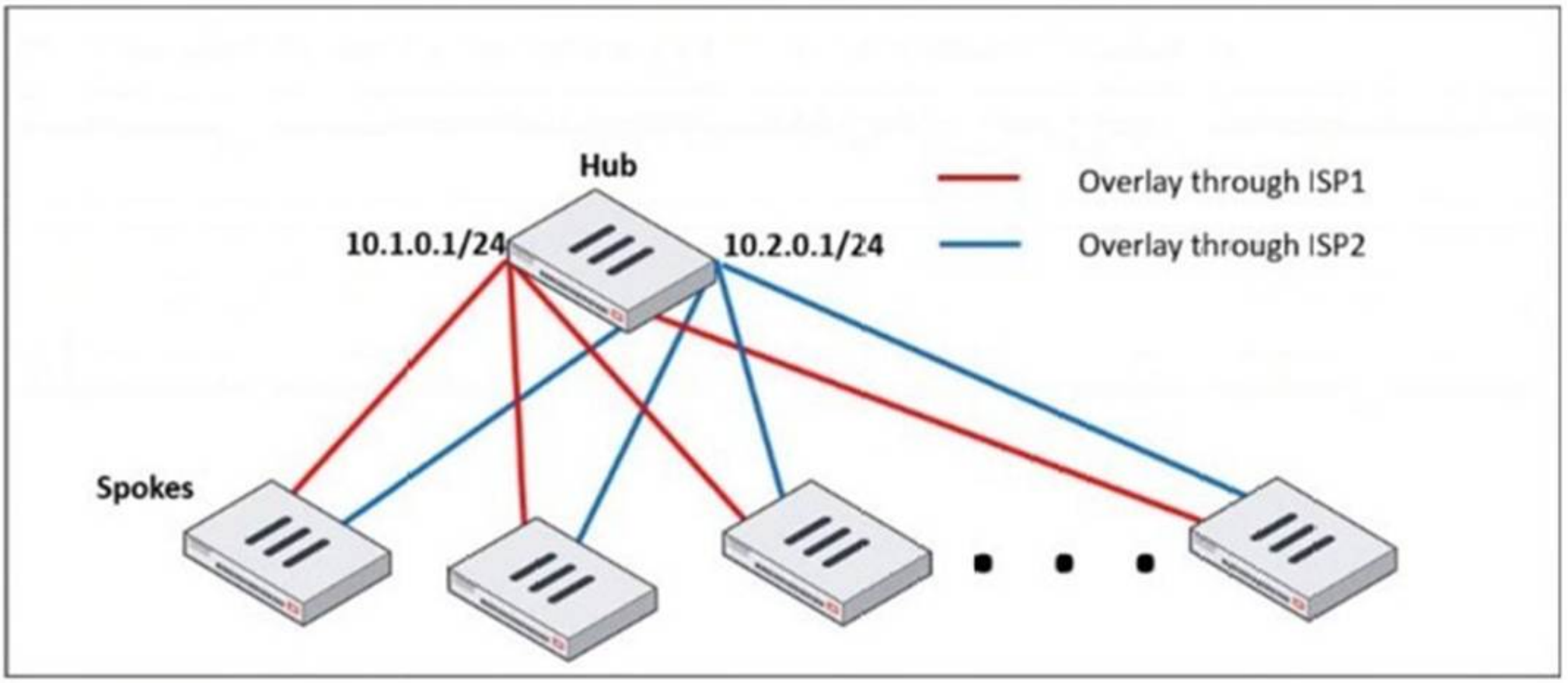
Fortinet

Exam Questions FCSS_EFW_AD-7.6

FCSS - Enterprise Firewall 7.6 Administrator

NEW QUESTION 1
Refer to the exhibit, which shows a hub and spokes deployment.

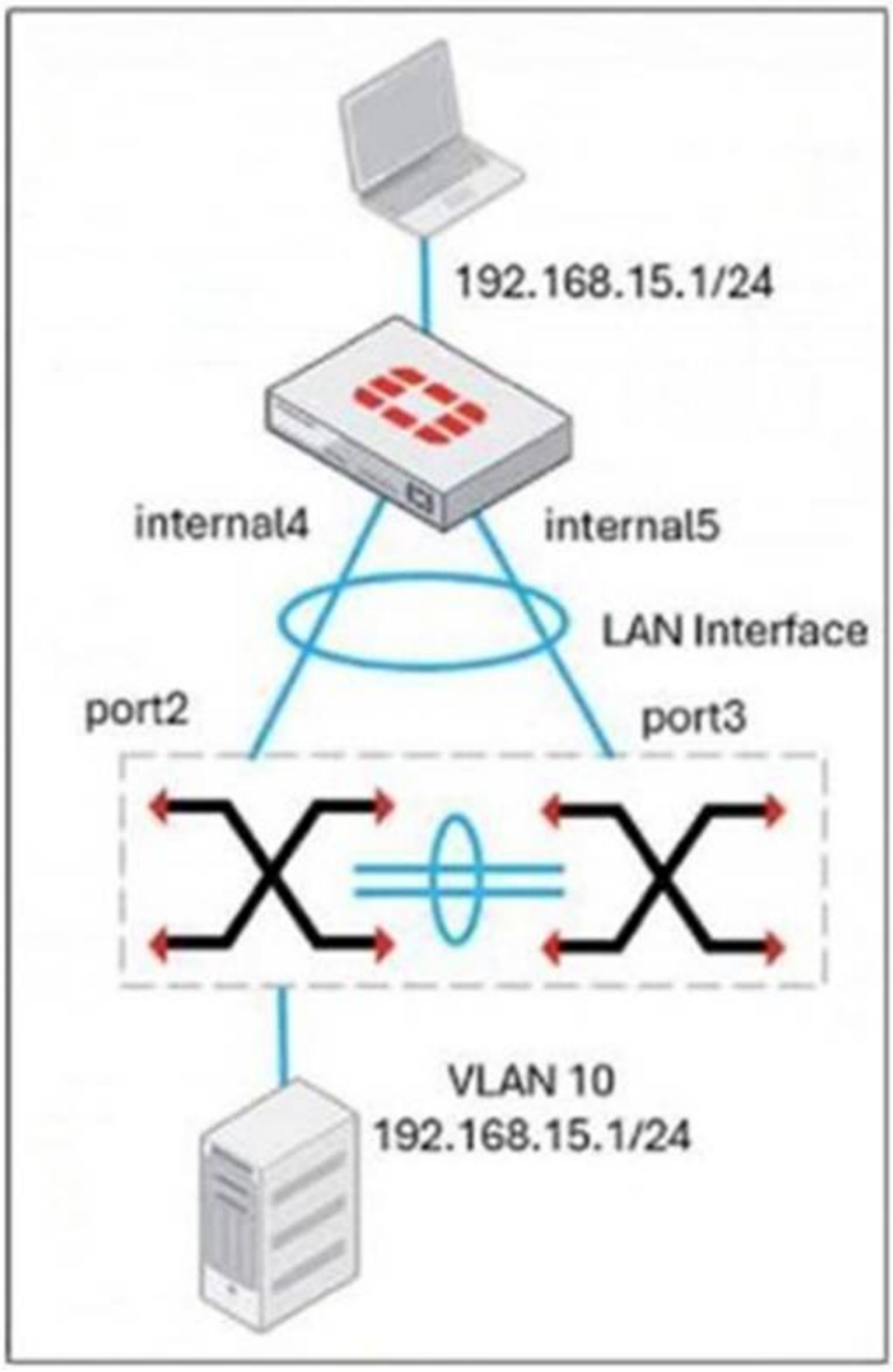


An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub.
Which two commands allow the administrator to minimize the configuration? (Choose two.)

A. neighbor-group
B. route-reflector-client
C. neighbor-range
D. ibgp-enforce-multihop

Answer: AC

NEW QUESTION 2
Refer to the exhibit, which shows a LAN interface connected from FortiGate to two FortiSwitch devices.

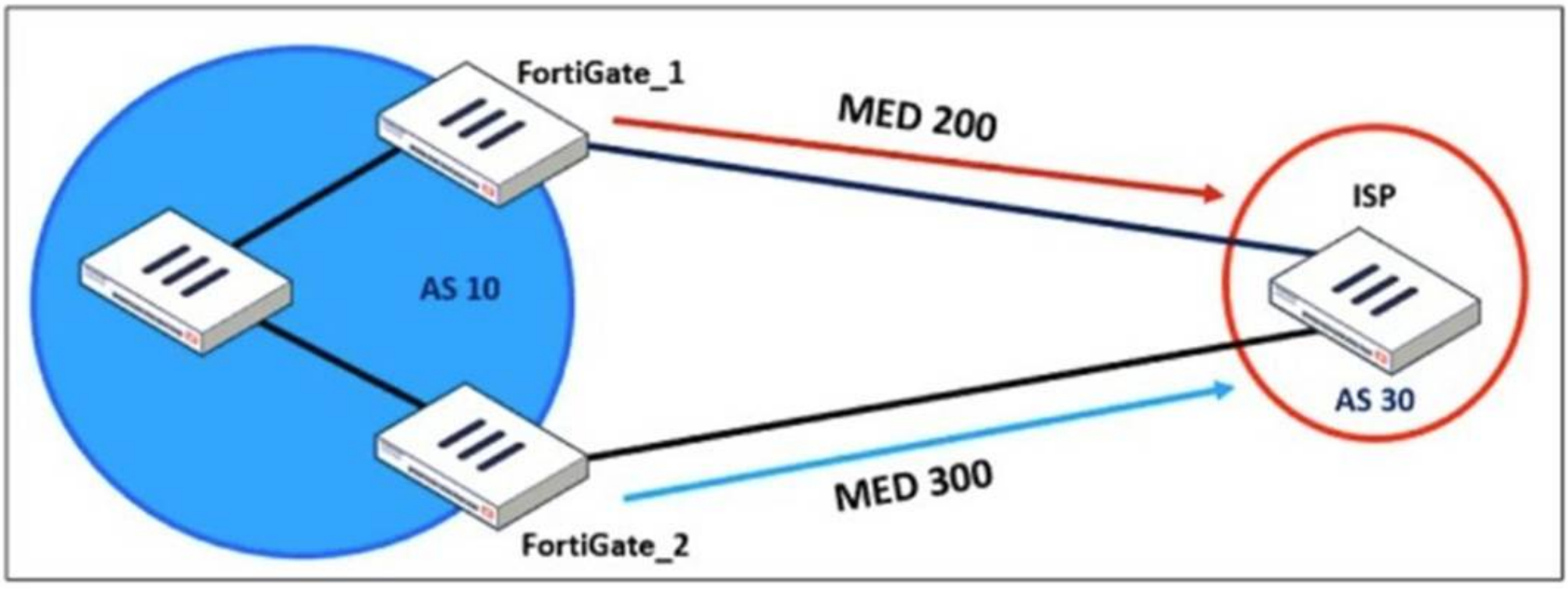


What two conclusions can you draw from the corresponding LAN interface? (Choose two.)

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 3
Refer to the exhibit, which shows a network diagram.



An administrator would like to modify the MED value advertised from FortiGate_1 to a BGP neighbor in the autonomous system 30.
What must the administrator configure on FortiGate_1 to implement this?

A. route-map-out
B. network-import-check
C. prefix-list-out
D. distribute-list-out

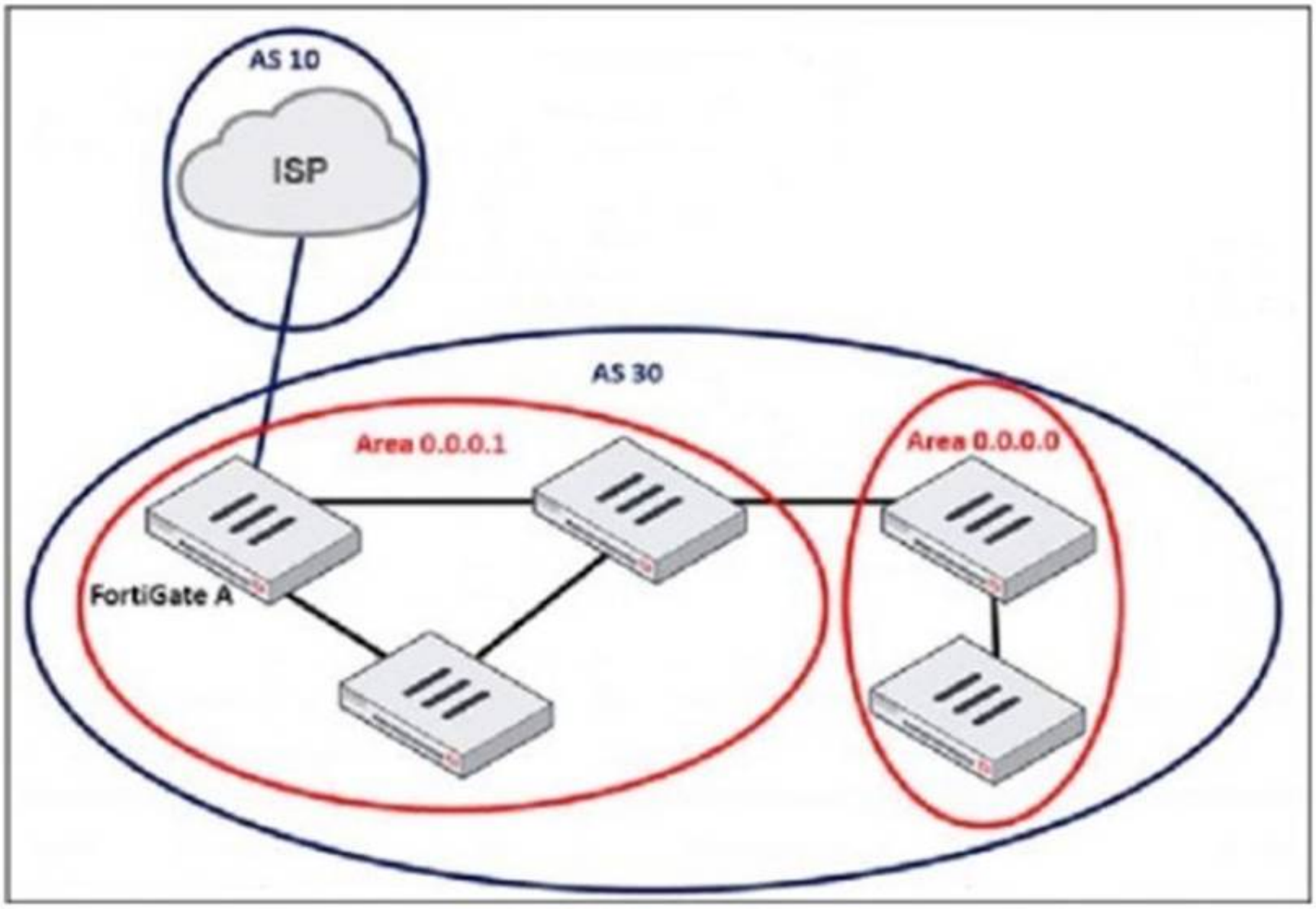
Answer: A

NEW QUESTION 4
An administrator is checking an enterprise network and sees a suspicious packet with the MAC address e0:23:ff:fc:00:86.
What two conclusions can the administrator draw? (Choose two.)

A. The suspicious packet is related to a cluster that has VDOMs enabled.
B. The network includes FortiGate devices configured with the FGSP protocol.
C. The suspicious packet is related to a cluster with a group-id value lower than 255.
D. The suspicious packet corresponds to port 7 on a FortiGate device.

Answer: AC

NEW QUESTION 5
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 6
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.

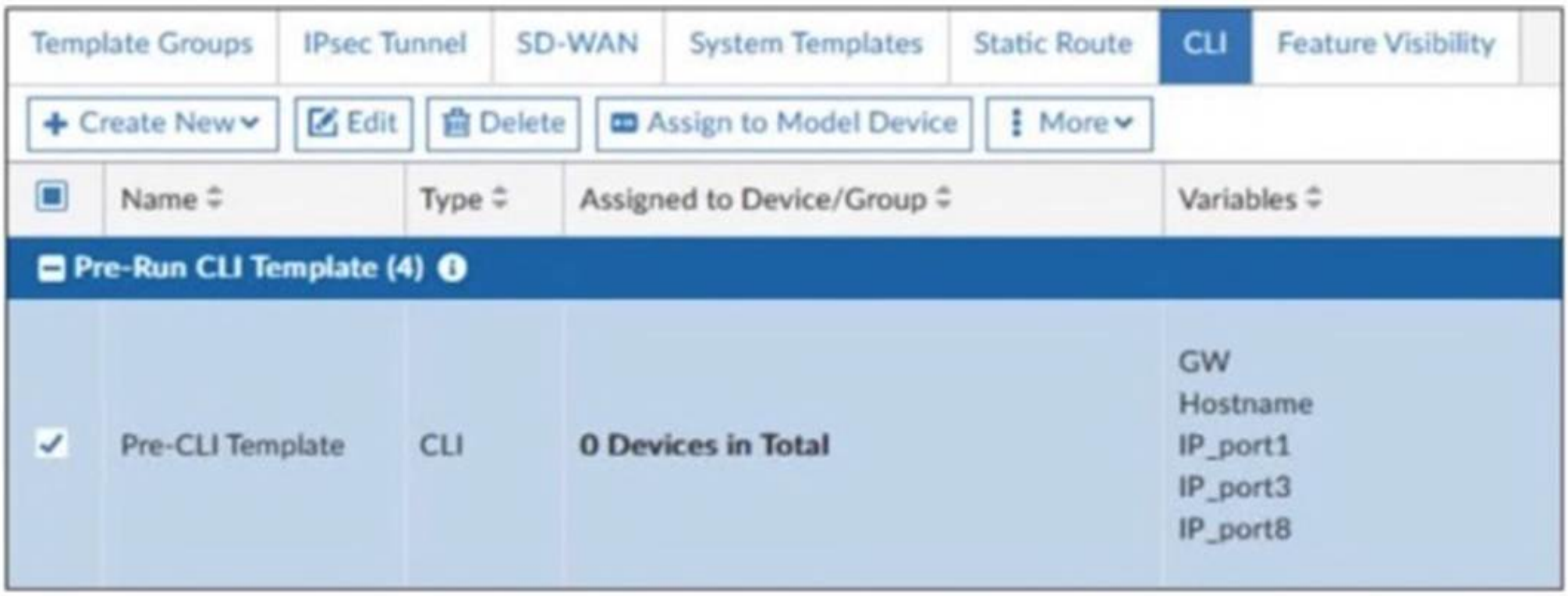
Answer: D

NEW QUESTION 7
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

NEW QUESTION 8
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 9
How will configuring set tcp-mss-sender and set tcp-mss-receiver in a firewall policy affect the size and handling of TCP packets in the network?

A. The maximum segment size permitted in the firewall policy determines whether TCP packets are allowed or denied.
B. Applying commands in a firewall policy determines the largest payload a device can handle in a single TCP segment.
C. The administrator must consider the payload size of the packet and the size of the IP header to configure a correct value in the firewall policy.
D. The TCP packet modifies the packet size only if the size of the packet is less than the one the administrator configured in the firewall policy.

Answer: B

NEW QUESTION 10
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 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
```

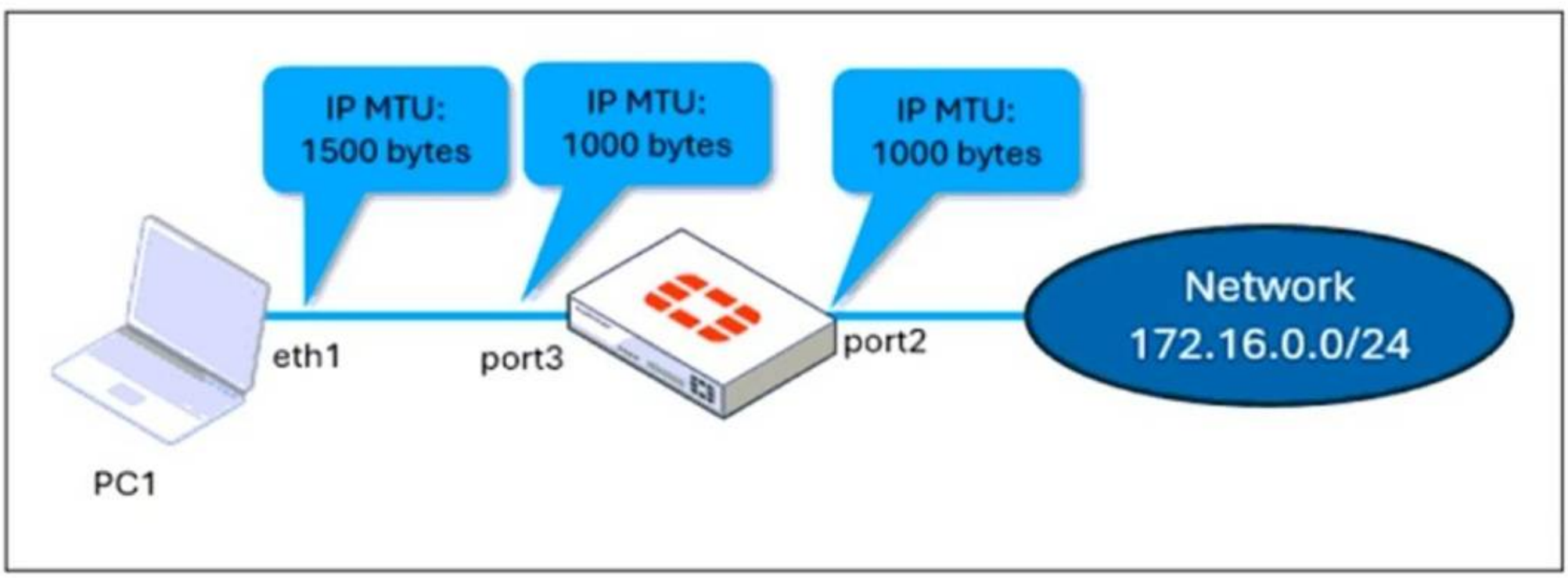
What can you conclude from this VPN IPsec phase 1 configuration?

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

NEW QUESTION 15
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 18
Refer to the exhibit, which shows the HA status of an active-passive cluster.

Status	Priority	Hostname	Virtual Domains	Role	System Uptime
Virtual cluster 1 2					
Synchronized	150	FortiGate_A	Core1 root	Primary	4h 52m
Synchronized	100	FortiGate_B	Core1 root	Secondary	4h 52m
Virtual cluster 2 2					
Synchronized	150	FortiGate_A	Core2	Primary	
Synchronized	128	FortiGate_B	Core2	Secondary	

An administrator wants FortiGate_B to handle the Core2 VDOM traffic.
Which modification must the administrator apply to achieve this?

A. The administrator must disable override on FortiGate_A.
B. The administrator must change the priority from 100 to 160 for FortiGate_B.
C. The administrator must change the load balancing method on FortiGate_B.
D. The administrator must change the priority from 128 to 200 for FortiGate_B.

Answer: D

NEW QUESTION 21
Refer to the exhibit, which shows a command output.

```
FortiGate_B # get system session list | grep icmp

FortiGate_B #
```

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 22
An administrator must minimize CPU and RAM use on a FortiGate firewall while also enabling essential security features, such as web filtering and application control for HTTPS traffic.
Which SSL inspection setting helps reduce system load while also enabling security features, such as web filtering and application control for encrypted HTTPS traffic?

A. Use full SSL inspection to thoroughly inspect encrypted payloads.
B. Disable SSL inspection entirely to conserve resources.
C. Configure SSL inspection to handle HTTPS traffic efficiently.
D. Enable SSL certificate inspection mode to perform basic checks without decrypting traffic.

Answer: D

NEW QUESTION 24
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

NEW QUESTION 29
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 34
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 39
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

NEW QUESTION 40
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
```

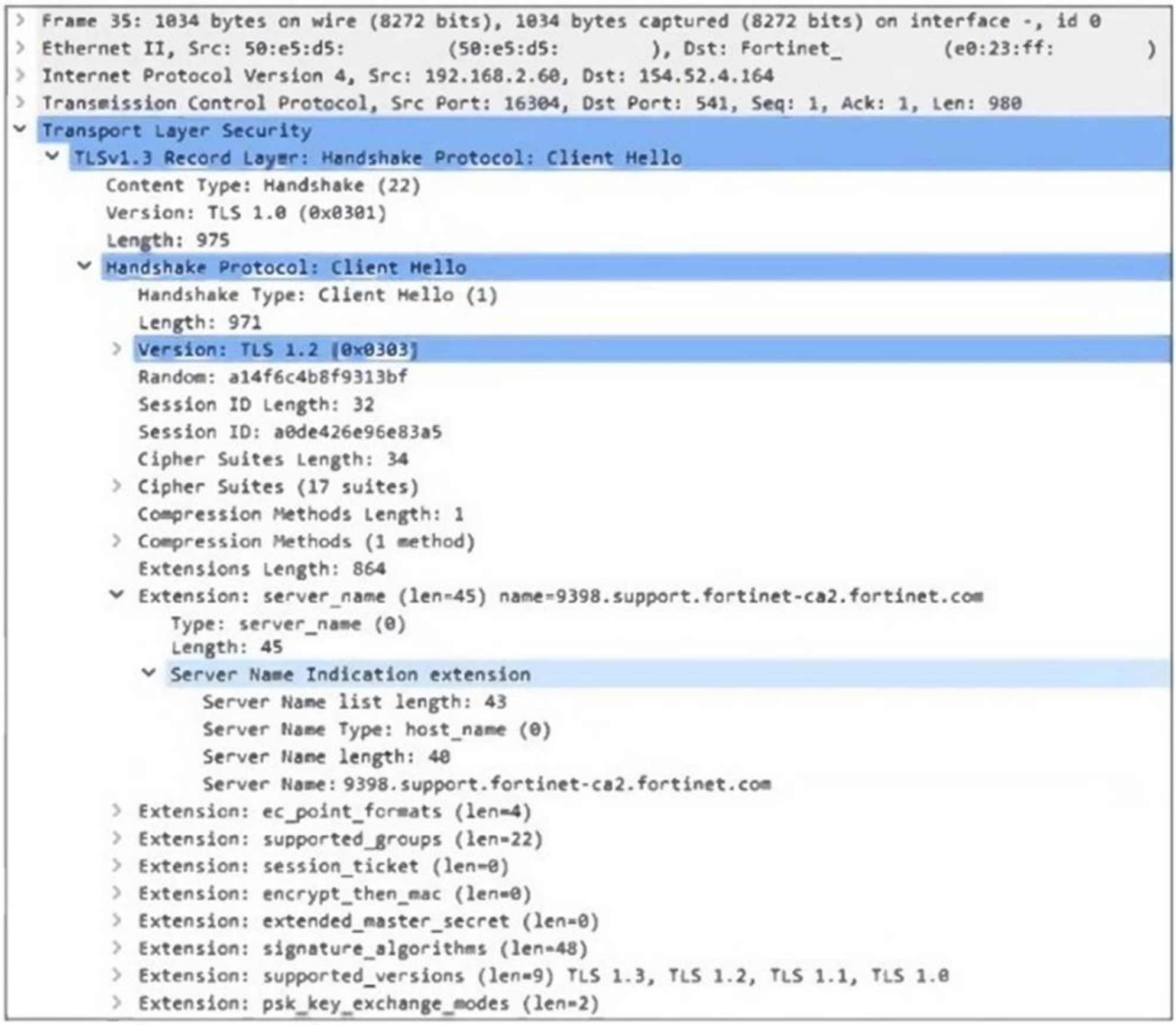
An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.
Which statement on this FortiGate device is correct?

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

NEW QUESTION 43
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 44
.....

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