.
- This is especially useful in ADVPN deployments with multiple hubs, where routes might need to cross from one hub to another.

Question: 51

A FortiGate device with UTM profiles is reaching the resource limits, and the administrator expects the traffic in the enterprise network to increase.

The administrator has received an additional FortiGate of the same model.

Which two protocols should the administrator use to integrate the additional FortiGate device into this enterprise network? (Choose two.)

A. FGSP with external load balancers

B. FGCP in active-active mode and with switches

C. FGCP in active-passive mode and with VDOM disabled

D. VRRP with switches

Answer: A, B

Explanation:

When adding an additional FortiGate to an enterprise network that is already reaching its resource limits, the goal is to distribute traffic efficiently and ensure high availability.

FGSP (FortiGate Session Life Support Protocol) with external load balancers

- FGSP allows session-aware load balancing between multiple FortiGate units without requiring them to be in an HA (High Availability) cluster.
- With external load balancers, incoming traffic is evenly distributed across multiple FortiGate devices.
- This approach is useful for scaling out traffic handling capacity while ensuring that sessions remain synchronized between firewalls.
- FGSP is effective when stateful failover is required but without the constraints of traditional HA.

FGCP (FortiGate Clustering Protocol) in active-active mode and with switches

- FGCP active-active mode enables multiple FortiGate devices to share traffic loads, increasing throughput and efficiency.
- Active-active mode is suitable for balancing UTM processing across multiple FortiGates, making it ideal when resource limits are a concern.
- Using switches ensures redundancy and avoids single points of failure in the network.
- This mode is commonly used in enterprise networks where both scalability and redundancy are required.

Question: 52

Refer to the exhibit.

Routing table on FortlGate_A

```
FortiGate_A # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       0 - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       El - OSPF external type 1, E2 - OSPF external type 2
       I - IS IS, LI - IS IS level-1, L2 - IS IS level-2, ia - IS IS inter area
       V -BGP VPNv4
       * ■ candidate default

Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.1.0.254, portl, [1/0]
C 10.1.0.0/24 is directly connected, portl
C 10.1.4.0/24 is directly connected, port3
B      100.64.1.0/24 [200/0] via 10.1.0.254 (recursive is directly connected, portl), 00:39:45, [1/0]
B      172.16.1.252/30 [200/0] via 10.1.0.1 (recursive is directly connected, portl), 00:42:48, (1/0)
C 172.16.100.0/24 is directly connected, port8
```

Routing table on FortlGate_B

```
FortiGate_B # get router info routing-table all
Codes: K - kernel, C - connected, $ - static, R - RIP, B - BGP
       0 - OSPF, IA - OSPF inter area
       N1 • OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       El - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, LI - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V -BGP VPNv4
       * - candidate default

Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.1.0.254, portl, [1/0]
S 4.2.2.2/32 [10/0] via 10.1.5.254, port4, [1/0]
C 10.1.0.0/24 is directly connected, portl
B 10.1.4.0/24 [200/0] via 10.1.0.100 (recursive is directly connected, portl), 00:41:02, (1/0)
```

C 10.1.5.0/24 is directly connected, port4
B 100.64.1.0/24 [200/0] via 10.1.0.254 (recursive is directly connected, portl), 00:38:14, [1/0]
C 172.16.1.248/30 is directly connected, CO
C 172.16.1.252/30 is directly connected, AO
C 172.16.100.0/24 is directly connected, port8

The routing tables of FortiGate_A and FortiGate_B are shown. FortiGate_A and FortiGate_B are in the same autonomous system.

The administrator wants to dynamically add only route 172.16.1.248/30 on FortiGate_A.

What must the administrator configure?

A. The prefix 172.16.1.248/30 in the BGP Networks section on FortiGate_B

B. A BGP route map out for 172.16.1.248/30 on FortiGate_B

C. Enable Redistribute Connected in the BGP section on FortiGate_B.

D. A BGP route map in for 172.16.1.248/30 on FortiGate_A

Answer: B

Explanation:

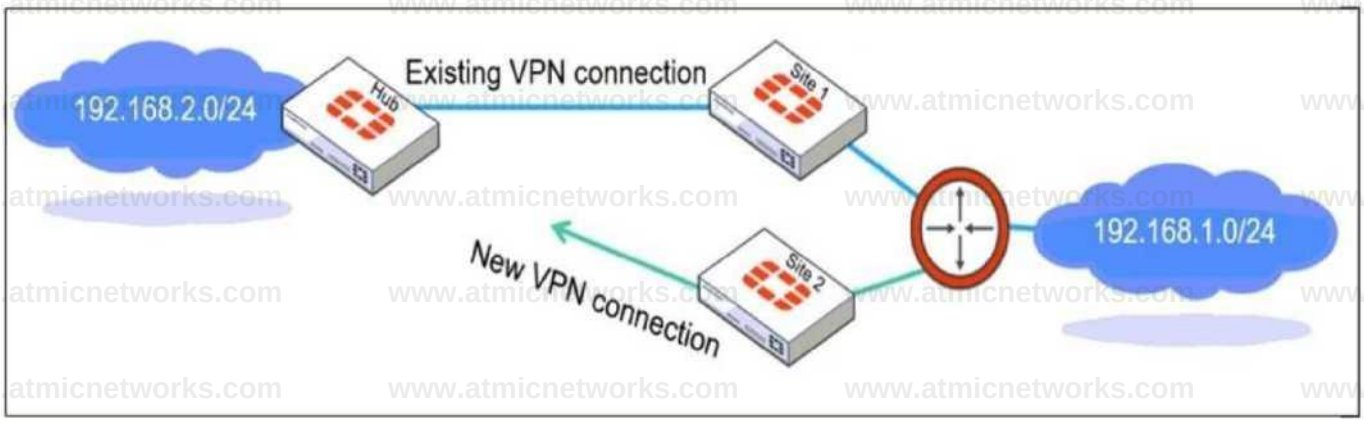
FortiGate_A and FortiGate_B are in the same autonomous system (AS), and FortiGate_A does not currently have route 172.16.1.248/30 in its routing table. However, FortiGate_B has this route as a connected route.

To dynamically advertise only 172.16.1.248/30 from FortiGate_B to FortiGate_A, the administrator must configure a BGP route map out on FortiGate_B that specifically permits only this prefix.

A BGP route map out on FortiGate_B controls which routes FortiGate_B advertises to FortiGate_A. If no filtering is applied, FortiGate_B might advertise all BGP-learned and connected routes, which is not what the administrator wants. The route map should include a prefix-list that explicitly allows only 172.16.1.248/30 and denies everything else.

Question: 53

Refer to the exhibit, which shows a network diagram showing the addition of site 2 with an overlapping network segment to the existing VPN IPsec connection between the hub and site 1.



Which IPsec phase 2 configuration must an administrator make on the FortiGate hub to enable equal-cost multi-path (ECMP) routing when multiple remote sites connect with overlapping subnets?

A. Set route-overlap to either use-new or use-old

B. Set net-device to ecmp

C. Set single-source to enable

D. Set route-overlap to allow

Answer: A

Explanation:

When multiple remote sites connect to the same hub using overlapping subnets, FortiGate needs to determine which route should be used for traffic forwarding. The route-overlap setting in IPsec Phase 2 allows FortiGate to handle this scenario by deciding whether to keep the existing route (use-old) or replace it with a new route (use-new).

In an ECMP (Equal-Cost Multi-Path) routing setup, both routes should be retained and balanced, but FortiGate does not support ECMP directly over overlapping routes in IPsec Phase 2. Instead, an administrator must decide which connection takes precedence using route-overlap settings.

Question: 54

An administrator wants to scale the IBGP sessions and optimize the routing table in an IBGP network.

Which parameter should the administrator configure?

A. network-import-check

B. ibgp-enforce-multihop

C. neighbor-group

D. route-reflector-client

Answer: D

Explanation:

In an IBGP (Internal BGP) network, all routers must be fully meshed, meaning every router must establish a BGP session with every other router in the same autonomous system (AS). This does not scale well in large networks due to the exponential increase in BGP sessions.

To optimize and scale IBGP, Route Reflectors (RRs) are used. A Route Reflector (RR) reduces the number of IBGP peer connections by allowing a centralized router (RR) to redistribute IBGP routes to other IBGP peers (called clients). This eliminates the need for a full mesh, significantly reducing BGP session overhead.

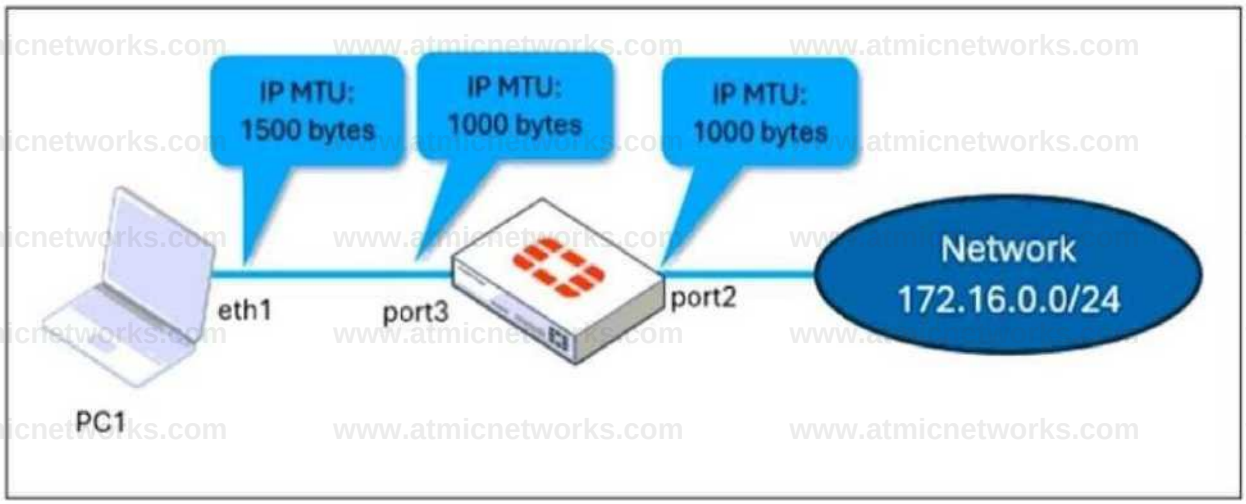
By configuring the route-reflector-client setting on IBGP peers, an administrator can:

- Scale IBGP sessions by reducing the number of direct BGP peer connections.
- Optimize the routing table by ensuring routes are efficiently propagated within the IBGP network.
- Eliminate the need for full mesh topology, making IBGP more manageable.

Question: 55

Refer to the exhibits.

Network topology



port 3 configuration on FortiGate

```
config system interface edit "port3" set vdom "root" set
ip 10.0.0.1 255.255.255.0 set alicwaccess ping https ssh
snap http fgfm fem set type physical set alias "LAN" set
snap-index 3 set mtu-override enable set mtu 1000 next end
```

ping output

```
C:\U8ers\foxtineoping 172.16.0.254 -   f -1 1400

Pinging 172.16.0.254 with 1400 bytesof data:
Reply from 10.0.0.1: Packet needs tobe fragmented but DF set.
Packet needs tobe fragmented but DF beset.
Packet needs tofragmented but DF beset.
Packet needs to fragmented but DF     set.

Fing statisticsfor 172.16.0.254: Los
Packets: Sent ■ 4, Received ■ 1,   t      - 3 (751 loss).
```

The configuration of a user's Windows PC, which has a default MTU of 1500 bytes, along with FortiGate interfaces set to an MTU of 1000 bytes, and the results of PC1 pinging server 172.16.0.254 are shown.

Why is the user in Windows PC1 unable to ping server 172.16.0.254 and is seeing the message: Packet needs to be fragmented but DF set?

A. Option ip.flags.mf must be set to enable on FortiGate. The user has to adjust the ping MTU to 1000 to succeed.

B. Fragmented packets must be encrypted. To connect any application successfully, the user must install the Fortinet_CA certificate in the Microsoft Management Console.

C. FortiGate honors the do not fragment bit and the packets are dropped. The user has to adjust the ping MTU to 972 to succeed.

D. The user must trigger different traffic because path MTU discovery techniques do not recognize ICMP payloads.

Answer: C

Explanation:

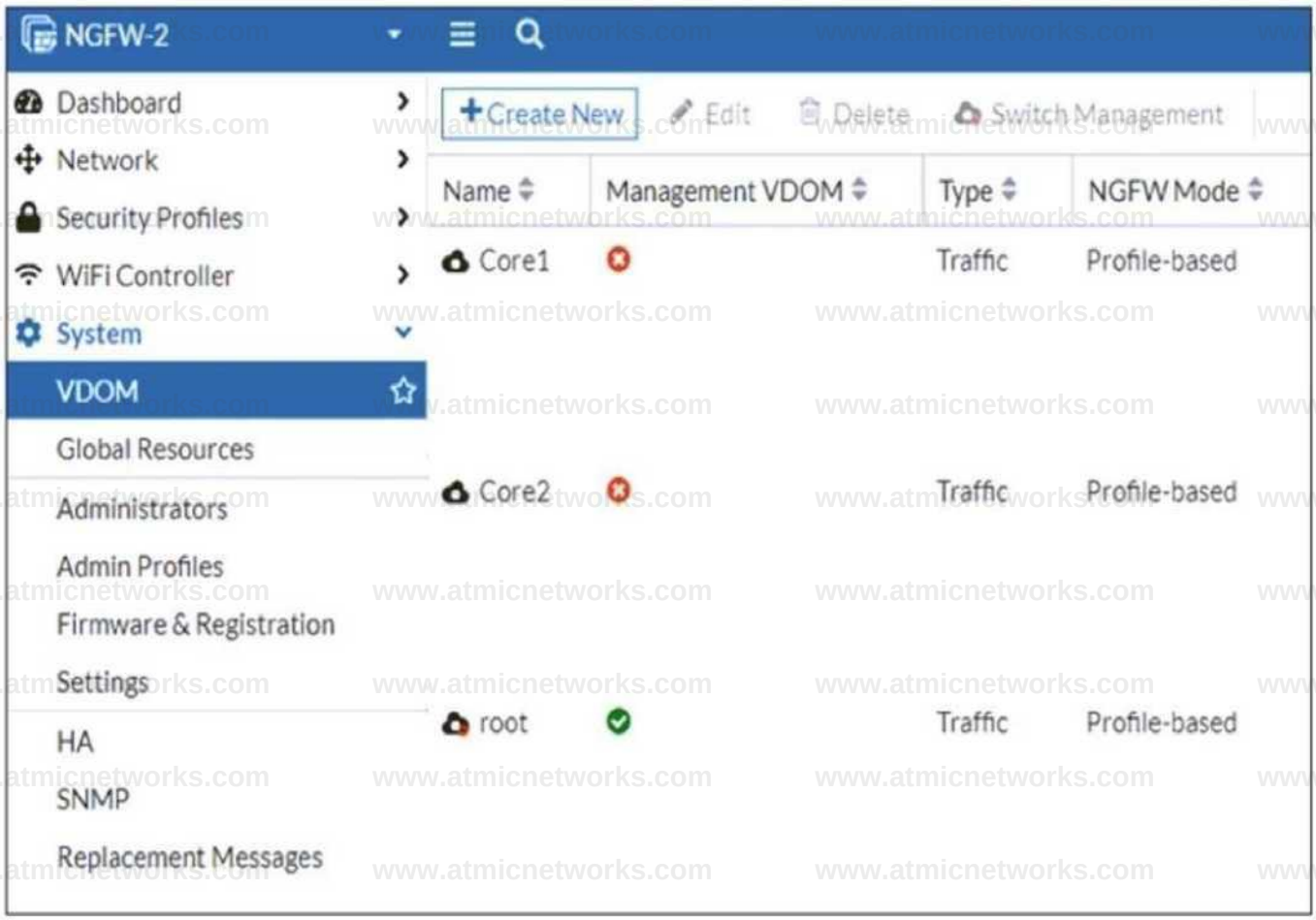
The issue occurs because FortiGate enforces the "do not fragment" (DF) bit in the packet, and the packet size exceeds the MTU of the network path. When the Windows PC1 (with an MTU of 1500 bytes) attempts to send a 1400-byte packet, the FortiGate interface (with an MTU of 1000 bytes) needs to fragment it. However, since the DF bit is set, FortiGate drops the packet instead of

fragmenting it.

To resolve this, the user should adjust the ping packet size to fit within the path MTU. In this case, reducing the packet size to 972 bytes (1000 bytes MTU minus 28 bytes for the IP and ICMP headers) should allow successful transmission.

Question: 56

Refer to the exhibit, which shows the VDOM section of a FortiGate device.



An administrator discovers that webfilter stopped working in Core1 and Core2 after a maintenance window.

Which two reasons could explain why webfilter stopped working? (Choose two.)

A. The root VDOM does not have access to FortiManager in a closed network.

B. The root VDOM does not have a VDOM link to connect with the Corel and Core2 VDOMs.

C. The Core1 and Core2 VDOMs must also be enabled as Management VDOMs to receive FortiGuard updates

D. The root VDOM does not have access to any valid public FDN.

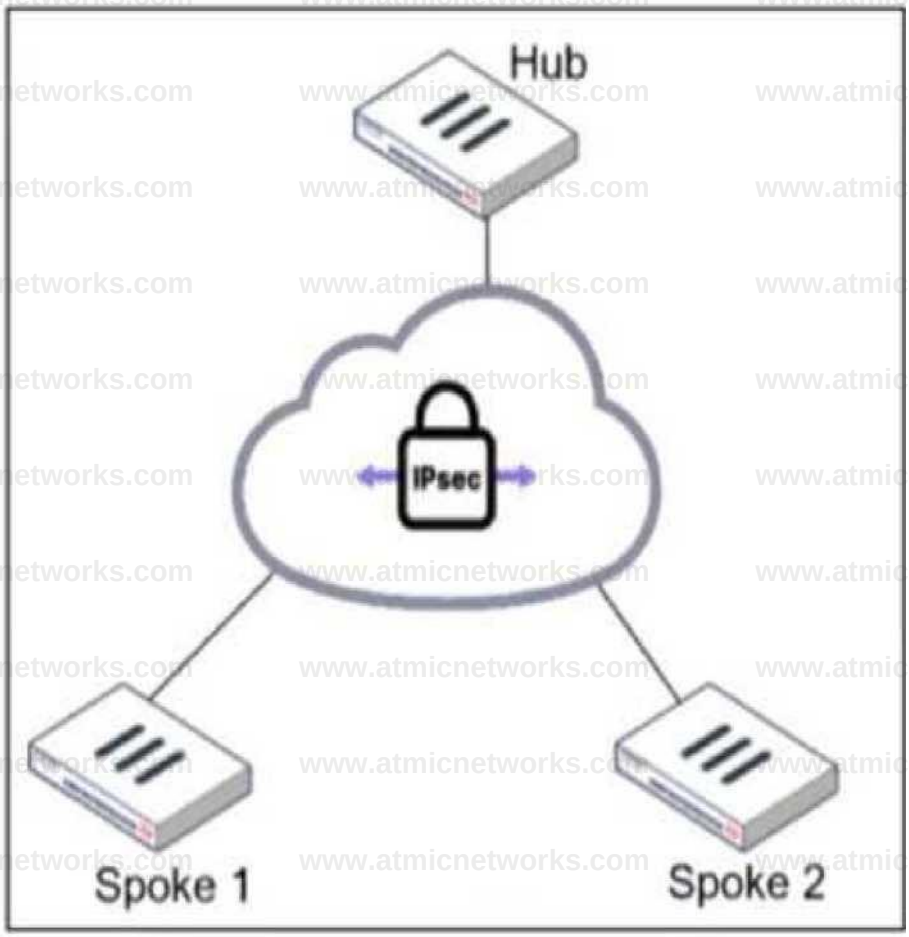
Answer: B, D

Explanation:

Since Core1 and Core2 are not designated as management VDOMs, they rely on the root VDOM for connectivity to external resources such as FortiGuard updates. If the root VDOM lacks a VDOM link to these VDOMs or cannot reach FortiGuard services, security features like web filtering will stop working.

Question: 57

Refer to the exhibit.



An administrator is deploying a hub and spokes network and using OSPF as dynamic protocol.

Which configuration is mandatory for neighbor adjacency?

A. Set bfd enable in the router configuration

B. Set network-type point-to-multipoint in the hub interface

C. Set rfc1583-compatible enable in the router configuration

D. Set virtual-link enable in the hub interface

Answer: B

Explanation:

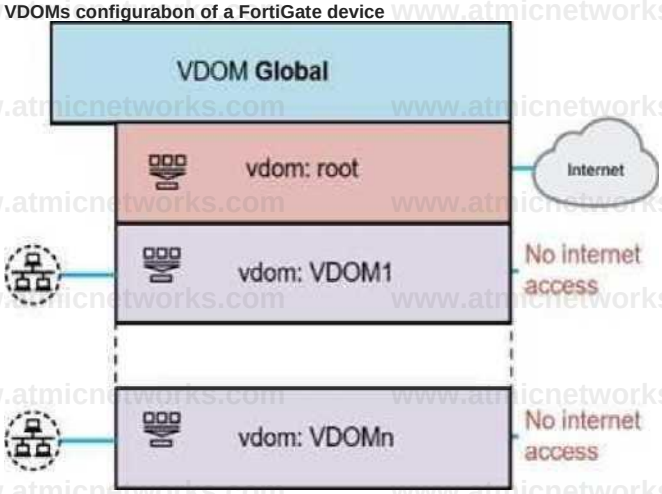
In a hub-and-spoke topology using OSPF over IPsec VPNs, the point-to-multipoint network type is necessary to establish neighbor adjacencies between the hub and spokes. This network type ensures that OSPF operates correctly without requiring a designated router (DR) and allows dynamic routing

updates across the IPsec tunnels.

Question: 58

Refer to the exhibit.

VDOMs configurabon of a FortiGate device



A FortiGate segmented into VDOMs is shown. You must ensure effective and accelerated internet access for all of the VDOMs in this enterprise network. How can you achieve this? (Choose one answer)

A. Connect a physical interface from each VDOM to the root VDOM.

B. Create VDOM links.

C. Configure network processing unit (NPU) vlinks.

D. Create VLANs over network processing unit (NPU) vlinks.

Answer: C

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

According to the FortiOS 7.6 Administration Guide and the FortiGate Infrastructure study materials, inter-VDOM communication can be achieved using either software-based VDOM links or hardware- accelerated NPU VDOM links (vlinks).

While standard VDOM links (Option B) allow traffic to pass between VDOMs, they are processed by the system CPU, which can become a bottleneck in high-throughput environments. To ensure accelerated internet access as specified in the

requirements, NPU vlinks (Option C) must be used. NPU vlinks are virtual interfaces created in pairs that allow traffic to be ofloaded to the FortiGate's Network Processor (NP6, NP7, etc.), significantly reducing latency and CPU overhead.

In the provided exhibit, the root VDOM has direct internet access, while VDOM1 and VDOMn do not. By configuring NPU vlinks between the non-root VDOMs and the root VDOM, you create a hardware- accelerated path. Traffic from the internal VDOMs is sent through the vlink to the root VDOM, which then forwards it to the Internet. This "hub-and-spoke" VDOM architecture, powered by NPU acceleration, ensures that all VDOMs share the internet connection without sacrificing performance.

Question: 59

Refer to the exhibit.

HA Configuration

```
HQ-NGFW-1 (ha) # show
config system ha
    set group-name "fortinet"
    set mode a-p
    set password ENC cdodjrWF
    set hbdev "port 7" 0
    set session-pickup enable
    set vcluster-status enable
    config vcluster
        edit 1
            set override disable
            set priority 200
            set vdom "Corel" "root"
        next
        edit 2
            set override disable
            set priority 150
            set vdom "Core2"
        next
    end
end
```

```
HQ-NGFW-2 (ha) # show
config system ha
    set group-name "fortinet"
    set mode a-P
    set password ENC eLESAZ
    set hbdev "port?" 0
    set session-pickup enable
    set vcluster-status enable
    config vcluster
        edit 1
            setoverride disable
            setpriority 100
            setvdom "Corel" "root"
        next
                b
        edit 2
            setoverride disable
            setpriority 120
            setvdom "Core2"
        next
    end
end
```

An HA configuration of an active-active (A-A) cluster with the same HA uptime is shown. You want HQ-NGFW-2 to handle the Core2 VDOM traffic. Which modification must you make to achieve this outcome? (Choose one answer)

A. Reboot HQ-NGFW-2.

B. Change the priority from 100 to 160 for HQ-NGFW-2.

C. Change the priority from 120 to 200 for HQ-NGFW-2.

D. Enable override in virtual cluster 2 for HQ-NGFW-2.

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

Based on the FortiOS 7.6 Administration Guide and the HA Virtual Clustering documentation, the exhibit demonstrates a Virtual Clustering environment where multiple VDOMs are distributed across an HA cluster.

In a virtual cluster setup, VDOMs are assigned to either virtual cluster 1 (vcluster 1) or virtual cluster 2 (vcluster 2). Each virtual cluster has its own independent primary unit selection process. The primary unit for a virtual cluster is determined based on the standard HA selection criteria: Monitored Interfaces > HA Uptime > Priority > Serial Number.

According to the exhibit:
Virtual Cluster 1 (edit 1) contains VDOMs "Core1" and "root".

Virtual Cluster 2 (edit 2) contains VDOM "Core2".

The HA uptime is stated to be the same for both devices.

For edit 2 (Core2), HQ-NGFW-1 has a priority of 150, while HQ-NGFW-2 has a priority of 120.

In both units, override is disabled (default).

Since the uptime is equal and no monitored interfaces are down, the cluster uses the Priority value to select the primary unit for each vcluster. Currently, HQ-NGFW-1 is the primary for Core2 because its priority (150) is higher than HQ-NGFW-2's (120). To ensure HQ-NGFW-2 handles the Core2 traffic, its priority for virtual cluster 2 must be increased to a value higher than 150. Option C (changing the priority from 120 to 200) achieves this.

Question: 60

Refer to the exhibit.

```
FortiGate # get router info ospf status
 Routing Process "ospf 0" with ID 0.0.0.5
  Process uptime is 0 minute
  Process bound to VRF default
  Conforms to RFC2328, and RFC1583Compatibility flag is enabled
  Supports only single TOS(TOSO) routes
  Supports opaque LSA
  Do not support Restarting
  This router is an ABR
```

The partial output of an OSPF command is shown. While checking the OSPF status of FortiGate, you receive the output shown in the exhibit. Based on the output, which two statements about FortiGate are correct? (Choose two answers)

A. FortiGate has OSPF ECMP enabled.

B. FortiGate is a backup designated router.

C. FortiGate injects external routing information.

D. FortiGate is connected to multiple areas.

Answer: A, D

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

Based on the FortiOS 7.6 Infrastructure study guide and official documentation regarding OSPF monitoring, the command output get router info ospf status provides critical details about the OSPF process.

Multiple Areas (Option D): The last line of the exhibit explicitly states, "This router is an ABR" (Area Border Router). By definition in the OSPF protocol, an ABR is a router that is connected to multiple OSPF areas, typically Area 0 (the backbone) and at least one other non-backbone area.

OSPF ECMP (Option A): The output indicates that the OSPF process "Conforms to RFC2328". RFC 2328 is the standard for OSPFv2, which includes the capability for Equal-Cost Multi-Path (ECMP). In

FortiOS, when OSPF is enabled and multiple routes to the same destination have the same cost, ECMP is supported by default unless specifically limited by the maximum-paths configuration. The mention of this RFC compliance in the status output confirms the engine's capability and support for multi-path routing.

Option C is incorrect because the output does not label the device as an ASBR (Autonomous System Boundary Router), which would be required to inject external routing information. Option B is incorrect because "ABR" refers to area hierarchy, not the election status (DR/BDR) on a specific network segment.

Question: 61

To secure your enterprise network traffic, which step does FortiGate perform first, when handling the first packets of a session? (Choose one answer)

A. Installation of the session key in the network processor (NP)

B. Decryption

C. A reverse path forwarding (RPF) check

D. IP integrity header checking

Answer: D

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

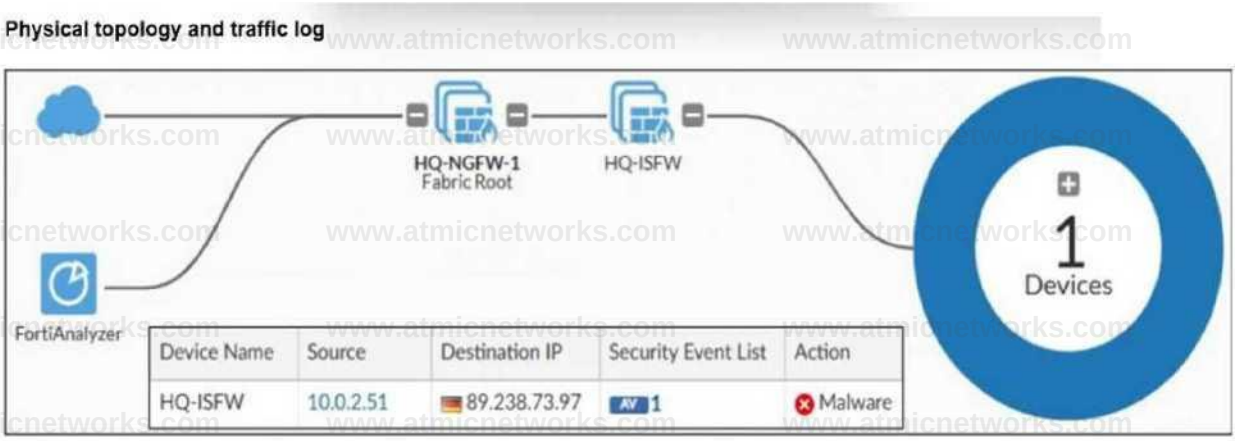
Based on the FortiOS 7.6 Administration Guide and the Life of a Packet documentation (Parallel Path Processing), the FortiGate follows a specific, hardcoded sequence when processing the first packet of a new session. This process is divided into several stages: Ingress, Kernel, and Egress.

The very first stage is Ingress, where all packets accepted by a network interface are processed by the TCP/IP stack. Immediately following this, the packet must pass through IP integrity header checking. This step involves reading the packet headers to verify that the packet is a valid protocol (TCP, UDP, ICMP, etc.) and that the header length is correct. This sanity check is performed before any other security functions, such as decryption (which occurs later in the Ingress stage) or the Reverse Path Forwarding (RPF) check (which occurs even later during the Routing step in the Kernel stage).

Installation of the session key (Option A) only occurs after the packet has matched a firewall policy and the session has been fully established and ofloaded to the NPU. Therefore, IP integrity header checking is the absolute first security-related validation performed on an incoming packet.

Question: 62

Refer to the exhibit.



A physical topology along with a traffic log is shown. You are using FortiAnalyzer to monitor traffic from the device with IP address 10.0.2.51, which is located behind the FortiGate internal segmentation firewall (ISFW) device. Unified threat management (UTM) is not enabled in the firewall policy on the HQ-ISFW device, and you are surprised to see a log with the action Malware, as shown in the exhibit. What are two reasons why FortiAnalyzer would display this log? (Choose two answers)

A. HQ-ISFW is not connected to FortiAnalyzer and traffic must go through HQ-NGFW-1.

B. UTM is enabled in the firewall policy in HQ-NGFW-1.

C. HQ-ISFW is in a Security Fabric environment.

D. Security rating is enabled in HQ-ISFW.

Answer: B, C

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

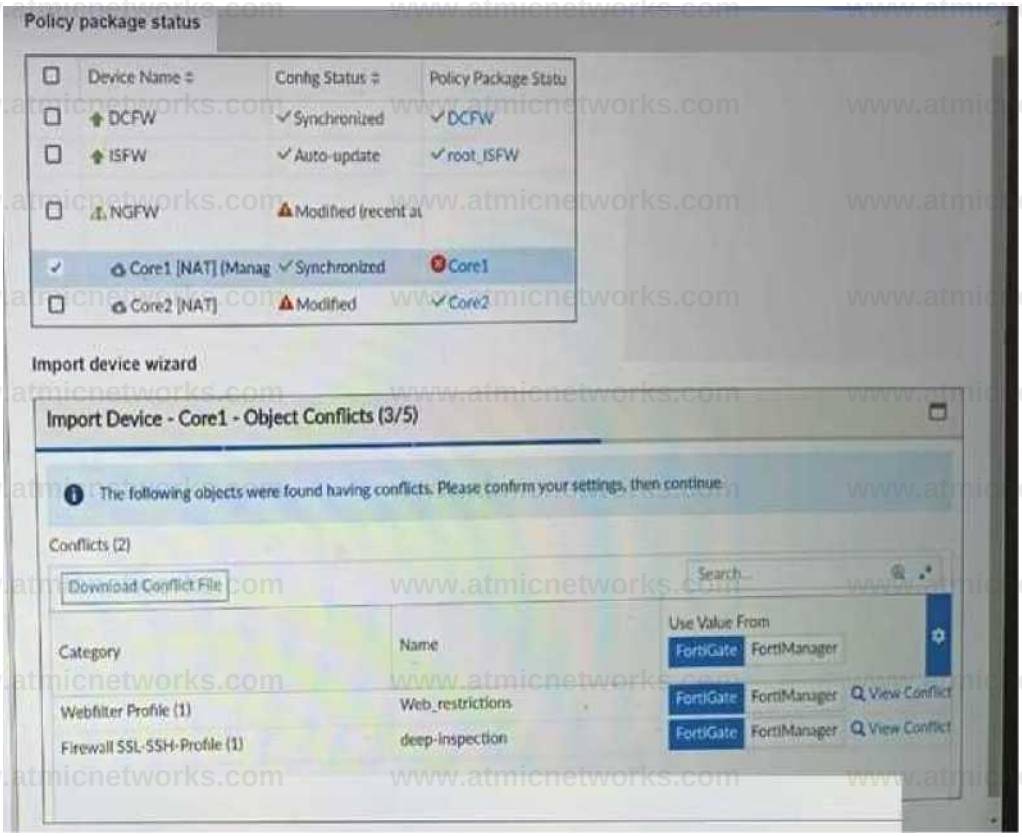
According to the Fortinet Security Fabric 7.6 documentation and FortiAnalyzer study materials, when multiple FortiGate devices are part of a Security Fabric, logs are typically sent to a centralized FortiAnalyzer for a unified view of the network.

In the provided exhibit, the topology shows HQ-NGFW-1 as the Fabric Root and HQ-ISFW as a downstream device. One of the key benefits of the Security Fabric (Option C) is topology-wide visibility, where logs from different devices are correlated.

The traffic log table shows a "Malware" action for traffic originating from 10.0.2.51 (located behind HQ-ISFW) destined for a public IP. If UTM is not enabled on the HQ-ISFW itself, it cannot generate an Antivirus (AV) log. However, because HQ-ISFW is part of the Security Fabric, the traffic eventually passes through the upstream device, HQ-NGFW-1, to reach the internet. If UTM is enabled on HQ- NGFW-1 (Option B), that device will inspect the traffic, detect the malware, and generate the security log. FortiAnalyzer then displays this log as part of the unified threat view, associating it with the original source and the inspection point in the fabric path.

Question: 63

Refer to the exhibits.



A policy package conflict status and information from the import device wizard in the Core1 VDOM are shown. When you import a policy package, the following message appears for the Web_restrictions web filter profile and the deep-inspection SSL-SSH profile: "The following objects were found having conflicts. Please confirm your settings, then continue." The Web_restrictions and deep-inspection profiles are used by other FortiGate devices within FortiManager. Which step must you take to resolve the issue? (Choose one answer)

A. Retrieve the FortiGate configuration to automatically export correct objects and policies.

B. Create uniquely named objects on FortiGate and reimport them into the policy package.

C. Select the FortiManager configuration that accepts changes on FortiManager and preserves existing configurations on FortiGate devices.

D. Use non-default object values because FortiManager is unable to alter default values.

Answer: B

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

According to the FortiManager 7.6 Study Guide regarding Object Management and the Import Device Wizard, FortiManager uses a centralized database where objects are shared across an ADOM. When importing a configuration from a FortiGate, the wizard compares local objects with those already existing in the FortiManager ADOM database.

As shown in the exhibit, conflicts exist for the Web_restrictions and deep-inspection profiles. Since these profiles are shared with other FortiGate devices, a decision must be made:

Selecting "FortiManager": The local FortiGate settings will be overwritten by the FortiManager's database version upon the next installation, potentially losing site-specific configurations.

Selecting "FortiGate": The FortiManager ADOM database is updated with the new values. This causes all other FortiGate devices using these shared objects to move into a "Modified" status, as their local configurations no longer match the updated central database.

To resolve this conflict properly when different devices require different settings for the same profile type, the best practice is to create uniquely named objects (Option B) on the FortiGate before reimporting. This ensures that the specific requirements for the Core1 VDOM are met without affecting the global objects used by the rest of the enterprise network.

Question: 64

You are using Virtual eXtensible LAN (VXLAN) extensively on FortiGate. Which specialized acceleration hardware must you use to improve FortiGate performance? (Choose one answer)

A. NP7

B. SP5

C. CP9

D. NTurbo

Answer: A

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

According to the FortiOS 7.6 Infrastructure study guide and Hardware Acceleration documentation, the Network Processor 7 (NP7) is the flagship hardware component designed to ofload high- performance network traffic from the system CPU. A critical advancement of the NP7 over previous generations (such as the NP6) is its native support for Virtual eXtensible LAN (VXLAN) hardware acceleration.

In enterprise environments where VXLAN is used to extend Layer 2 segments over a Layer 3 network, the encapsulation and decapsulation of VXLAN headers can be computationally expensive. The NP7 provides specialized circuitry to perform these operations at line rate, significantly reducing latency and preventing CPU saturation. This allows the FortiGate to maintain high throughput even when handling complex overlay tunnels.

While the CP9 (Content Processor) (Option C) provides acceleration for SSL/TLS inspection and IPsec encryption, it does not

handle network layer encapsulation like VXLAN. NTurbo (Option D) is a software feature that ofloads firewall sessions to the network processors but is not a hardware chip itself. The SP5 (Option B) also supports VXLAN ofloading in newer mid-range models, but the NP7 is the primary "specialized acceleration hardware" referenced for high-end enterprise performance in the 7.6 curriculum.

Question: 65

Refer to the exhibit.

```
FortiGate # get router info ospf status
Routing Process "ospf 0" with ID 0.0.0.5
Process uptime is 0 minute
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is enabled
Supports only single TOS(TOSO) routes
Supports opaque LSA
Do not support Restarting
This router is an ASBR
```

The partial output of an OSPF command is shown. You are checking the OSPF status of a FortiGate device when you receive the output shown in the exhibit. Based on the output, which two statements about FortiGate are correct? (Choose two answers)

A. FortiGate is a backup designated router.

B. FortiGate supports OSPF ECMP.

C. FortiGate is in the area 0.0.0.5.

D. FortiGate can inject external routing information.

Answer: B, D

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

Based on the FortiOS 7.6 Infrastructure study guide and official documentation regarding OSPF monitoring, the command output get router info ospf status provides critical details about the OSPF process.

Injecting External Information (Option D): The last line of the exhibit explicitly states, "This router is an ASBR" (Autonomous System Boundary Router). By definition in the OSPF protocol, an ASBR is a router that connects the OSPF network to another routing domain (such as BGP, Static, or Connected routes) and is responsible for injecting external routing information into the OSPF domain.

OSPF ECMP Support (Option B): The output indicates that the OSPF process "Conforms to RFC2328". RFC 2328 is the standard for OSPFv2, which includes the capability for Equal-Cost Multi-Path (ECMP).

In FortiOS, the OSPF engine supports multi-path routing by default, allowing the device to utilize multiple paths to the same destination if they share the same cost.

Option A is incorrect because the output does not indicate the router's DR/BDR election status on a specific segment. Option C is incorrect because "ID 0.0.0.5" refers to the Router ID, not the OSPF Area ID.