Fortinet

Exam Questions FCSS_EFW_AD-7.4

FCSS - Enterprise Firewall 7.4 Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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: AC

Explanation:
The MAC addresse0:23:ff:fc:00:86follows the format used in FortiGate High Availability (HA) clusters. When FortiGate devices are in an HA configuration, they use virtual MAC addresses for failover and redundancy purposes.
The suspicious packet is related to a cluster that has VDOMs enabled:FortiGate devices with Virtual Domains (VDOMs)enabled use specific MAC address ranges to differentiate HA-related traffic. This MAC address is likely part of that mechanism.
The suspicious packet is related to a cluster with a group-id value lower than 255: FortiGate HA clusters assign virtual MAC addresses based on thegroup ID. The last octet (00:86) corresponds to agroup IDthat isbelow 255, confirming this option.

NEW QUESTION 2
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) 2.0is the optimal solution for enablingdirect spoke-to- spoke communicationwithout passing through the hub, while also allowingautomatic link selectionbased on quality metrics.
Dynamic Direct Tunnels:
ADVPN 2.0 allowsspokes to establish direct IPsec tunnels dynamicallybased 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 2.0monitors the qualityof multiple internet connections on each spoke.
It automatically switches to the best available connection when the primary linkdegrades or fails.
This is achieved by dynamically adjusting BGP-based routing or leveraging SD-WAN integration.

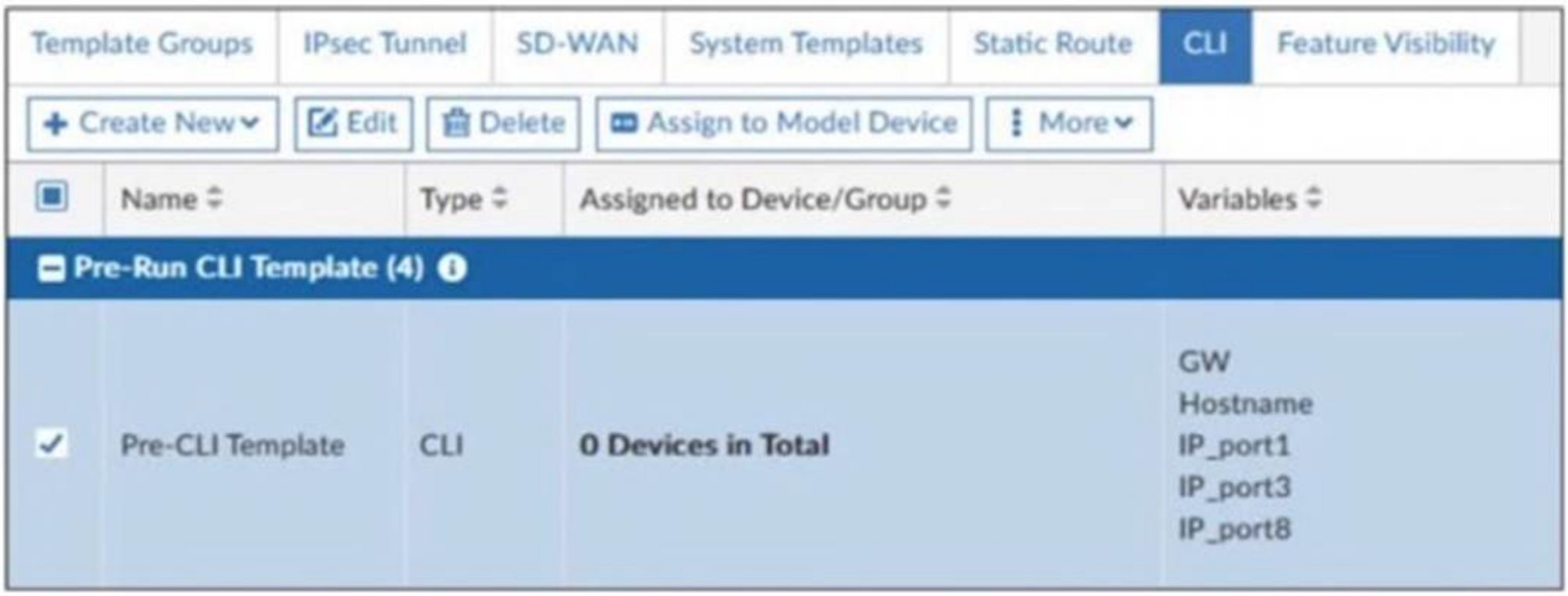
NEW QUESTION 3
How will configuring set tcp-mss-sender and set tcp-mss-receiver in a firewall policy affect the size and handling of TCP packets in the network?

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:
Theset tcp-mss-senderandset tcp-mss-receivercommands in afirewall policyallow an administrator to adjust theMaximum Segment Size (MSS)of TCP packets.
This setting controls thelargest payload sizethat a device can handle in a singleTCP segment, ensuring that packets do not exceed the allowed MTU (Maximum Transmission Unit) along the network path.
set tcp-mss-senderadjusts the MSS value foroutgoing TCP traffic. set tcp-mss-receiveradjusts the MSS value forincoming TCP traffic.
This helps prevent issues withfragmentationandMTU mismatches, improving network performance and avoiding retransmissions.

NEW QUESTION 4
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.



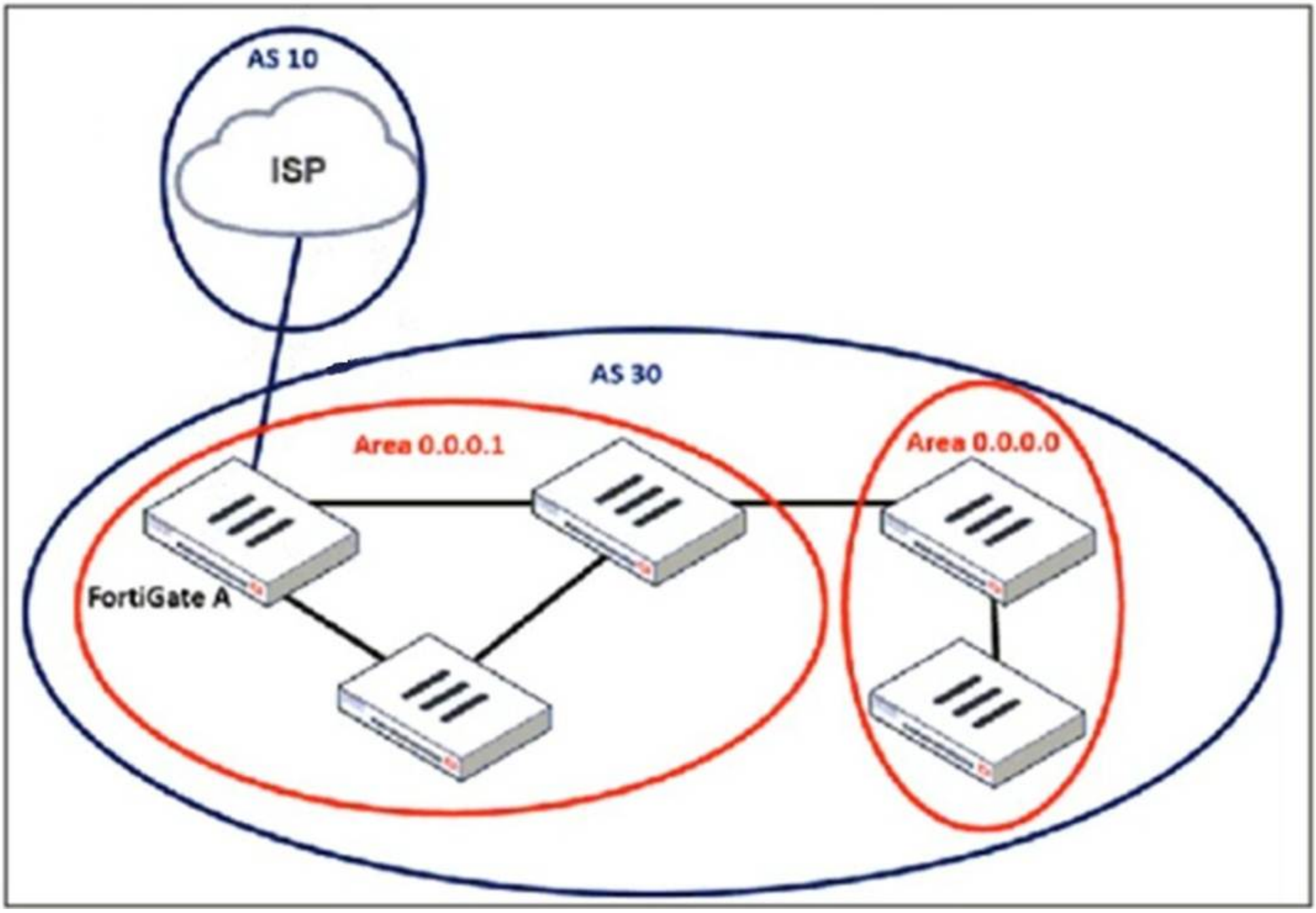
The template is not assigned even though the configuration has already been installed on FortiGate.
What is true about this scenario?

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:
InFortiManager,pre-run CLI templatesare used inZero-Touch Provisioning (ZTP)and Low-Touch Provisioning (LTP)to configure a FortiGate devicebeforeit is fully managed by FortiManager.
These templatesapply configurationswhen a device is initially provisioned.Once the pre- run CLI template is executed, FortiManagerautomatically unassignsit from the device because it isnot meant to persistlike other policy configurations. This prevents conflicts and ensures that the FortiGate configuration isnot repeatedly appliedafter the initial setup.

NEW QUESTION 5
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.)

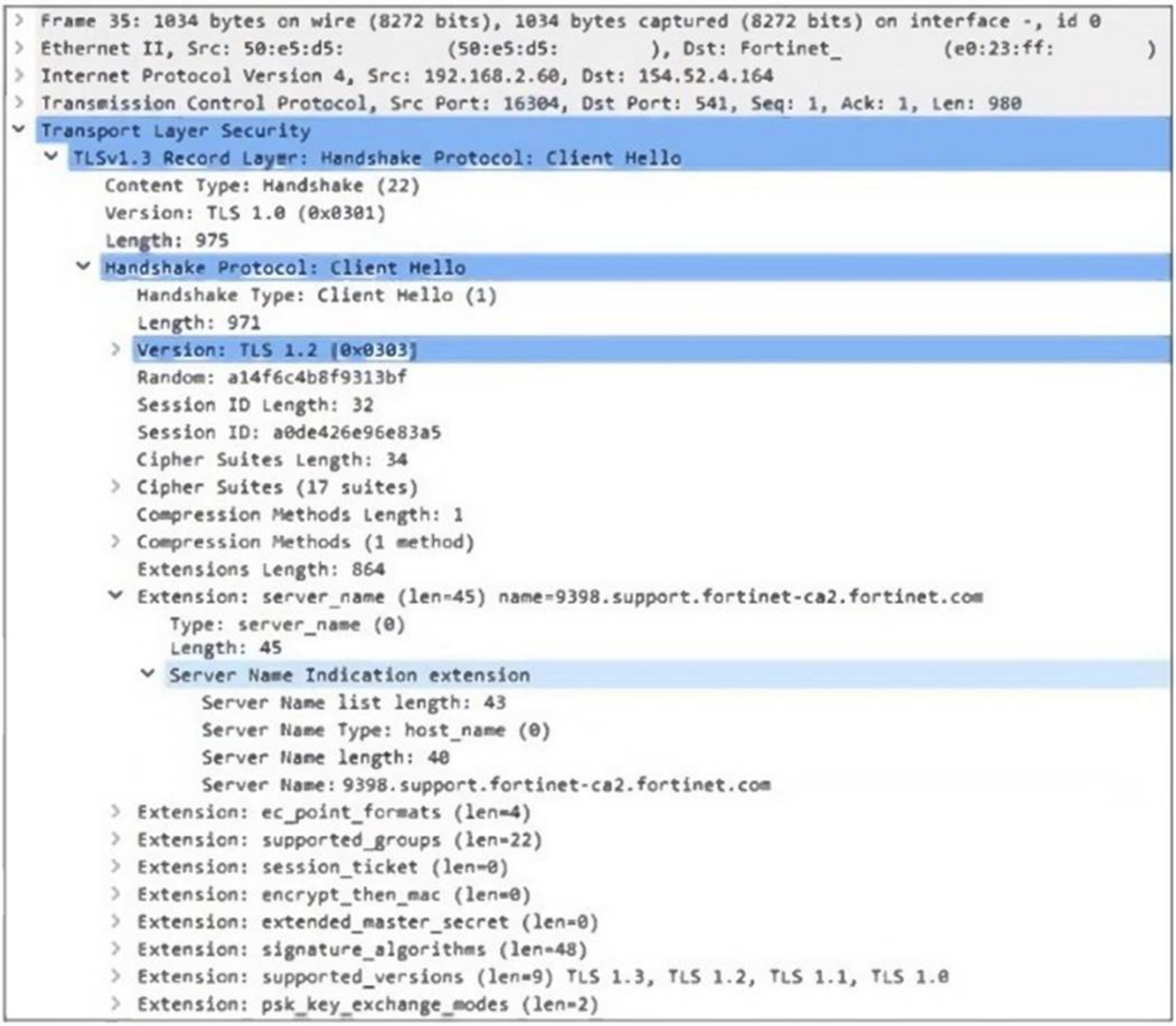
A. ebgp-enforce-multihop
B. update-source
C. ibgp-enforce-multihop
D. recursive-next-hop

Answer: AB

Explanation:
When configuring aloopback interface as the BGP sourceforconnecting 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 usingloopback interfaces,packets will not be sent directly between their physical interfaces.
Theebgp-enforce-multihopcommandallows BGP to form an eBGP peering over multiple hops.
* 2. Set the Update Source (update-source)
Since FortiGate is using aloopback interface as the source, theupdate-sourcecommand ensures thatBGP updates originate from the loopback interfacerather than a physical interface.
This is essential becauseBGP peers must match the source IP with the configured neighbor address.

NEW QUESTION 6
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



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

Answer: D

Explanation:
The packet capture output displays aTLS Client Hellomessage from FortiGate to FortiManager Cloud. This message containsServer Name Indication (SNI), which is used to indicate the domain name that FortiGate is trying to connect to. FortiGate will receive a certificate that supports multiple domains because FortiManager operates in a cloud computing environment.
FortiManager Cloud hostsmultiple customersand domains under ashared infrastructure.
The TLS handshake includesSNI (Server Name Indication), which allows FortiManager Cloud toserve multiple certificatesbased on the requested domain.
This means FortiGate will likely receive amulti-domain or wildcard certificatethat can be used for multiple customers under FortiManager Cloud.
The wildcard for the domain .fortinet-ca2.support.fortinet.com must be supported by FortiManager Cloud.
The SNI extension contains the domain9398.support.fortinet-ca2.fortinet.com. FortiManager Cloud must supportwildcard certificatessuch as *.fortinet-ca2.support.fortinet.com to securely manage multiple subdomains and customers. This ensures that FortiGate can validate the server certificate without any TLS errors.

NEW QUESTION 7
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.)

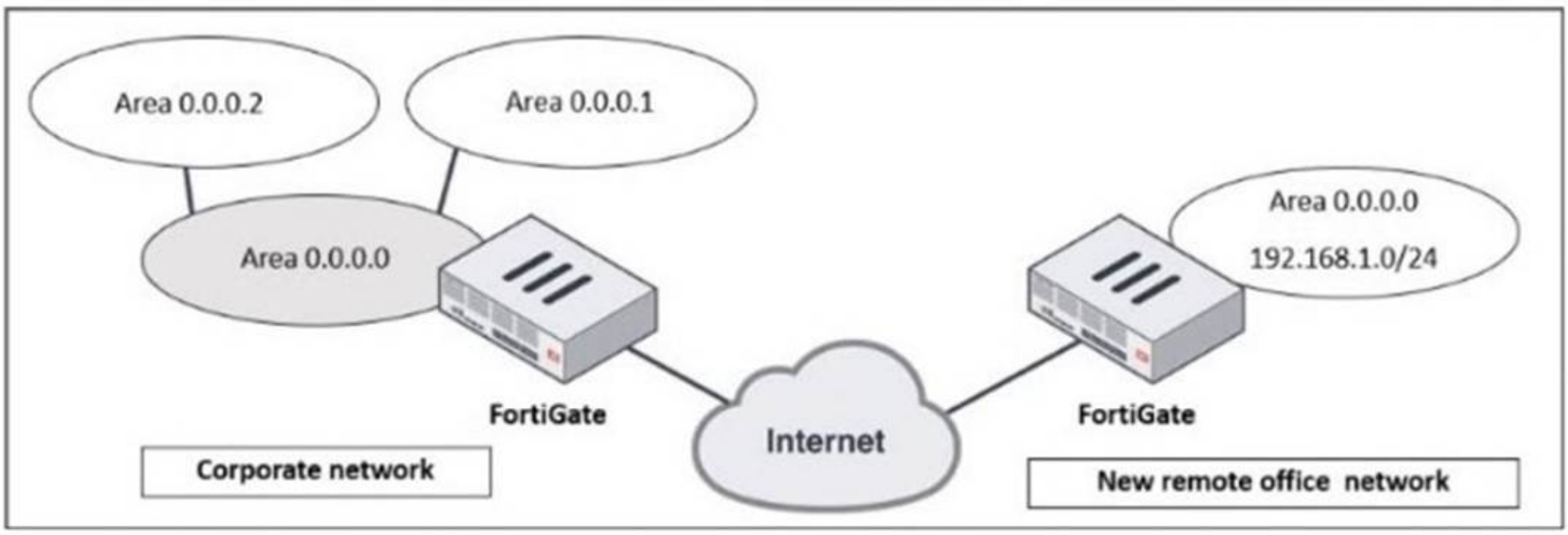
A. Use metadata variables to dynamically assign values according to each FortiGate device.
B. Use provisioning templates and install configuration settings at the device layer.
C. Use the Global ADOM to deploy global object configurations to each FortiGate device.

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 8
Refer to the exhibit, which shows a corporate network and a new remote office network.



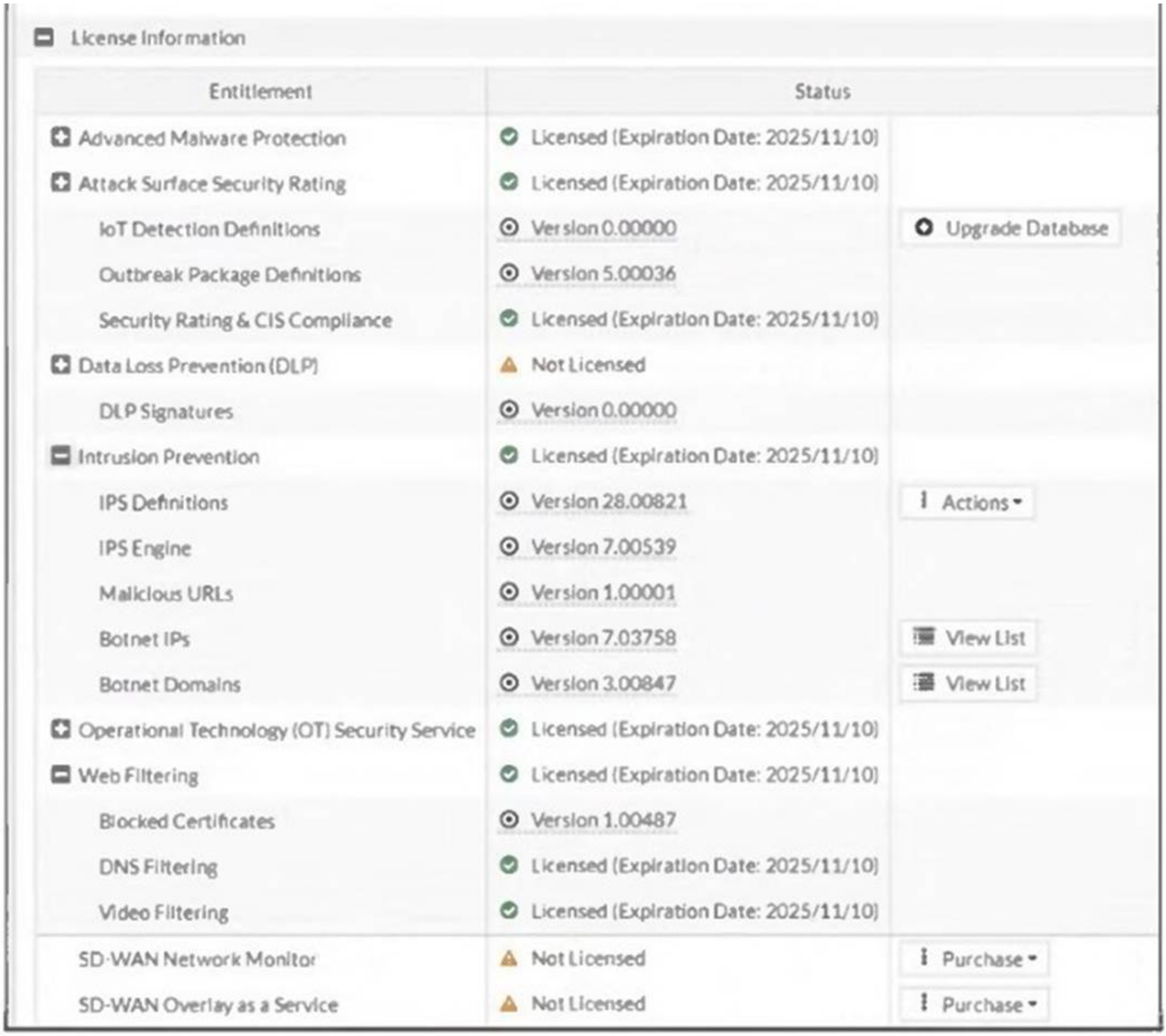
An administrator must integrate the new remote office network with the corporate enterprise network.
What must the administrator do to allow routing between the two networks?

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



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 GU
C. It requires enabling debug mode to make it visible.
D. The web filter database is not hosted on FortiGate: FortiGate queries FortiGuard or FortiManager for web filter ratings on demand.
E. 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, FortiGatequeries FortiGuard (or FortiManager, if configured) dynamicallyto 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:
UnlikeIPS and antivirus, which download and store signature updates locally,web filtering relies on cloud-based queries.
This is whyno database version appears in the GUI. Flow mode vs Proxy mode:
Inproxy mode, FortiGate cancachesome web filter data, improving performance. Inflow mode, all queries happen dynamically, with no locally stored database.

NEW QUESTION 10
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 minimizeCPU and RAM usagewhile still enforcingsecurity features like web filtering and application control,SSL certificate inspection modeis the best choice.
SSL certificate inspectionallows FortiGate to inspectonly the SSL/TLS handshake, including theServer Name Indication (SNI) and certificate details, without decrypting the full encrypted payload.
This enables features likeweb filtering and application controlbecause FortiGate can determine thedestination website or applicationbased onSNI and certificate information.
Itsignificantly reduces system loadcompared tofull SSL inspection, which requires full decryption and re-encryption of traffic.

NEW QUESTION 10
Refer to the exhibit, which contains a partial VPN configuration.

```
config vpn ipsec phase1-interface
edit tunnel
set type dynamic
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 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:
ThisIPsec Phase 1 configurationdefines adynamicVPN tunnel that can accept connections from multiple peers. The settings chosen here suggest a configuration optimized fornetworks with intermittent traffic patternswhile 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 UsesIKEv2, which is more efficient and supports features like EAP
authentication and reduced rekeying overhead.
set dpd on-idle Dead Peer Detection (DPD) is triggeredonly 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 alonger key lifetime(8 hours), reducing the frequency of rekeying, which is beneficial for stable connections.
BecauseDPD 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 fornetworks with regular but non-continuous traffic, balancing security and resource efficiency.

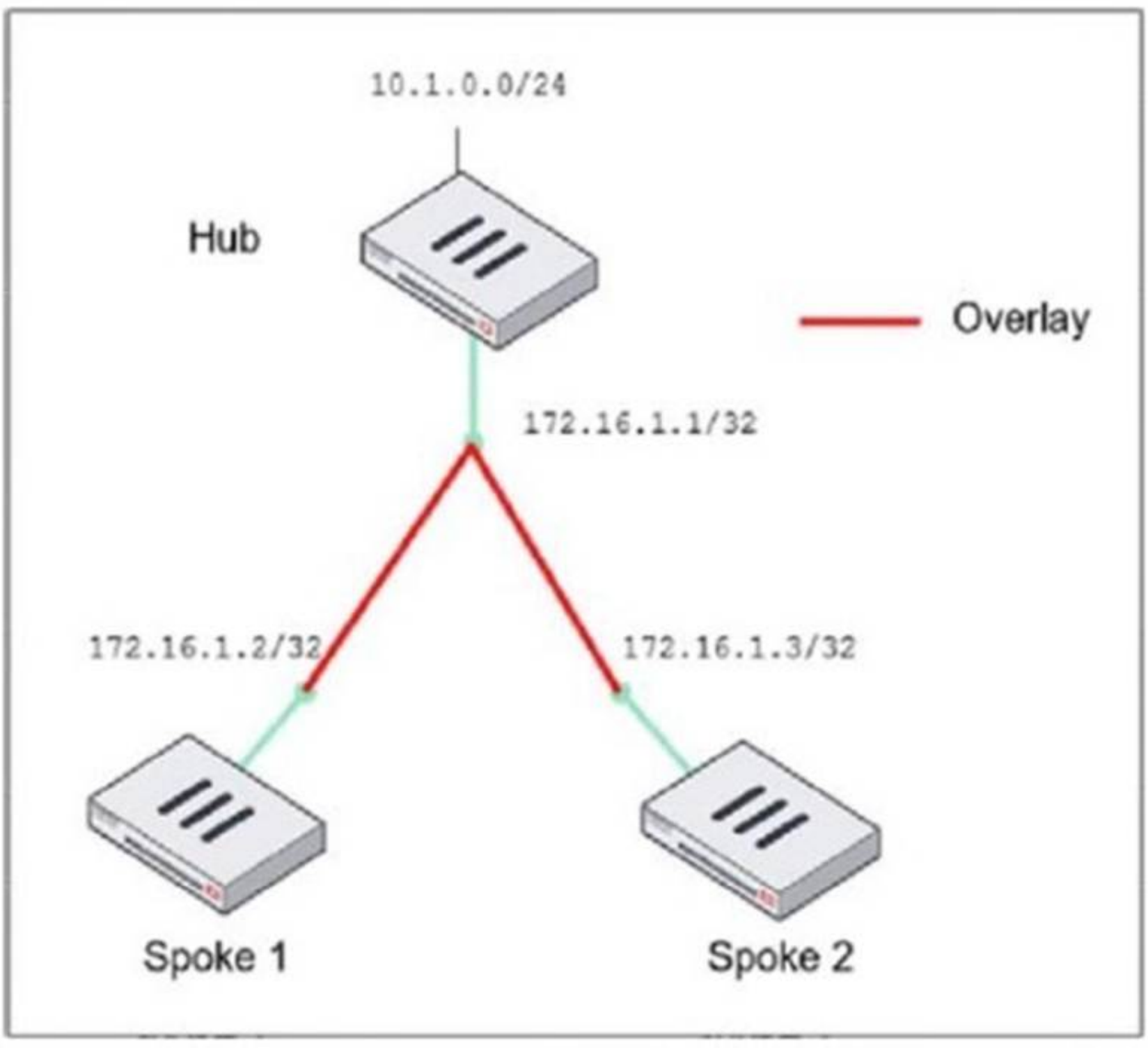
NEW QUESTION 14
A vulnerability scan report has revealed that a user has generated traffic to the website example.com (10.10.10.10) using a weak SSL/TLS version supported by the HTTPS web server.
What can the firewall administrator do to block all outdated SSL/TLS versions on any HTTPS web server to 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:
Thebest wayto block outdated SSL/TLS versions is toconfigure the SSL/SSH inspection profileto enforce aminimum SSL/TLS versionand disable weak SSL versions.
By setting theminimum allowed SSL versionin theHTTPS settings of the SSL/SSH inspection profile, FortiGate will:
Block any connection usingoutdated SSL/TLS versions(such as SSLv3, TLS 1.0, or TLS 1.1).
Enforce secure communication usingonly strong SSL/TLS versions(such as TLS 1.2 or TLS 1.3).
Protect users fromman-in-the-middle (MITM) and downgrade attacksthat exploit weak encryption.

NEW QUESTION 17
Refer to the exhibit, which shows the ADVPN network topology and partial BGP configuration.



Partial BGP configuration

```
Hub # 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
```

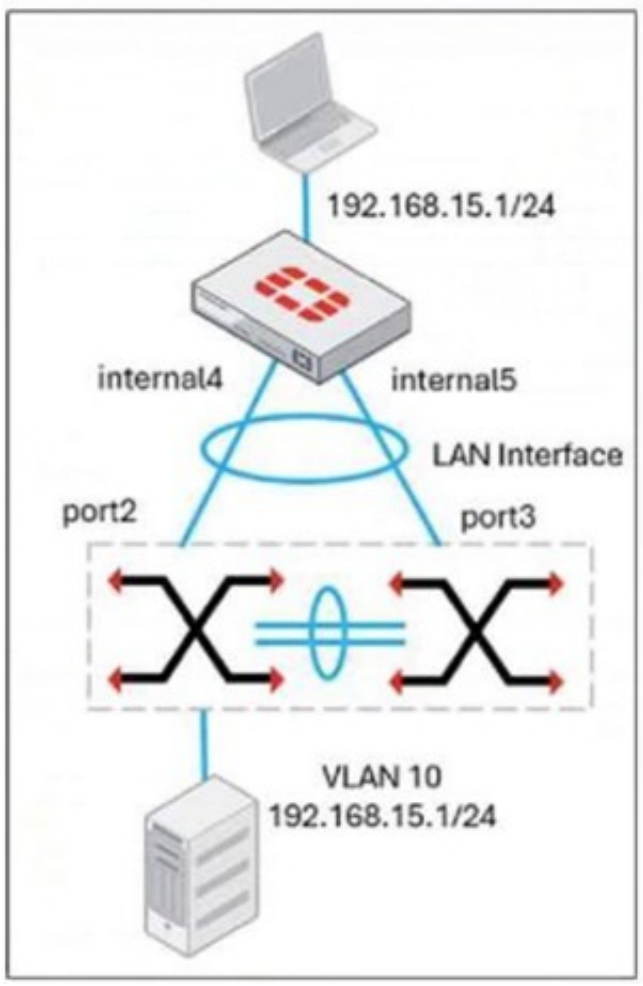
Which two parameters must an administrator configure in the config neighbor range for spokes shown in the exhibit? (Choose two.)

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: BD

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
Theneighbor-groupparameter is used to apply pre-defined settings (such as AS number) to dynamically discovered BGP neighbors.
Theadvpnneighbor-group is already defined in the configuration, and assigning it to the neighbor-range ensures consistent BGP settings for all spoke neighbors.
set prefix 172.16.1.0 255.255.255.0
This command allowsdynamic BGP peer discoveryby defining a range of potential neighbor IPs (172.16.1.1 - 172.16.1.255).
Sinceeach spoke has a unique /32 IPwithin this subnet, this ensures that any spoke within the172.16.1.0/24range can automatically establish a BGP session with the hub.

NEW QUESTION 21
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.

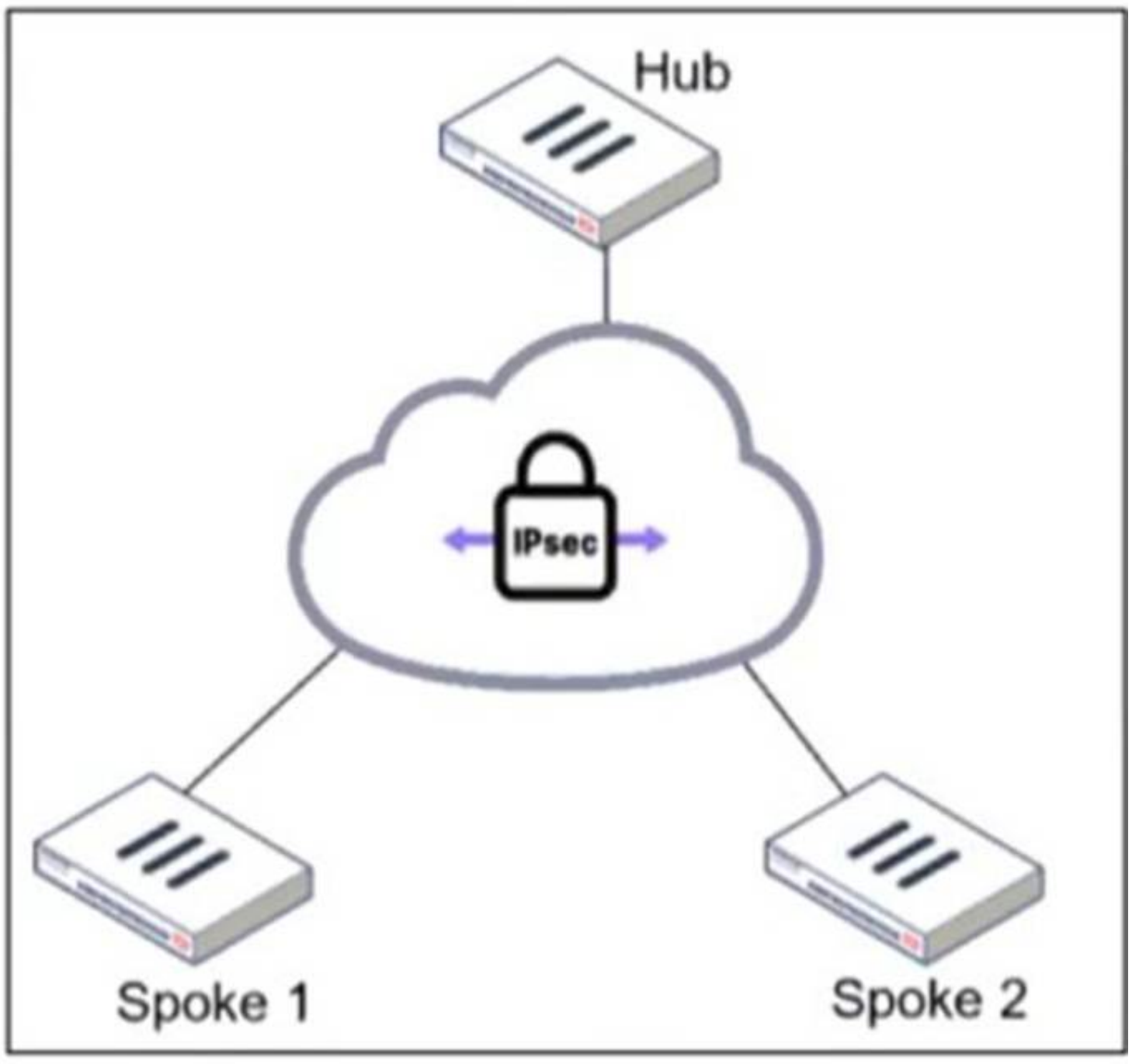
NEW QUESTION 23
A FortiGate device with UTM profiles is reaching the resource limits, and the administrator expects the traffic in the enterprise network to increase.
The administrator has received an additional FortiGate of the same model.
Which two protocols should the administrator use to integrate 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 24
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 26
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 interfacebased 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 atransparent mode Virtual Domain (VDOM)configuration, FortiGate operates as a
Layer 2 bridgerather than performing Layer 3 routing. Theset forward-domain
<domain_ID>command is used to control how traffic is forwarded between interfaces within the sametransparent VDOM.
Aforward-domainacts as abroadcast domain, meaning only interfaces with thesame forward-domain IDcan exchange traffic. This setting is commonly used toseparate different VLANs or network segmentswithin the transparent VDOM while still allowing FortiGate to apply security policies.

NEW QUESTION 29
Refer to the exhibit.

Routing table on FortiGate_A

```
FortiGate_A  # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - 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, port1, [1/0]
C       10.1.0.0/24 is directly connected, port1
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, port1), 00:39:45, [1/0]
B       172.16.1.252/30 [200/0] via 10.1.0.1 (recursive is directly connected, port1), 00:42:48, [1/0]
C       172.16.100.0/24 is directly connected, port8
```

Routing table on FortiGate_B

```
FortiGate_B  # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - 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, port1, [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, port1
B       10.1.4.0/24 [200/0] via 10.1.0.100 (recursive is directly connected, port1), 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, port1), 00:38:14, [1/0]
C       172.16.1.248/30 is directly connected, C0
C       172.16.1.252/30 is directly connected, A0
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 route172.16.1.248/30on FortiGate_A. What must the administrator configure?

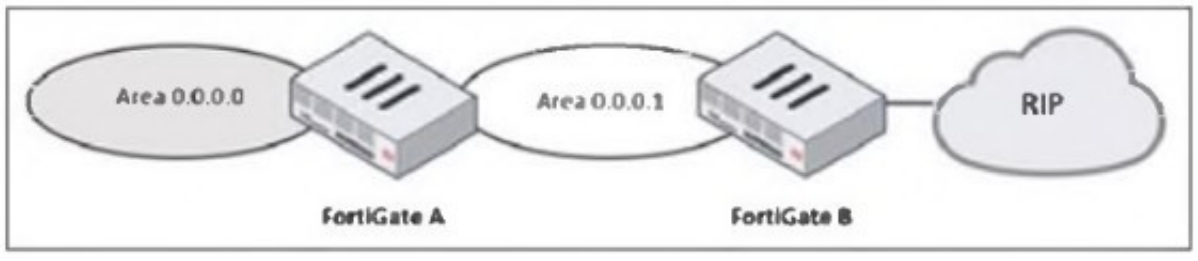
A. The prefix 172.16.1.248/30 in the BGP Networks section on FortiGate_B
B. A BGP route map out for 172.16.1.248/30 on FortiGate_B
C. Enable Redistribute Connected in the BGP section on FortiGate_B.
D. A BGP route map in for 172.16.1.248/30 on FortiGate_A

Answer: B

Explanation:
FortiGate_A and FortiGate_B are in thesame autonomous system (AS), andFortiGate_Adoesnot currently have route 172.16.1.248/30in its routing table. However, FortiGate_B has this routeas a connected route.

To dynamically advertiseonly172.16.1.248/30 fromFortiGate_B to FortiGate_A, the administrator must configure aBGP route map outonFortiGate_Bthat specifically permitsonlythis prefix.
A BGP route map out on FortiGate_Bcontrols which routes FortiGate_B advertises to FortiGate_A. If no filtering is applied, FortiGate_B might advertiseall BGP-learned and connected routes, which is not what the administrator wants. The route map should include aprefix-listthat explicitlyallows only172.16.1.248/30 and denies everything else.

NEW QUESTION 33
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 amulti-area OSPF networkwhere: FortiGate Ais inOSPF Area 0 (Backbone area).
FortiGate Bis inOSPF Area 0.0.0.1and is connected to anRIP network.
To ensure thatOSPF Area 0 (0.0.0.0) learns routes from the external RIP network, FortiGate B mustredistribute RIP routes into OSPF.
Steps to achieve this:
* 1. Enable route redistribution on FortiGate Bto inject RIP-learned routes into OSPF.
* 2. This allows OSPFArea 0.0.0.1to forward RIP routes toOSPF Area 0 (0.0.0.0), making the external network visible.

NEW QUESTION 34
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(TOS0) 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: 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 35
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:
Thebest way to automate a firewall policyusing a daily updated list ofIP addressesis by using anexternal connector from Threat Feeds. This allows FortiGate to dynamically retrievereal-time threat intelligencefrom external sources and apply it directly to security policies.
By configuringThreat Feeds, the administrator can:
Automatically updatefirewall policies with the latest malicious IPs daily.
Block trafficfrom those IPs in real-time without manual intervention.
Integrate with FortiGuard, third-party threat intelligence sources, or custom feeds (CSV, STIX/TAXII, etc.).

NEW QUESTION 38
.....

Relate Links

100% Pass Your FCSS_EFW_AD-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_EFW_AD-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/