Fortinet

Exam Questions FCSS_EFW_AD-7.4

FCSS - Enterprise Firewall 7.4 Administrator

NEW QUESTION 1
An administrator is setting up an ADVPN configuration and wants to ensure that peer IDs are not exposed during VPN establishment.
Which protocol can the administrator use to enhance security?

A. Use IKEv2, which encrypts peer IDs and prevents exposure.
B. Opt for SSL VPN web mode because it does not use peer IDs at all.
C. Choose IKEv1 aggressive mode because it simplifies peer identification.
D. Stick with IKEv1 main mode because it offers better performance.

Answer: A

Explanation:
InADVPN (Auto-Discovery VPN) configurations, security concerns includeprotecting peer IDsduring VPN establishment. Peer IDs are exchanged in theIKE (Internet Key Exchange) negotiation phase, and their exposure could lead toprivacy risks or targeted attacks.
IKEv2 encrypts peer IDs, making itmore securecompared to IKEv1, where peer IDs can beexposed in plaintextin aggressive mode.
IKEv2 also provides better performance and flexibilitywhile supporting dynamic tunnel establishment in ADVPN.

NEW QUESTION 2
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.

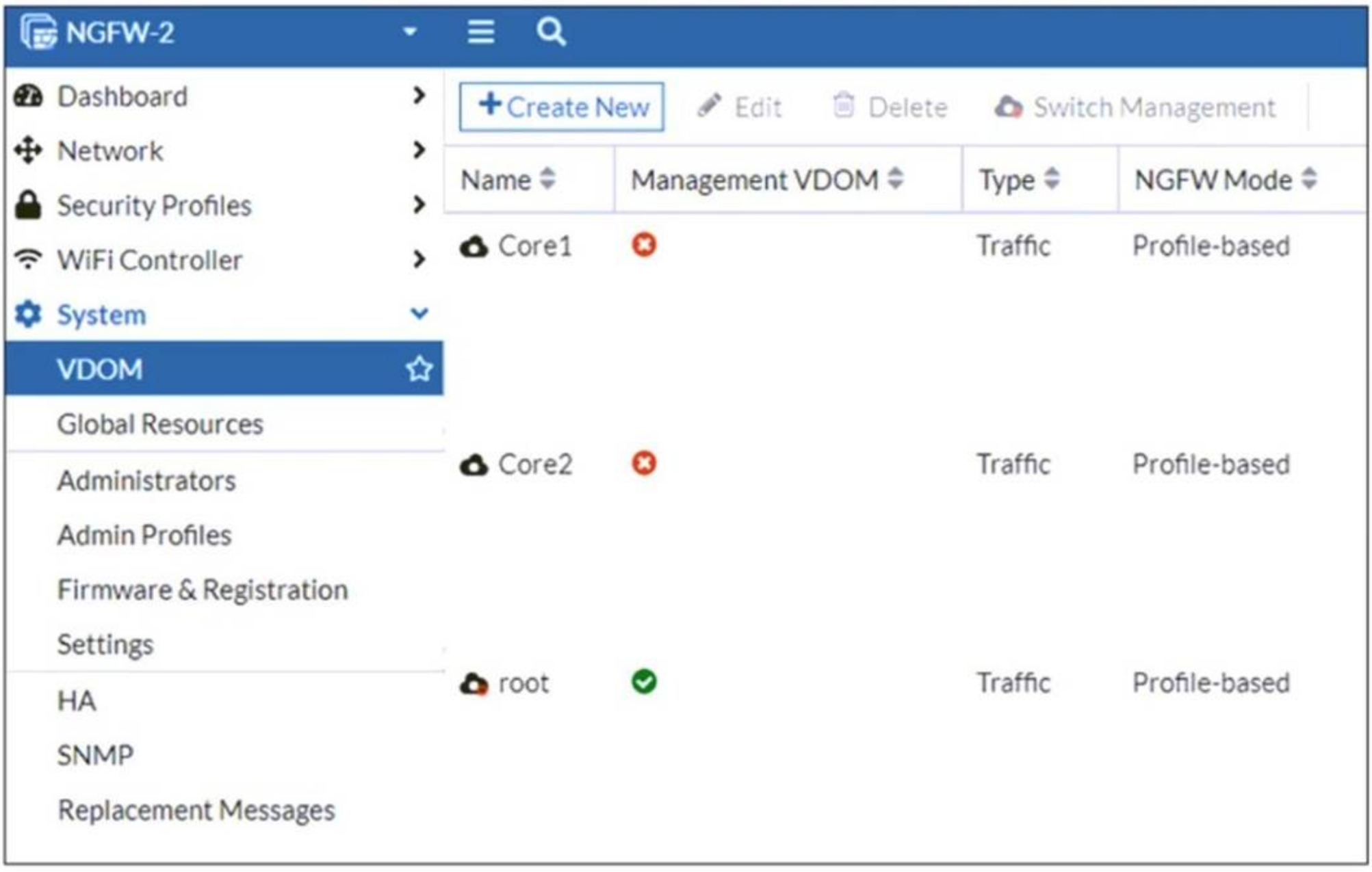
NEW QUESTION 3
An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection.
The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best 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 4
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 5
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?

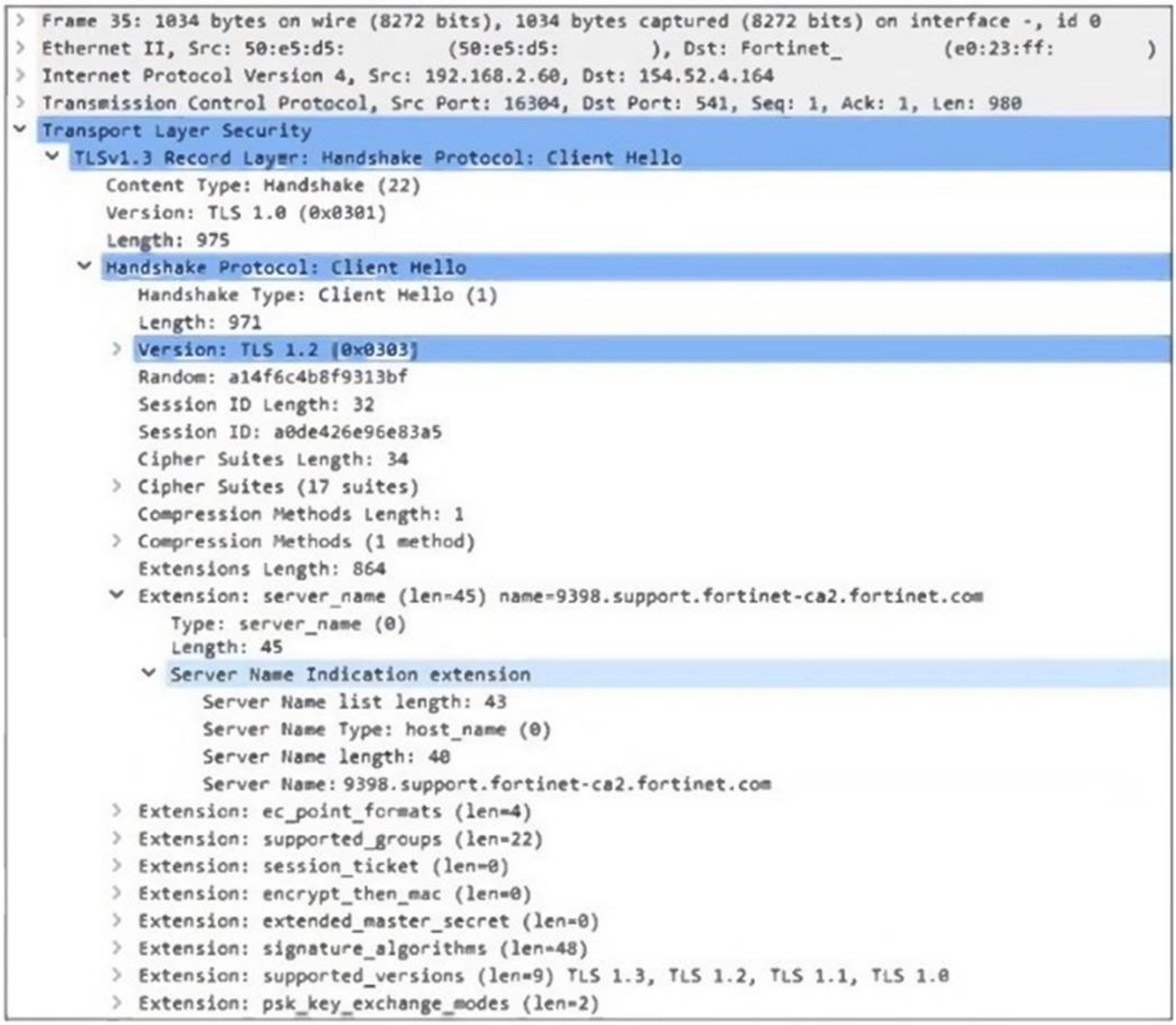
A. Use the IPS profile extension to select an operating system, protocol, and application for all the network internal services and users to prevent false positives.
B. Enable Scan Outgoing Connections to avoid clickingsuspicious links or attachments that can deliver botnet malware and create false positives.
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 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.

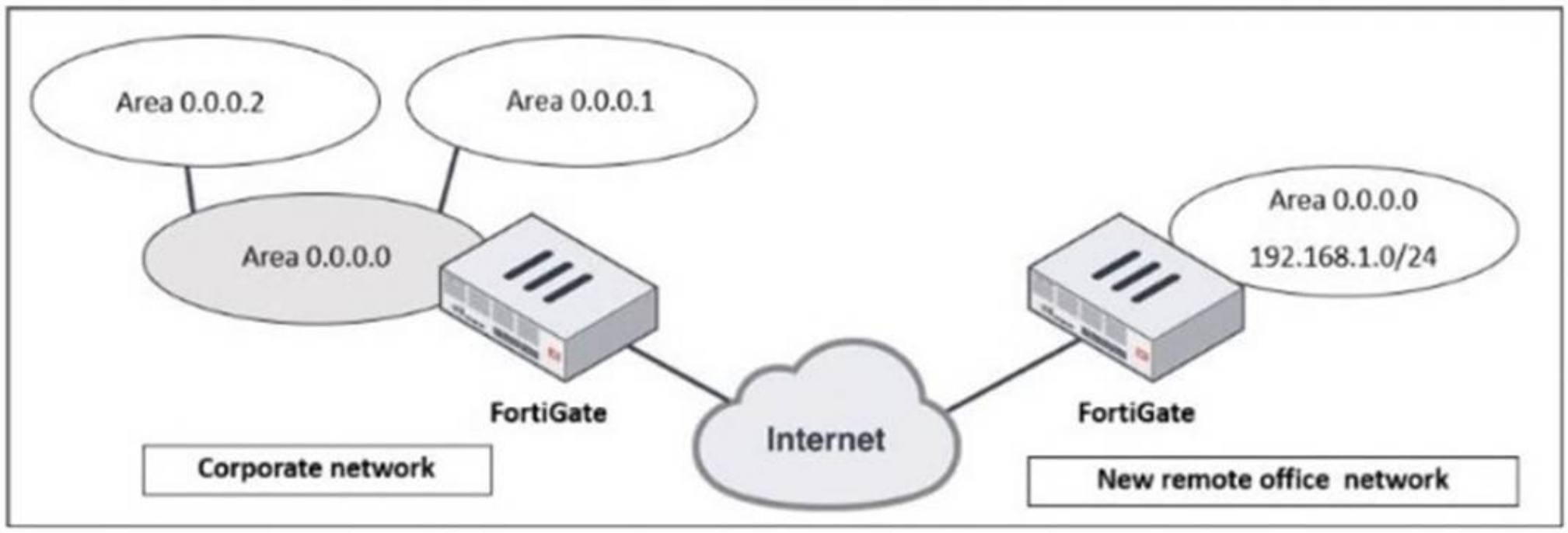
NEW QUESTION 7
Which two statements about IKEv2 are true if an administrator decides to implement IKEv2 in the VPN topology? (Choose two.)

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 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 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
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 10
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 11
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
```

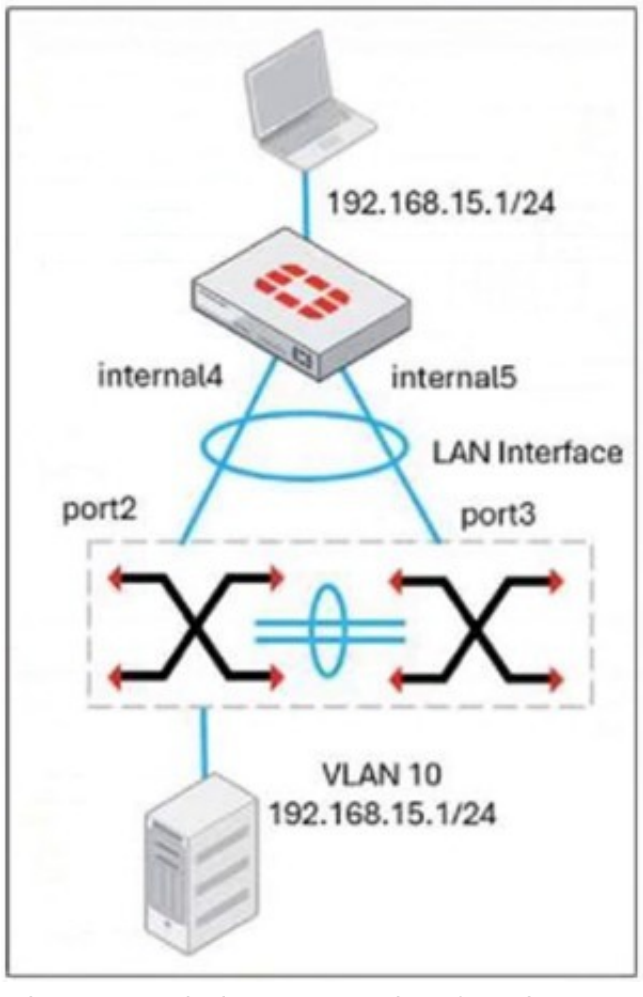
An administrator is extensively using IPsec on FortiGate. Many tunnels show information similar to the output shown in the exhibit.
What can the administrator conclude?

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 14
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

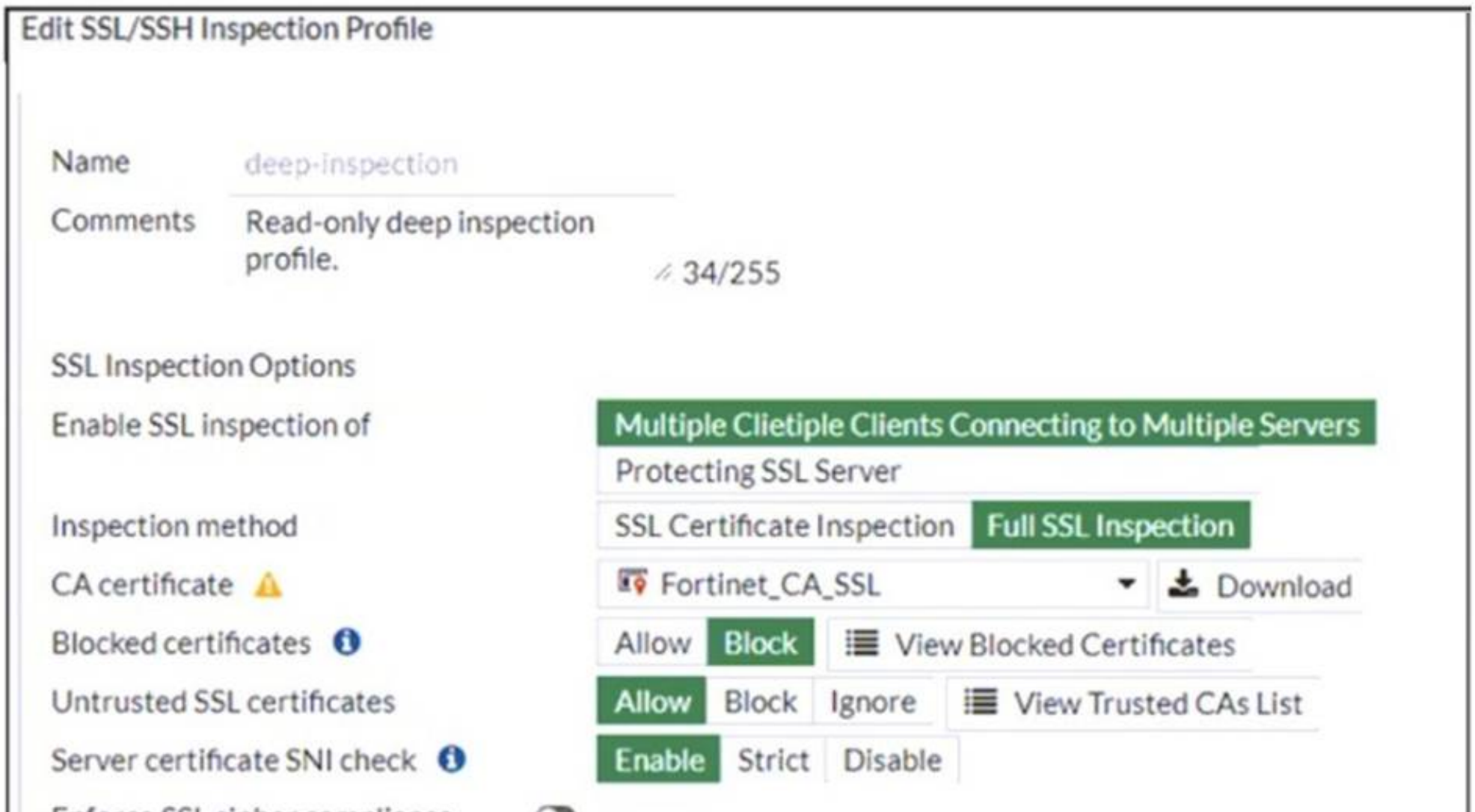
Explanation:
The diagram shows a FortiGate connected to two FortiSwitches, which suggests the use of FortiLink, Fortinet's protocol for managing switches directly from a FortiGate. Since multiple connections are being used, the LAN interface must be set to802.3ad (LAG)mode to aggregate the links for 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 19
Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

Firewall policy on FortiGate

```
DCFW # sh firewall policy 3
config firewall policy
edit 3
set name "To Linux Servers"
set uuid bf77d59e-5513-51ef-147d-e35066c267e9
set srcintf "port1"
set dstintf "port3"
set action accept
set srcaddr "all"
set dstaddr "10.1.4."
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set ssl-ssh-profile "deep-inspection”
set ips-sensor "IPS Monitor"
set logtraffic all
next
end
```

SSL/SSH inspection profile



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

A. The administrator must set the policy to inspection mode to analyze the HTTPS packets as expected.
B. The administrator must enable HTTPS in the protocol port mapping of the deep- inspection SSL/SSH inspection profile.
C. The administrator must enable SSL inspection of the SSL server and upload the certificate of the Linux server website to the SSL/SSH inspection profile.
D. The administrator must enable cipher suites in the SSL/SSH inspection profile to decrypt the message.

Answer: C

Explanation:
The FortiGateSSL/SSH inspection profileis configured forFull SSL Inspection, which is necessary to analyze encrypted HTTPS traffic. However, the firewallpolicy is protecting an SSL server (the Linux server hosting the website), and currently, the SSL/SSH profileonly applies to client-side SSL inspection.
To detect HTTPS-based attacks targeting the Linux server:
FortiGate must act as an SSL intermediaryto inspect encrypted traffic destined for the web server.
The administratormust upload the SSL certificate of the Linux web serverto FortiGate so that theserver-side SSL inspectioncan decrypt incoming HTTPS traffic before analyzing it.

NEW QUESTION 21
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 22
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 24
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 28
.....

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