Fortinet

Exam Questions FCSS_EFW_AD-7.4

FCSS - Enterprise Firewall 7.4 Administrator

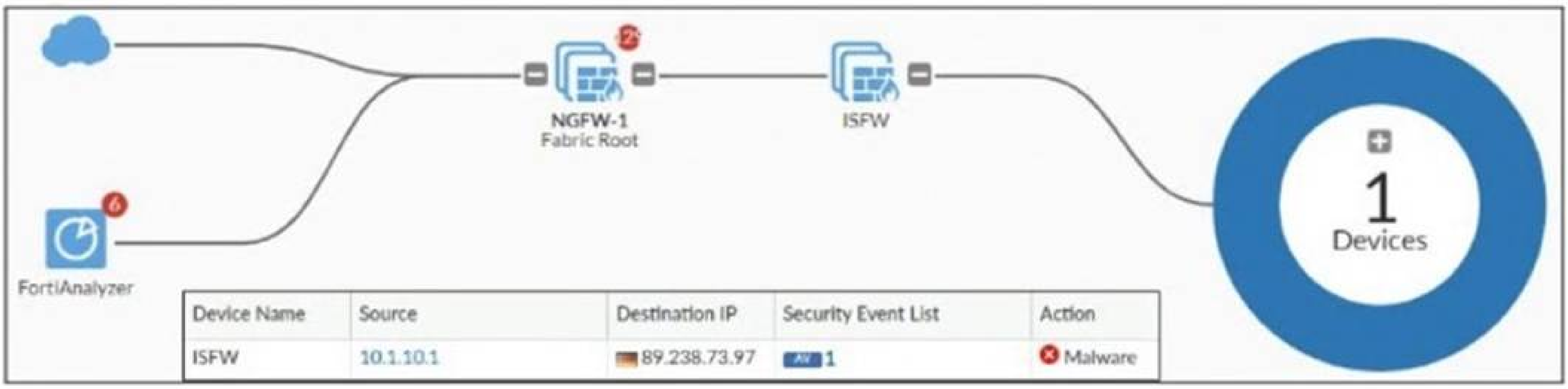
NEW QUESTION 1
An administrator is setting up an ADVPN configuration and wants to ensure that peer IDs are not exposed during VPN establishment.
Which protocol can the administrator use to enhance security?

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

Explanation:
InADVPN (Auto-Discovery VPN) configurations, security concerns includeprotecting peer IDsduring VPN establishment. Peer IDs are exchanged in theIKE (Internet Key Exchange) negotiation phase, and their exposure could lead toprivacy risks or targeted attacks.
IKEv2 encrypts peer IDs, making itmore securecompared to IKEv1, where peer IDs can beexposed in plaintextin aggressive mode.
IKEv2 also provides better performance and flexibilitywhile supporting dynamic tunnel establishment in ADVPN.

NEW QUESTION 2
Refer to the exhibit, which shows a physical topology and a traffic log.



Device Name	Source	Destination IP	Security Event List	Action
ISFW	10.1.10.1	89.238.73.97	AV 1	Malware

The administrator is checking on FortiAnalyzer traffic from the device with IP address10.1.10.1, located behind the FortiGate ISFW device.
The firewall policy in on the ISFW device does not have UTM enabled and the administrator is surprised to see a log with the actionMalware, as shown in the exhibit.
What are the two reasons FortiAnalyzer would display this log? (Choose two.)

A. Security rating is enabled in ISFW.
B. ISFW is in a Security Fabric environment.
C. ISFW is not connected to FortiAnalyzer and must go through NGFW-1.
D. The firewall policy in NGFW-1 has UTM enabled.

Answer: BD

Explanation:
From the exhibit, ISFW is part of a Security Fabric environment with NGFW-1 as the Fabric Root. In this architecture, FortiGate devices share security intelligence, including logs and detected threats.
ISFW is in a Security Fabric environment:
Security Fabric allows devices like ISFW toreceive threat intelligencefrom NGFW-1, even if UTM is not enabled locally.
If NGFW-1 detects malware fromIP 10.1.10.1 to 89.238.73.97, this information can be
propagated to ISFW and FortiAnalyzer.
The firewall policy in NGFW-1 has UTM enabled:
Even thoughISFW does not have UTM enabled, NGFW-1 (which sits between ISFW and the external network)does have UTM enabledand is scanning traffic.
Since NGFW-1 detects malware in the session, it logs the event, which is then sent to FortiAnalyzer.

NEW QUESTION 3
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

Explanation:
ADVPN (Auto-Discovery VPN) 2.0is the optimal solution for enablingdirect spoke-to- spoke communicationwithout passing through the hub, while also allowingautomatic link selectionbased on quality metrics.
Dynamic Direct Tunnels:
ADVPN 2.0 allowsspokes to establish direct IPsec tunnels dynamicallybased on traffic patterns, reducing latency and improving performance.
Unlike static VPNs, spokes do not need to pre-configure tunnels for each other.
Automatic Link Optimization:
ADVPN 2.0monitors the qualityof multiple internet connections on each spoke.
It automatically switches to the best available connection when the primary linkdegrades or fails.
This is achieved by dynamically adjusting BGP-based routing or leveraging SD-WAN integration.

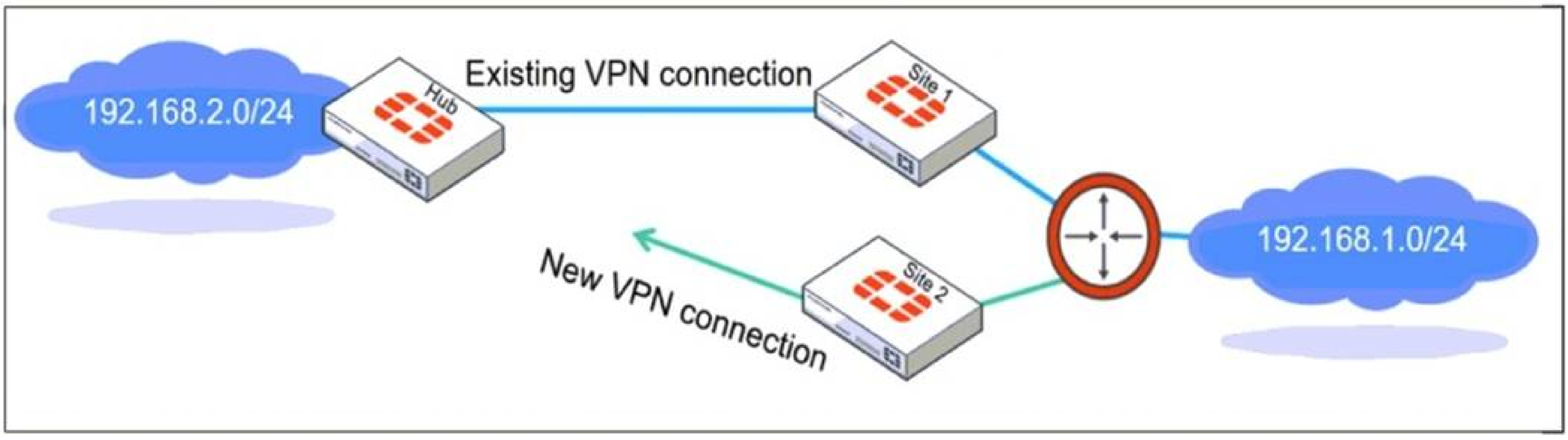
NEW QUESTION 4
What is the initial step performed by FortiGate when handling the first packets of a session?

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

Explanation:
When FortiGate processes the first packets of a session, it follows a sequence of steps to determine how the traffic should be handled before establishing a session. The initial step involves:
Access Control List (ACL) checks: Determines if the traffic should be allowed or blocked based on predefined security rules.
Hardware Packet Engine (HPE) inspections: Ensures that packet headers are valid and comply with protocol standards.
IP Integrity Header Checking: Verifies if the IP headers are intact and not malformed or spoofed.
Once these security inspections are completed and the session is validated, FortiGate then installs the session in hardware (if offloading is enabled) or processes it in software.

NEW QUESTION 5
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.



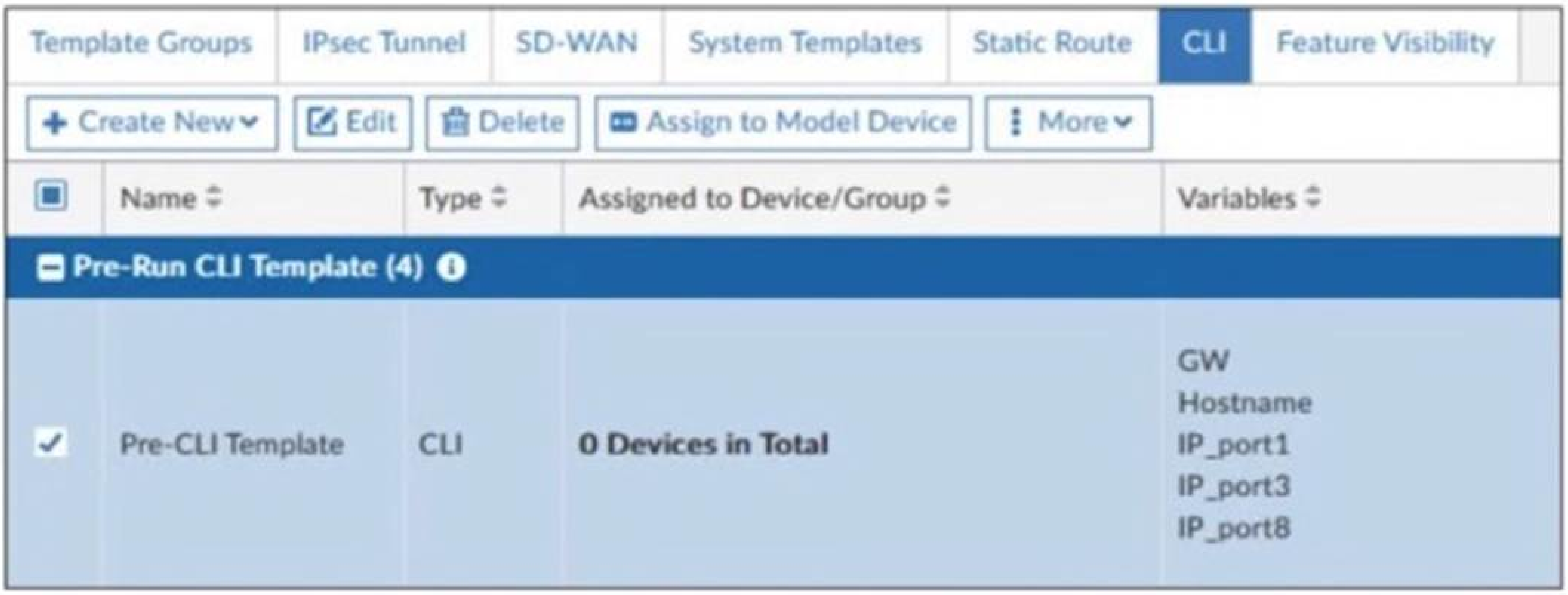
Which IPsec phase 2 configuration must an administrator make on the FortiGate hub to enable equal-cost multi-path (ECMP) routing when multiple remote sites connect with overlapping subnets?

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

Explanation:
When multiple remote sites connect to thesame hubusingoverlapping subnets, FortiGate needs to determine which route should be used for traffic forwarding. Theroute- overlapsetting in IPsec Phase 2 allows FortiGate to handle this scenario by deciding whether to keep theexisting route(use-old) or replace it with anew route(use-new).
In anECMP (Equal-Cost Multi-Path) routing setup,both routes should be retained and balanced, but FortiGate does not supportECMP directly over overlapping routesin IPsec Phase 2. Instead, an administrator must decide which connection takes precedence usingroute-overlapsettings.

NEW QUESTION 6
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.



☐	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

Explanation:
InFortiManager,pre-run CLI templatesare used inZero-Touch Provisioning (ZTP)and Low-Touch Provisioning (LTP)to configure a FortiGate devicebeforeit is fully managed by FortiManager.
These templatesapply configurationswhen a device is initially provisioned.Once the pre- run CLI template is executed, FortiManagerautomatically unassignsit from the device because it isnot meant to persistlike other policy configurations. This prevents conflicts and ensures that the FortiGate configuration isnot repeatedly appliedafter the initial setup.

NEW QUESTION 7
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

Explanation:
IKEv2 (Internet Key Exchange version 2) is an improvement over IKEv1, offering enhanced security, efficiency, and flexibility in VPN configurations.
It includes stronger Diffie-Hellman (DH) groups, such as Elliptic Curve (ECP) groups. IKEv2 supports stronger cryptographic algorithms, includingElliptic Curve Diffie- Hellman (ECDH)groups such asECP256 and ECP384, providing improved security compared to IKEv1.
It supports the extensible authentication protocol (EAP).
IKEv2 natively supports EAP authentication, which allows integration with external authentication mechanisms such asRADIUS, certificates, and smart cards. This is particularly useful forremote access VPNswhere user authentication must be flexible and secure.

NEW QUESTION 8
An administrator wants to scale the IBGP sessions and optimize the routing table in an IBGP network.
Which parameter should the administrator configure?

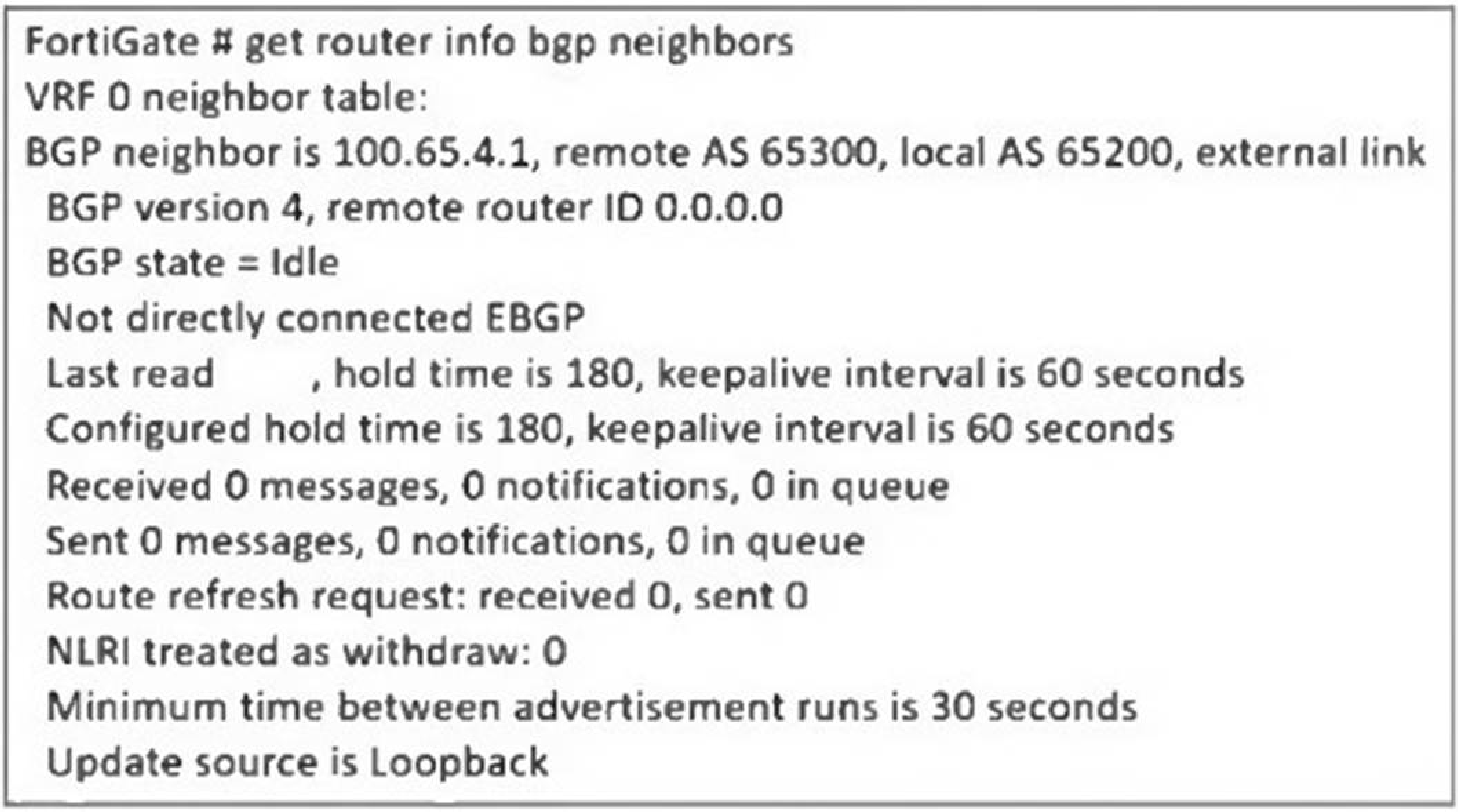
A. network-import-check
B. ibgp-enforce-multihop
C. neighbor-group
D. route-reflector-client

Answer: D

Explanation:
In anIBGP (Internal BGP) network, all routers must befully meshed, meaning every router must establish a BGP session with every other router in the sameautonomous system (AS). Thisdoes not scale wellin large networks due to the exponential increase in BGP sessions.
Tooptimize and scale IBGP,Route Reflectors (RRs)are used. ARoute Reflector (RR)reduces the number ofIBGP peer connectionsby allowing acentralized router (RR)to redistribute IBGP routes to other IBGP peers (calledclients). This eliminates the need for afull mesh, significantlyreducing BGP session overhead.
By configuring theroute-reflector-clientsetting on IBGP peers, an administrator can: Scale IBGP sessionsby reducing the number of direct BGP peer connections.
Optimize the routing tableby ensuring routes are efficiently propagated within the IBGP network.
Eliminate the need for full mesh topology, making IBGP more manageable.

NEW QUESTION 9

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

Explanation:
From theBGP neighbor status output, the key issue is thatBGP is stuck in the "Idle" state, meaning the FortiGate is unable to establish a BGP session with its peer100.65.4.1 (Remote AS 65300).
The output also shows:
"Not directly connected EBGP" This means the BGP peer is not on the same subnet, requiring multihop BGP.
"Update source is Loopback" Since a loopback interface is used, FortiGate must be configured to allow BGP neighbors over multiple hops.
To resolve this issue, the administrator must enableebgp-enforce-multihop, which allows BGP sessions to be established even when the neighbors are not directly connected.

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

Explanation:
Whenstandardizing the deployment of FortiGate devices across branchesusing FortiManager, thebest practiceis to usemetadata variables. This allows fordynamic interface configurationwhile maintaining asingle, consistent policy packagefor all branches.
Metadata variablesin FortiManager enableinterface roles and configurations to be dynamically assignedbased on the specific FortiGate device.
This ensuresscalabilityandconsistent security policy enforcementacross all branches without manually adjusting interface settings for each device.
When a new branch FortiGate is deployed, metadata variables automaticallymap to the correct physical interfaces, reducing manual configuration errors.

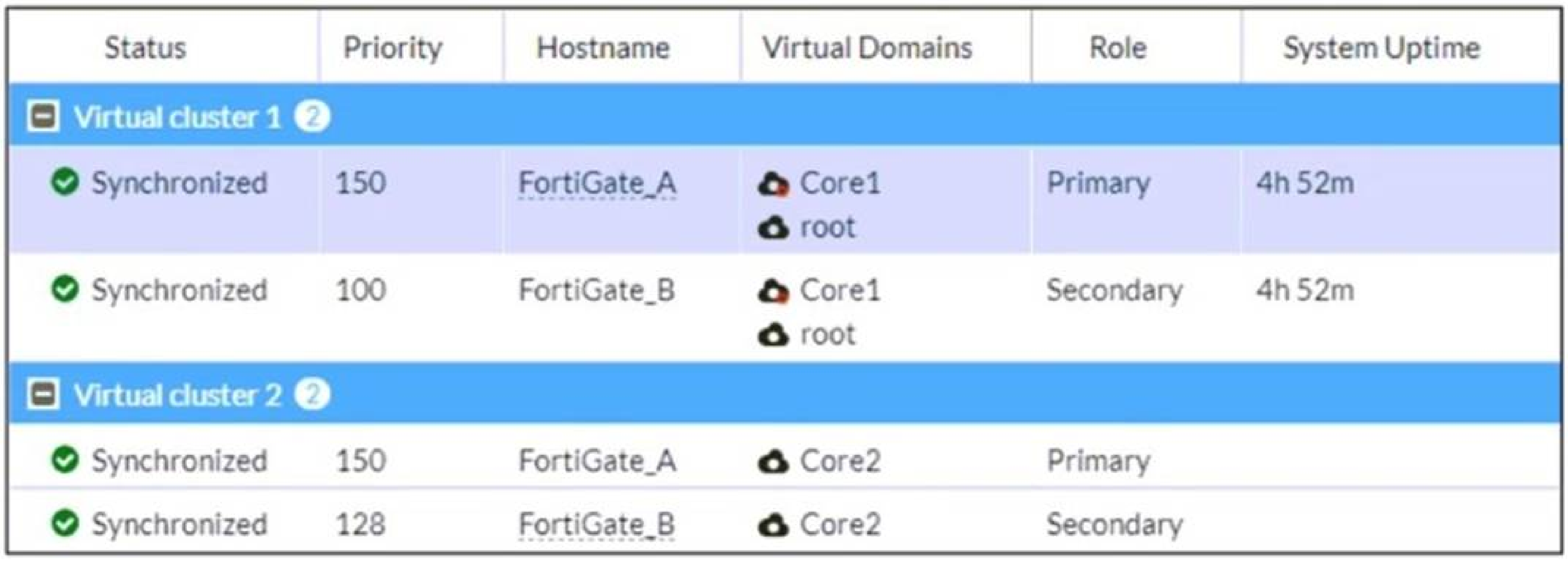
NEW QUESTION 10
What action can be taken on a FortiGate to block traffic using IPS protocol decoders, focusing on network transmission patterns and application signatures?

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

Explanation:
FortiGate'sIPS protocol decodersanalyzenetwork transmission patternsandapplication signaturesto identify and block malicious traffic.Application Controlis the feature that allows FortiGate todetect, classify, and block applicationsbased on their behavior and signatures, even when they do not rely on traditional URLs.
Application Controlworks alongsideIPS protocol decodersto inspect packet payloads and enforce security policies based on recognized application behaviors.
It enablesgranular control over non-URL-based applicationssuch asP2P traffic, VoIP, messaging apps, and other non-web-based protocolsthat IPS can identify through protocol decoders.
IPS and Application Control together can detect evasive or encrypted applications that
might bypass traditional firewall rules.

NEW QUESTION 12
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	

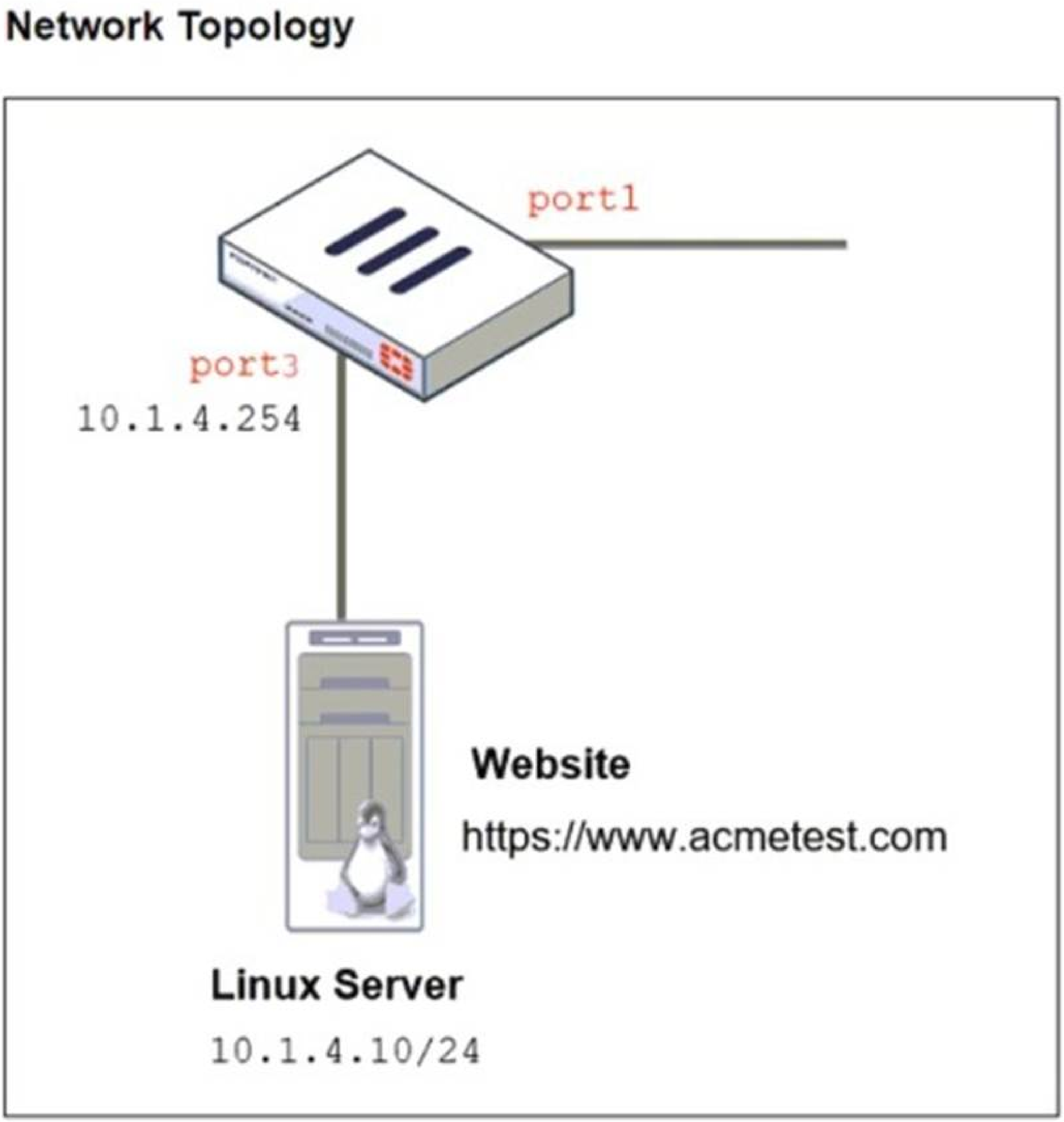
An administrator wants FortiGate_B to handle the Core2 VDOM traffic. Which modification must the administrator apply to achieve this?

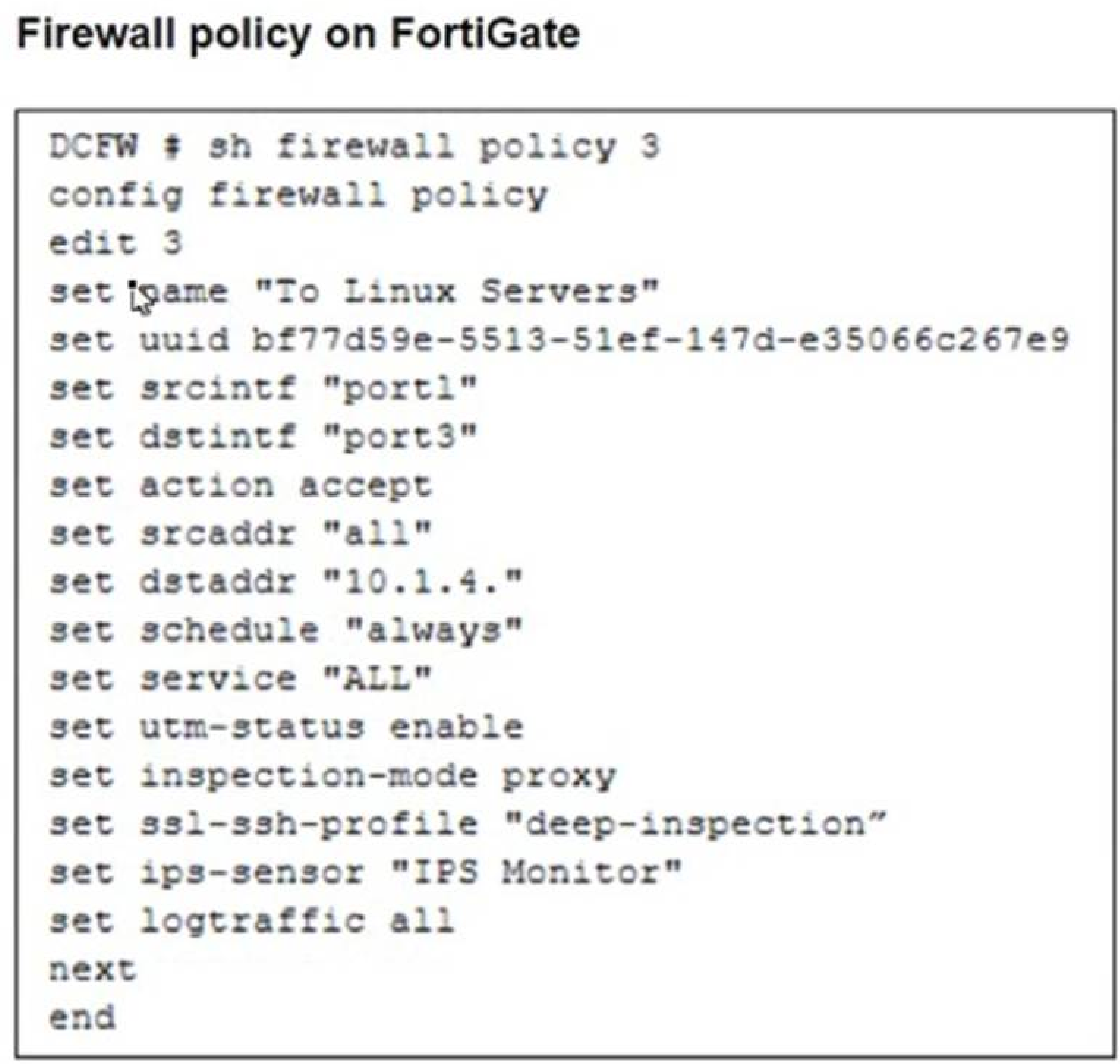
A. The administrator must disable override on FortiGate_A.
B. The administrator must change the priority from 100 to 160 for FortiGate_B.
C. The administrator must change the load balancing method on FortiGate_B.
D. The administrator must change the priority from 128 to 200 for FortiGate_B.

Answer: D

Explanation:
The exhibit shows anactive-passive HA (high availability) clusterwith two virtual clusters, where FortiGate_A is the primary device for both Core1 and Core2. If the goal is to haveFortiGate_B take over Core2 traffic, itspriority must be higherthan FortiGate_A forVirtual Cluster 2.
Currently, FortiGate_A has a priority of150for Core2, while FortiGate_B has128. Increasing FortiGate_B??s priority to 200ensures it becomes theprimary for Virtual Cluster 2, taking over the Core2 VDOM traffic while keeping Core1 traffic on FortiGate_A.
Disabling override would prevent forced failovers but wouldn??t change the role distribution.
Adjusting the load-balancing method is irrelevant in anactive-passive setup, as it only applies to active-active configurations.

NEW QUESTION 14
Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

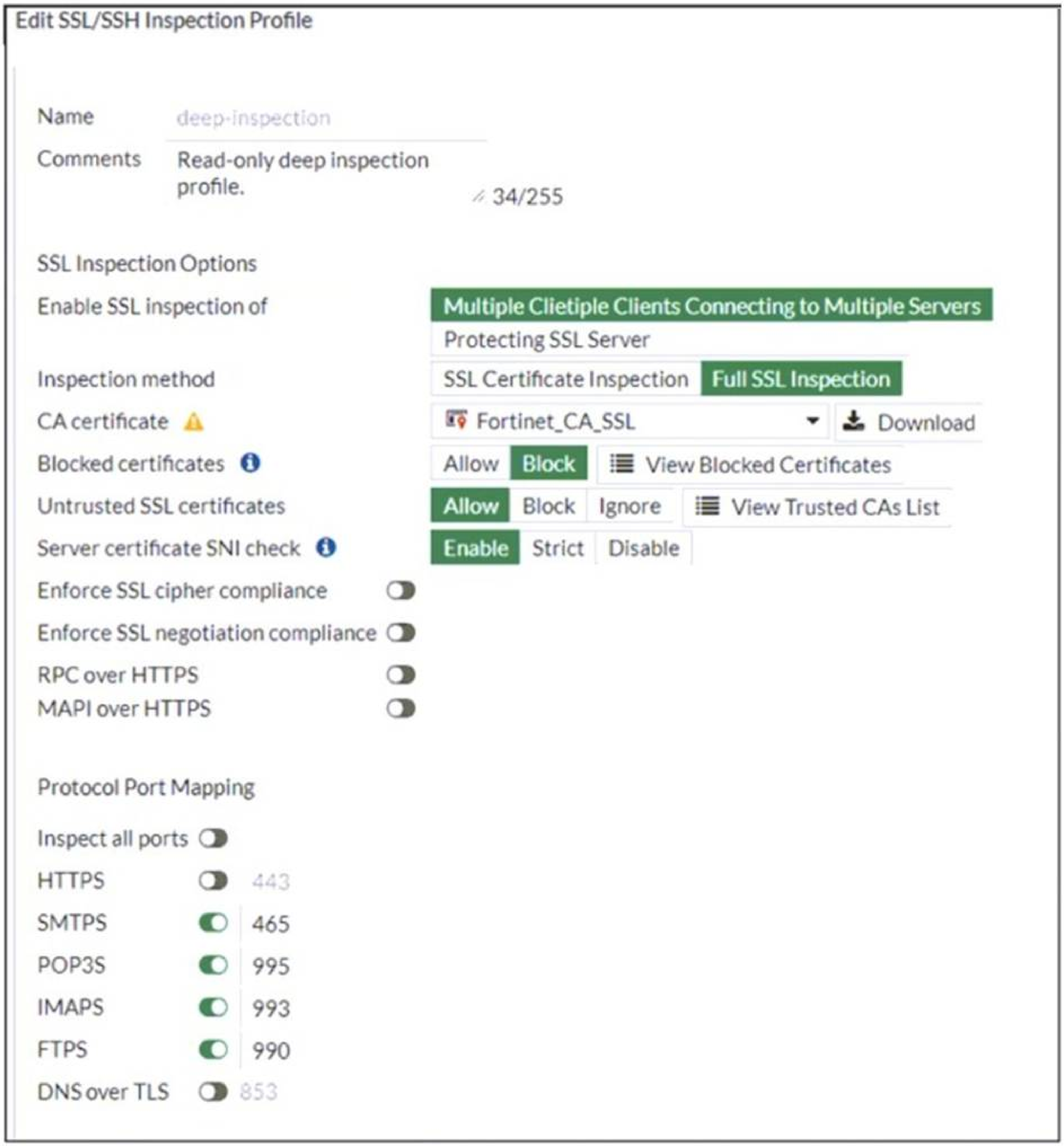

Network Topology
port1
port3
10.1.4.254
Website
https://www.acmetest.com
Linux Server
10.1.4.10/24



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: deep-inspection

Comments: Read-only deep inspection profile. 34/255

SSL Inspection Options

Enable SSL inspection of: [✓ Multiple Clietiple Clients Connecting to Multiple Servers] Protecting SSL Server

Inspection method: SSL Certificate Inspection [✓ Full SSL Inspection]

CA certificate ⚠: Fortinet_CA_SSL ▾ Download

Blocked certificates ℹ: Allow [✓ Block] View Blocked Certificates

Untrusted SSL certificates: [✓ Allow] Block Ignore View Trusted CAs List

Server certificate SNI check ℹ: [✓ Enable] Strict Disable

Enforce SSL cipher compliance ○

Enforce SSL negotiation compliance ○

RPC over HTTPS ○

MAPI over HTTPS ○

Protocol Port Mapping

Inspect all ports ○

HTTPS	○	443
SMTPS	●	465
POP3S	●	995
IMAPS	●	993
FTPS	●	990
DNS over TLS	○	853

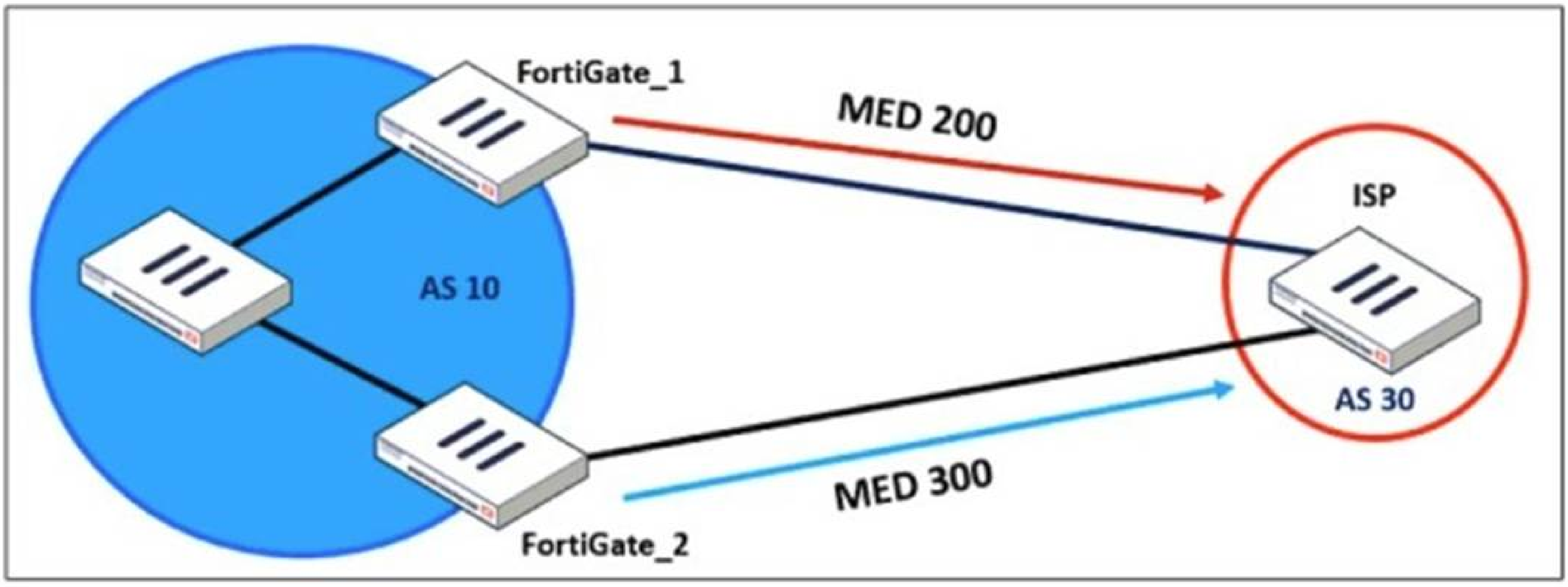
Why is FortiGate unable to detect HTTPS attacks on firewall policy ID 3 targeting the Linux server?

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

Explanation:
The FortiGateSSL/SSH inspection profileis configured forFull SSL Inspection, which is necessary to analyze encrypted HTTPS traffic. However, the firewallpolicy is protecting an SSL server (the Linux server hosting the website), and currently, the SSL/SSH profileonly applies to client-side SSL inspection.
To detect HTTPS-based attacks targeting the Linux server:
FortiGate must act as an SSL intermediaryto inspect encrypted traffic destined for the web server.
The administratormust upload the SSL certificate of the Linux web serverto FortiGate so that theserver-side SSL inspectioncan decrypt incoming HTTPS traffic before analyzing it.

NEW QUESTION 18
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?

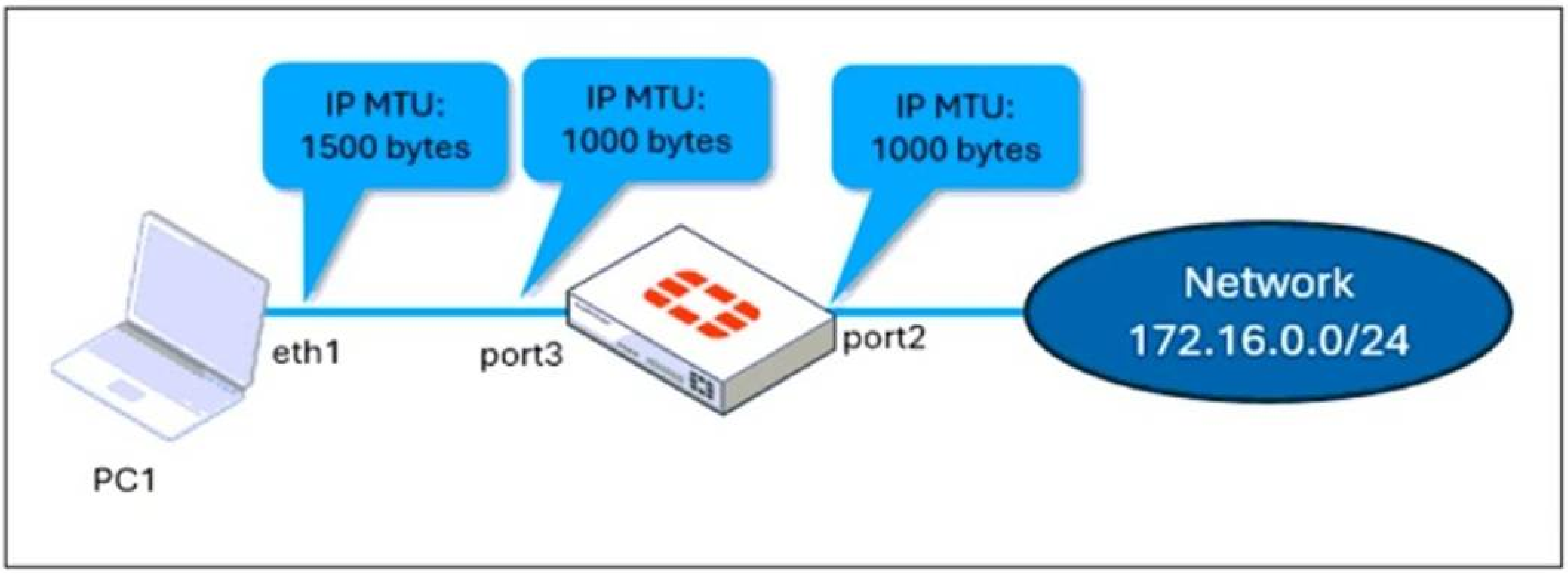
A. route-map-out
B. network-import-check
C. prefix-list-out
D. distribute-list-out

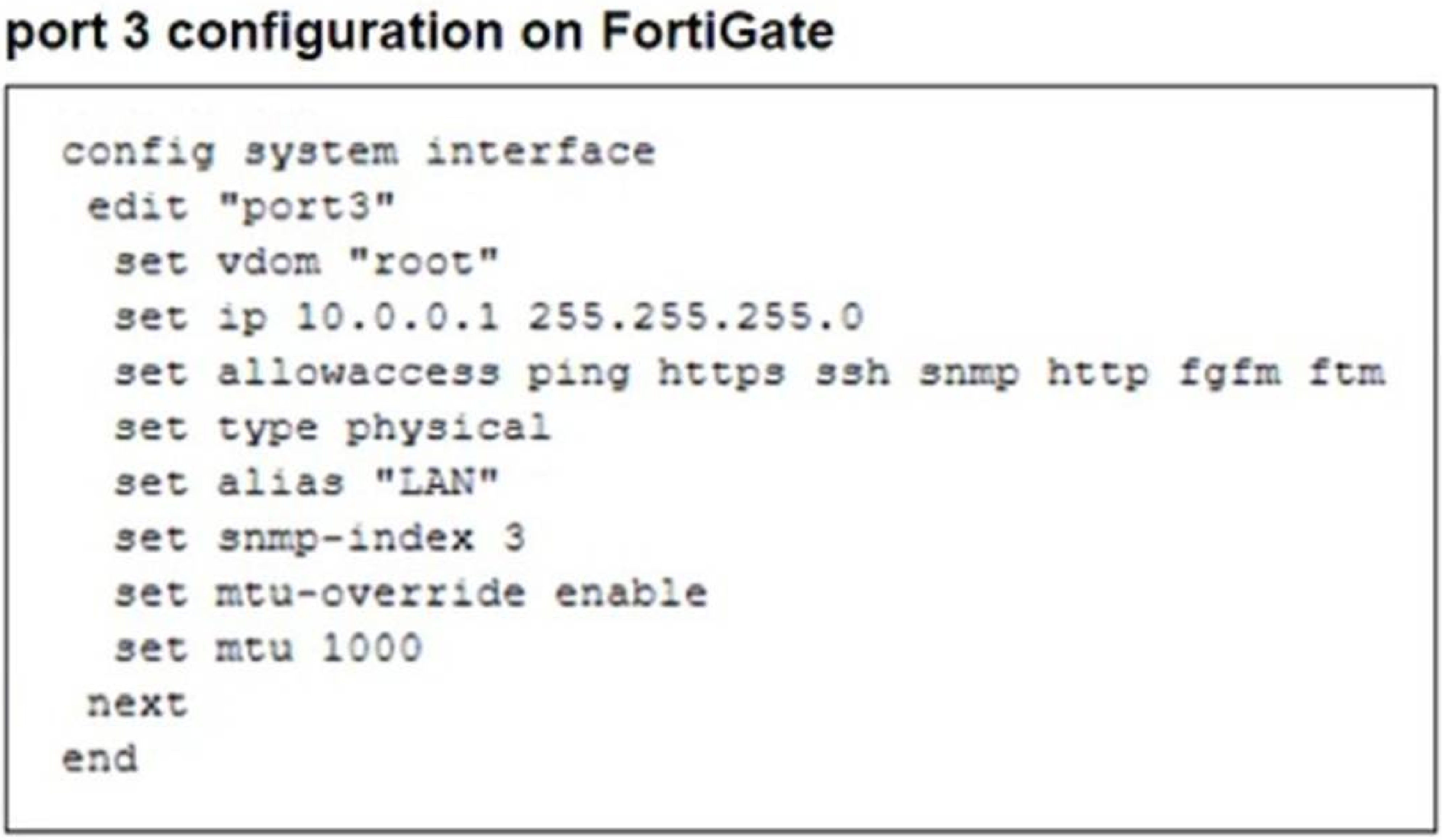
Answer: A

Explanation:
TheMulti-Exit Discriminator (MED)is aBGP attributeused to influence the preferred path for incoming traffic from an external autonomous system (AS). The diagram shows that FortiGate_1 advertisesMED 200, while FortiGate_2 advertisesMED 300, meaningthe ISP will prefer the route through FortiGate_1because alower MED is preferredin BGP.
To modify theMED valueon FortiGate_1 for routes advertised to AS 30, the administrator must configure aroute-map-out. A route map canmatch specific routesandset the MED valuebefore sending them to the BGP neighbor.

NEW QUESTION 22
Refer to the exhibits.

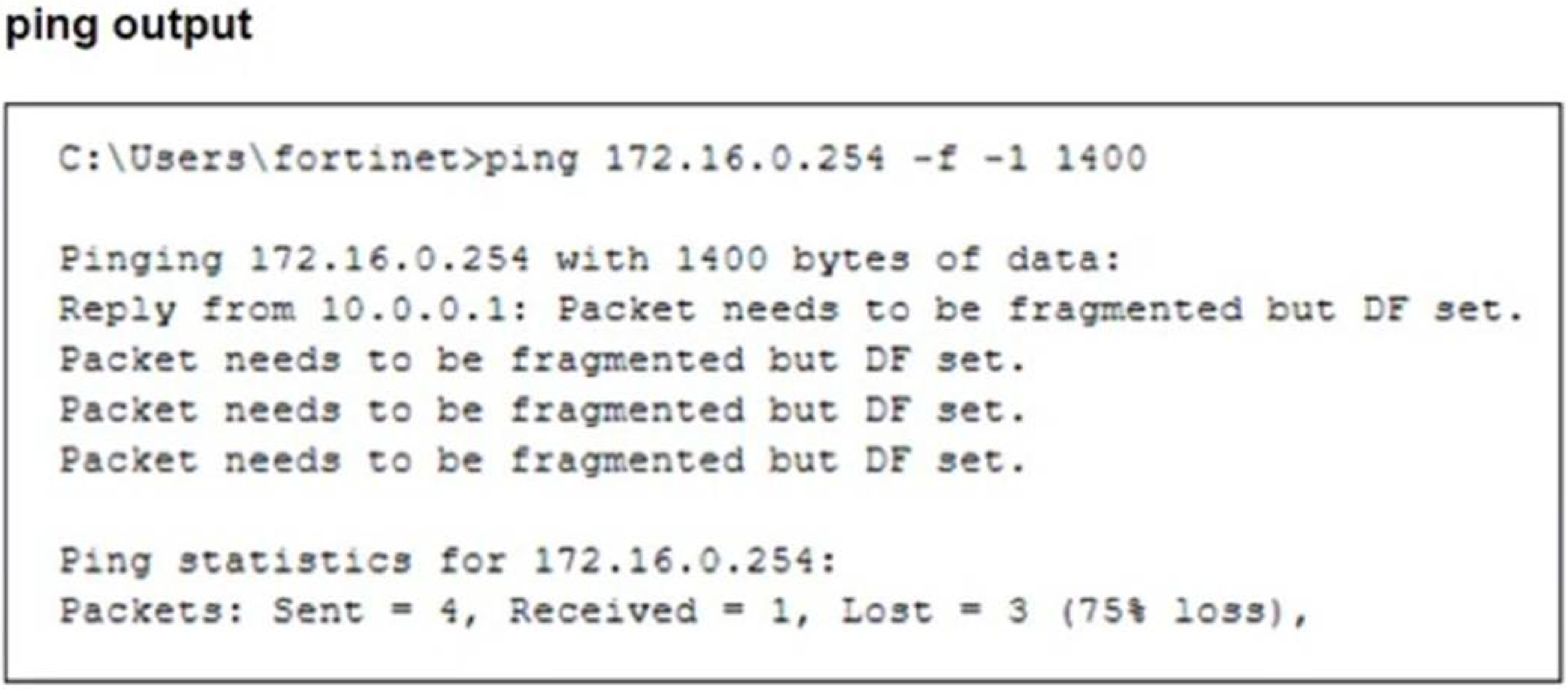
Network topology





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),
```

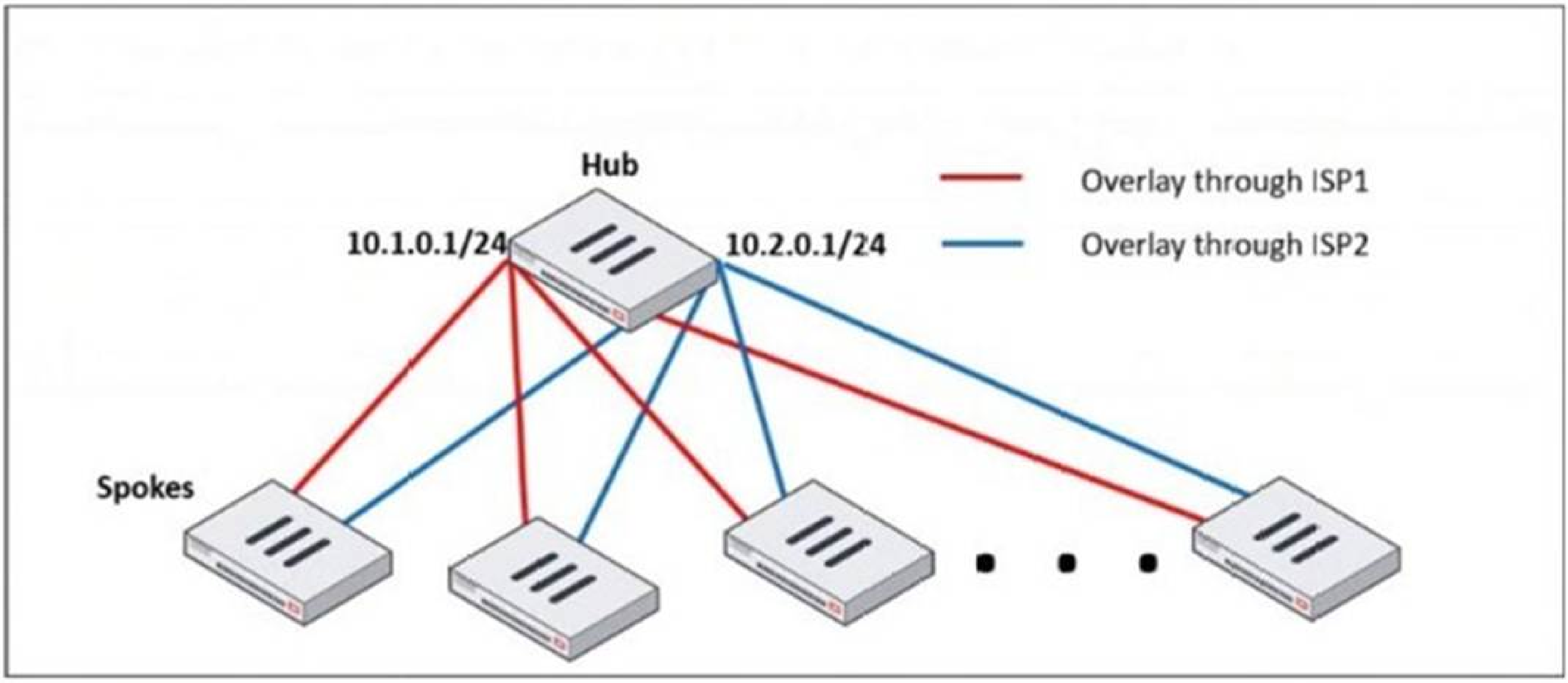
with FortiGate interfaces set to an MTU of1000bytes, and the results of PC1 pinging server172.16.0.254are shown.
Why is the user in Windows PC1 unable to ping server172.16.0.254and is seeing the message:Packet needs to be fragmented but DF set?

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

Explanation:
The issue occurs because FortiGate enforces the "do not fragment" (DF) bit in the packet, and the packet size exceeds the MTU of the network path. When the Windows PC1 (with an MTU of 1500 bytes) attempts to send a 1400-byte packet, the FortiGate interface (with an MTU of 1000 bytes) needs to fragment it. However, since the DF bit is set, FortiGate drops the packet instead of fragmenting it.
To resolve this, the user should adjust the ping packet size to fit within the path MTU. In this case, reducing the packet size to972 bytes(1000 bytes MTU minus 28 bytes for the IP and ICMP headers) should allow successful transmission.

NEW QUESTION 26
Refer to the exhibit, which shows a hub and spokes deployment.



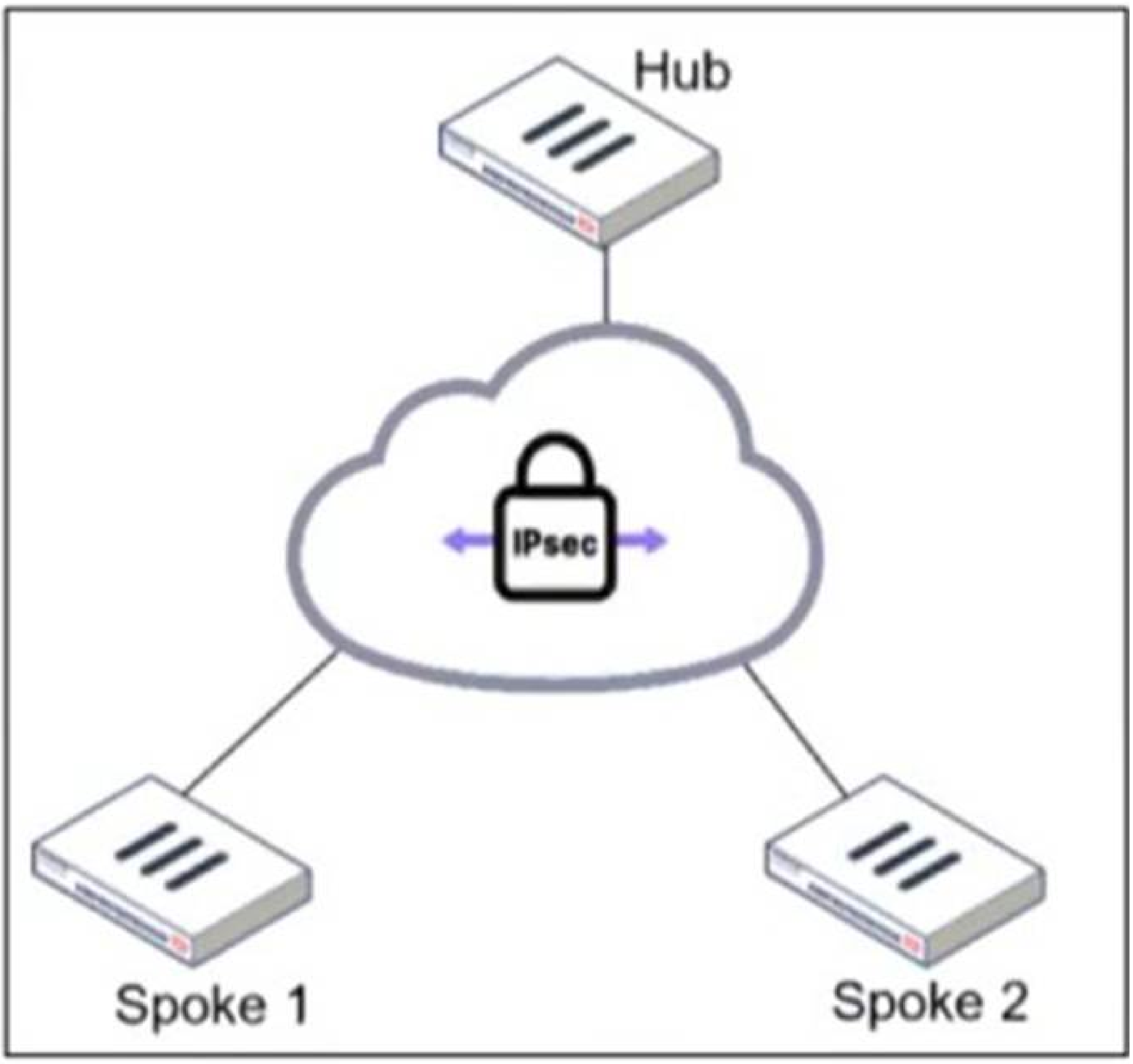
An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub.
Which two commands allow the administrator to minimize the configuration? (Choose two.)

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

Answer: AC

Explanation:
neighbor-group:
This command is used to group multipleBGP neighborswith the same configuration, reducing redundant configuration.
Instead of defining individual BGP settings for each spoke, the administrator can create a neighbor-groupand apply the same policies, reducing manual work.
neighbor-range:
This command allows the configuration ofa range of neighbor IPs dynamically, reducing the need to manually define each spoke neighbor.
It automatically addsBGP neighborsthat match a given prefix, simplifying deployment.

NEW QUESTION 29
Refer to the exhibit.



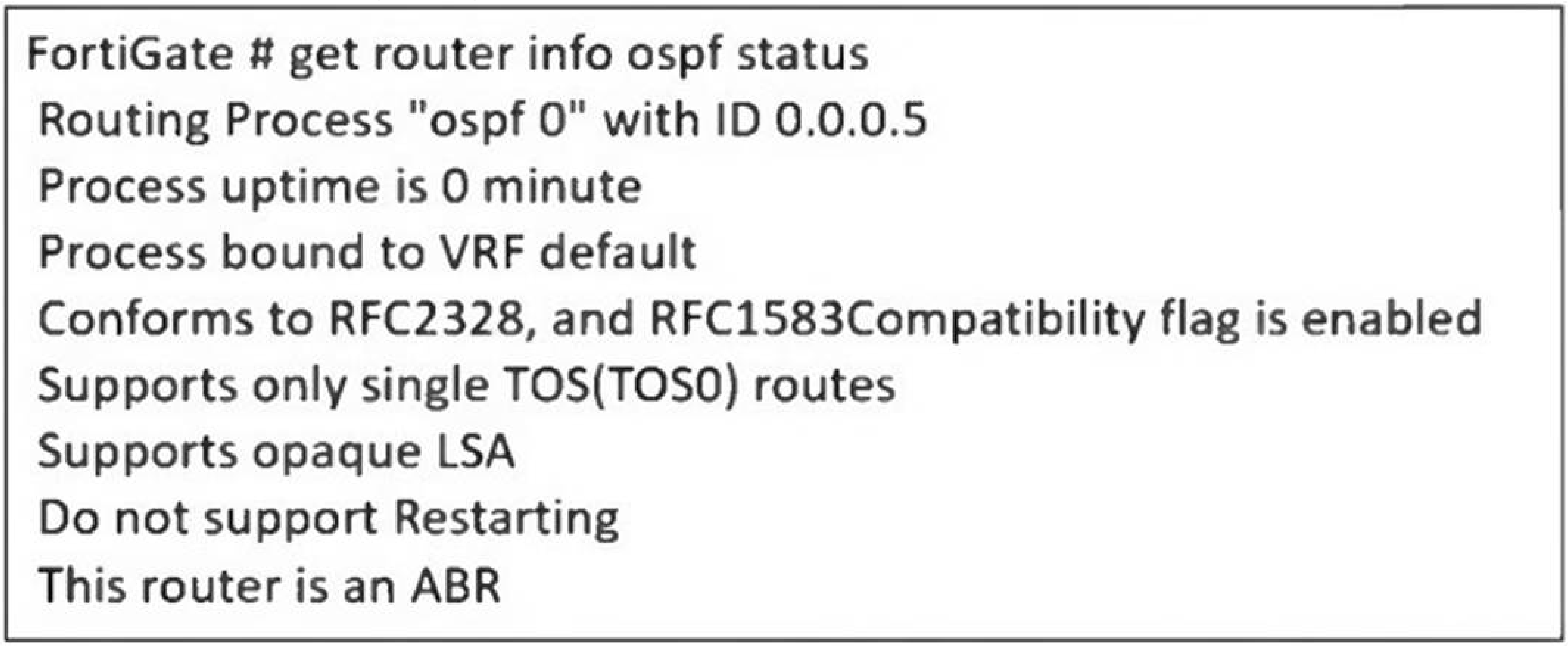
An administrator is deploying a hub and spokes network and using OSPF as dynamic protocol.
Which configuration is mandatory for neighbor adjacency?

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

Explanation:
In a hub-and-spoke topology using OSPF over IPsec VPNs, thepoint-to-multipointnetwork type is necessary to establish neighbor adjacencies between the hub and spokes. This network type ensures that OSPF operates correctly without requiring a designated router (DR) and allows dynamic routing updates across the IPsec tunnels.

NEW QUESTION 31
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

Explanation:
The output of the get router info ospf status command provides key information about the OSPF (Open Shortest Path First) configuration on the FortiGate device.
The FortiGate device is connected to multiple areas
The output states: "This router is an ABR"
ABR (Area Border Router)means the device is connected tomultiple OSPF areasand maintains routing information between them.
This confirms that the FortiGate isnot just in one area, but at leastone backbone area (Area 0) and another OSPF area.
The FortiGate device injects external routing information
The output states: "Supports opaque LSA"
Opaque LSAs(Type 9, 10, and 11) are used inOSPF extensions, including those that support external route injection.
Typically, ABRs or ASBRs (Autonomous System Boundary Routers)inject external routes, allowing routes fromother routing protocols (such as BGP or static routes) to be advertised into OSPF.

NEW QUESTION 33
......

Relate Links

Contact us