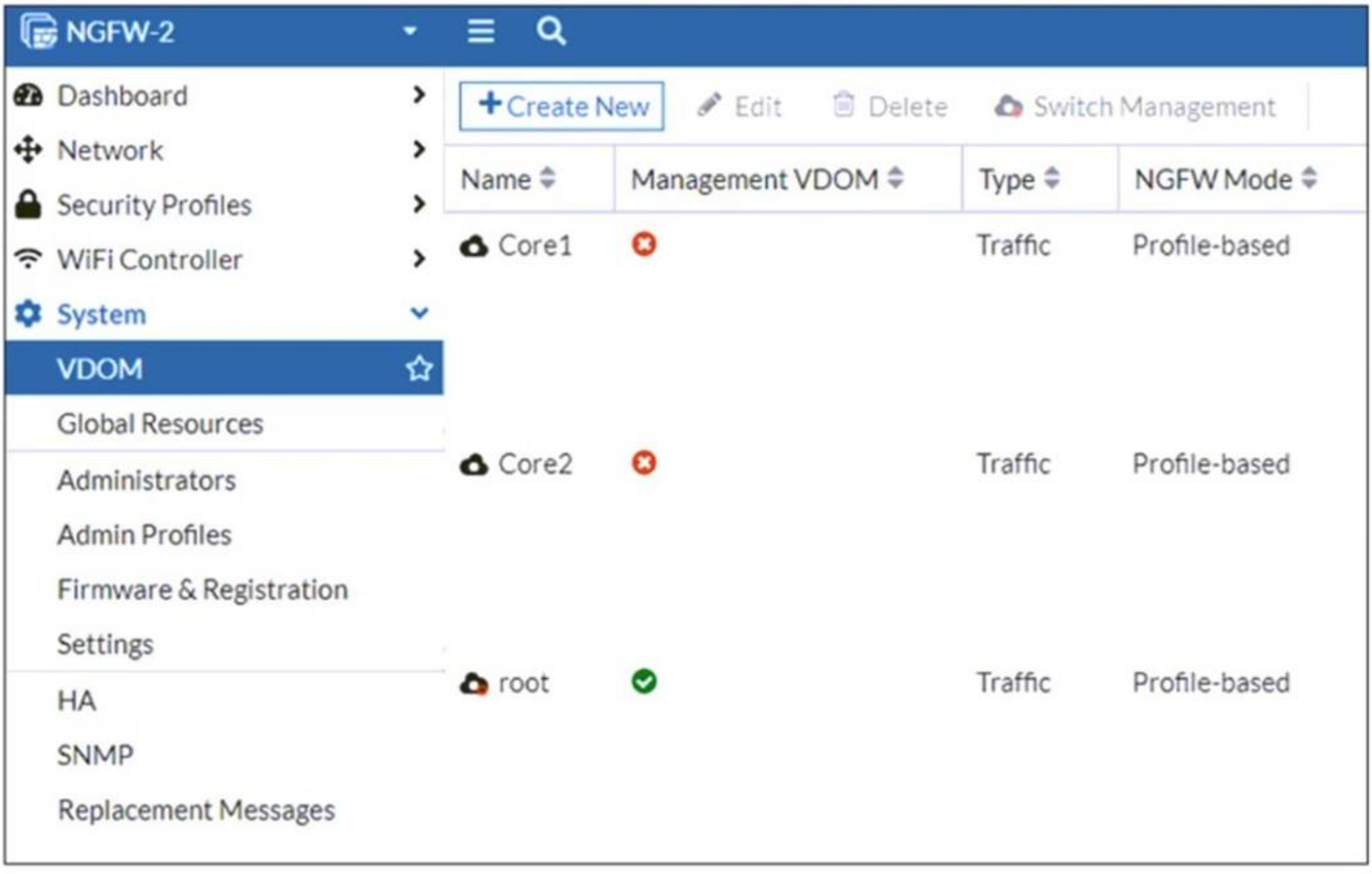
Fortinet

Exam Questions FCSS_EFW_AD-7.4

FCSS - Enterprise Firewall 7.4 Administrator

NEW QUESTION 1
Refer to the exhibit, which shows the VDOM section of a FortiGate device.



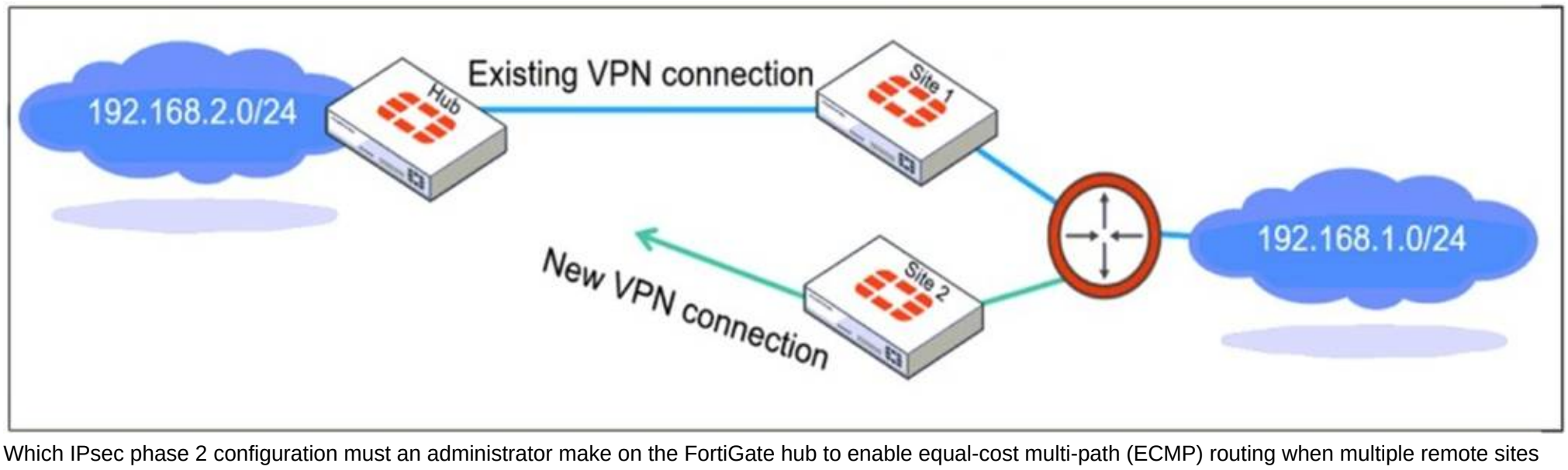
An administrator discovers that webfilter stopped working in Core1 and Core2 after a maintenance window.
Which two reasons could explain why webfilter stopped working? (Choose two.)

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: BD

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.

NEW QUESTION 2
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 thesame hubusingoverlapping subnets, FortiGate needs to determine which route should be used for traffic forwarding. Theroute- overlapsetting in IPsec Phase 2 allows FortiGate to handle this scenario by deciding whether to keep theexisting route(use-old) or replace it with anew route(use-new).
In anECMP (Equal-Cost Multi-Path) routing setup,both routes should be retained and balanced, but FortiGate does not supportECMP directly over overlapping routesin IPsec Phase 2. Instead, an administrator must decide which connection takes precedence usingroute-overlapsettings.

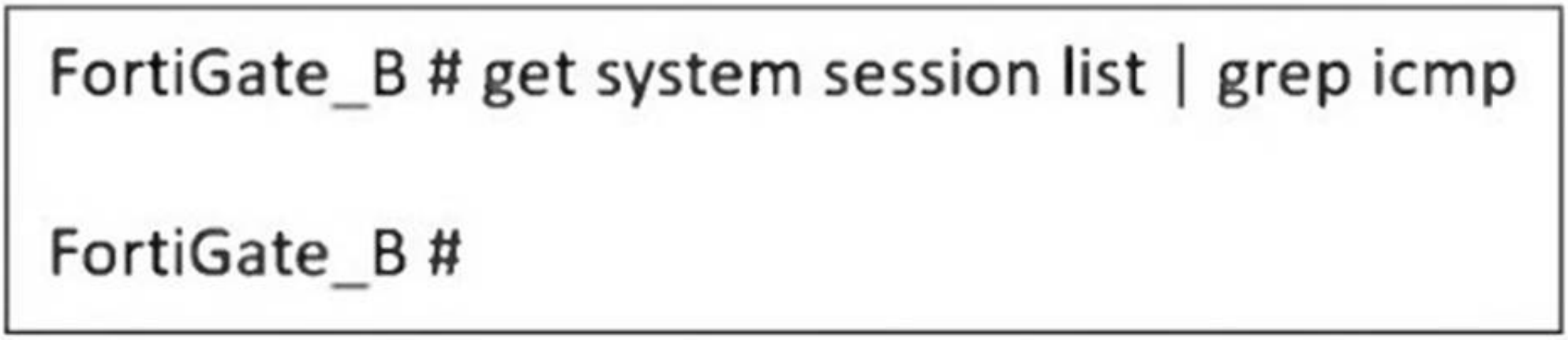
NEW QUESTION 3
An administrator needs to install an IPS profile without triggering false positives that can impact applications and cause problems with the user's normal traffic flow. Which action can the administrator take to prevent false positives on IPS analysis?

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 clickingsuspicious 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 missingor expired SSUTLS certificates on the client PC to prevent expected false positives.

Answer: A

Explanation:
False positives inIntrusion 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 typesto ensure that IPS signatures match the network's actual traffic patterns, reducing false positives.
Customize signature selectionbased on the network??s specific services, filtering out unnecessary or irrelevant signatures.

NEW QUESTION 4
Refer to the exhibit, which shows a command output.



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:
TheFortinet FGSP (FortiGate Session Life Support Protocol) clusterallows session synchronization betweentwo FortiGate devicesto 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 commandget system session list | grep icmponFortiGate_Breturnsno output, meaning that ICMP sessions arenot being synchronizedfrom FortiGate_A.
Ifsession-pickup-connectionlessis disabled,FortiGate_B will not receive ICMP sessions, causingpacket lossduring failover.

NEW QUESTION 5
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: AD

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, includingElliptic Curve Diffie- Hellman (ECDH)groups such asECP256 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 asRADIUS, certificates, and smart cards. This is particularly useful forremote access VPNswhere user authentication must be flexible and secure.

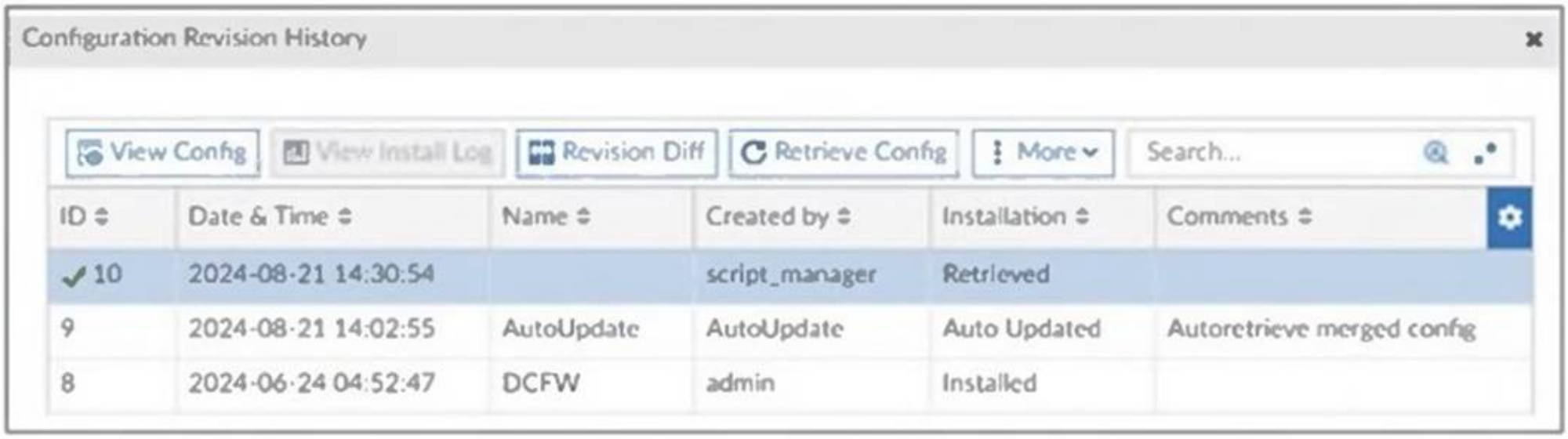
NEW QUESTION 6
A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices.
Which three approaches can the company 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: ABE

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.

NEW QUESTION 7
Refer to the exhibit, which shows a revision history window in the FortiManager device layer.



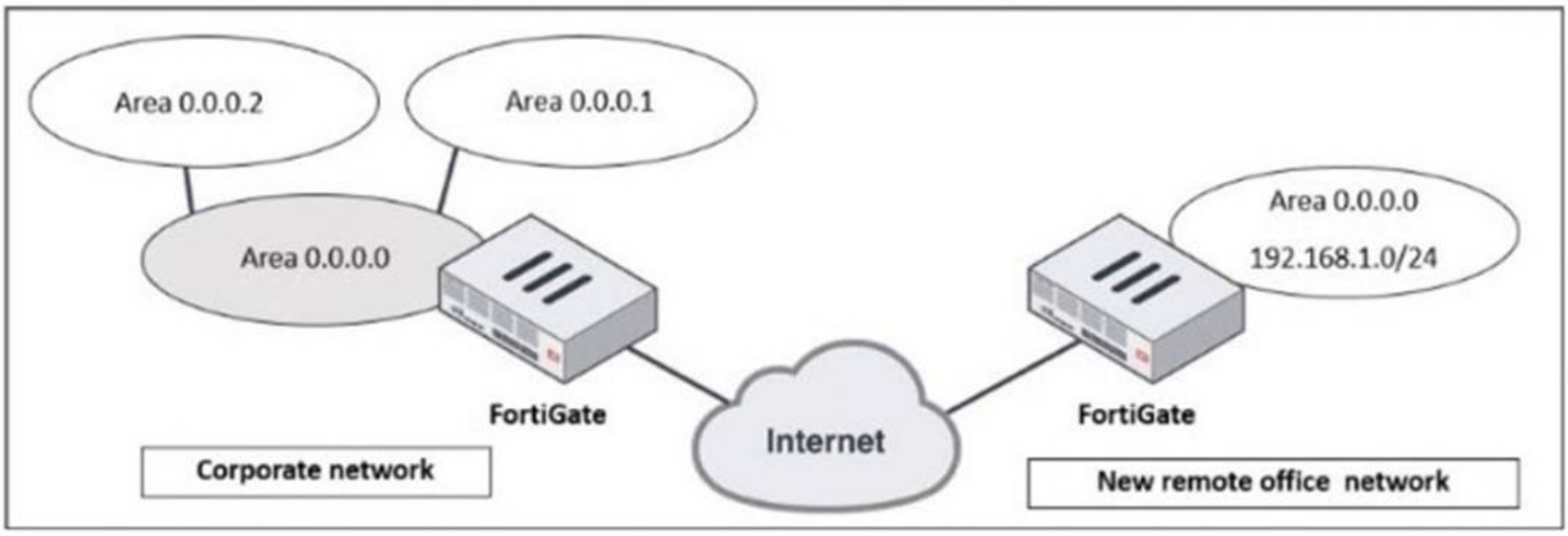
The IT team is trying to identify the administrator responsible for the most recent update in the FortiGate device database.
Which conclusion can you draw about this scenario?

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:
TheConfiguration Revision Historywindow inFortiManagershows that the most recent configuration change (ID 10) was created byscript_managerwith the actionRetrieved.
Sincescript_manageris a system-level script execution user, the IT team needs to find who actually triggered this script. This can be done by:
Checking theFortiManager system logsforscript execution events.
Using thetype=scriptfilter to locate the administrator associated with the script execution.

NEW QUESTION 8
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, thecorporate networkand thenew remote office networkneed to communicate over theInternet, which requires asecure and dynamic routing method. Since both networks are usingOSPF (Open Shortest Path First)as the routing protocol, the best approach is to establish anOSPF over IPsec VPNto 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 encryptionfor 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's192.168.1.0/24 subnetwill be advertised dynamically to the corporate network without additional configuration.

NEW QUESTION 9
An administrator is extensively using VXLAN on FortiGate.
Which specialized acceleration hardware does FortiGate need to improve its performance?

A. NP7
B. SP5
C. 9
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 offloading
Firewall policy enforcement
Advanced threat protection at wire speed
NP7 significantlyreduces latency and improves throughputwhen handling VXLAN traffic, making it the best choice for large-scale VXLAN deployments.

NEW QUESTION 10
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 anADVPN (Auto-Discovery VPN) networkfor alarge enterprisewith spokes that havevarying numbers of internet links, the main challenge is tominimize the number of peer connections and routesat the hub while maintainingscalability and efficiency.
Using a dynamic routing protocol (such as BGP or OSPF) with loopback interfaces helps in several ways:
Reduces the number of peer connectionsat the hub byusing a single loopback address per spokeinstead of individual physical interfaces.
Enables simplified route advertisementby dynamically learning and propagating routes instead of manually configuring static routes.
Supports multiple internet links per spokeefficiently, as dynamic routing can automatically adjust to the best available path.
Allows seamless failoverif a spoke??s internet link fails, ensuring continuous connectivity.

NEW QUESTION 10
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 anaggressive IPS profilewithout prior testing candisrupt legitimate applicationsby incorrectly identifying normal traffic as malicious. To prevent disruptions while still monitoring for threats:
Enable IPS in "Monitor Mode" first:
This allows FortiGate tolog and analyzepotential threatswithout actively blockingtraffic. 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 candisable or modifyspecific rules causing false positives.

NEW QUESTION 12
An administrator received a FortiAnalyzer alert that a 1 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 excessiveDNS log requests with random subdomainssuggest aDNS exfiltration attack, where attackers encode and transmit data via DNS queries. Since this technique can useboth UDP and TLS (DoH - DNS over HTTPS), a comprehensive security approach is needed.
Using anIPS profile with DNS exfiltration-specific signaturesallows FortiGate to: Detect and block abnormal DNS query patternsoften used in exfiltration. Inspect encrypted DNS (DoH, DoT) trafficif SSL inspection is enabled.
Identify known exfiltration domains and techniquesbased on FortiGuard threat intelligence.

NEW QUESTION 16
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 usingIPsec VPNsandVXLAN, additional headers are added to packets, which can exceed thedefault 1500-byte MTU. This can lead tofragmentation issues, dropped packets, or degraded performance.
To resolve this, theMTU (Maximum Transmission Unit)should be adjustedonly 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 overheadto packets.
IPsec adds additional encapsulation(ESP, GRE, etc.), increasing the packet size.
If packets exceed the MTU, they may befragmented or dropped, causing intermittent connectivity issues.
Lowering the MTU on interfaces ensurespackets stay within the supported size limit across all network devices.

NEW QUESTION 21
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: AC

Explanation:
Zero phase selectors inIPsec Phase 2mean thatno specific traffic selectors (subnets) are defined, allowingany traffic to be encryptedthrough the VPN tunnel. This can cause unintended traffic forwarding issuesand disrupt network operations.
To prevent this from happening during future migrations:
Using routing protocolsensures thatonly 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 selectorsavoids the problem of encrypting all traffic by explicitly stating the allowed source and destination subnets. This prevents the tunnel from affecting unrelated network traffic.

NEW QUESTION 26
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?

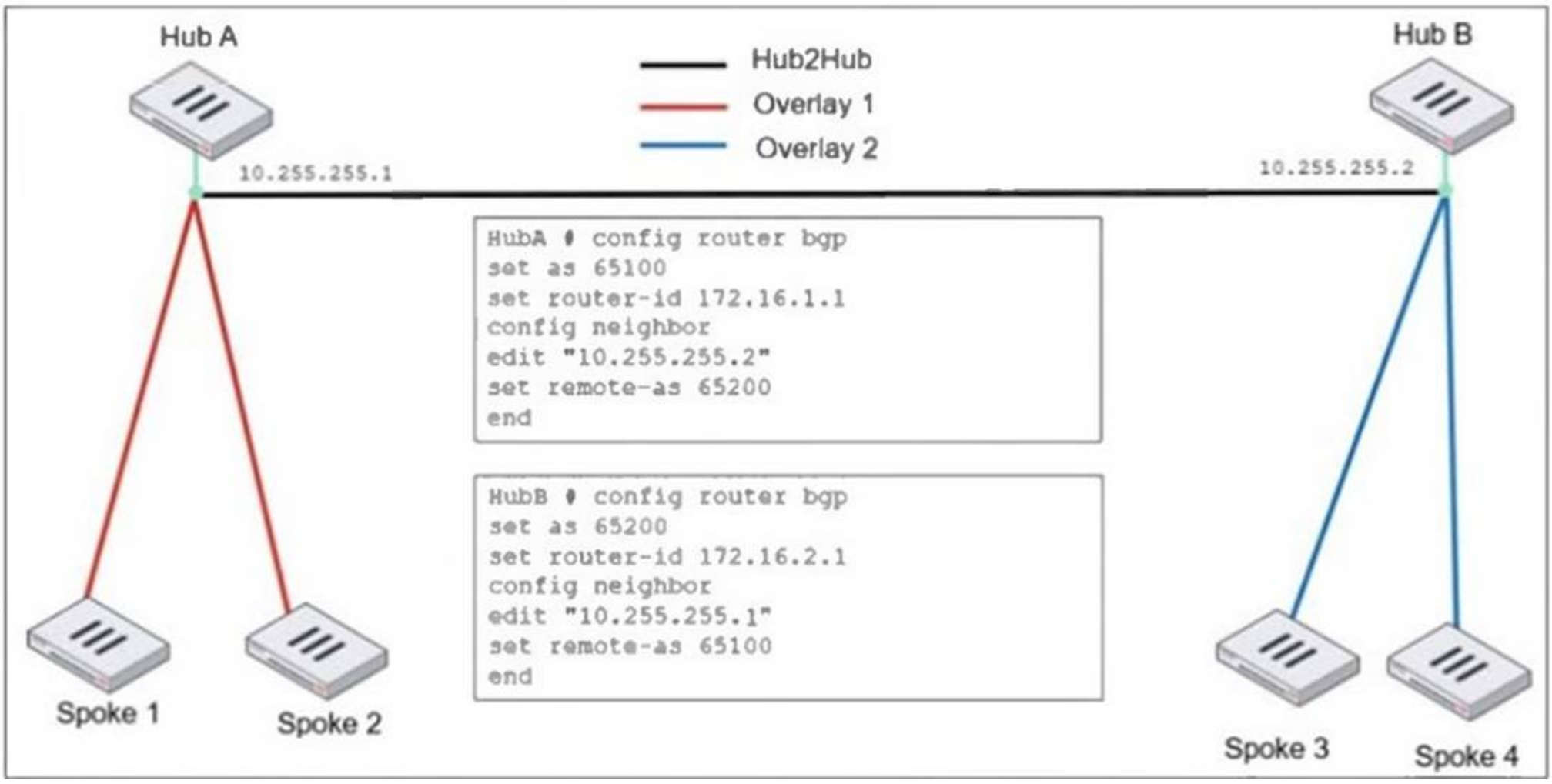
A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.
B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.
C. To analyze nonstandard ports in web 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 inproxy modewithfull SSL inspection enabled, it inspects encrypted HTTPS traffic by default onport 443. However, some websites may usenon- standard HTTPS ports(such as 8443), which FortiGate does not inspect unless explicitly configured.

To ensure that FortiGate inspects HTTPS traffic onport 8443, administrators must manually add port 8443in theProtocol Port Mappingsection of theSSL/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 ofFortiGuard category-based web filtering.

NEW QUESTION 31
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: AB

Explanation:
In thisADVPN (Auto-Discovery VPN) network, there are two hubs (Hub A and Hub B) connected viaEBGP, whileIBGPis 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.

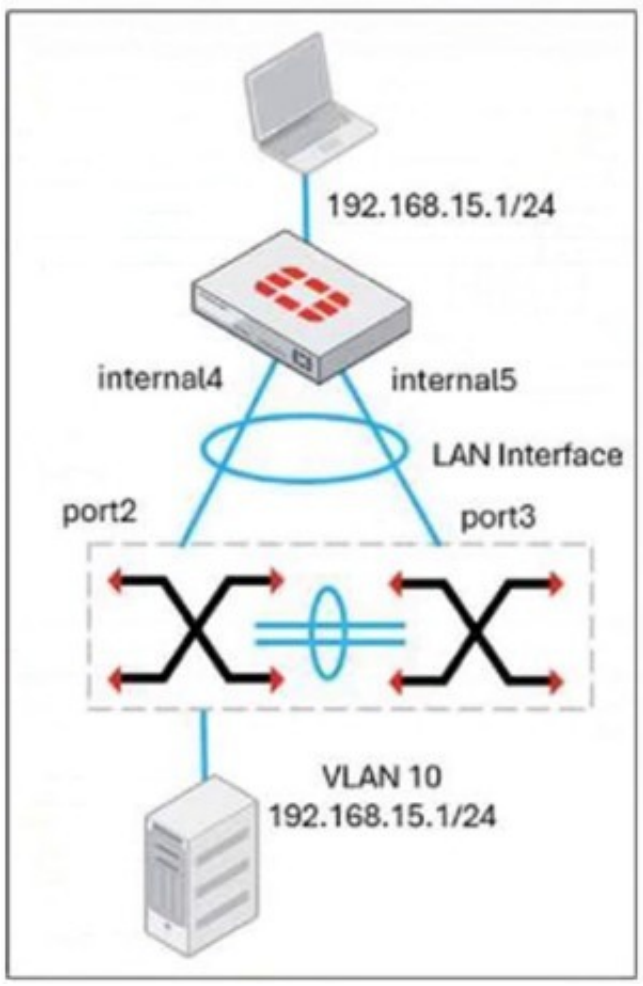
NEW QUESTION 35
An administrator must standardize the deployment of FortiGate devices across branches with consistent interface roles and policy packages using FortiManager.
What is the recommended best practice for interface assignment in this scenario?

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:
Whenstandardizing the deployment of FortiGate devices across branchesusing FortiManager, thebest practiceis to usemetadata variables. This allows fordynamic interface configurationwhile maintaining asingle, consistent policy packagefor all branches.
Metadata variablesin FortiManager enableinterface roles and configurations to be dynamically assignedbased on the specific FortiGate device.
This ensuresscalabilityandconsistent security policy enforcementacross all branches without manually adjusting interface settings for each device.
When a new branch FortiGate is deployed, metadata variables automaticallymap to the correct physical interfaces, reducing manual configuration errors.

NEW QUESTION 38
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: BC

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 to802.3ad (LAG)mode to aggregate the links for redundancy and load balancing.
This setup allows FortiGate to handle VLAN assignments dynamically, as seen withVLAN 10 (192.168.15.1/24). FortiLink ensures seamless integration between FortiGate and FortiSwitches, making STP unnecessary because Fortinet'sMCLAGprevents 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.

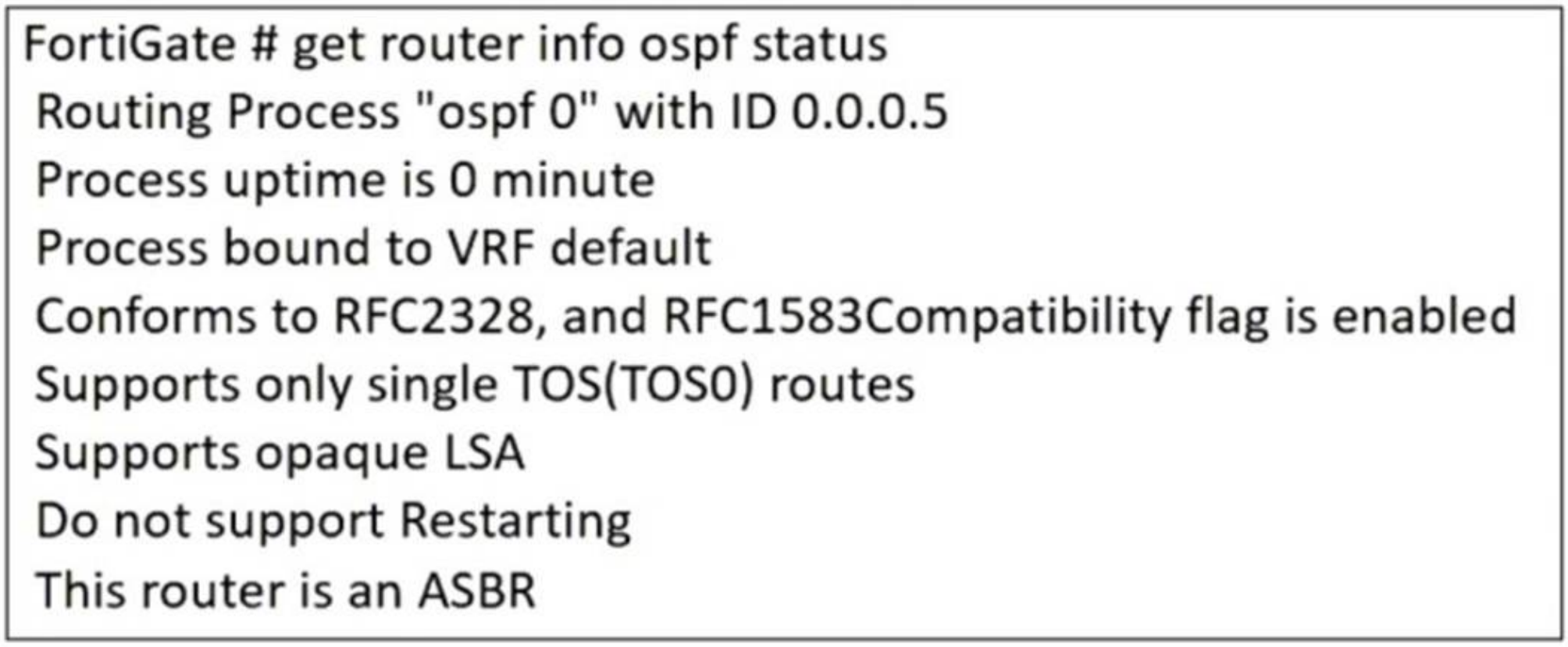
NEW QUESTION 39
A FortiGate device with UTM profiles is reaching the resource limits, and the administrator expects the traffic in the enterprise network to increase.
The administrator has received an additional FortiGate of the same model.
Which two protocols should the administrator use to integrate 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: AB

Explanation:
Whenadding an additional FortiGateto an enterprise network that is already reaching itsresource limits, the goal is to distribute traffic efficiently and ensurehigh availability.
FGSP (FortiGate Session Life Support Protocol) with external load balancers
FGSP allowssession-aware load balancingbetween multiple FortiGate units without
requiring them to be in an HA (High Availability) cluster.
Withexternal load balancers, incoming traffic isevenly distributedacross multiple FortiGate devices.
This approach is useful forscaling outtraffic handling capacity while ensuring that sessions remainsynchronizedbetween firewalls.
FGSP is effectivewhen stateful failover is requiredbut without the constraints of traditional HA.
FGCP (FortiGate Clustering Protocol) in active-active mode and with switches FGCPactive-active modeenables multiple FortiGate devices toshare traffic loads, increasing throughput and efficiency.
Active-active mode is suitable forbalancing UTM processingacross multiple FortiGates, making it ideal whenresource limits are a concern.
Usingswitchesensures redundancy and avoids single points of failure in the network.
This mode is commonly used inenterprise networkswhere bothscalability and redundancyare required.

NEW QUESTION 43
Refer to the exhibit, which contains the partial output of an OSPF command.



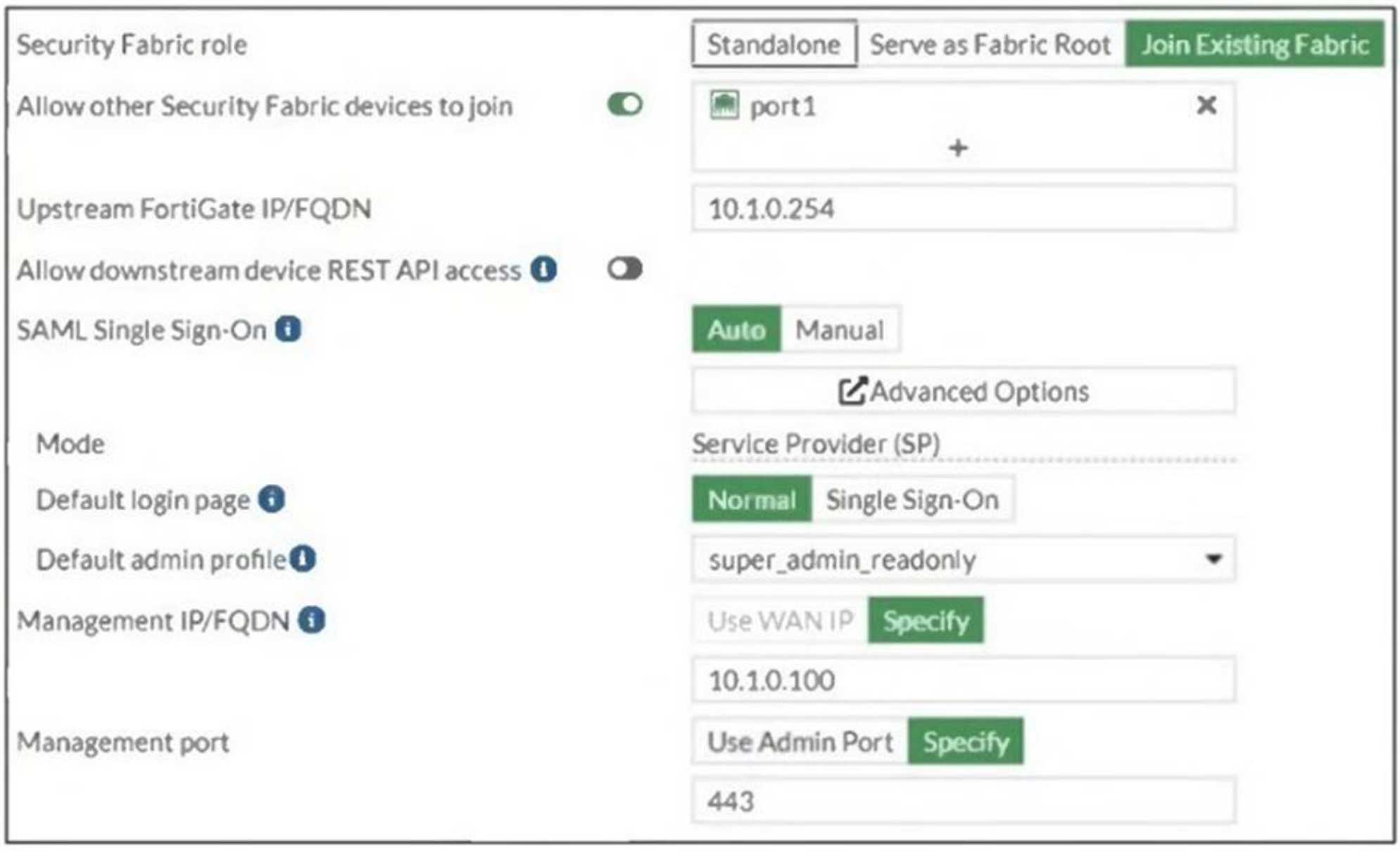
An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.
Which statement on this FortiGate device is correct?

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 theOSPF status output, the key information is:
"This router is an ASBR" This means the FortiGate is acting as anAutonomous System Boundary Router (ASBR).
AnASBRis responsible for injectingexternal routing informationinto OSPF from another routing protocol (such as BGP, static routes, or connected networks).

NEW QUESTION 48
Refer to the exhibits.



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 theRoot FortiGate - System Administrator Configurationexhibit: TheAdminSSOaccount has thesuper_admin_readonlyrole.
From theDownstream FortiGate - Security Fabric Settingsexhibit:
TheSecurity Fabric roleis set toJoin Existing Fabric, meaning it will authenticate with the root FortiGate.
SAML Single Sign-On (SSO) is enabled, and thedefault admin profileis set to
super_admin_readonly.
When theAdminSSOuser logs into the downstream FortiGate usingSSO, the authentication request is sent to the root FortiGate, where AdminSSO has super_admin_readonlypermissions. Since the downstream FortiGate inherits this permission through the Security Fabric configuration, the user will be granted super_admin_readonlyaccess.

NEW QUESTION 52
Refer to the exhibit, which shows the HA status of an active-passive cluster.

Status	Priority	Hostname	Virtual Domains	Role	System Uptime
Virtual cluster 1 2					
Synchronized	150	FortiGate_A	Core1 root	Primary	4h 52m
Synchronized	100	FortiGate_B	Core1 root	Secondary	4h 52m
Virtual cluster 2 2					
Synchronized	150	FortiGate_A	Core2	Primary	
Synchronized	128	FortiGate_B	Core2	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 anactive-passive HA (high availability) clusterwith two virtual clusters, where FortiGate_A is the primary device for both Core1 and Core2. If the goal is to haveFortiGate_B take over Core2 traffic, itspriority must be higherthan FortiGate_A forVirtual Cluster 2.
Currently, FortiGate_A has a priority of150for Core2, while FortiGate_B has128. Increasing FortiGate_B??s priority to 200ensures it becomes theprimary 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 anactive-passive setup, as it only applies to active-active configurations.

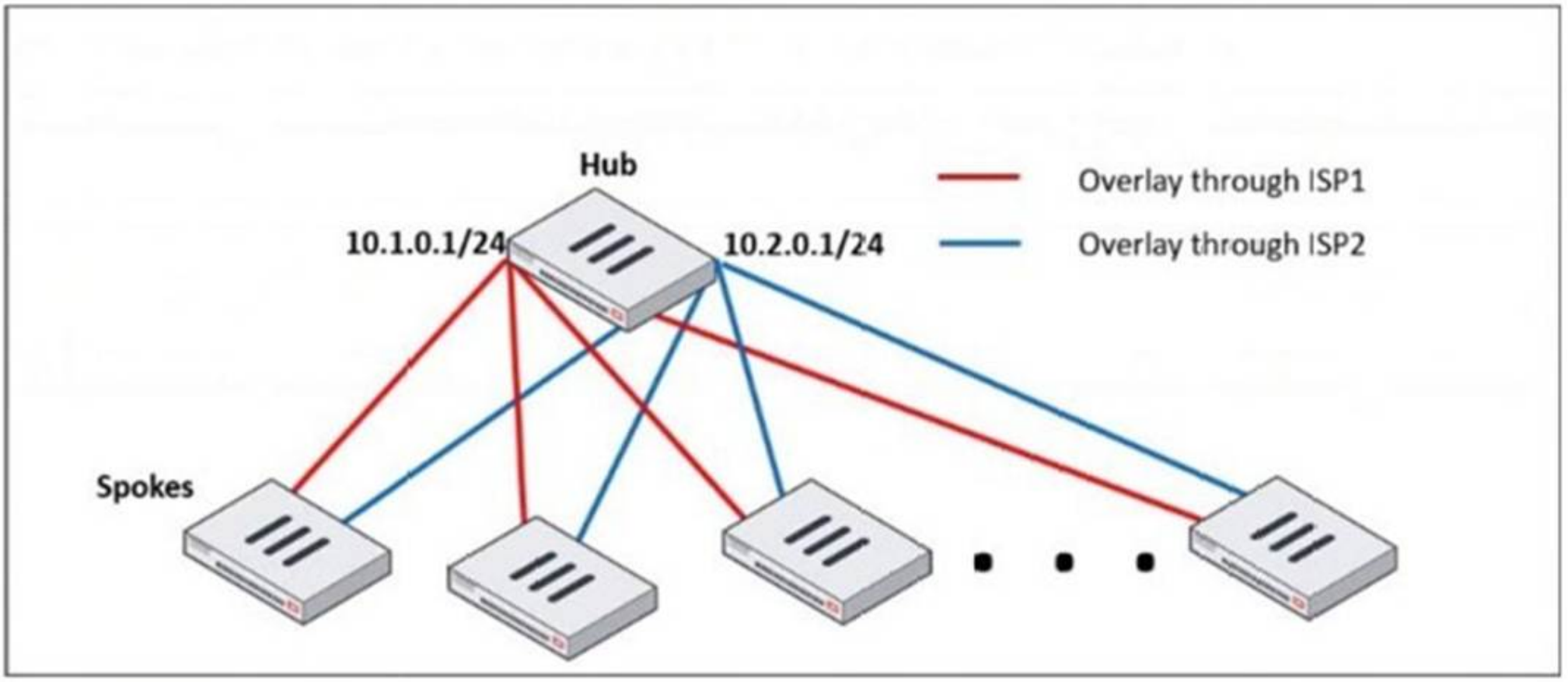
NEW QUESTION 56
A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on 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 decryptsit first. Ifonly certificate inspectionis enabled, FortiGate can see the certificate details (such as the domain and issuer) butcannot 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 theSSL/SSH Inspection Profile.
This allows FortiGate todecrypt the HTTPS traffic, inspect the content, and then re-Without full SSL inspection, threats embedded in encrypted traffic may go undetected.

NEW QUESTION 57
Refer to the exhibit, which shows a hub and spokes deployment.



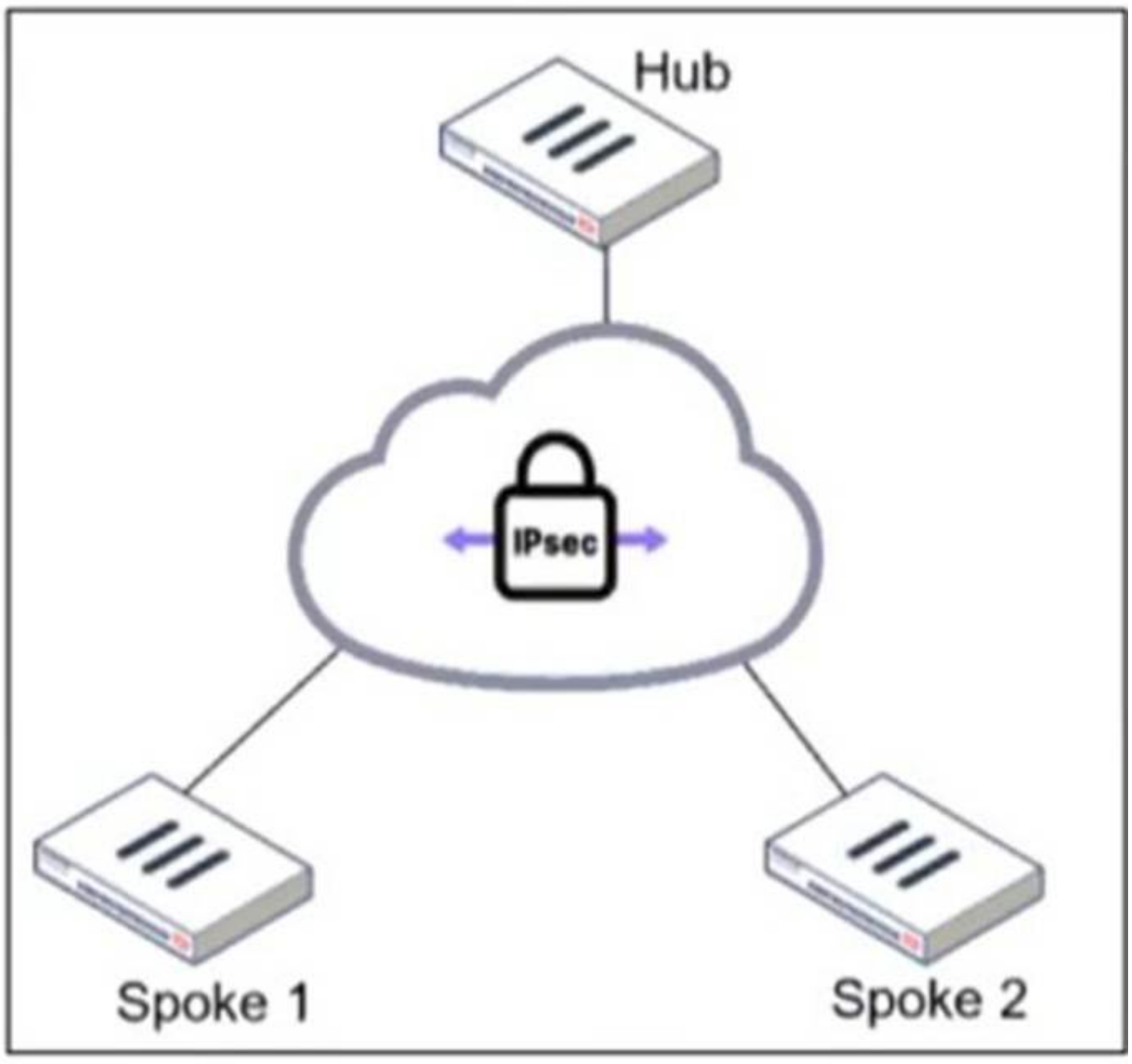
An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub.
Which two commands allow the administrator to minimize the configuration? (Choose two.)

A. neighbor-group
B. route-reflector-client
C. neighbor-range
D. ibgp-enforce-multihop

Answer: AC

Explanation:
neighbor-group:
This command is used to group multipleBGP neighborswith the same configuration, reducing redundant configuration.
Instead of defining individual BGP settings for each spoke, the administrator can create a neighbor-groupand apply the same policies, reducing manual work.
neighbor-range:
This command allows the configuration ofa range of neighbor IPs dynamically, reducing the need to manually define each spoke neighbor.
It automatically addsBGP neighborsthat match a given prefix, simplifying deployment.

NEW QUESTION 60
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, thepoint-to-multipointnetwork 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.

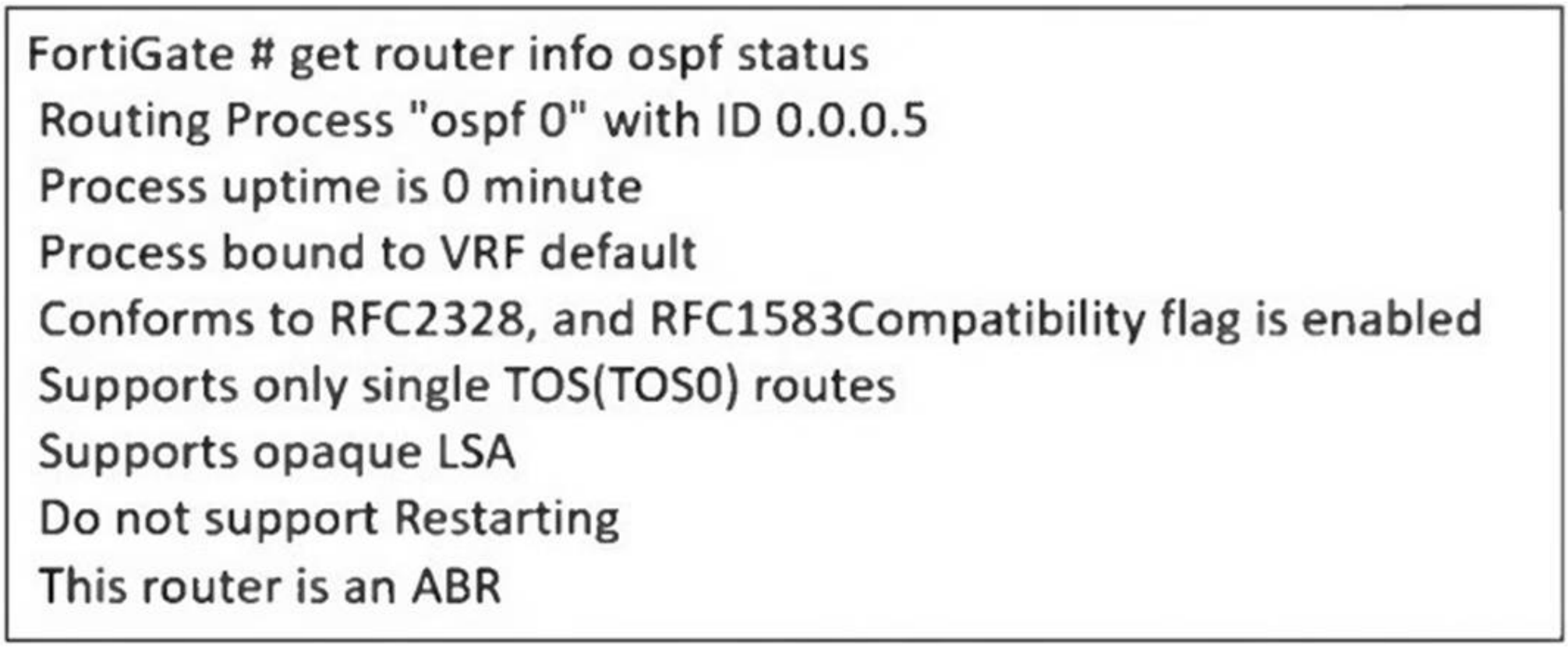
NEW QUESTION 65
Why does the ISDB block layers 3 and 4 of the OSI model when applying content filtering? (Choose two.)

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: AB

Explanation:
TheInternet 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 theirpredefined IP addresses and ports.
FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard:
FortiGate retrieves and updates apredefined listof IPs and ports for different internet services fromFortiGuard.
This allows FortiGate to block specific services atLayer 3 and Layer 4without requiring deep packet inspection.
The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard:
ISDB works by matching traffic to knownIP addresses and portsof categorized services. When an application or service is blocked, FortiGate prevents communication bydenying traffic based on its destination IP and port number.

NEW QUESTION 67
Refer to the exhibit, which contains the partial output of an OSPF command.



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: BC

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 tomultiple OSPF areasand maintains routing information between them.
This confirms that the FortiGate isnot just in one area, but at leastone 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 inOSPF extensions, including those that support external route injection.
Typically, ABRs or ASBRs (Autonomous System Boundary Routers)inject external routes, allowing routes fromother routing protocols (such as BGP or static routes) to be advertised into OSPF.

NEW QUESTION 72
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 withNP6 (Network Processor 6) accelerationoffload traffic directly to hardware, bypassing the CPU for improved performance. Whenauto-asic-offloadis enabled in a firewall policy, most of the trafficdoes 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, onlya 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 offloading using:
config firewall policy edit <policy_ID>
set auto-asic-offload disable end
Disabling ASIC offload forces traffic to be processed by the CPU, allowing the sniffer tool to capture all packets.

NEW QUESTION 76
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCSS_EFW_AD-7.4 Practice Exam Features:

* FCSS_EFW_AD-7.4 Questions and Answers Updated Frequently

* FCSS_EFW_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_EFW_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_EFW_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year