Fortinet

Exam Questions FCSS_EFW_AD-7.6

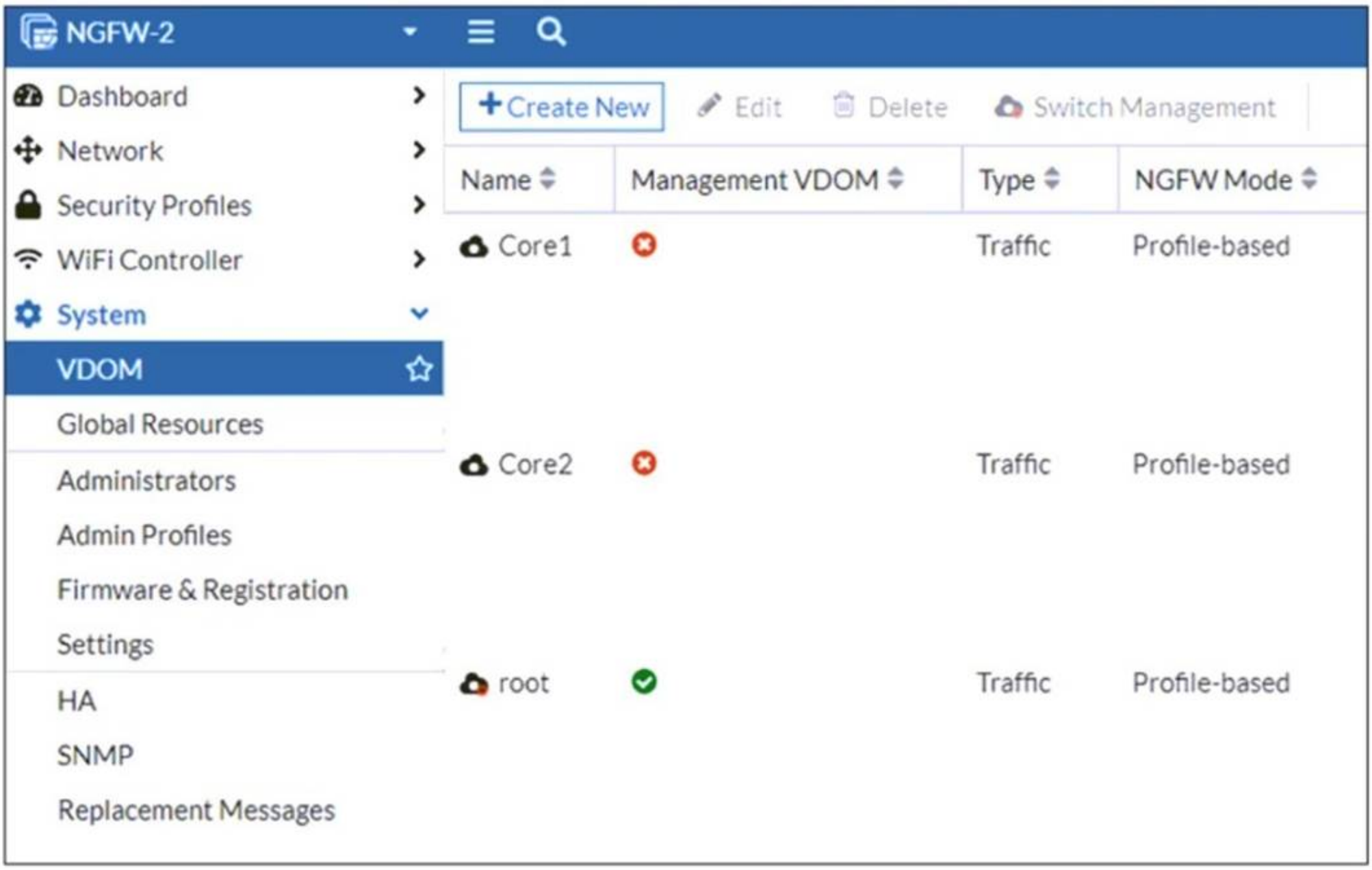
FCSS - Enterprise Firewall 7.6 Administrator

NEW QUESTION 1
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

NEW QUESTION 2
Refer to the exhibit, which shows the VDOM section of a FortiGate device.

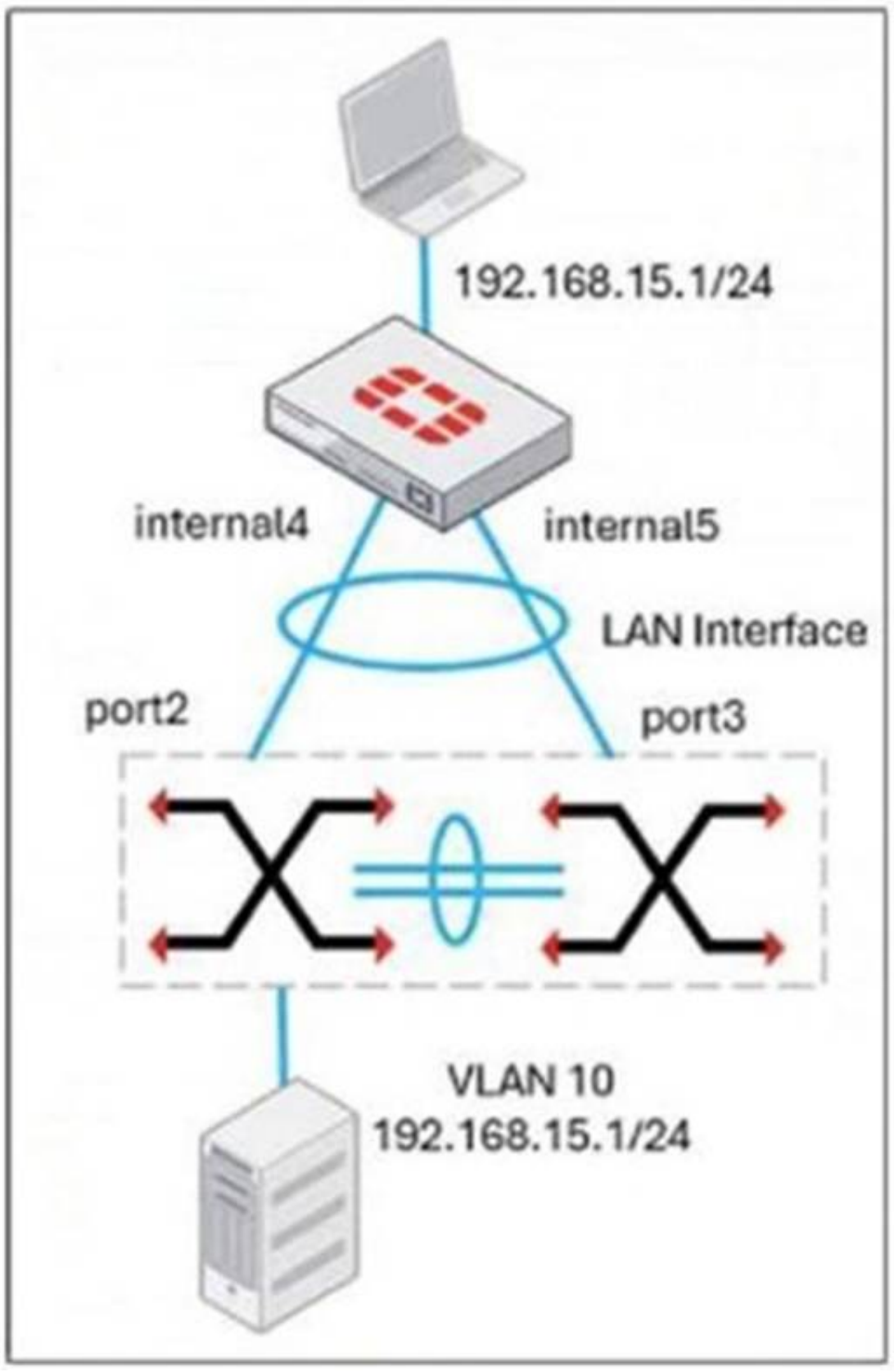


An administrator discovers that webfilter stopped working in Core1 and Core2 after a maintenance window.
Which two reasons could explain why webfilter stopped working? (Choose two.)

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

NEW QUESTION 3
Refer to the exhibit, which shows a LAN interface connected from FortiGate to two FortiSwitch devices.

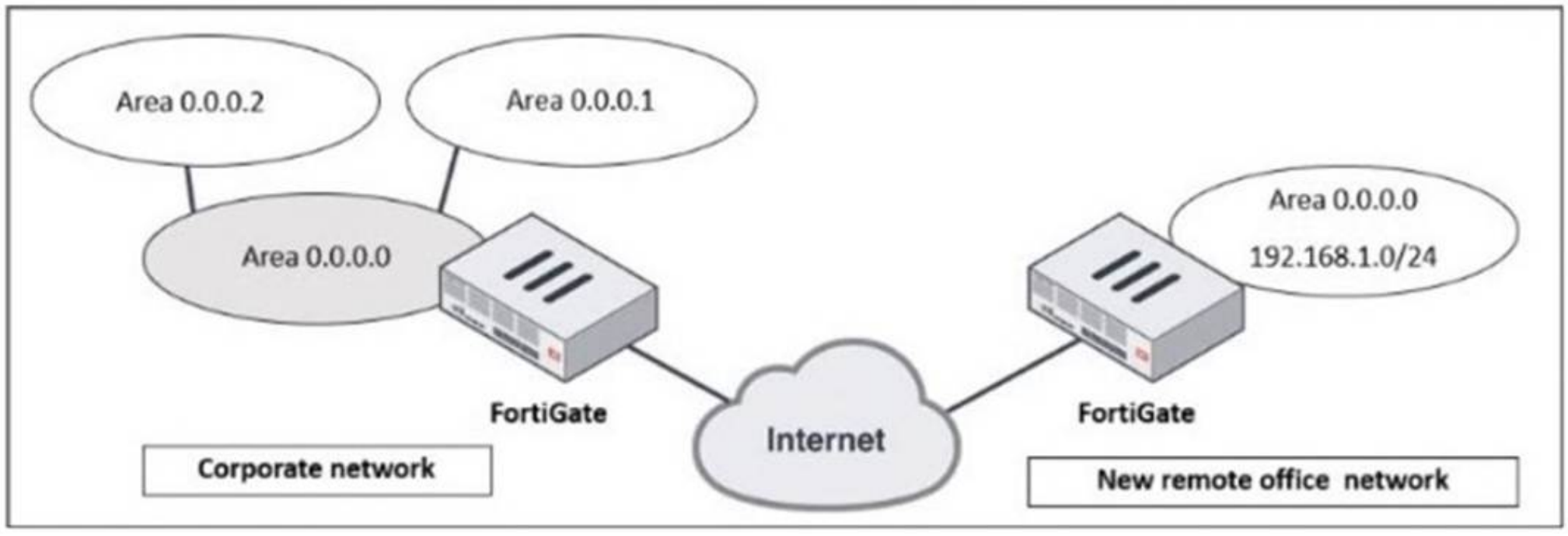


What two conclusions can you draw from the corresponding LAN interface? (Choose two.)

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

NEW QUESTION 4
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

NEW QUESTION 5
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

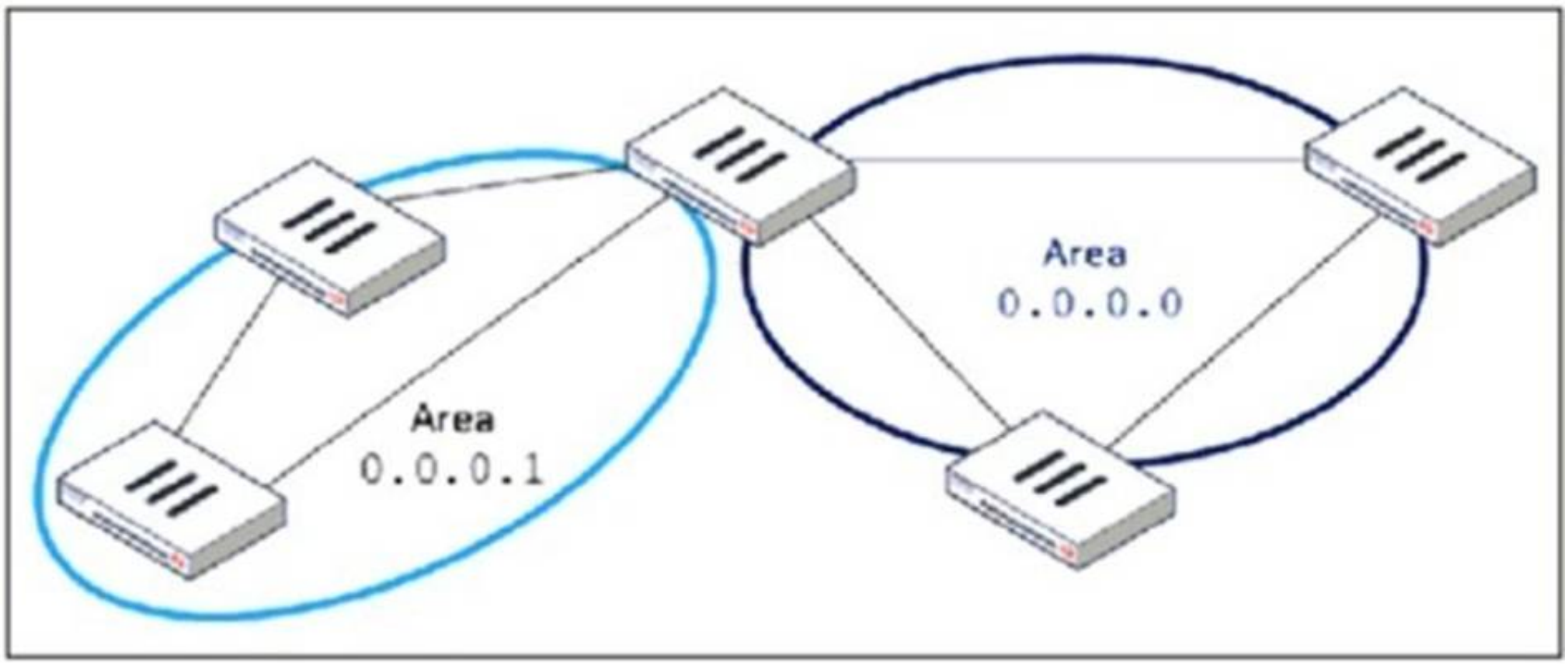
Answer: AB

NEW QUESTION 6
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

NEW QUESTION 7
Refer to the exhibit, which shows an OSPF network.

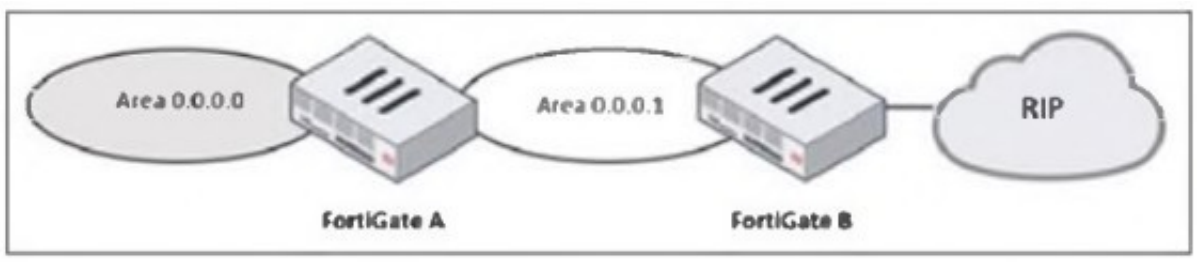


Which configuration must the administrator apply to optimize the OSPF database?

A. Set a route map in the AS boundary FortiGate.
B. Set the area 0.0.0.1 to the type STUB in the area border FortiGate.
C. Set an access list in the AS boundary FortiGate.
D. Set the area 0.0.0.1 to the type NSSA in the area border FortiGate.

Answer: B

NEW QUESTION 8
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.

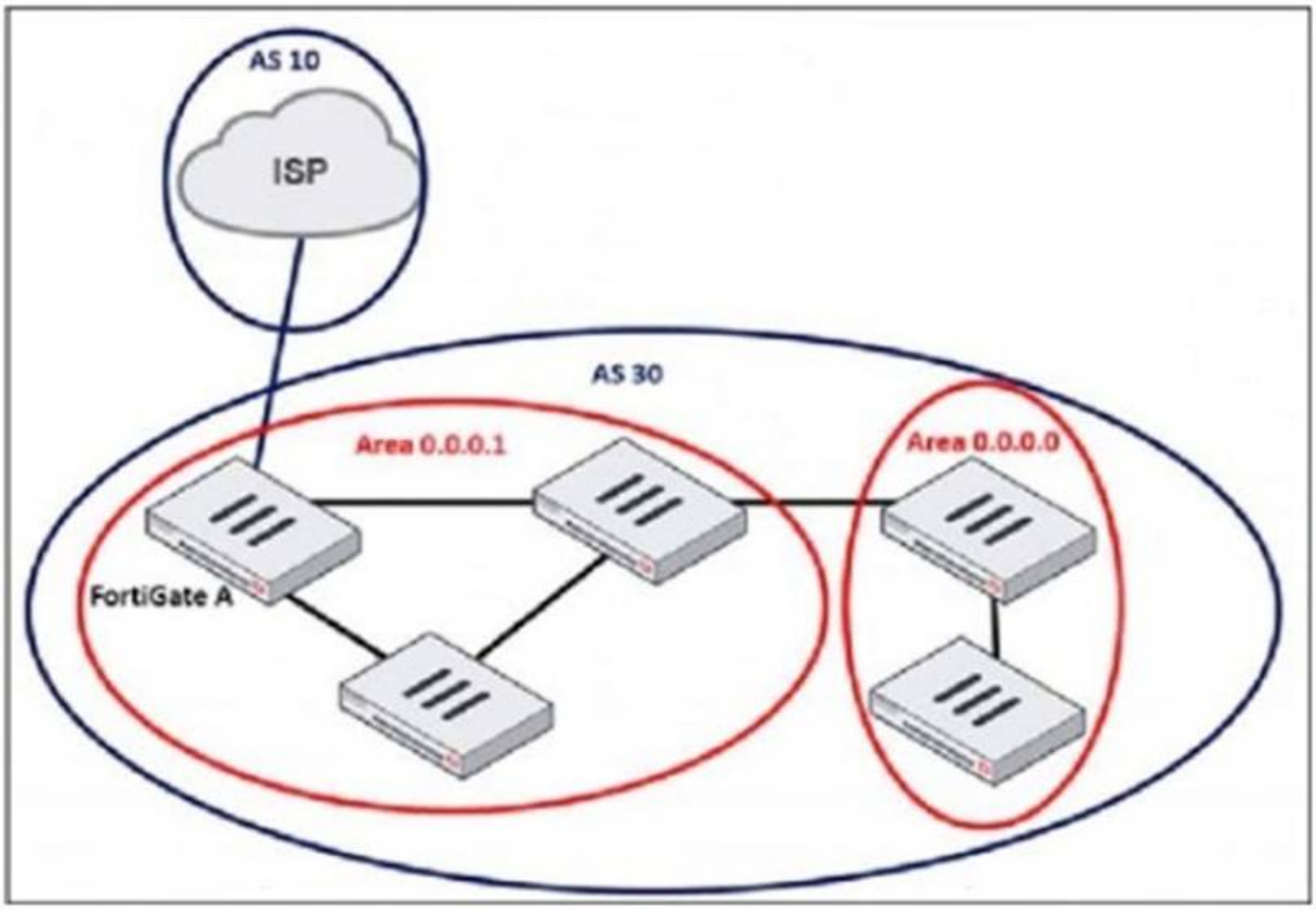
Answer: A

NEW QUESTION 9
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

NEW QUESTION 10
Refer to the exhibit, which shows an enterprise network connected to an internet service provider.



The administrator must configure the BGP section of FortiGate A to give internet access to the enterprise network.
Which command must the administrator use to establish a connection with the internet service provider?

A. config neighbor
B. config redistribute bgp
C. config router route-map
D. config redistribute ospf

Answer: A

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

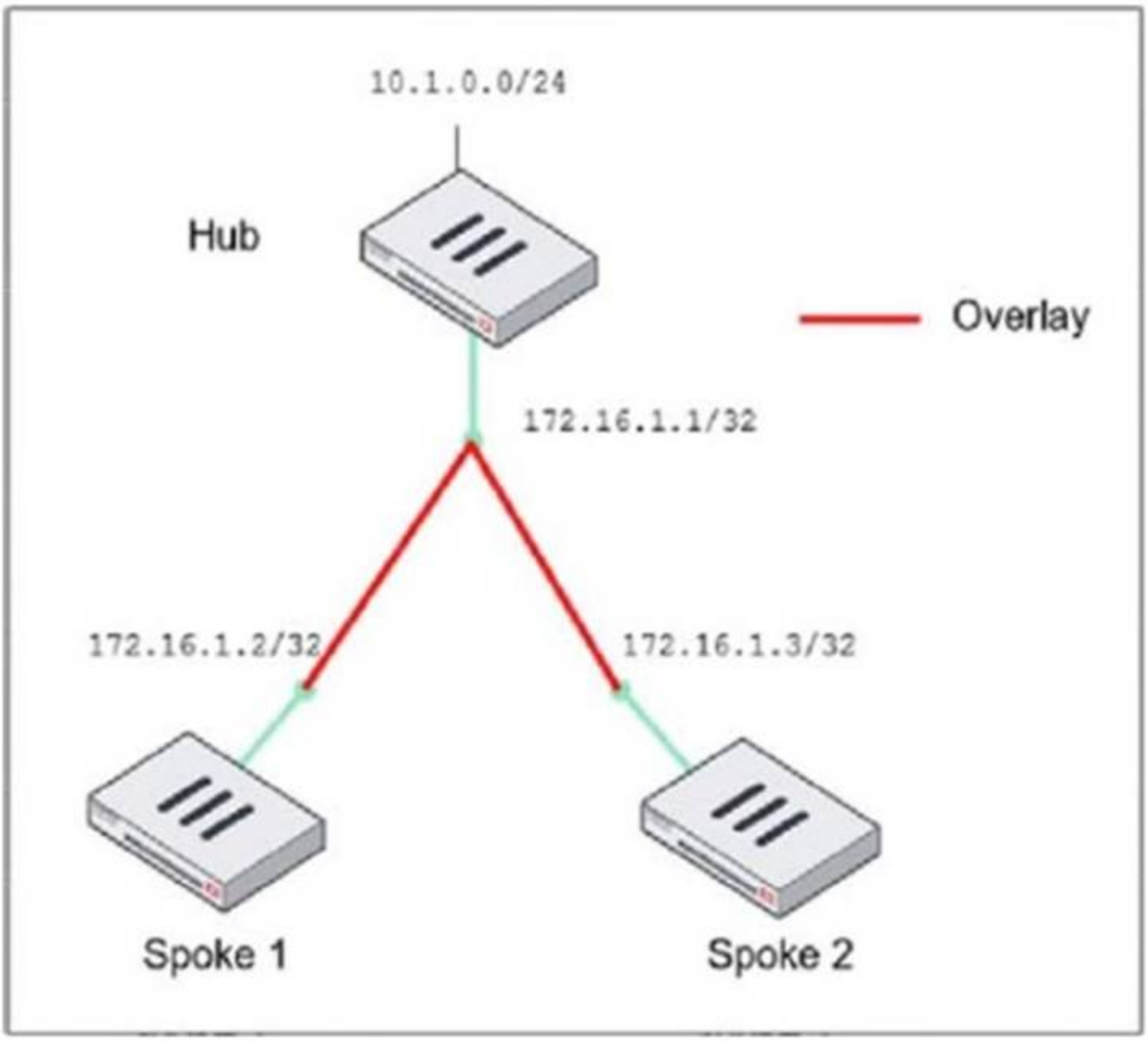
NEW QUESTION 12
An administrator must standardize the deployment of FortiGate devices across branches with consistent interface roles and policy packages using FortiManager.
What is the recommended best practice for interface assignment in this scenario?

A. Enable metadata variables to use dynamic configurations in the standard interfaces of FortiManager.
B. Use the Install On feature in the policy package to automatically assign different interfaces based on the branch.
C. Create interfaces using device database scripts to use them on the same policy package of FortiGate devices.
D. Create normalized interface types per-platform to automatically recognize device layer interfaces based on the FortiGate model and interface name.

Answer: A

NEW QUESTION 15
Refer to the exhibit, which shows the ADVPN network topology and partial BGP configuration.

ADVPN network topology



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

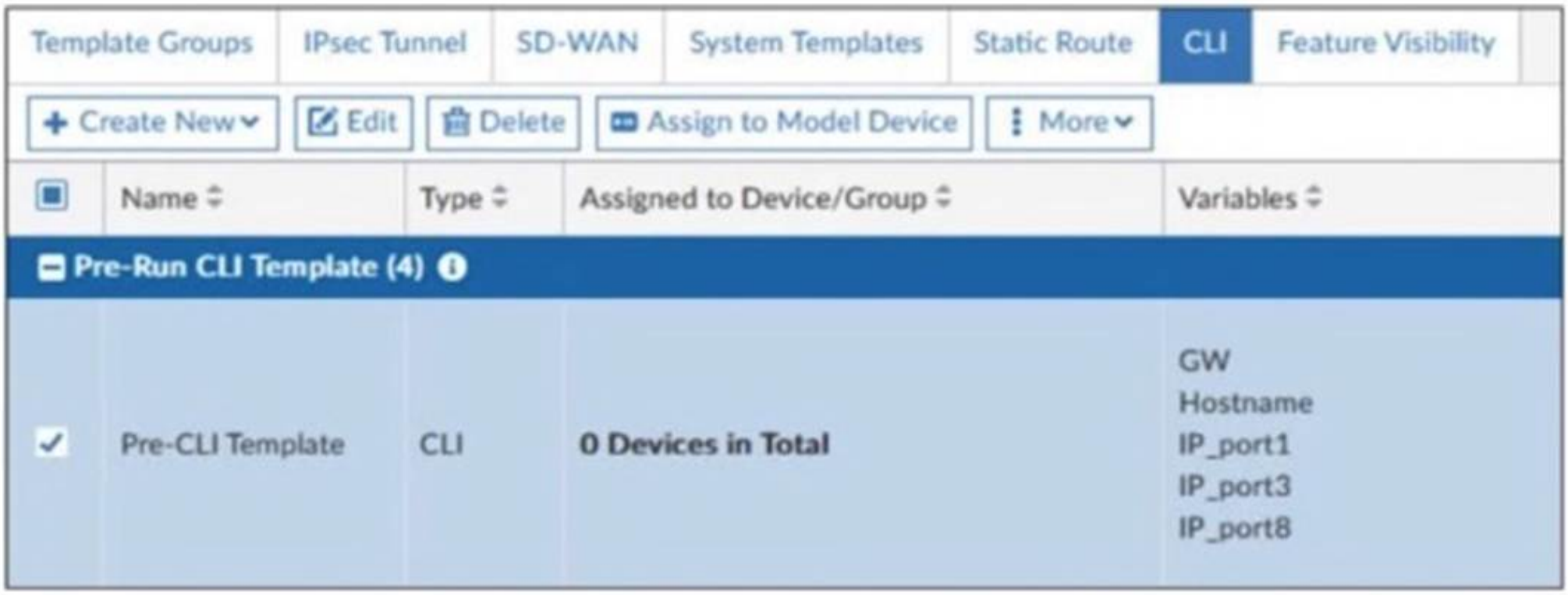
Answer: BD

NEW QUESTION 17
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

NEW QUESTION 19
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

NEW QUESTION 22
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

NEW QUESTION 26
A company's guest internet policy, operating in proxy mode, blocks access to Artificial Intelligence Technology sites using FortiGuard. However, a guest user accessed a page in this category using port 8443.
Which configuration changes are required for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443 when full SSL inspection is active in the guest policy?

A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.
B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.
C. To analyze nonstandard ports in web filter profiles, use TLSv1.3 in the SSL/SSH Inspection Profile.
D. Administrators can block traffic on nonstandard ports by enabling the SNI check in the SSL/SSH Inspection Profile.

Answer: B

NEW QUESTION 29
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

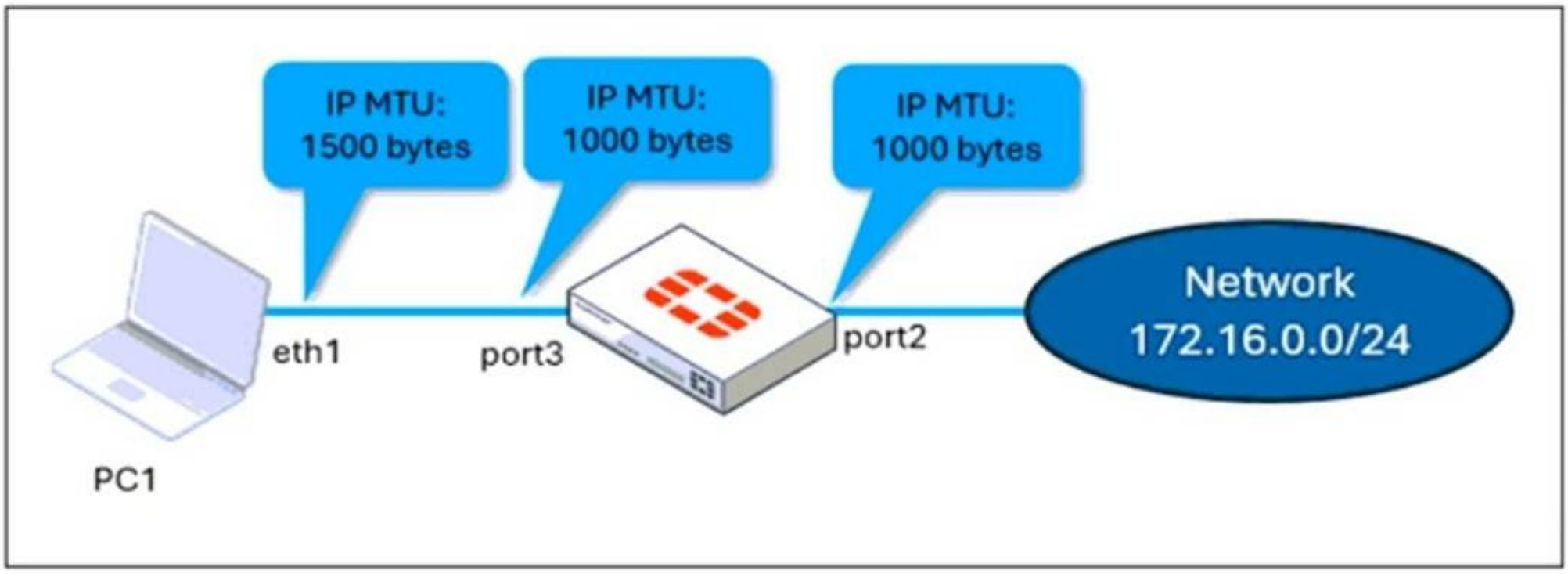
NEW QUESTION 31
An administrator is designing an ADVPN network for a large enterprise with spokes that have varying numbers of internet links. They want to avoid a high number of routes and peer connections at the hub.
Which method should be used to simplify routing and peer management?

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

NEW QUESTION 34
Refer to the exhibits.

Network topology



port 3 configuration on FortiGate

```
config system interface
 edit "port3"
  set vdom "root"
  set ip 10.0.0.1 255.255.255.0
  set allowaccess ping https ssh snmp http fgfm ftm
  set type physical
  set alias "LAN"
  set snmp-index 3
  set mtu-override enable
  set mtu 1000
 next
end
```

ping output

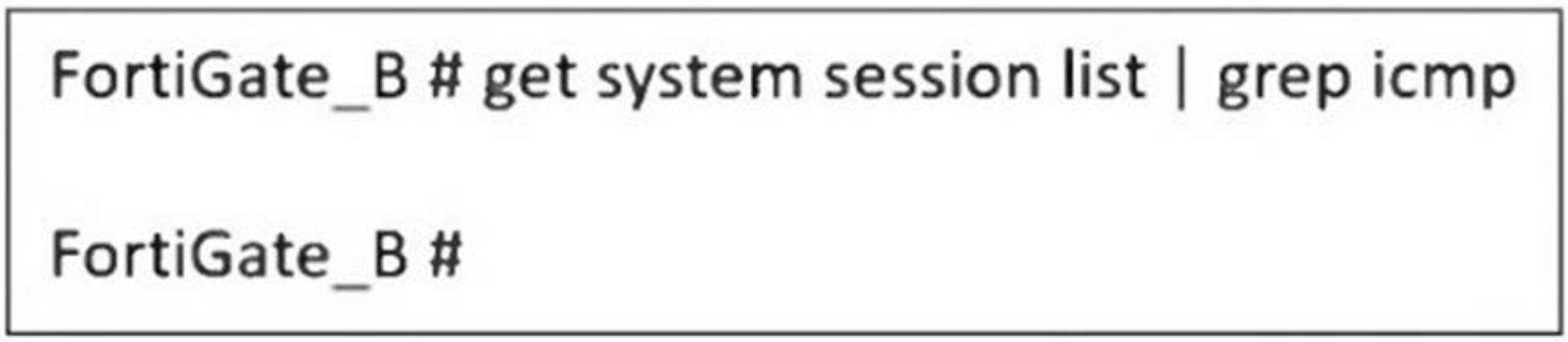
```
C:\Users\fortinet>ping 172.16.0.254 -f -l 1400

Pinging 172.16.0.254 with 1400 bytes of data:
Reply from 10.0.0.1: Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 172.16.0.254:
Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
```

The configuration of a user's Windows PC, which has a default MTU of 1500 bytes, along with FortiGate interfaces set to an MTU of 1000 bytes, and the results of PC1 pinging server 172.16.0.254 are shown.
Why is the user in Windows PC1 unable to ping server 172.16.0.254 and is seeing the message: Packet needs to be fragmented but DF set?

A. Option ip.flags.mf must be set to enable on FortiGat
B. The user has to adjust the ping MTU to 1000 to succeed.
C. Fragmented packets must be encrypte
D. To connect any application successfully, the user must install the Fortinet_CA certificate in the Microsoft Management Console.
E. FortiGate honors the do not fragment bit and the packets are droppe
F. The user has to adjust the ping MTU to 972 to succeed.
G. The user must trigger different traffic because path MTU discovery techniques do not recognize ICMP payloads.

Answer: C

NEW QUESTION 37
Refer to the exhibit, which shows a command output.

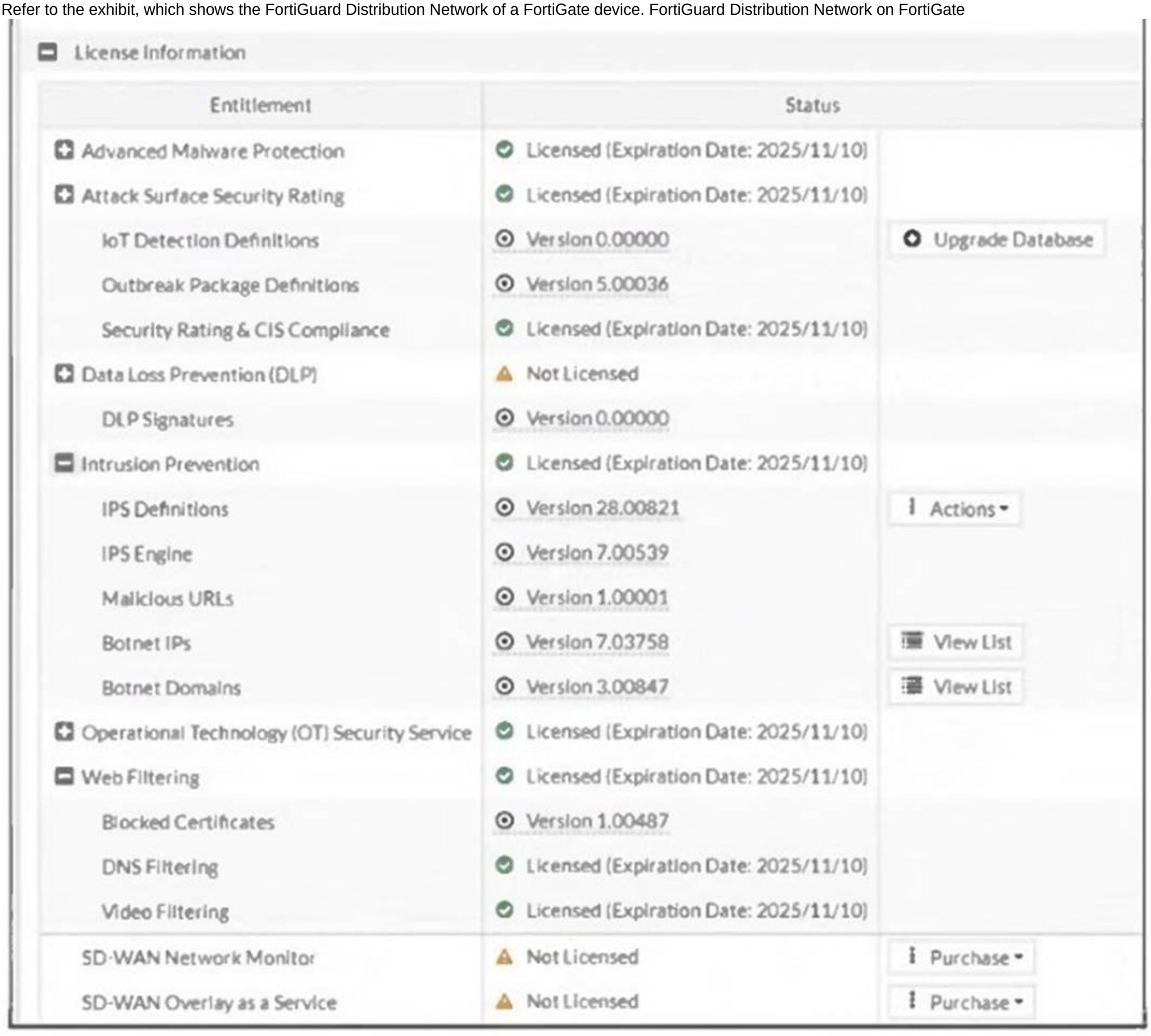


FortiGate_A and FortiGate_B are members of an FGSP cluster in an enterprise network. While testing the cluster using the ping command, the administrator monitors packet loss
and found that the session output on FortiGate_B is as shown in the exhibit.
What could be the cause of this output on FortiGate_B?

A. The session synchronization is encrypted.
B. session-pickup-connectionless is set to disable on FortiGate_B.
C. FortiGate_B is configured in passive mode.
D. FortiGate_A and FortiGate_B have the same standalone-group-id value.

Answer: B

NEW QUESTION 38
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

NEW QUESTION 40
What is the initial step performed by FortiGate when handling the first packets of a session?

A. Installation of the session key in the network processor (NP)
B. Data encryption and decryption
C. Security inspections such as ACL, HPE, and IP integrity header checking
D. Offloading the packets directly to the content processor (CP)

Answer: C

NEW QUESTION 42
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

NEW QUESTION 47
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

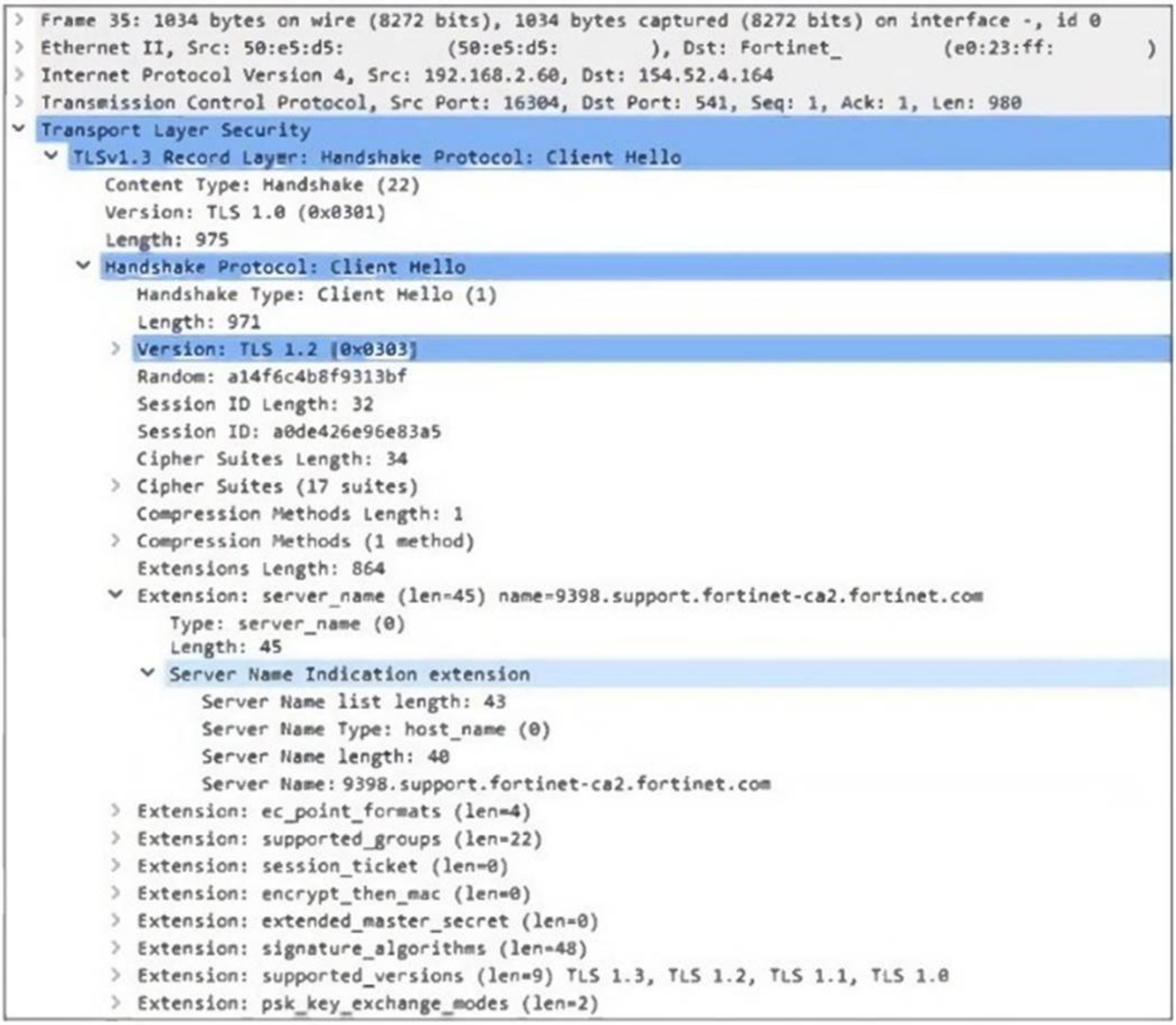
NEW QUESTION 51
An administrator applied a block-all IPS profile for client and server targets to secure the server, but the database team reported the application stopped working immediately after.
How can an administrator apply IPS in a way that ensures it does not disrupt existing applications in 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

NEW QUESTION 56
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 certificatefor 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

NEW QUESTION 61
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

NEW QUESTION 63
.....

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-7.6 Practice Exam Features:

* FCSS_EFW_AD-7.6 Questions and Answers Updated Frequently

* FCSS_EFW_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_EFW_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_EFW_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year