

Fortinet

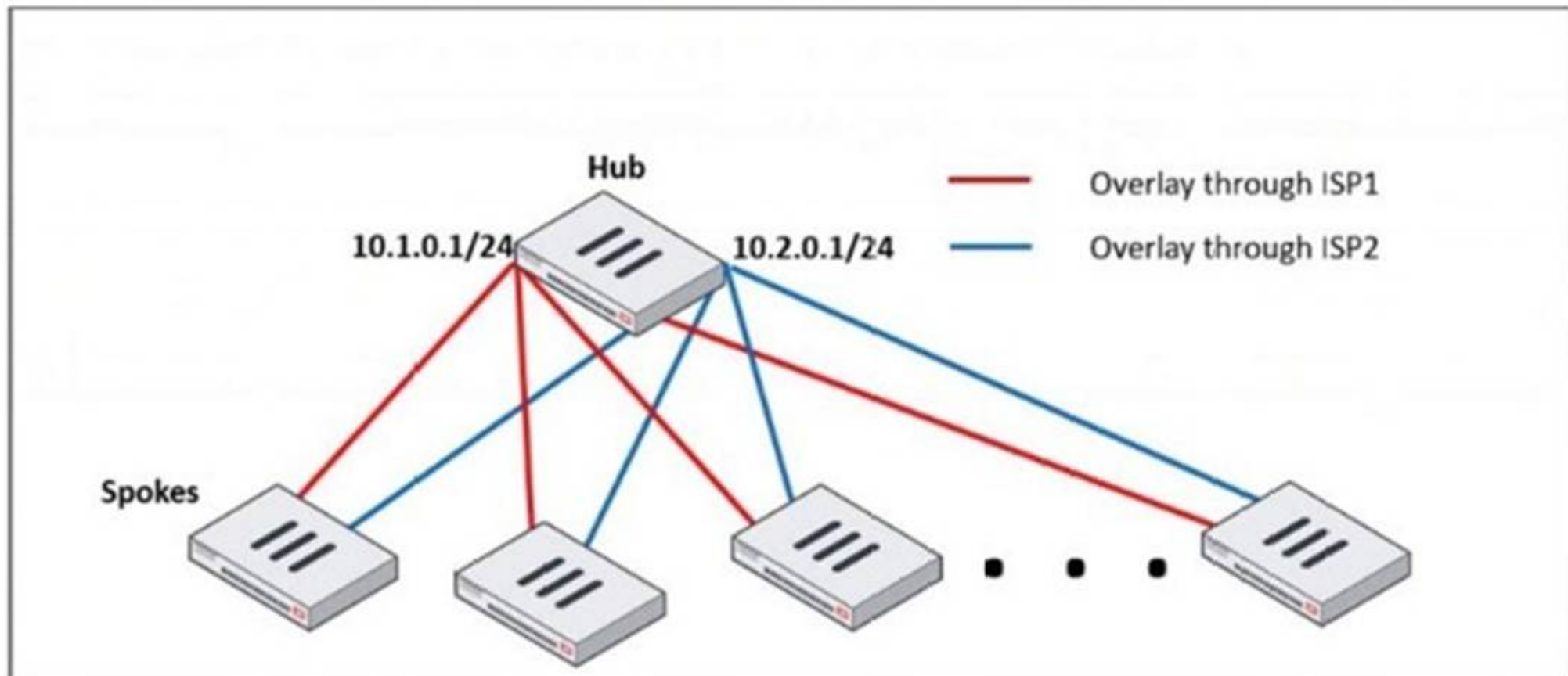
Exam Questions FCSS_EFW_AD-7.6

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

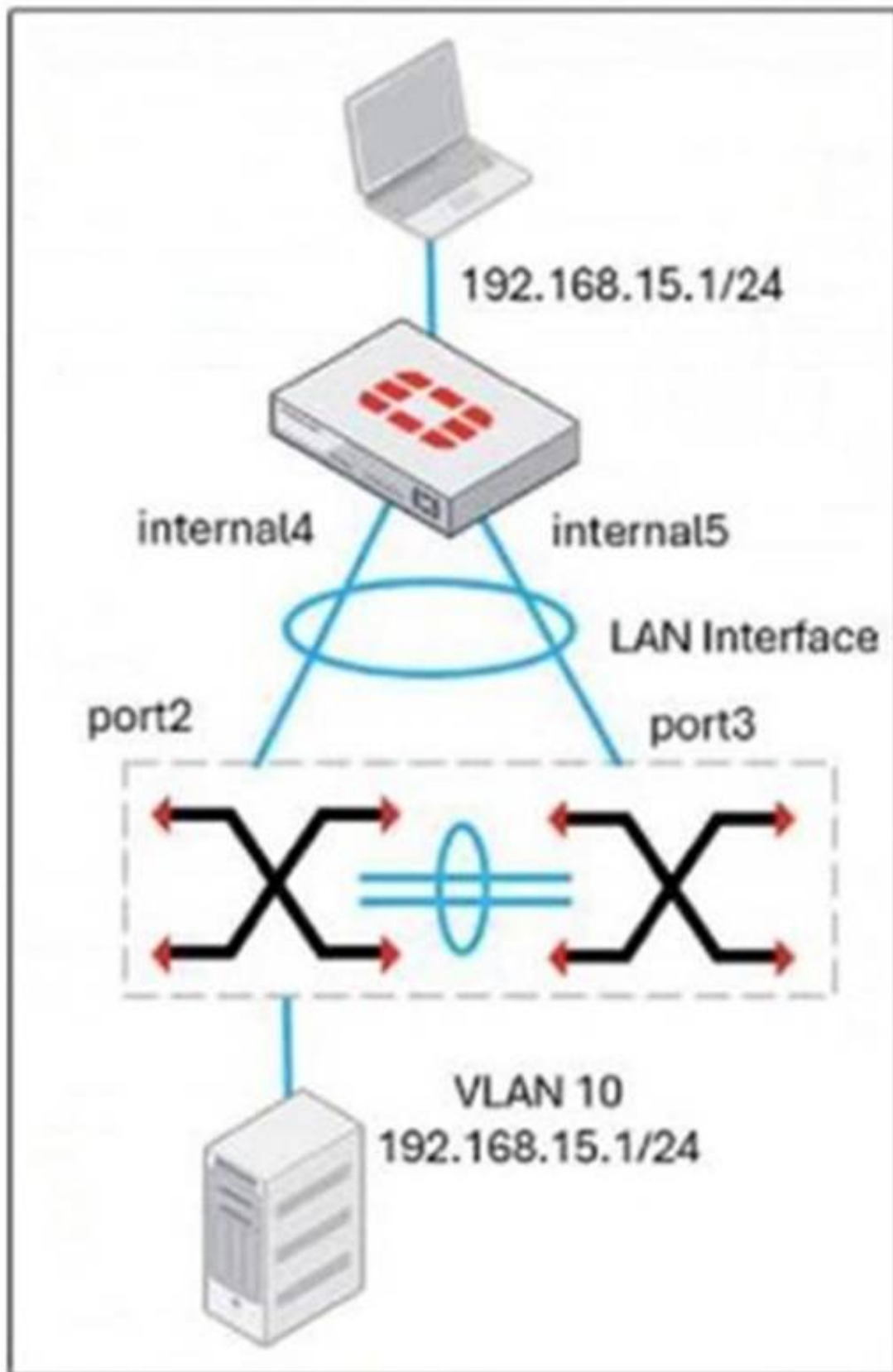
The IT department discovered during the last network migration that all zero phase selectors in phase 2 IPsec configurations impacted network operations. What are two valid approaches to prevent this during future migrations? (Choose two.)

- 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 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

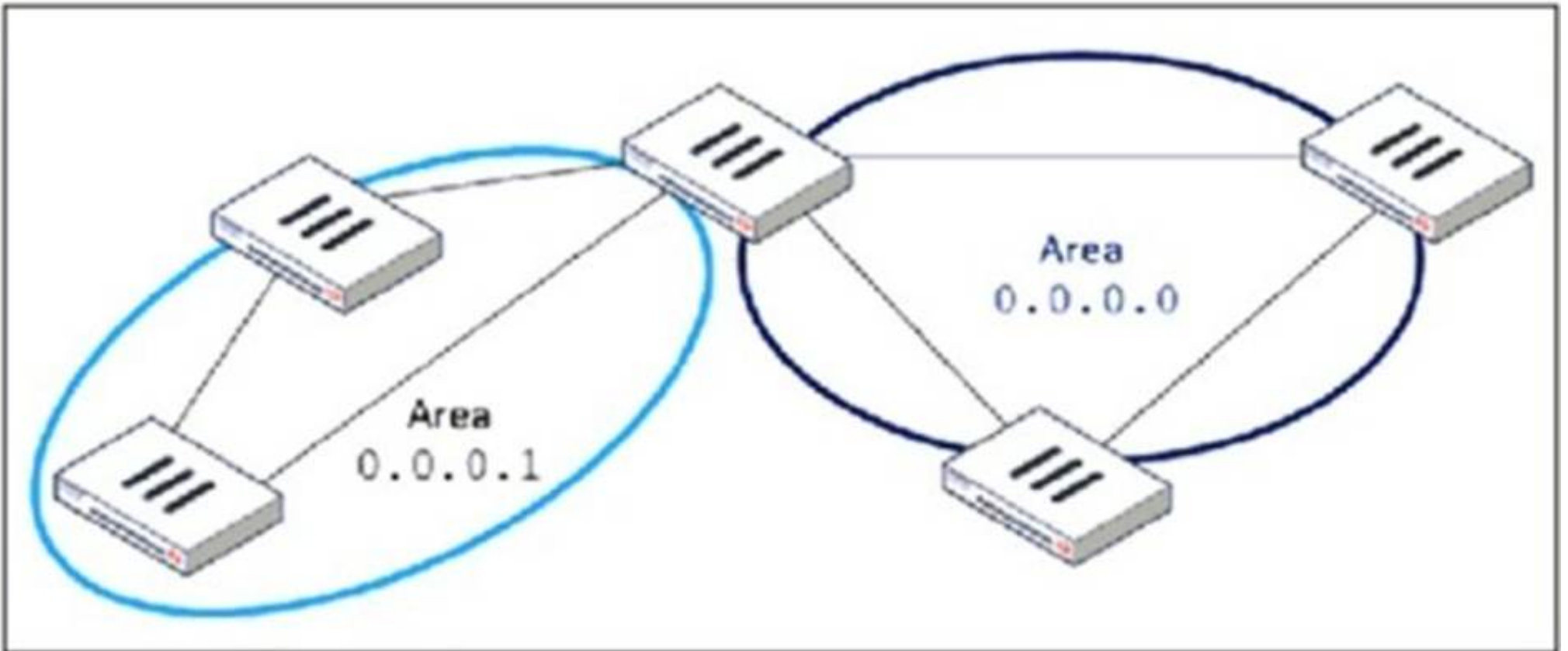
An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection. The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best available connection. 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 5

Refer to the exhibit, which shows an OSPF network.



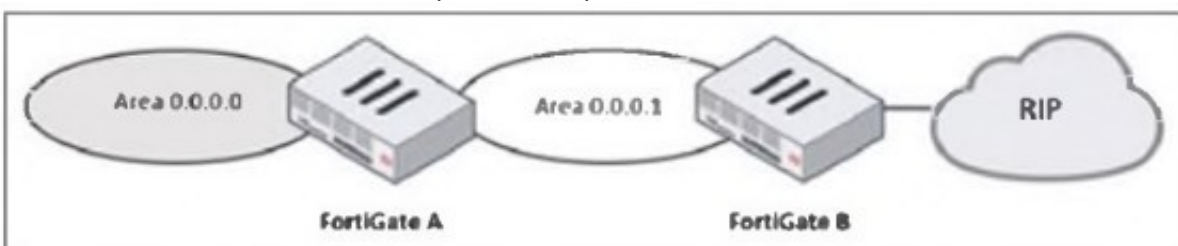
Which configuration must the administrator apply to optimize the OSPF database?

- 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 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 0.0.0.1 type to stub on FortiGate A and B.

Answer: A

NEW QUESTION 7

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
    
```

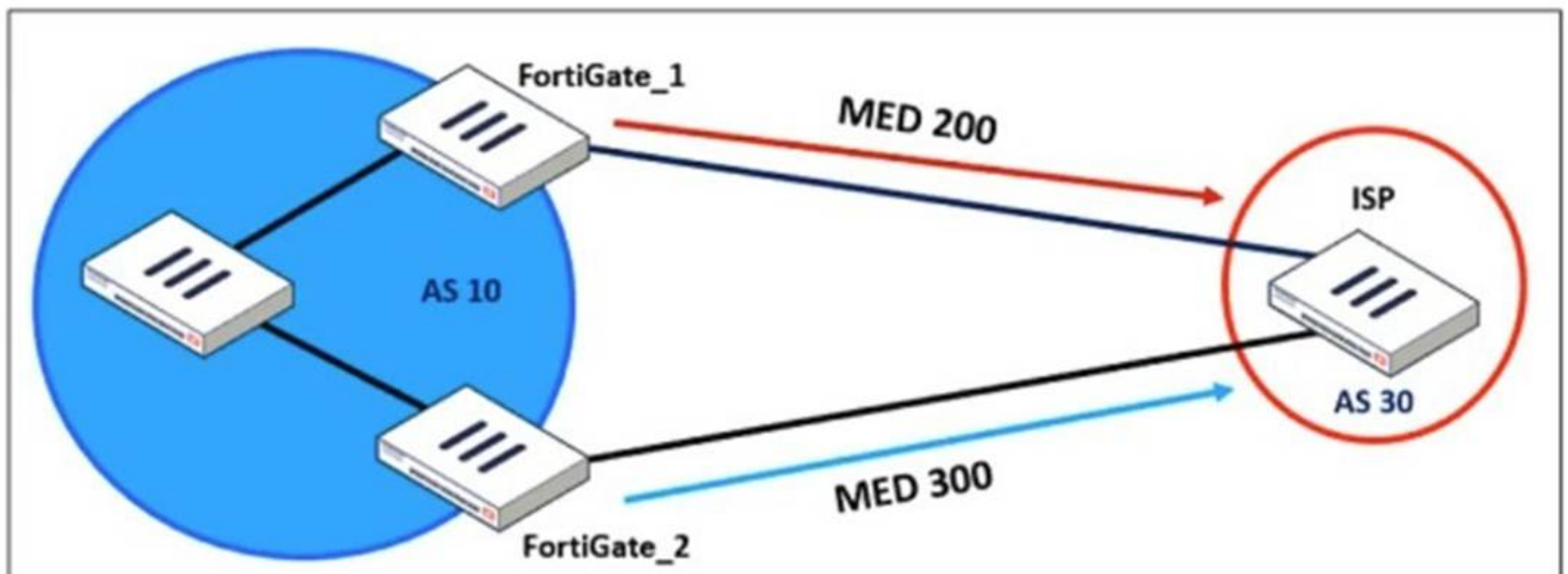
The administrator has configured BGP on FortiGate. The status of this new BGP configuration is shown in the exhibit. What configuration must the administrator consider next?

- 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 8

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 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 exhibits.

Root FortiGate - System Administrator configuration

System Administrator 2	
admin	super_admin
AdminSSO	super_admin_readonly

Downstream FortiGate - Security Fabric settings

Security Fabric role	Standalone Serve as Fabric Root Join Existing Fabric
Allow other Security Fabric devices to join	port1 + x
Upstream FortiGate IP/FQDN	10.1.0.254
Allow downstream device REST API access	Auto Manual
SAML Single Sign-On	Advanced Options
Mode	Service Provider (SP)
Default login page	Normal Single Sign-On
Default admin profile	super_admin_readonly
Management IP/FQDN	Use WAN IP Specify
	10.1.0.100
Management port	Use Admin Port Specify
	443

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 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 11

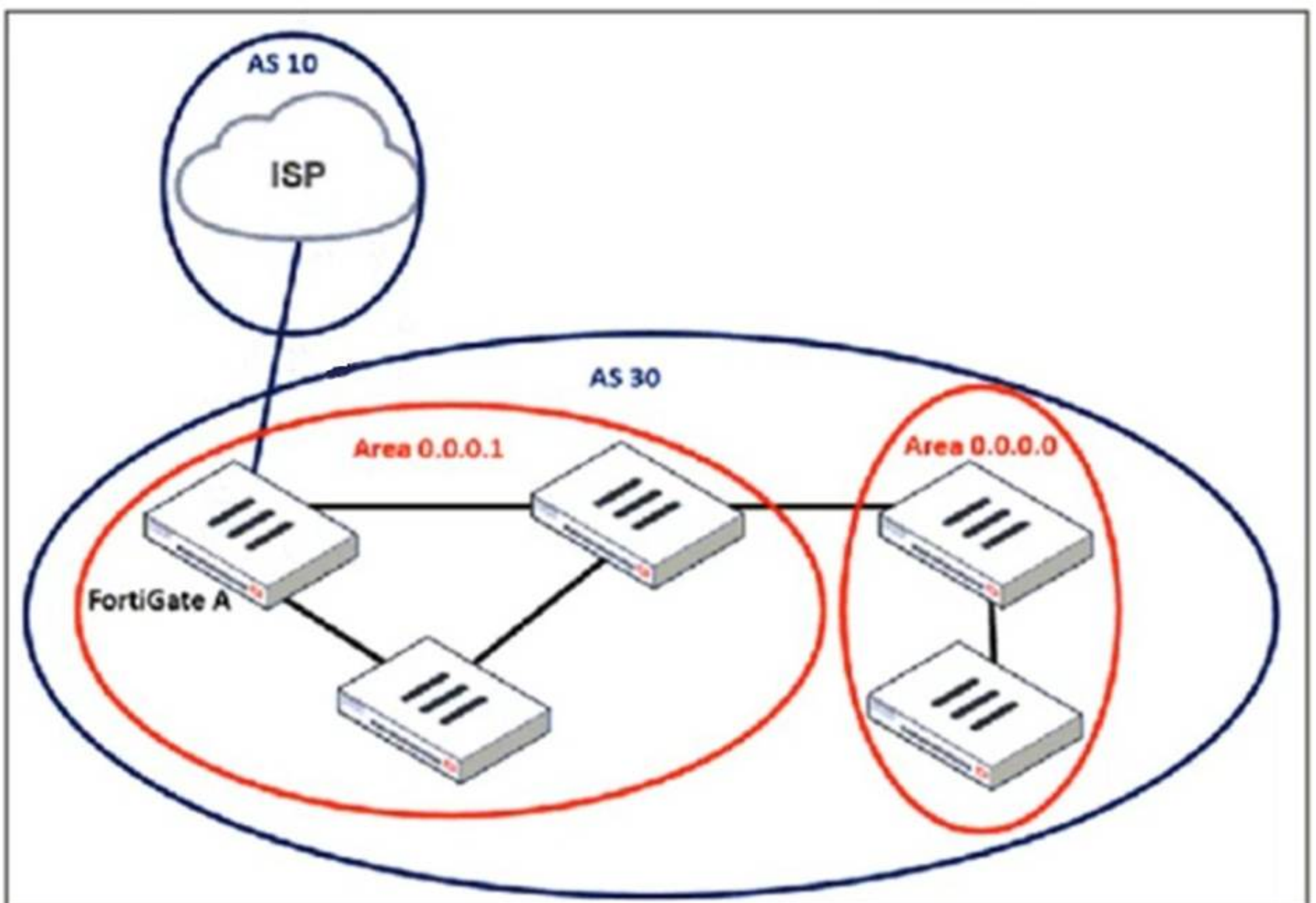
What does the command set forward-domain <domain_ID> in a transparent VDOM interface do?

- A. It configures the interface to prioritize traffic based on the domain ID, enhancing quality of service for specified VLANs.
- B. It isolates traffic within a specific VLAN by assigning a broadcast domain to an interface based on the VLAN ID.
- C. It restricts the interface to managing traffic only from the specified VLAN, effectively segregating network traffic.
- D. It assigns a unique domain ID to the interface, allowing it to operate across multiple VLANs within the same VDOM.

Answer: B

NEW QUESTION 12

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 15

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						
☐	Name	Type	Assigned to Device/Group		Variables	
Pre-Run CLI Template (4)						
☒	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 16

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 18

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?

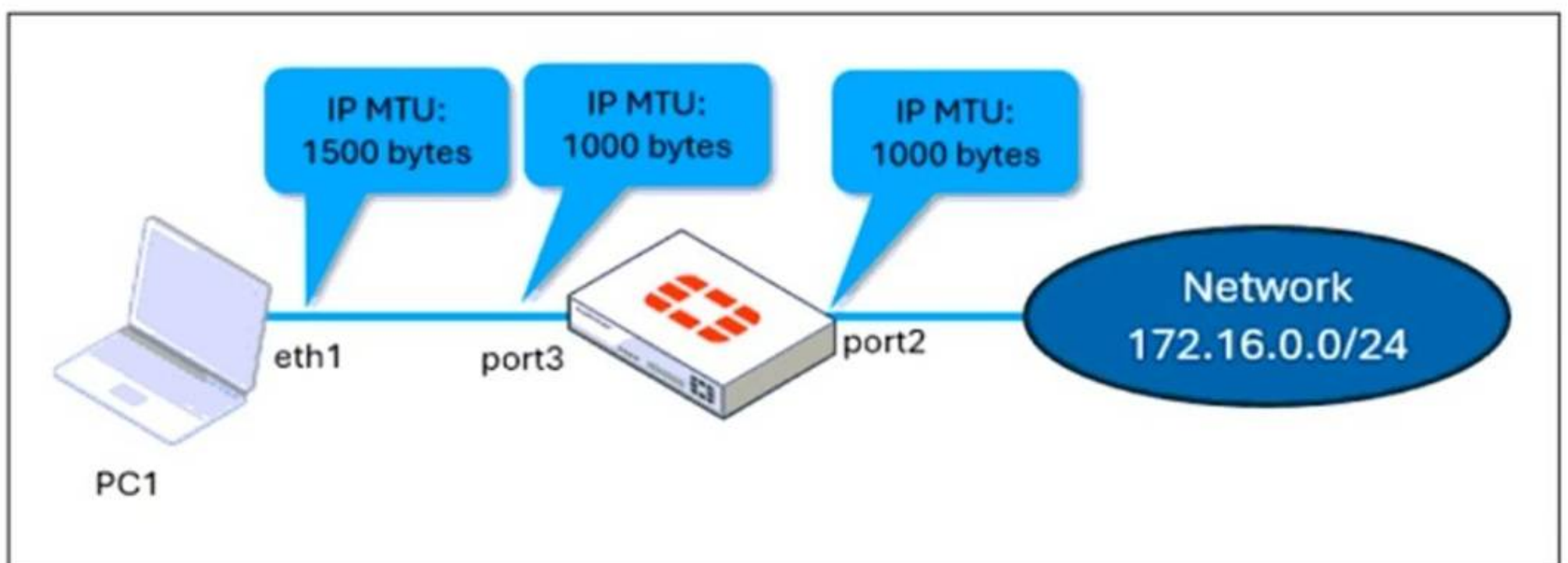
- A. This configuration is the best for networks with regular traffic intervals, providing a balance between connectivity assurance and resource utilization.
- B. Peer IDs are unencrypted and exposed, creating a security risk.
- C. FortiGate will not add a route to its routing or forwarding information 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 20

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 22

Refer to the exhibit, which shows the FortiGuard Distribution Network of a FortiGate device. FortiGuard Distribution Network on FortiGate

License Information		
Entitlement	Status	
Advanced Malware Protection	✔ Licensed (Expiration Date: 2025/11/10)	
Attack Surface Security Rating	✔ Licensed (Expiration Date: 2025/11/10)	
IoT Detection Definitions	⦿ Version 0.00000	⦿ Upgrade Database
Outbreak Package Definitions	⦿ Version 5.00036	
Security Rating & CIS Compliance	✔ Licensed (Expiration Date: 2025/11/10)	
Data Loss Prevention (DLP)	⚠ Not Licensed	
DLP Signatures	⦿ Version 0.00000	
Intrusion Prevention	✔ Licensed (Expiration Date: 2025/11/10)	
IPS Definitions	⦿ Version 28.00821	ⓘ Actions ▾
IPS Engine	⦿ Version 7.00539	
Malicious URLs	⦿ Version 1.00001	
Botnet IPs	⦿ Version 7.03758	ⓘ View List
Botnet Domains	⦿ Version 3.00847	ⓘ View List
Operational Technology (OT) Security Service	✔ Licensed (Expiration Date: 2025/11/10)	
Web Filtering	✔ Licensed (Expiration Date: 2025/11/10)	
Blocked Certificates	⦿ Version 1.00487	
DNS Filtering	✔ Licensed (Expiration Date: 2025/11/10)	
Video Filtering	✔ Licensed (Expiration Date: 2025/11/10)	
SD-WAN Network Monitor	⚠ Not Licensed	ⓘ Purchase ▾
SD-WAN Overlay as a Service	⚠ Not Licensed	ⓘ Purchase ▾

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 23

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 24

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 29

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

Configuration Revision History					
View Config View Install Log Revision Diff Retrieve Config More Search...					
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 31

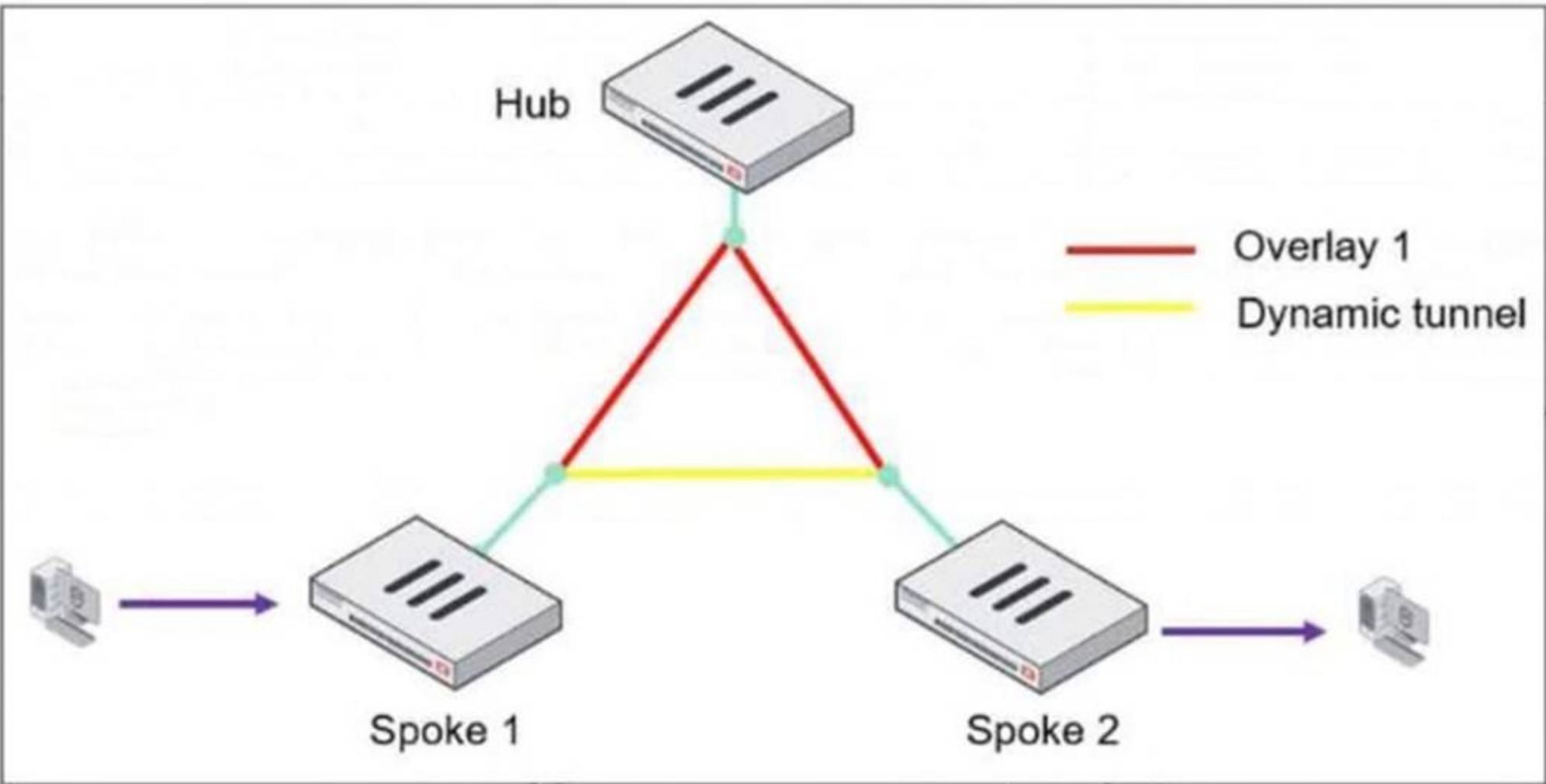
A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices. Which three approaches can the company take to successfully 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 34

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 38

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 42

.....

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](#)