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 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.

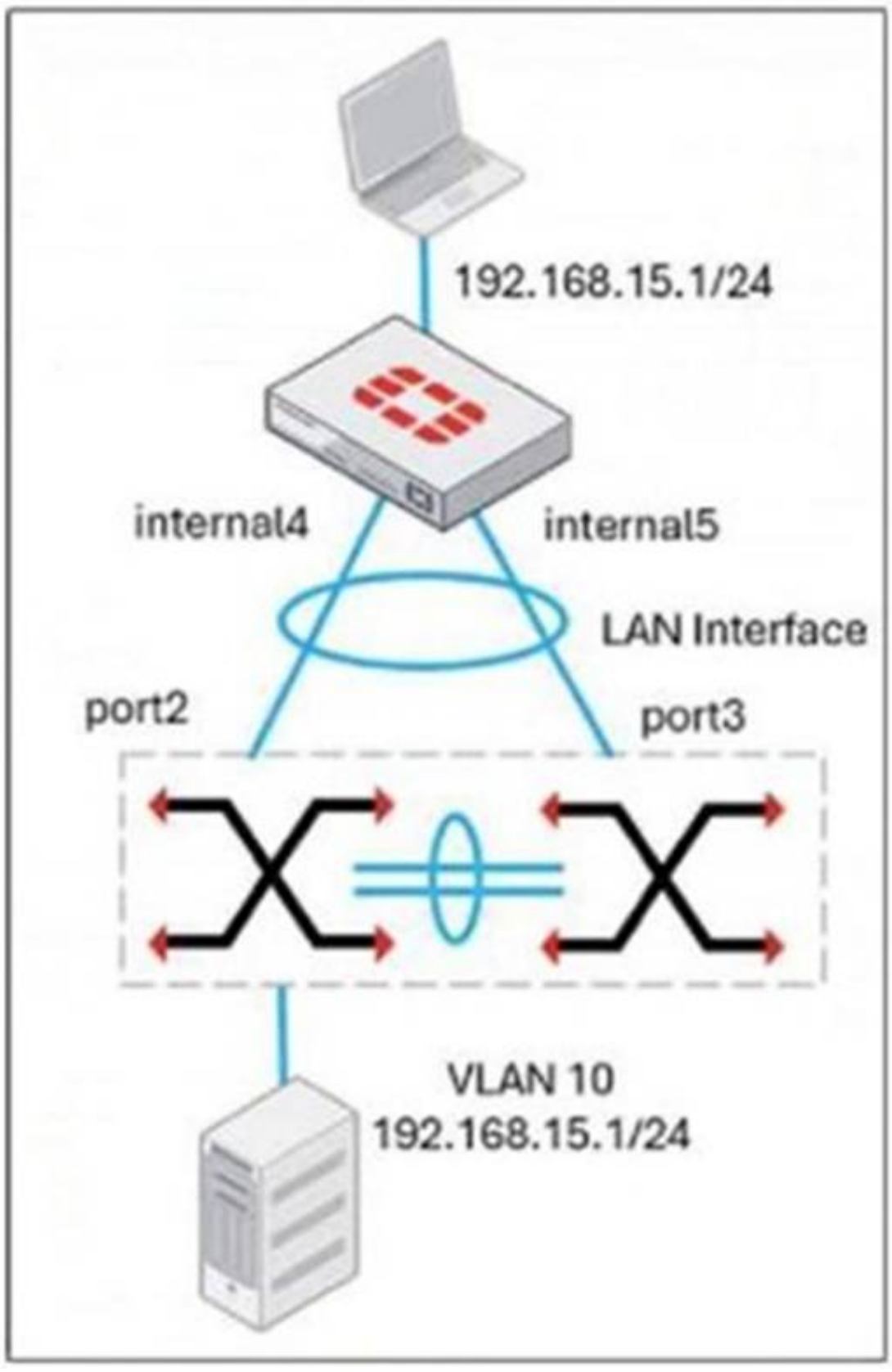
Answer: B

NEW QUESTION 3
The IT department discovered during the last network migration that all zero phase selectors in phase 2 IPsec configurations impacted network operations.
What are two valid approaches to prevent this during future migrations? (Choose two.)

A. Use routing protocols to specify allowed subnets over the tunnel.
B. Configure an IPsec-aggregate to create redundancy between each firewall peer.
C. Clearly indicate to the VPN which segments will be encrypted in the phase two selectors.
D. Configure an IP address on the IPsec interface of each firewall to establish unique peer connections and avoid impacting network operations.

Answer: AC

NEW QUESTION 4
Refer to the exhibit, which shows a LAN interface connected from FortiGate to two FortiSwitch devices.

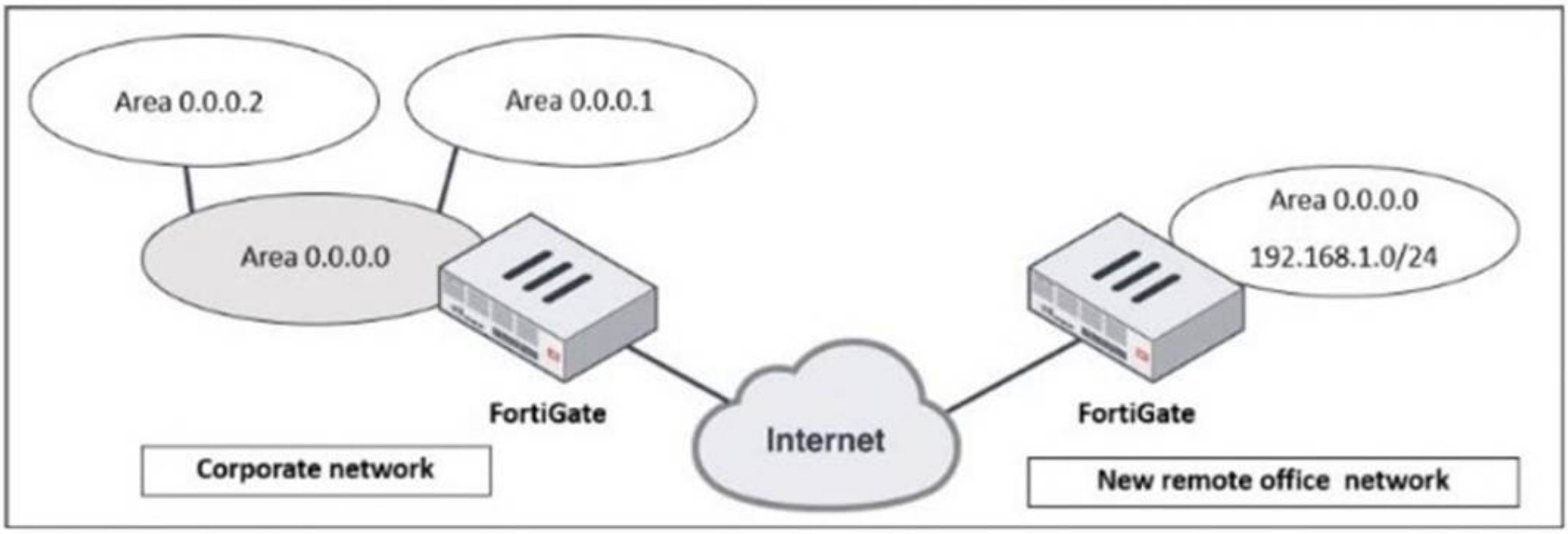


What two conclusions can you draw from the corresponding LAN interface? (Choose two.)

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 5
Refer to the exhibit, which shows a corporate network and a new remote office network.

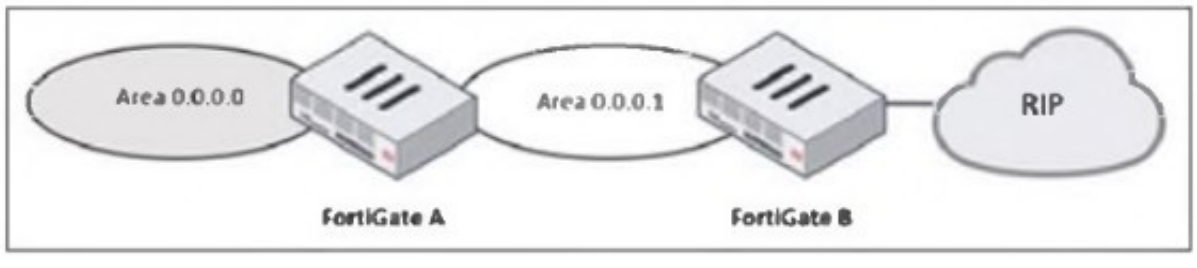


An administrator must integrate the new remote office network with the corporate enterprise network.
What must the administrator do to allow routing between the two networks?

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 6
Refer to the exhibit, which shows a partial enterprise network.

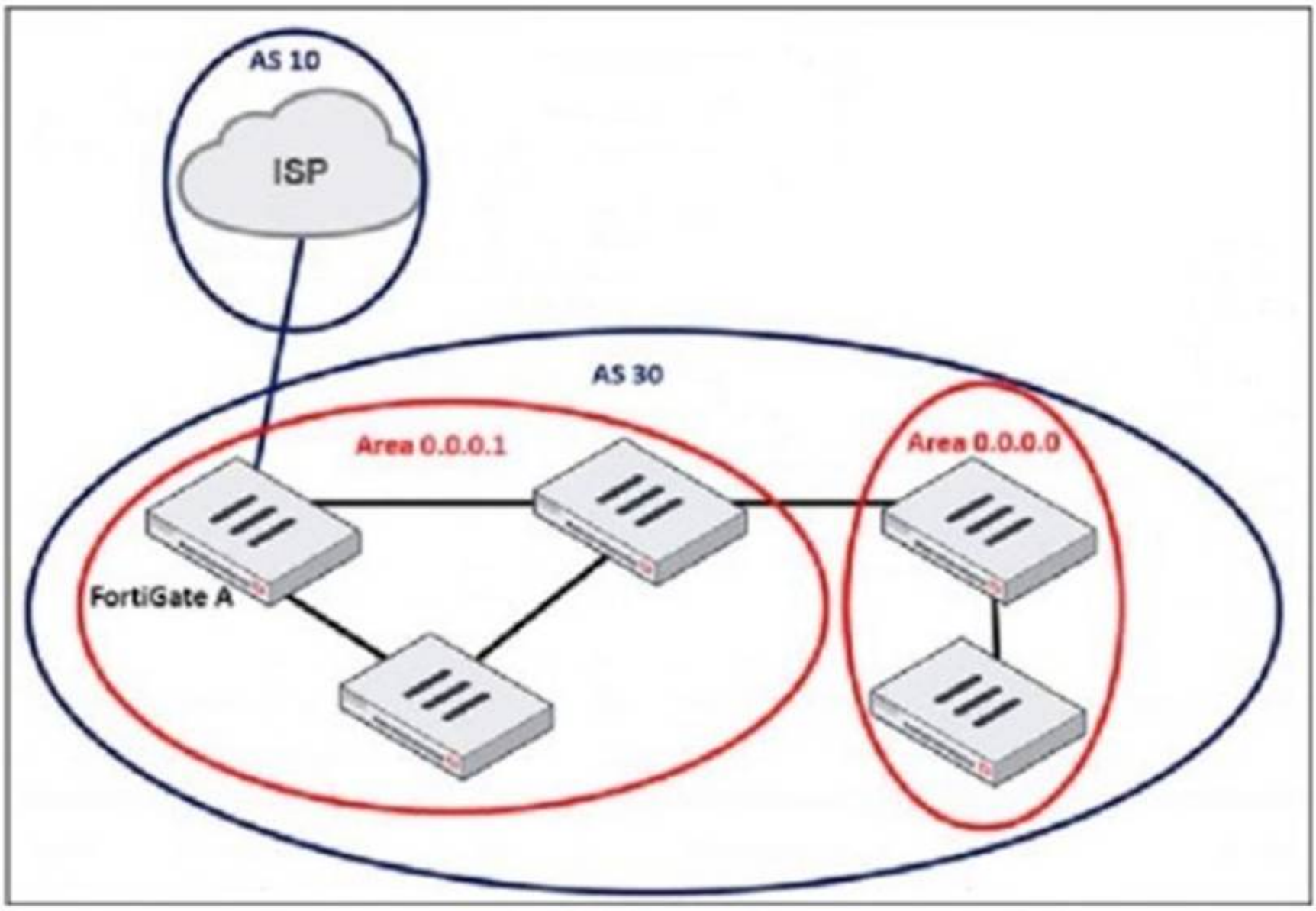


An administrator would like the area 0.0.0.0 to detect the external network. What must the administrator configure?

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 7
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 8
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 9
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.

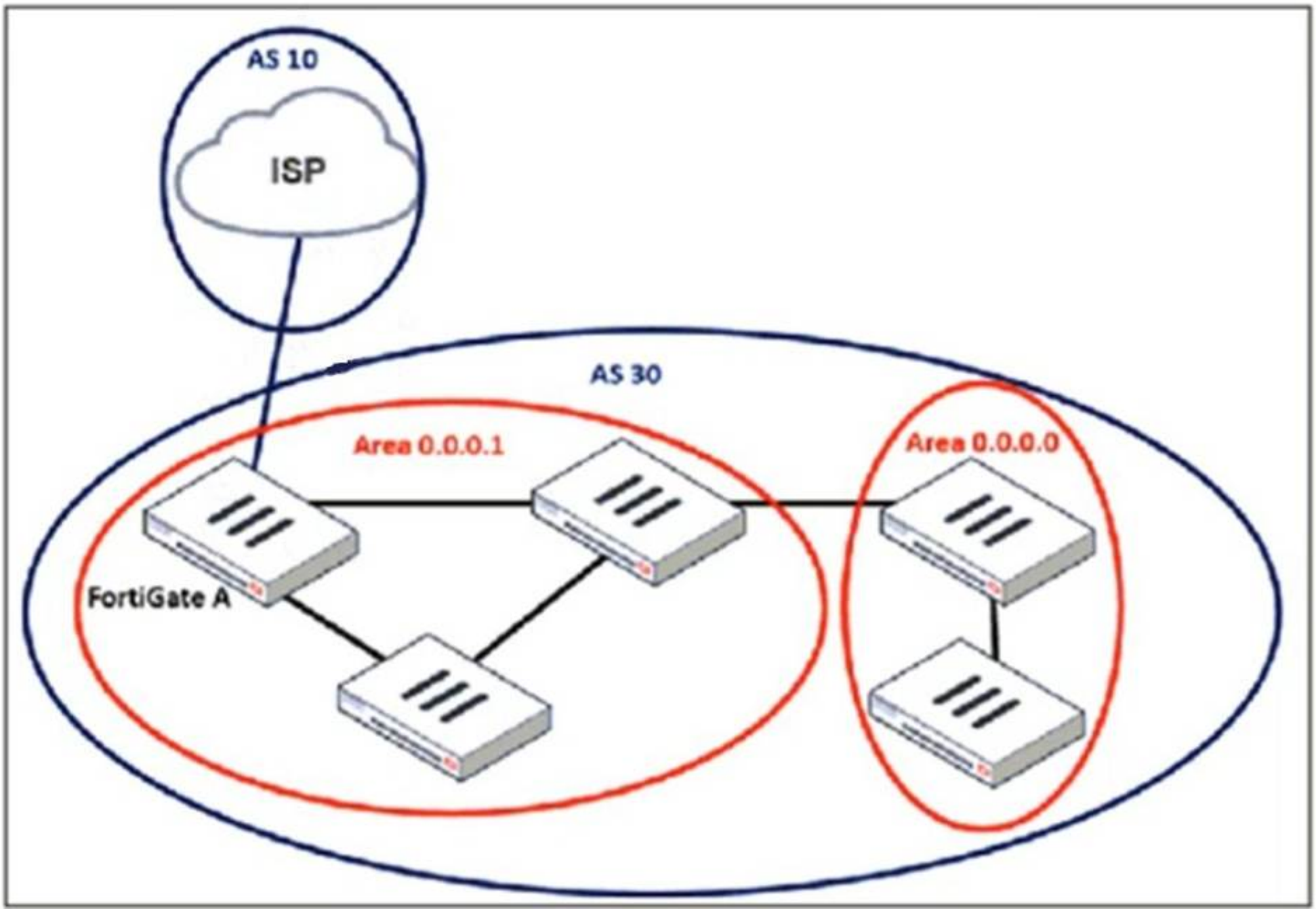
Answer: A

NEW QUESTION 10
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 10
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

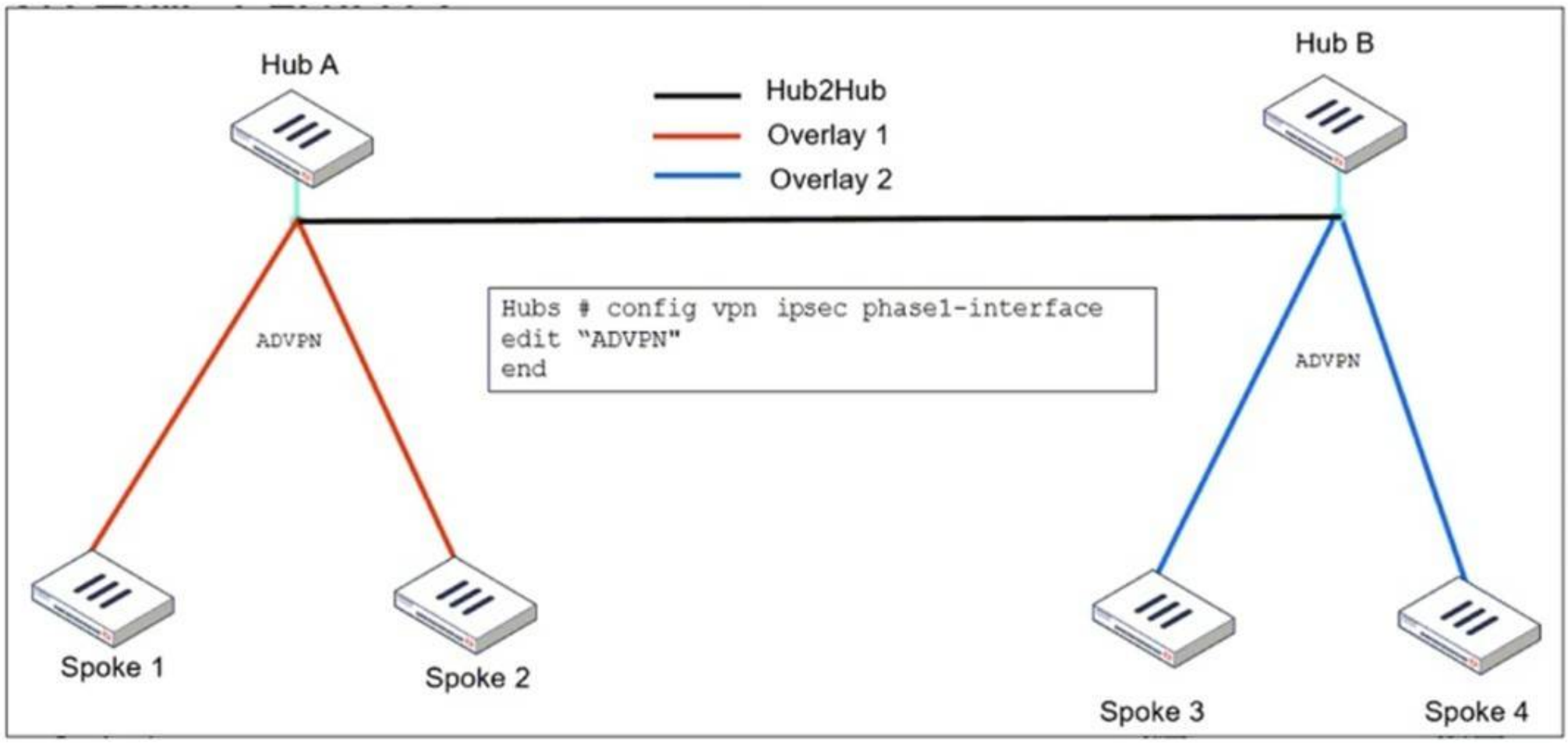
NEW QUESTION 12

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 15
Refer to the exhibit, which shows the ADVPN IPsec interface representing the VPN IPsec phase 1 from Hub A to Spoke 1 and Spoke 2, and from Hub to Spoke 3 and Spoke 4.



An administrator must configure an ADVPN using IBGP and EBGP to connect overlay network 1 with 2.
What must the administrator configure in the phase 1 VPN IPsec configuration of the ADVPN tunnels?

A. set auto-discovery-sender enable and set network-id x
B. set auto-discovery-forwarder enable and set remote-as x
C. set auto-discovery-crossover enable and set enforce-multihop enable
D. set auto-discovery-receiver enable and set npu-offload enable

Answer: C

NEW QUESTION 20
What action can be taken on a FortiGate to block traffic using IPS protocol decoders, focusing on network transmission patterns and application signatures?

A. Use the DNS filter to block application signatures and protocol decoders.
B. Use application control to limit non-URL-based software handling.
C. Enable application detection-based SD-WAN rules.
D. Configure a web filter profile in flow mode.

Answer: B

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 26
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 28
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 31
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 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.

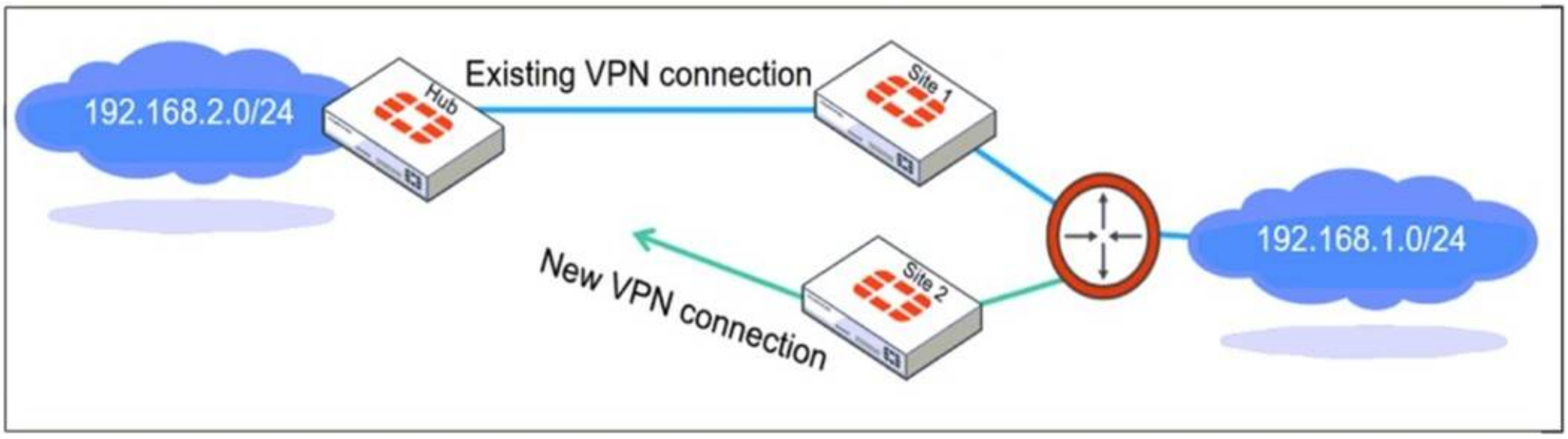
Answer: D

NEW QUESTION 36
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 41
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

NEW QUESTION 42
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 47
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 route 172.16.1.248/30 on 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

NEW QUESTION 52
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The FCSS_EFW_AD-7.6 Practice Test Here