Fortinet

Exam Questions FCSS_EFW_AD-7.4

FCSS - Enterprise Firewall 7.4 Administrator

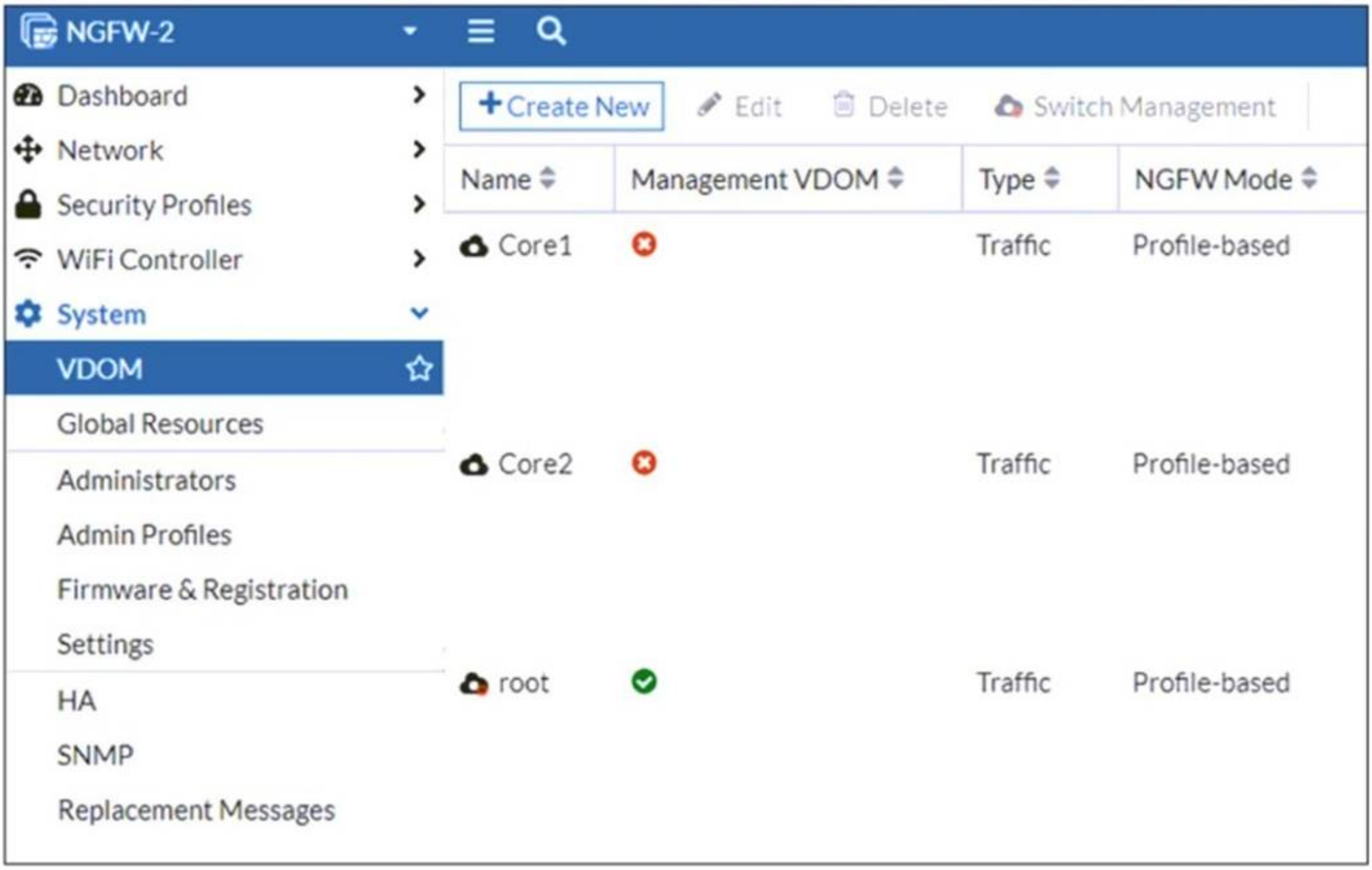
NEW QUESTION 1
An administrator is setting up an ADVPN configuration and wants to ensure that peer IDs are not exposed during VPN establishment.
Which protocol can the administrator use to enhance security?

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 the VDOM section of a FortiGate device.



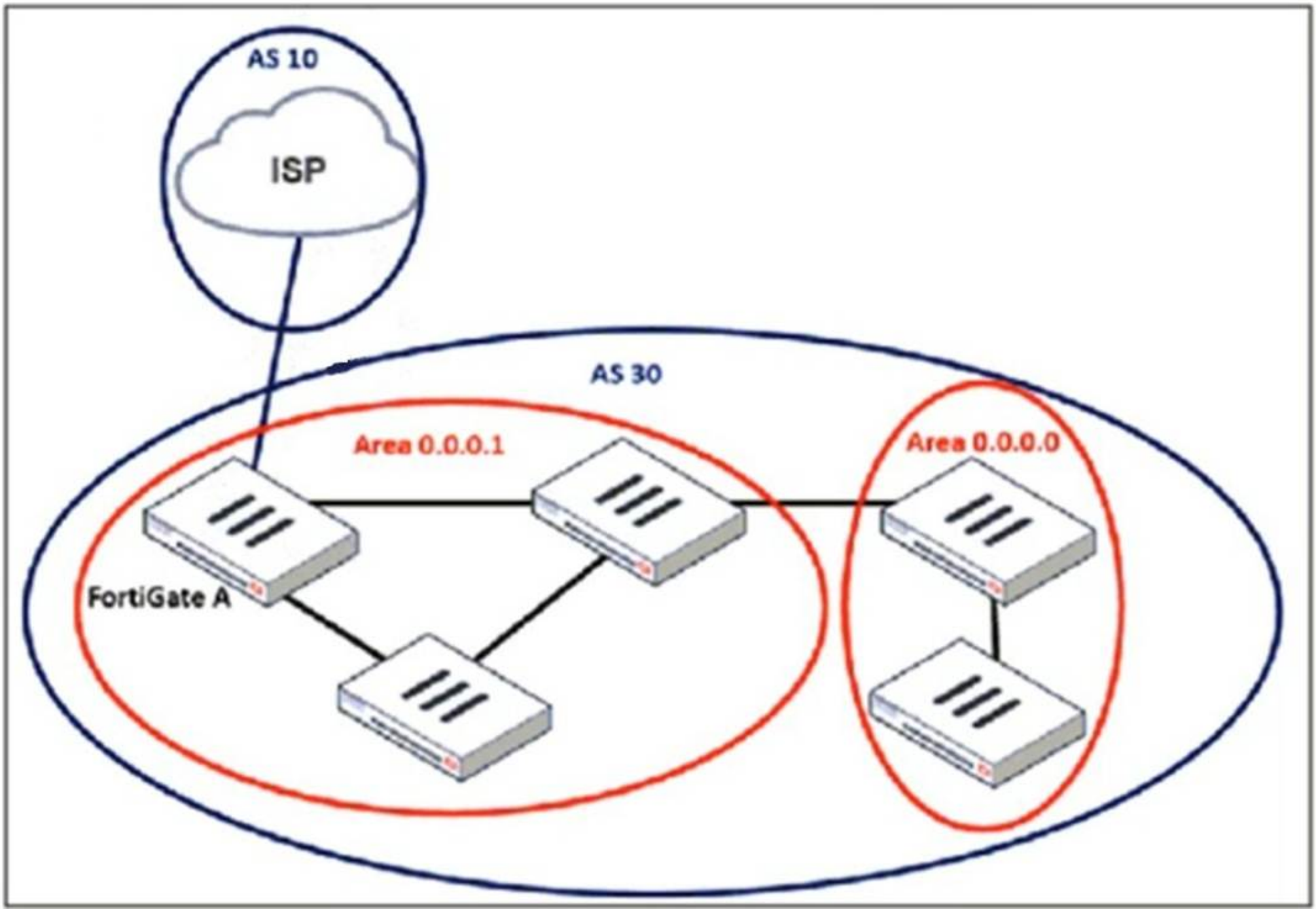
An administrator discovers that webfilter stopped working in Core1 and Core2 after a maintenance window.
Which two reasons could explain why webfilter stopped working? (Choose two.)

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 3
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.)

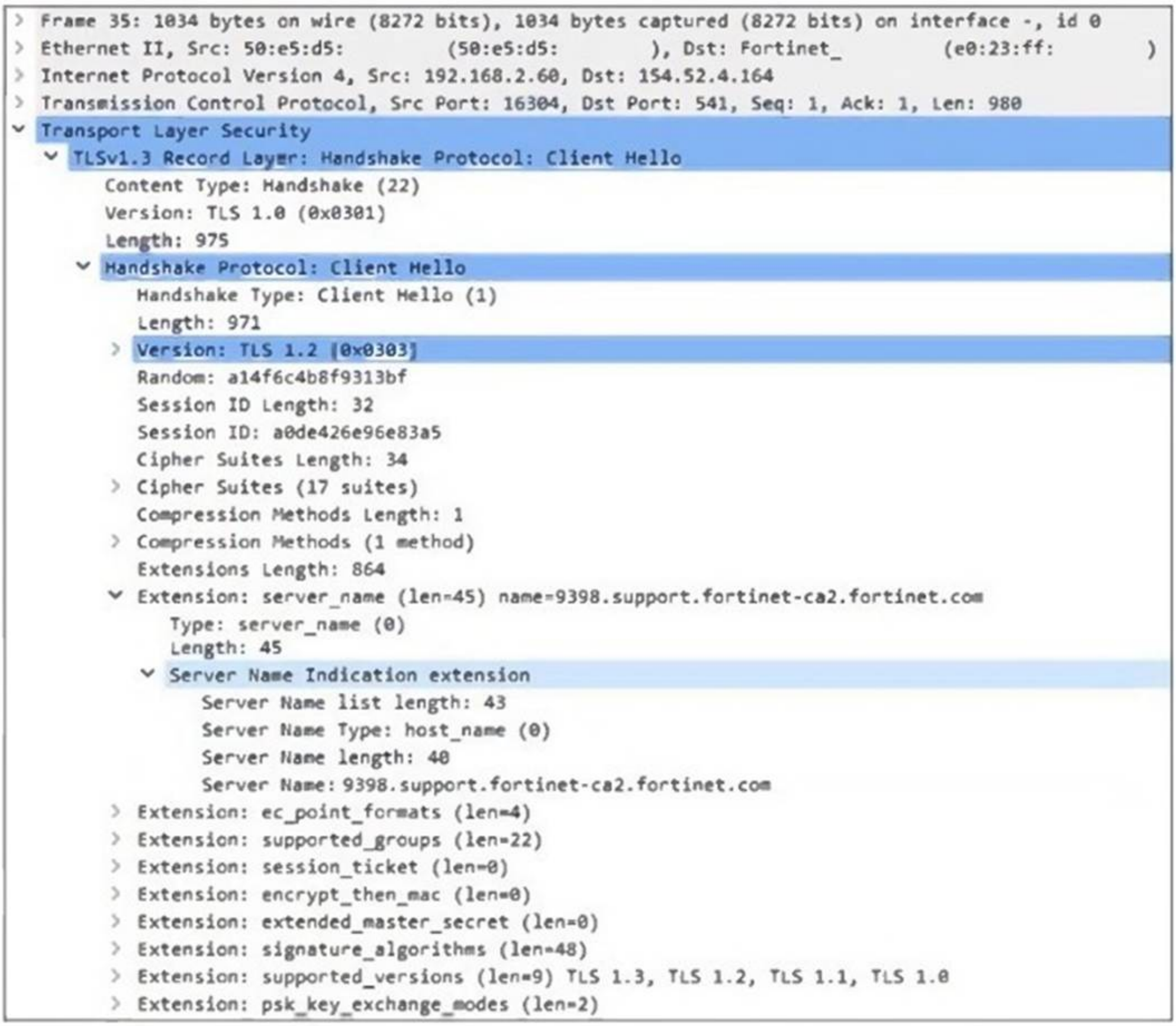
A. ebgp-enforce-multihop
B. update-source
C. ibgp-enforce-multihop
D. recursive-next-hop

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 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
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 6
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 7
A company's users on an IPsec VPN between FortiGate A and B have experienced intermittent issues since implementing VXLAN. The administrator suspects that packets exceeding the 1500-byte default MTU are causing the problems.
In which situation would adjusting the interface??s maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

A. Adjust the MTU on interfaces only if FortiGate has the FortiGuard enterprise bundle, which allows MTU modification.
B. Adjust the MTU on interfaces in all FortiGate devices that support the latest family of Fortinet SPUs: NP7, CP9 and SP5.
C. Adjust the MTU on interfaces in controlled environments where all devices along the path allow MTU interface changes.
D. Adjust the MTU on interfaces only in wired connections like PPPoE, optic fiber, and ethernet cable.

Answer: C

Explanation:
When usingIPsec VPNsandVXLAN, additional headers are added to packets, which can exceed thedefault 1500-byte MTU. This can lead tofragmentation issues, dropped packets, or degraded performance.
To resolve this, theMTU (Maximum Transmission Unit)should be adjustedonly if all devices in the network path support it. Otherwise, some devices may still drop or fragment packets, leading to continued issues.
Why adjusting MTU helps:
VXLAN adds a 50-byte overheadto packets.
IPsec adds additional encapsulation(ESP, GRE, etc.), increasing the packet size.
If packets exceed the MTU, they may befragmented or dropped, causing intermittent connectivity issues.
Lowering the MTU on interfaces ensurespackets stay within the supported size limit across all network devices.

NEW QUESTION 8
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 ASBR
```

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

A. The FortiGate device can inject external routing information.
B. The FortiGate device is in the area 0.0.0.5.
C. The FortiGate device does not support OSPF ECMP.
D. The FortiGate device is a backup designated router.

Answer: A

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

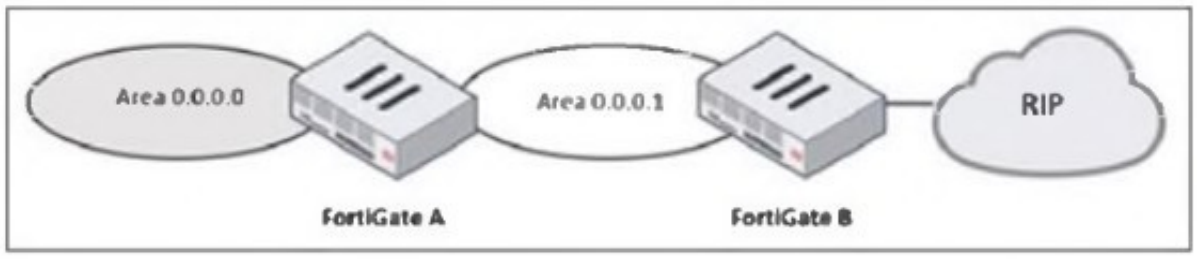
NEW QUESTION 9
Why does the ISDB block layers 3 and 4 of the OSI model when applying content filtering? (Choose two.)

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 10
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 10
During the maintenance window, an administrator must sniff all the traffic going through a specific firewall policy, which is handled by NP6 interfaces. The output of the sniffer trace provides just a few packets.
Why is the output of sniffer trace limited?

A. The traffic corresponding to the firewall policy is encrypted.
B. auto-asic-off load is set to enable in the firewall policy,
C. inspection-mode is set to proxy in the firewall policy.
D. The option npudbg is not added in the diagnose sniff packet command.

Answer: B

Explanation:
FortiGate devices withNP6 (Network Processor 6) accelerationoffload traffic directly to hardware, bypassing the CPU for improved performance. Whenauto-asic-offloadis enabled in a firewall policy, most of the trafficdoes not reach the CPU, which means it won't be captured by the standard sniffer trace command.
Since NP6-accelerated traffic is handled entirely in hardware, onlya small portion of initial packets(such as session setup packets or exceptions) might be seen in the sniffer output. To capture all packets, the administrator must disable hardware offloading using:
config firewall policy edit <policy_ID>
set auto-asic-offload disable end
Disabling ASIC offload forces traffic to be processed by the CPU, allowing the sniffer tool to capture all packets.

NEW QUESTION 12
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The FCSS_EFW_AD-7.4 Practice Test Here