Fortinet

Exam Questions FCSS_EFW_AD-7.4

FCSS - Enterprise Firewall 7.4 Administrator

NEW QUESTION 1
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 address10.1.10.1, 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 actionMalware, 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: BD

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 toreceive threat intelligencefrom NGFW-1, even if UTM is not enabled locally.
If NGFW-1 detects malware fromIP 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 thoughISFW does not have UTM enabled, NGFW-1 (which sits between ISFW and the external network)does have UTM enabledand is scanning traffic.
Since NGFW-1 detects malware in the session, it logs the event, which is then sent to FortiAnalyzer.

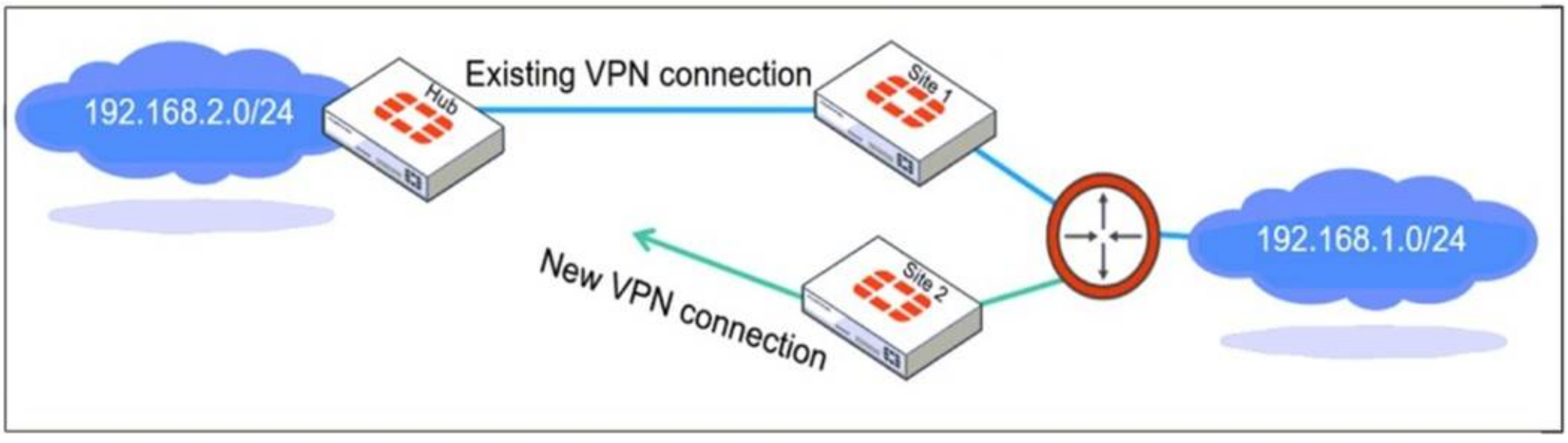
NEW QUESTION 2
An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection.
The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best 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
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?

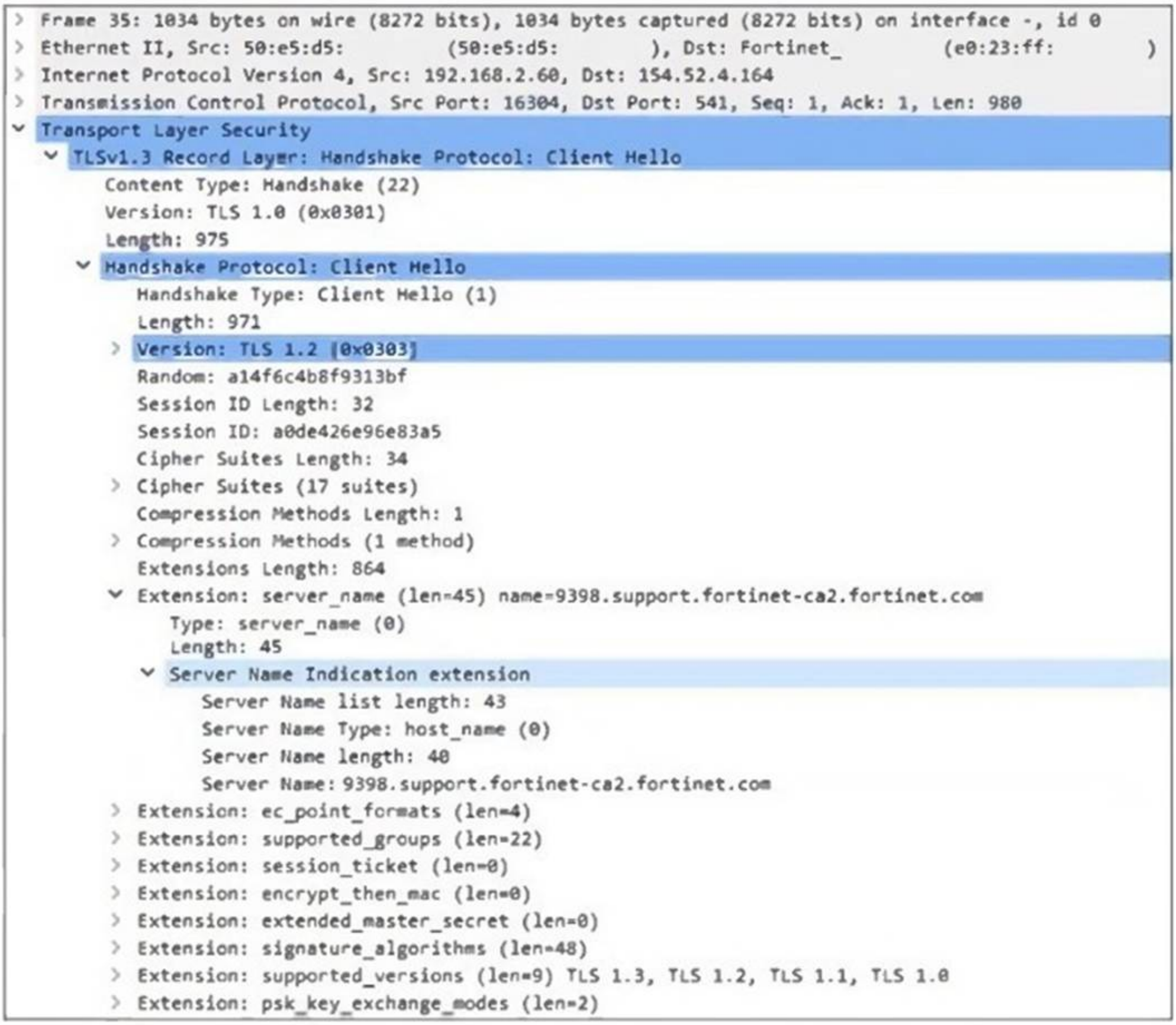
A. Set route-overlap to either use-new or use-old
B. Set net-device to ecmp
C. Set single-source to enable
D. Set route-overlap to allow

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 4
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 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.

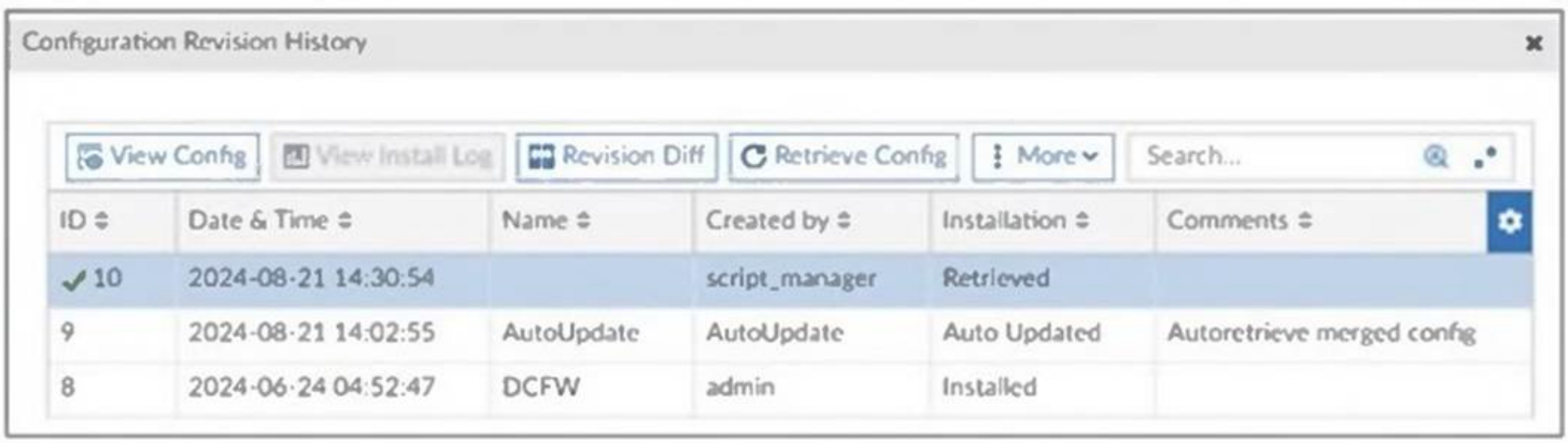
NEW QUESTION 6
A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices.
Which three approaches can the company 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
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 anIBGP (Internal BGP) network, all routers must befully meshed, meaning every router must establish a BGP session with every other router in the sameautonomous system (AS). Thisdoes not scale wellin large networks due to the exponential increase in BGP sessions.
Tooptimize and scale IBGP,Route Reflectors (RRs)are used. ARoute Reflector (RR)reduces the number ofIBGP peer connectionsby allowing acentralized router (RR)to redistribute IBGP routes to other IBGP peers (calledclients). This eliminates the need for afull mesh, significantlyreducing BGP session overhead.
By configuring theroute-reflector-clientsetting on IBGP peers, an administrator can: Scale IBGP sessionsby reducing the number of direct BGP peer connections.
Optimize the routing tableby ensuring routes are efficiently propagated within the IBGP network.
Eliminate the need for full mesh topology, making IBGP more manageable.

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
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 theBGP neighbor status output, the key issue is thatBGP is stuck in the "Idle" state, meaning the FortiGate is unable to establish a BGP session with its peer100.65.4.1 (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 enableebgp-enforce-multihop, which allows BGP sessions to be established even when the neighbors are not directly connected.

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 11
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 13
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 16
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 17
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 22
Refer to the exhibit, which shows a partial troubleshooting command output.

```
FortiGate # diagnose vpn tunnel list name Hub2Spoke1

list ipsec tunnel by names in vd 0

...

npu_flag=20 npu_rgwy=10.10.2.2 npu_lgwy=10.10.1.1 npu_selid=1
```

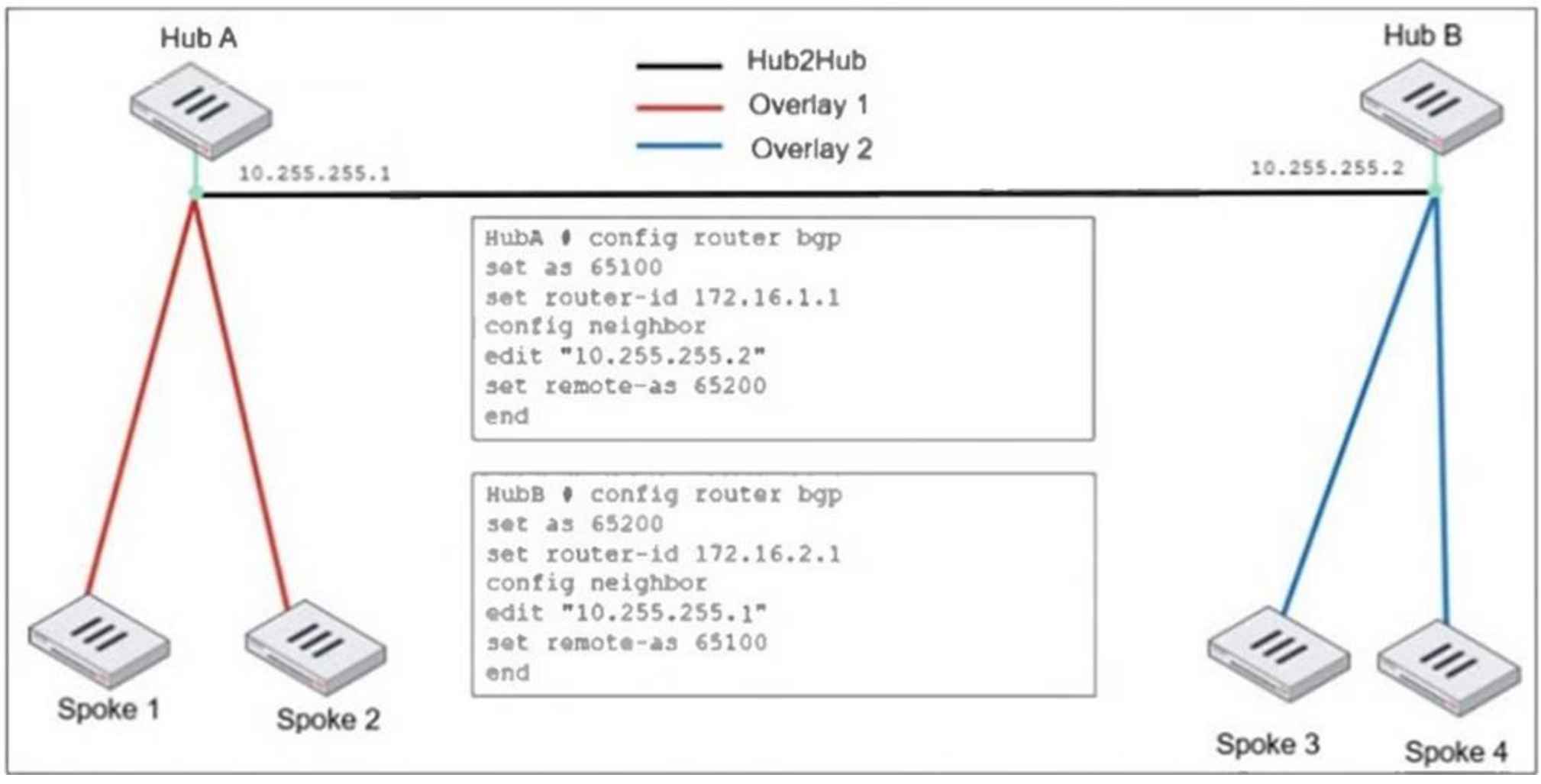
An administrator is extensively using IPsec on FortiGate. Many tunnels show information similar to the output shown in the exhibit.
What can the administrator conclude?

A. IPsec SAs cannot be offloaded.
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: B

Explanation:
The diagnose vpn tunnel list name Hub2Spoke1 command output provides key information about the offloading status of an IPsec VPN tunnel to the Network Processing Unit (NPU). npu_flag=20:
This flag indicates that both inbound and outbound IPsec Security Associations (SAs) have been offloaded to the NPU, meaning the VPN traffic is processed in hardware instead of the CPU.
npu_rgwy=10.10.2.2 and npu_lgwy=10.10.1.1:
These IPs represent the remote gateway (rgwy) and local gateway (lgwy), confirming that the tunnel is successfully offloaded.
npu_selid=1:
This value means the session selector for the NPU offloaded SA is active.
Since both inbound and outbound SAs are offloaded, the administrator can conclude that the FortiGate NPU is handling IPsec encryption and decryption efficiently, reducing CPU load and improving VPN performance.

NEW 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: 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 28
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.

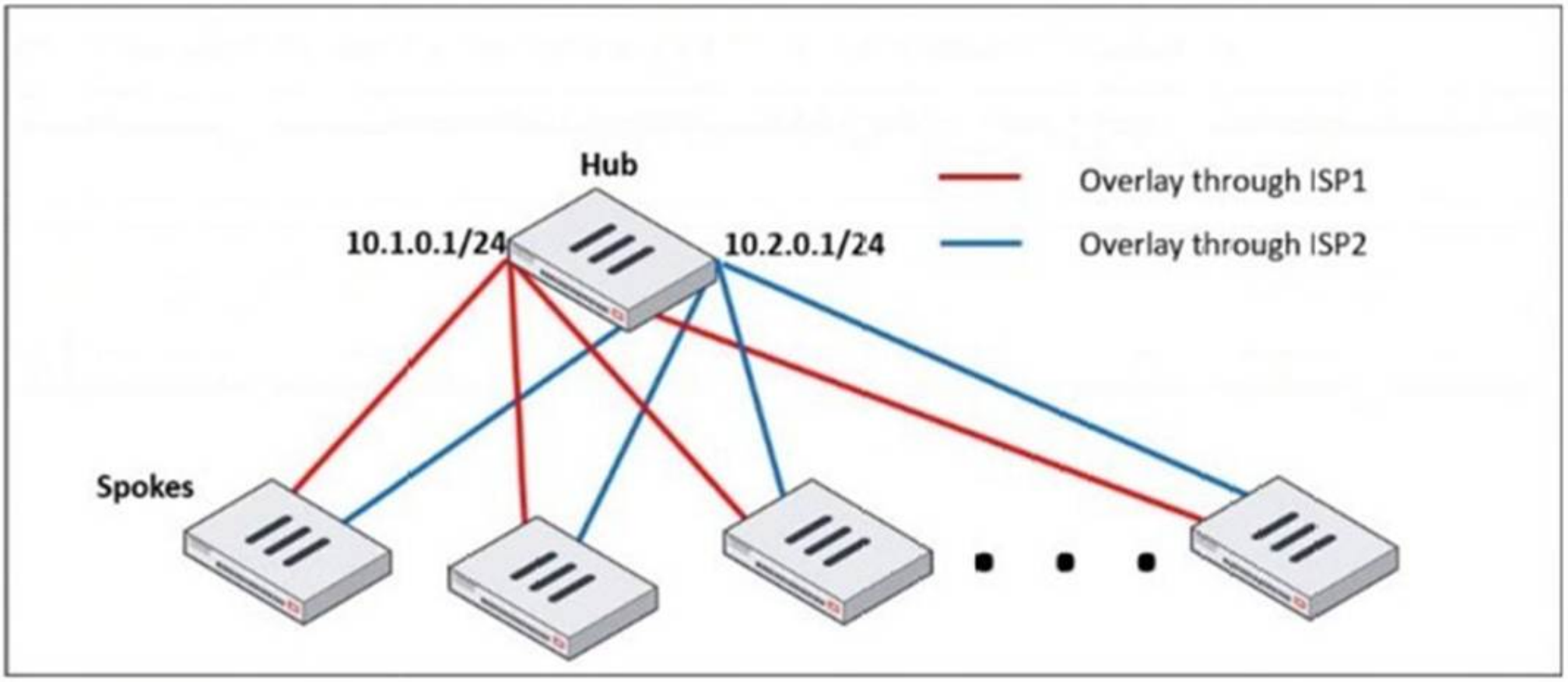
NEW QUESTION 31
A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on 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 35
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 38
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 42
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 43
.....

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