

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.

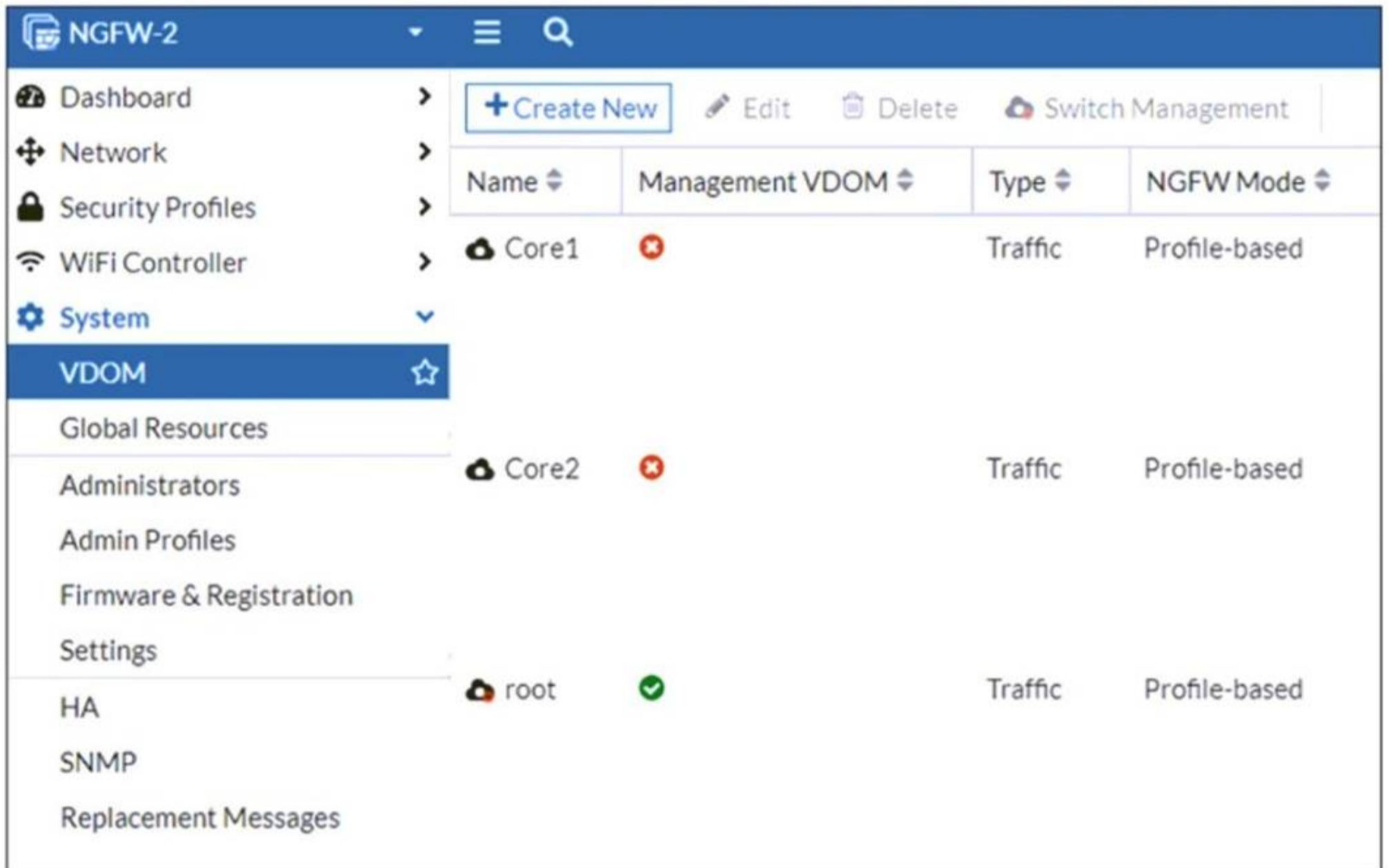
In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

- 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.



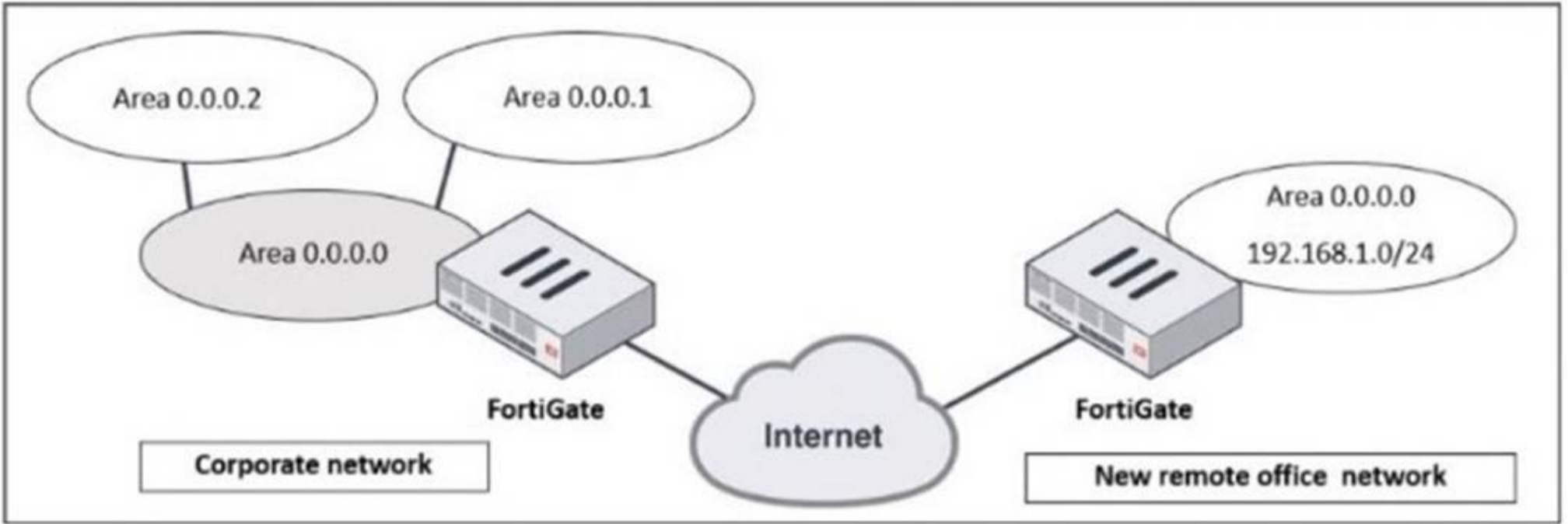
An administrator discovers that webfilter stopped working in Core1 and Core2 after a maintenance window. Which two reasons could explain why webfilter stopped working? (Choose two.)

- 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 Core1 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 corporate network and a new remote office network.



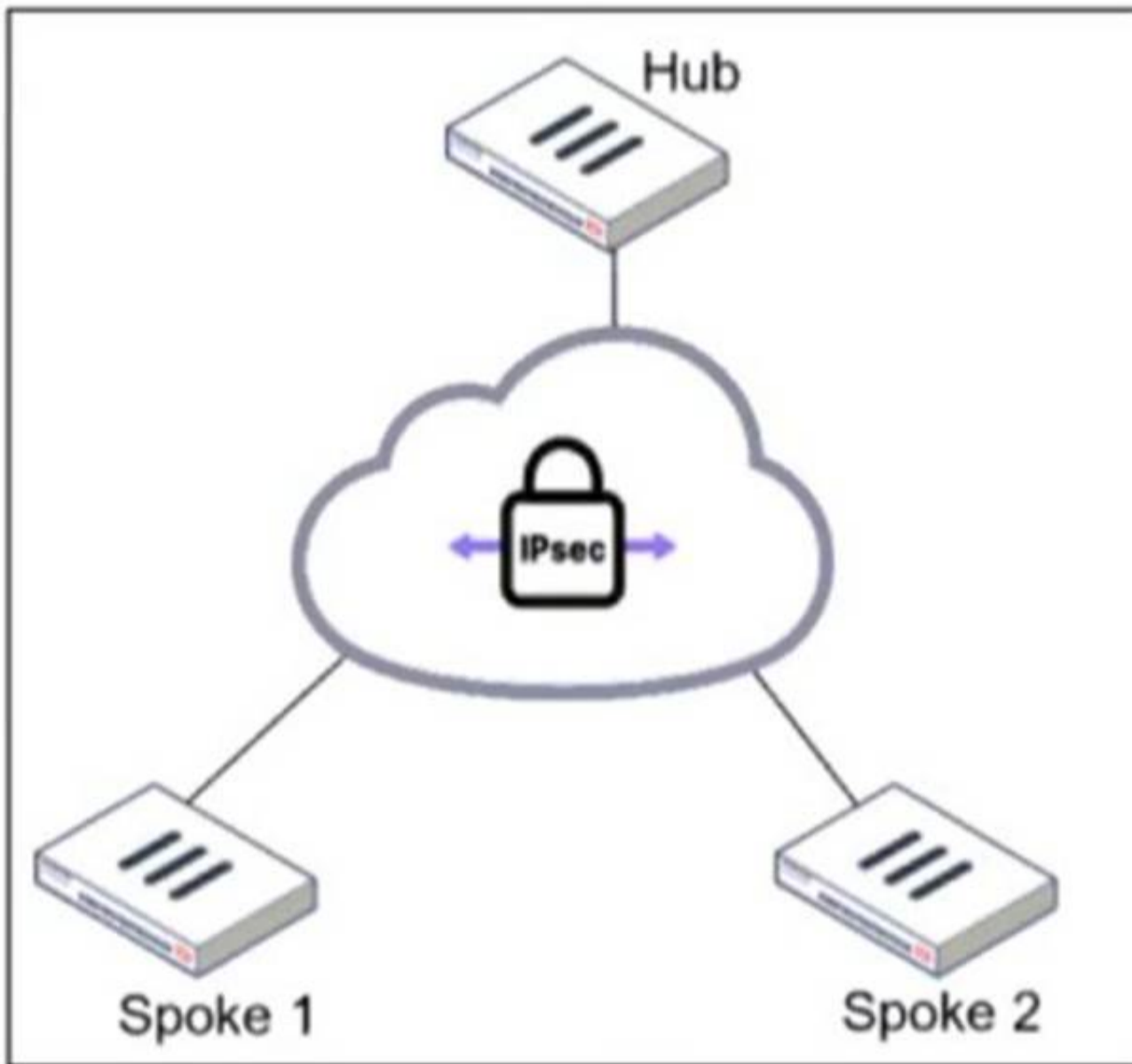
An administrator must integrate the new remote office network with the corporate enterprise network. What must the administrator do to allow routing between the two networks?

- 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 192.168.1.0/24 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 4

Refer to the exhibit.



An administrator is deploying a hub and spokes network and using OSPF as dynamic protocol. Which configuration is mandatory for neighbor adjacency?

- A. Set bfd enable in the router configuration
- B. Set network-type point-to-multipoint in the hub interface
- C. Set rfc1583-compatible enable in the router configuration
- D. Set virtual-link enable in the hub interface

Answer: B

NEW QUESTION 5

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
    
```

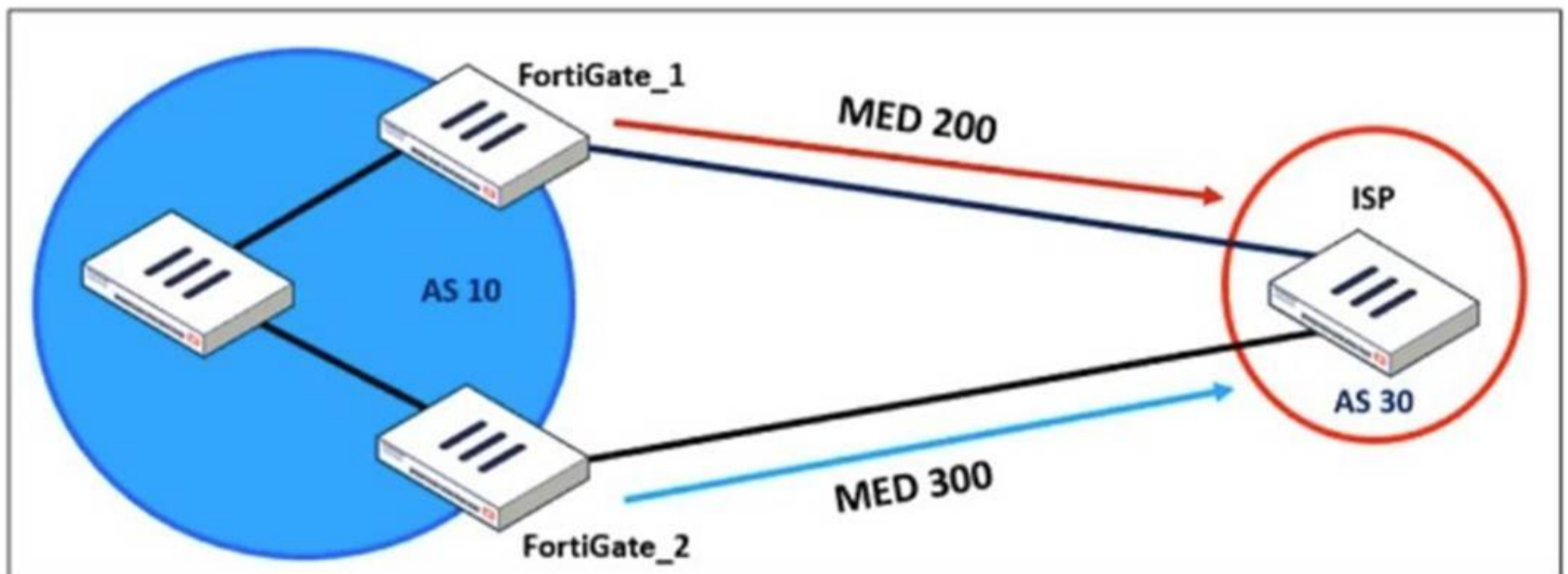
The administrator has configured BGP on FortiGate. The status of this new BGP configuration is shown in the exhibit. What configuration must the administrator consider next?

- 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

NEW QUESTION 6

Refer to the exhibit, which shows a network diagram.



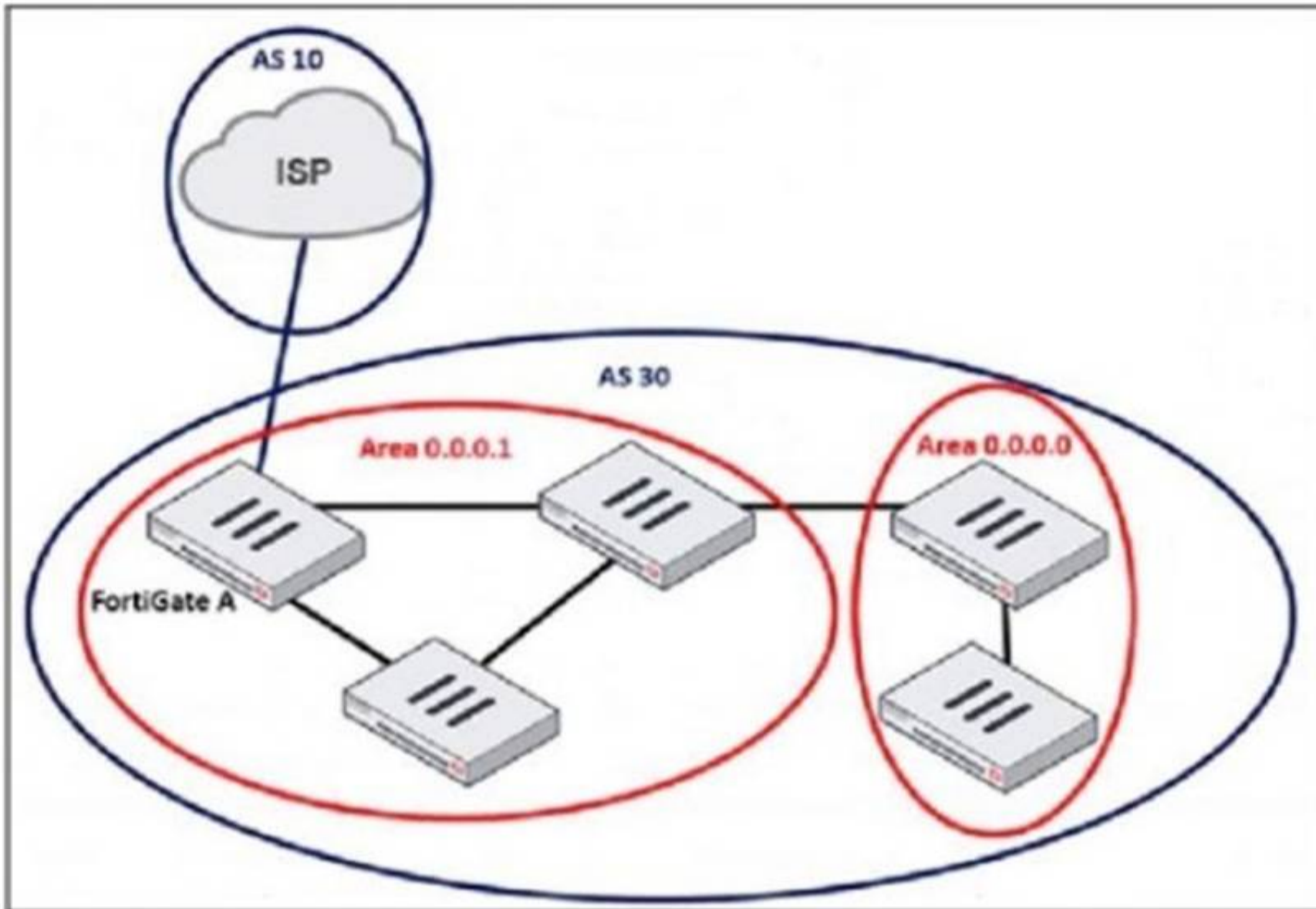
An administrator would like to modify the MED value advertised from FortiGate_1 to a BGP neighbor in the autonomous system 30. What must the administrator configure on FortiGate_1 to implement this?

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

Answer: A

NEW QUESTION 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 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 clicking suspicious 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 missing or expired SSUTLS certificates on the client PC to prevent expected false positives.

Answer: A


NEW QUESTION 9

Refer to the exhibits.

Root FortiGate - System Administrator configuration

System Administrator 2	
admin	super_admin
AdminSSO	super_admin_readonly

Downstream FortiGate - Security Fabric settings

Security Fabric role	<input type="radio"/> Standalone <input type="radio"/> Serve as Fabric Root <input checked="" type="radio"/> Join Existing Fabric
Allow other Security Fabric devices to join	<input checked="" type="checkbox"/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;">  port1 ✕ </div> <div style="text-align: center; margin-top: 5px;">+</div>
Upstream FortiGate IP/FQDN	<input type="text" value="10.1.0.254"/>
Allow downstream device REST API access	<input type="checkbox"/>
SAML Single Sign-On	<input checked="" type="radio"/> Auto <input type="radio"/> Manual <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px; text-align: center;"> Advanced Options </div>
Mode	Service Provider (SP)
Default login page	<input checked="" type="radio"/> Normal <input type="radio"/> Single Sign-On
Default admin profile	<input type="text" value="super_admin_readonly"/>
Management IP/FQDN	<input type="checkbox"/> Use WAN IP <input checked="" type="checkbox"/> Specify <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;">10.1.0.100</div>
Management port	<input type="checkbox"/> Use Admin Port <input checked="" type="checkbox"/> Specify <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;">443</div>

The Administrators section of a root FortiGate device and the Security Fabric Settings section of a downstream FortiGate device are shown. When prompted to sign in with Security Fabric in the downstream FortiGate device, a user enters the AdminSSO credentials. What is the next status for the user?

- A. The user is prompted to create an SSO administrator account for AdminSSO.
- B. The user receives an authentication failure message.
- C. The user accesses the downstream FortiGate with super_admin_readonly privileges.
- D. The user accesses the downstream FortiGate with super_admin privileges.

Answer: C

NEW QUESTION 10

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?

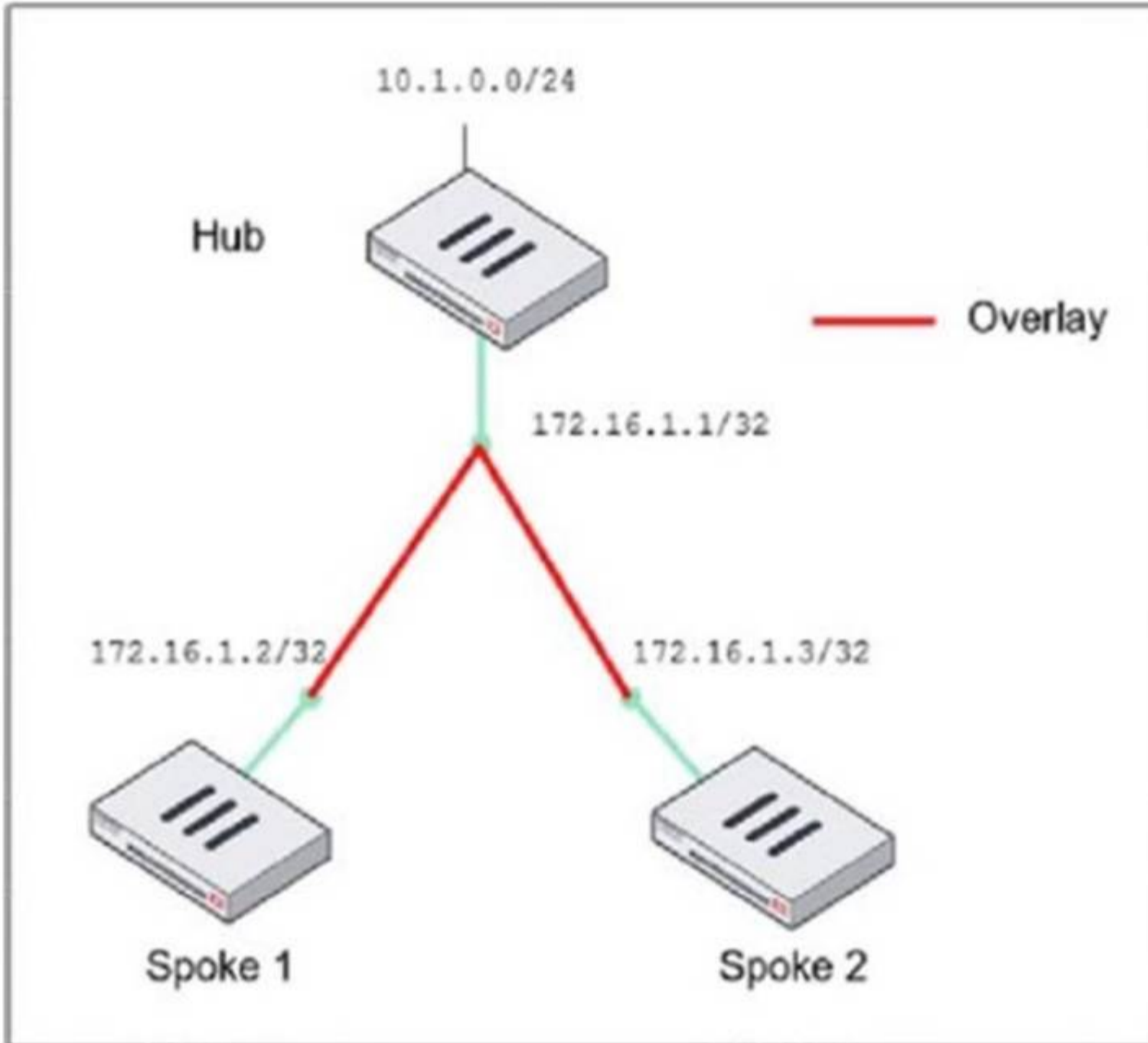
- A. Enable metadata variables to use dynamic configurations in the standard interfaces of FortiManager.
- B. Use the Install On feature in the policy package to automatically assign different interfaces based on the branch.
- C. Create interfaces using device database scripts to use them on the same 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

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 14

An administrator wants to scale the IBGP sessions and optimize the routing table in an IBGP network. Which parameter should the administrator configure?

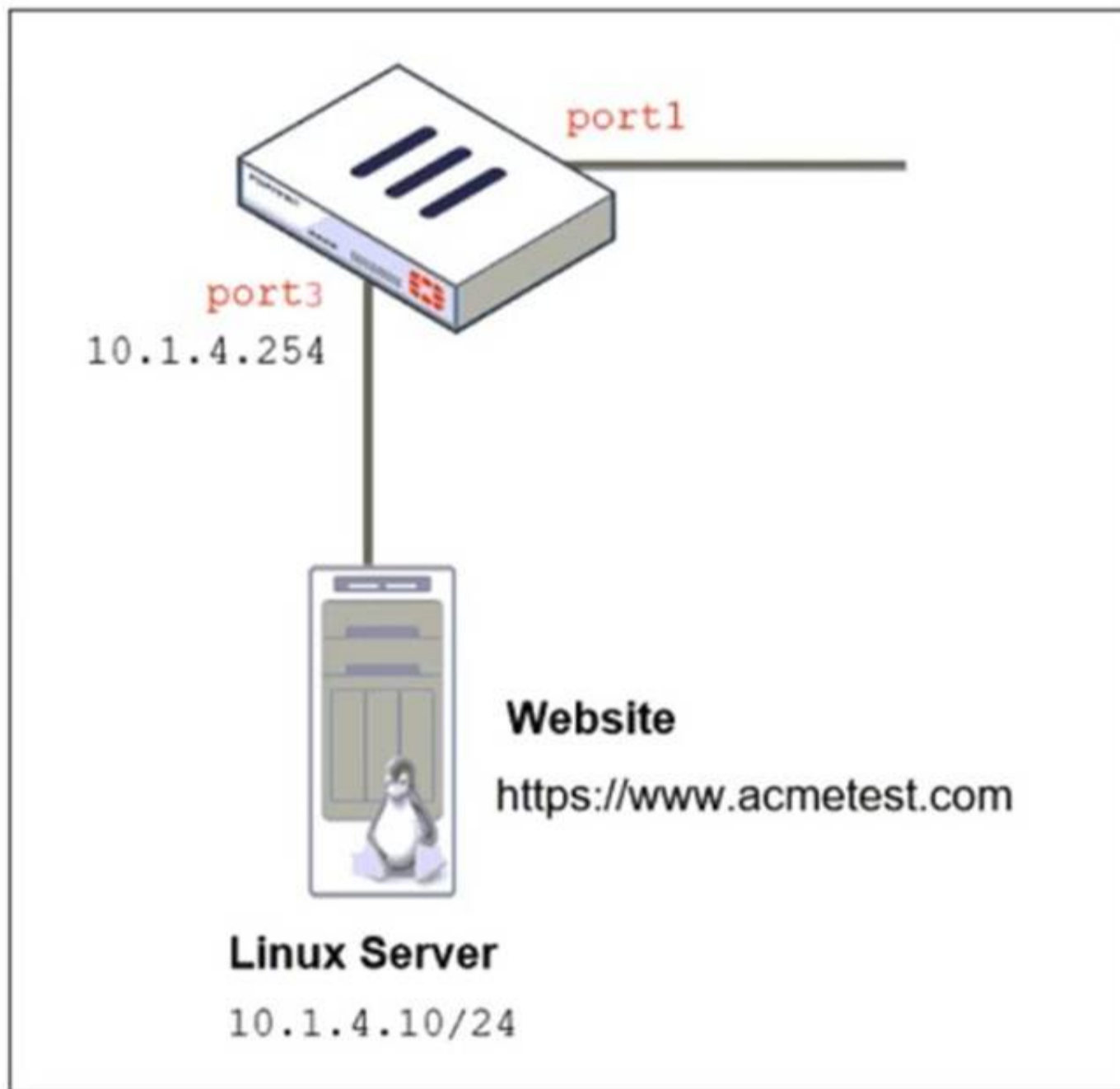
- A. network-import-check
- B. ibgp-enforce-multihop
- C. neighbor-group
- D. route-reflector-client

Answer: D

NEW QUESTION 15

Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

Network Topology



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

Edit SSL/SSH Inspection Profile



Name



Comments 34/255


SSL Inspection Options


Enable SSL inspection of Multiple Client Clients Connecting to Multiple Servers

Inspection method Full SSL Inspection

CA certificate   Download

Blocked certificates  Block  View Blocked Certificates

Untrusted SSL certificates Allow Block Ignore  View Trusted CAs List

Server certificate SNI check  Enable Strict Disable

Enforce SSL cipher compliance

Enforce SSL negotiation compliance

RPC over HTTPS

MAPI over HTTPS

Protocol Port Mapping

Inspect all ports

HTTPS	<input type="checkbox"/>	443
SMTS	<input checked="" type="checkbox"/>	465
POP3S	<input checked="" type="checkbox"/>	995
IMAPS	<input checked="" type="checkbox"/>	993
FTPS	<input checked="" type="checkbox"/>	990
DNS over TLS	<input type="checkbox"/>	853

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

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.

Template Groups		IPsec Tunnel	SD-WAN	System Templates	Static Route	CLI	Feature Visibility
+ Create New		Edit	Delete	Assign to Model Device	More		
<input type="checkbox"/>	Name	Type	Assigned to Device/Group		Variables		
Pre-Run CLI Template (4)							
<input checked="" type="checkbox"/>	Pre-CLI Template	CLI	0 Devices in Total		GW Hostname IP_port1 IP_port3 IP_port8		

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

A FortiGate device with UTM profiles is reaching the resource limits, and the administrator expects the traffic in the enterprise network to increase. The administrator has received an additional FortiGate of the same model. Which two protocols should the administrator use to integrate the additional FortiGate device into this enterprise network? (Choose two.)

- A. FGSP with external load balancers
- B. FGCP in active-active mode and with switches
- C. FGCP in active-passive mode and with VDOM disabled
- D. VRRP with switches

Answer: AB

NEW QUESTION 24

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
    
```

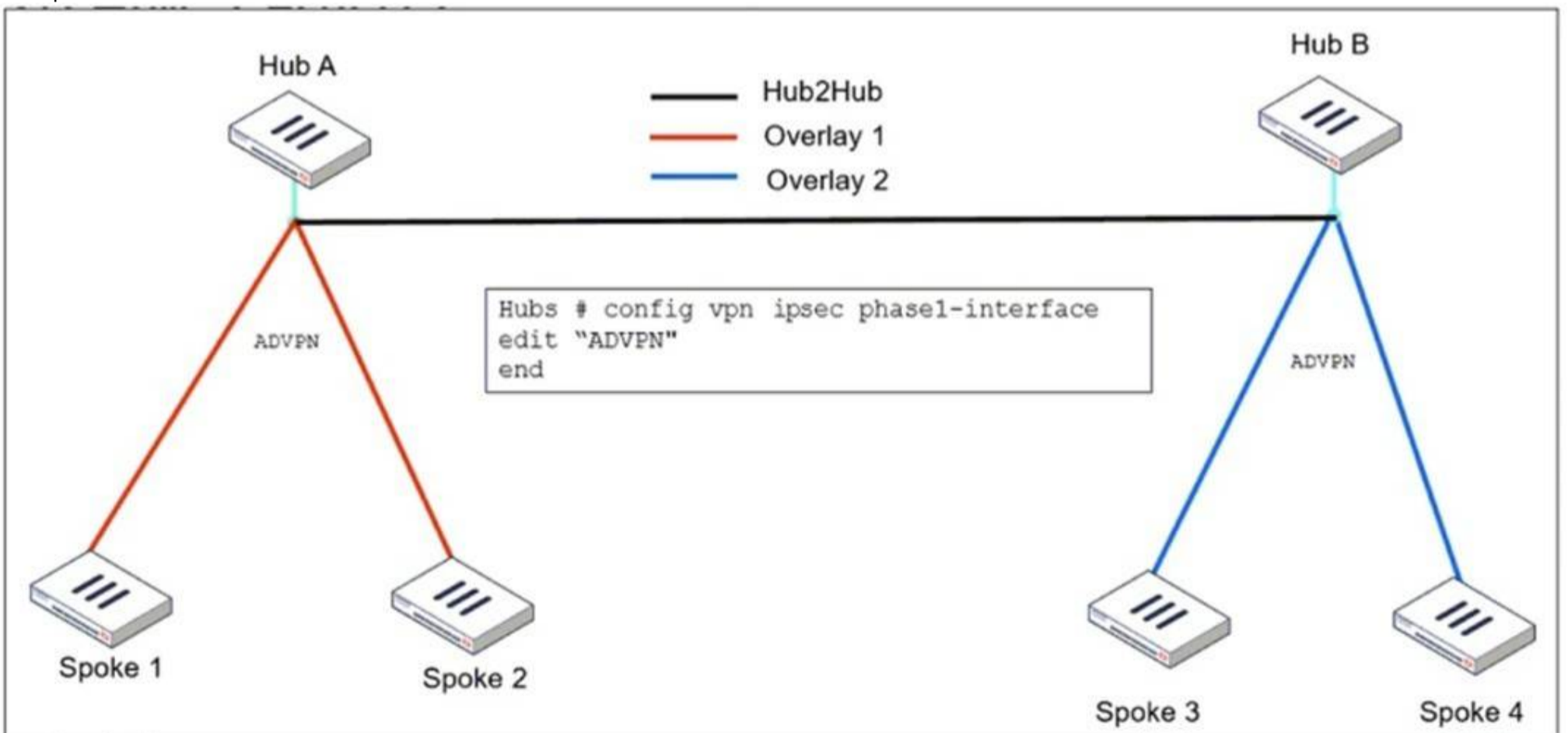
What can you conclude from this VPN IPsec phase 1 configuration?

- 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 28

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 32

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 34

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 35

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 38

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 39

Refer to the exhibit, which shows a revision history window in the FortiManager device layer.

ID	Date & Time	Name	Created by	Installation	Comments
✓ 10	2024-08-21 14:30:54		script_manager	Retrieved	
9	2024-08-21 14:02:55	AutoUpdate	AutoUpdate	Auto Updated	Autoretrieve merged config
8	2024-06-24 04:52:47	DCFW	admin	Installed	

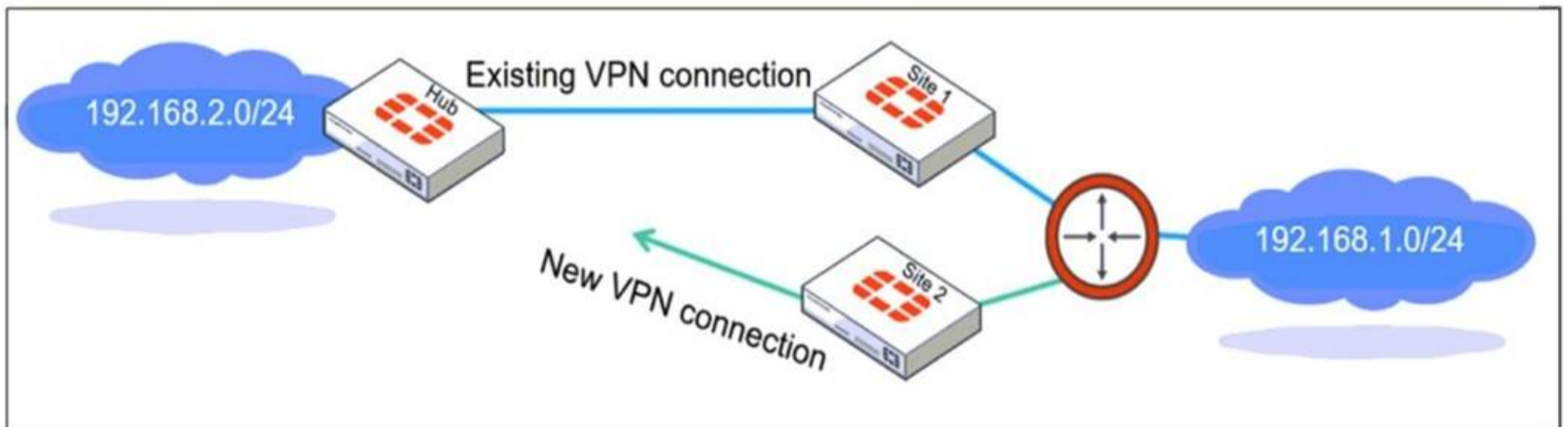
The IT team is trying to identify the administrator responsible for the most recent update in the FortiGate device database. Which conclusion can you draw about this scenario?

- A. This retrieved process was automatically triggered by a Remote FortiGate Directly (via CLI) script.
- B. The user script_manager is an API user from the Fortinet Developer Network (FDN) retrieving a configuration.
- C. To identify the user who created the event, check it on the Configuration and Installation widget on FortiGate within the FortiManager device layer.
- D. Find the user in the FortiManager system logs and use the type=script command to find the administrator user in the user field.

Answer: D

NEW QUESTION 43

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.



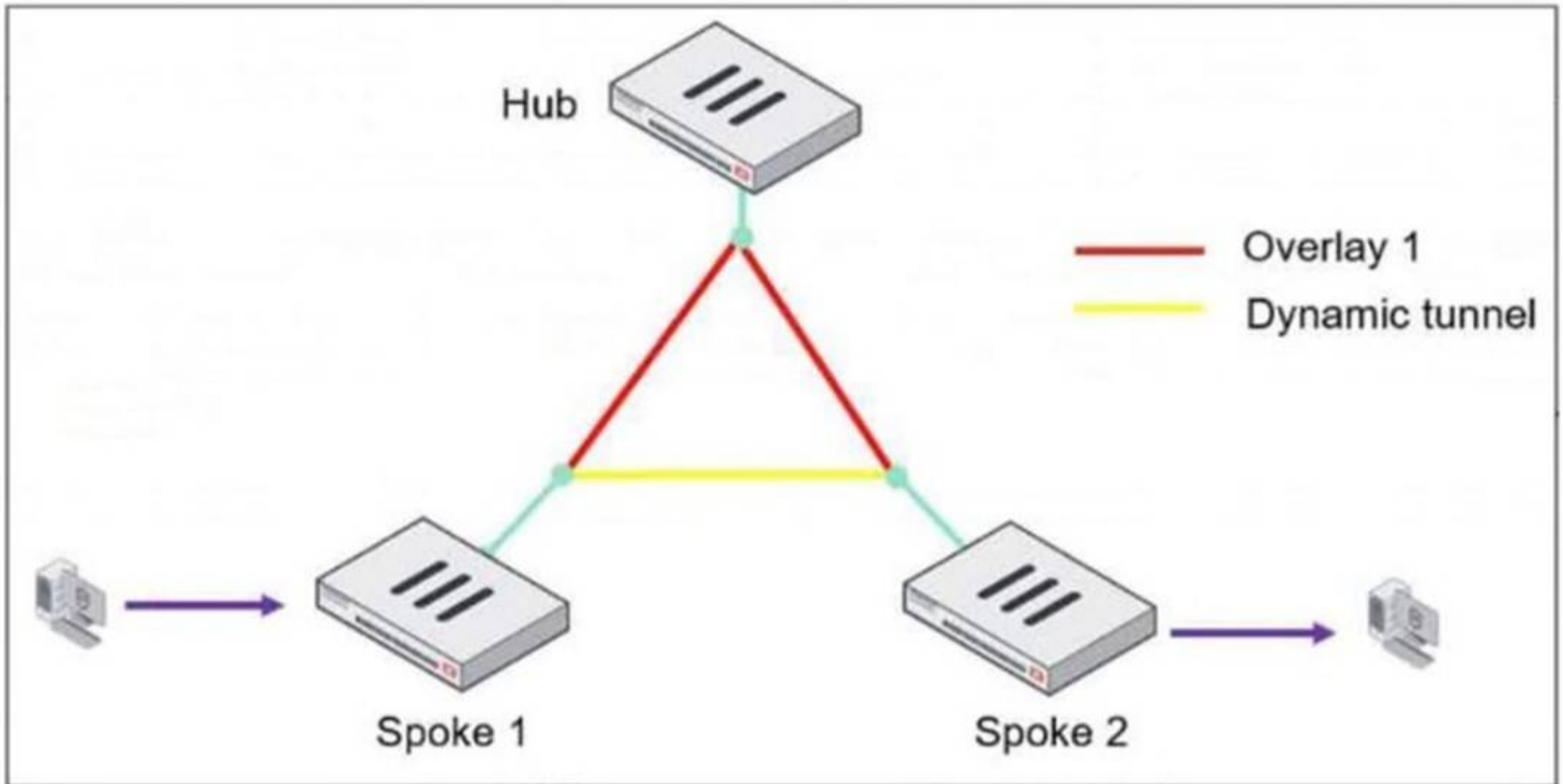
Which IPsec phase 2 configuration must an administrator make on the FortiGate hub to enable equal-cost multi-path (ECMP) routing when multiple remote sites connect with overlapping subnets?

- 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 48

Refer to the exhibit, which shows an ADVPN network.



The client behind Spoke-1 generates traffic to the device located behind Spoke-2.
 What is the first message that the hub sends to Spoke-1 to bring up the dynamic tunnel?

- A. Shortcut query
- B. Shortcut offer
- C. Shortcut reply
- D. Shortcut forward

Answer: B

NEW QUESTION 53

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 57

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

```

> Frame 35: 1034 bytes on wire (8272 bits), 1034 bytes captured (8272 bits) on interface -, id 0
> Ethernet II, Src: 50:e5:d5: (50:e5:d5: ), Dst: Fortinet_ (e0:23:ff: )
> Internet Protocol Version 4, Src: 192.168.2.60, Dst: 154.52.4.164
> Transmission Control Protocol, Src Port: 16304, Dst Port: 541, Seq: 1, Ack: 1, Len: 980
▼ Transport Layer Security
  ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 975
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 971
  > Version: TLS 1.2 [0x0303]
    Random: a14f6c4b8f9313bf
    Session ID Length: 32
    Session ID: a0de426e96e83a5
    Cipher Suites Length: 34
  > Cipher Suites (17 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 864
  ▼ Extension: server_name (len=45) name=9398.support.fortinet-ca2.fortinet.com
    Type: server_name (0)
    Length: 45
  ▼ Server Name Indication extension
    Server Name list length: 43
    Server Name Type: host_name (0)
    Server Name length: 40
    Server Name: 9398.support.fortinet-ca2.fortinet.com
  > Extension: ec_point_formats (len=4)
  > Extension: supported_groups (len=22)
  > Extension: session_ticket (len=0)
  > Extension: encrypt_then_mac (len=0)
  > Extension: extended_master_secret (len=0)
  > Extension: signature_algorithms (len=48)
  > Extension: supported_versions (len=9) TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0
  > Extension: psk_key_exchange_modes (len=2)

```

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

NEW QUESTION 59

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

NEW QUESTION 60

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 62

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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](#)