

FCSS_EFW_AD-7.6 Dumps

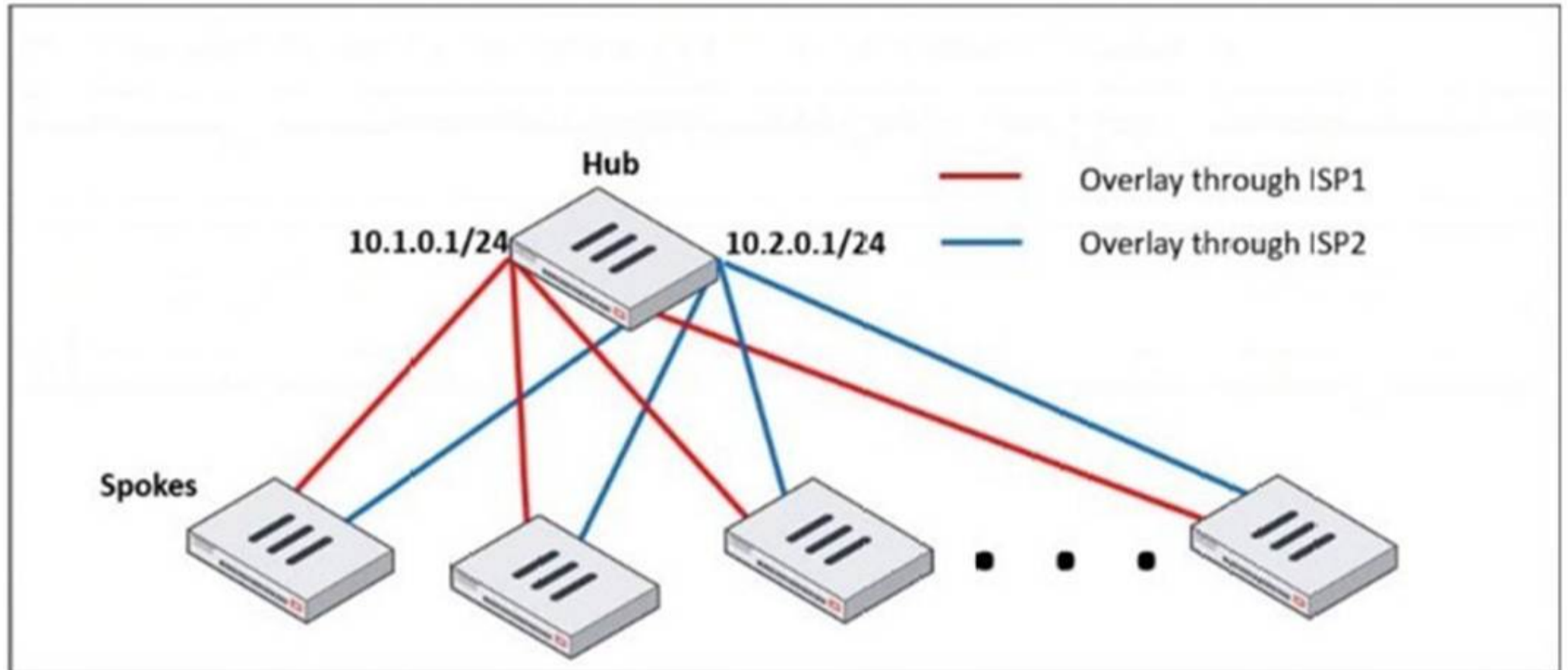
FCSS - Enterprise Firewall 7.6 Administrator

https://www.certleader.com/FCSS_EFW_AD-7.6-dumps.html



NEW QUESTION 1

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



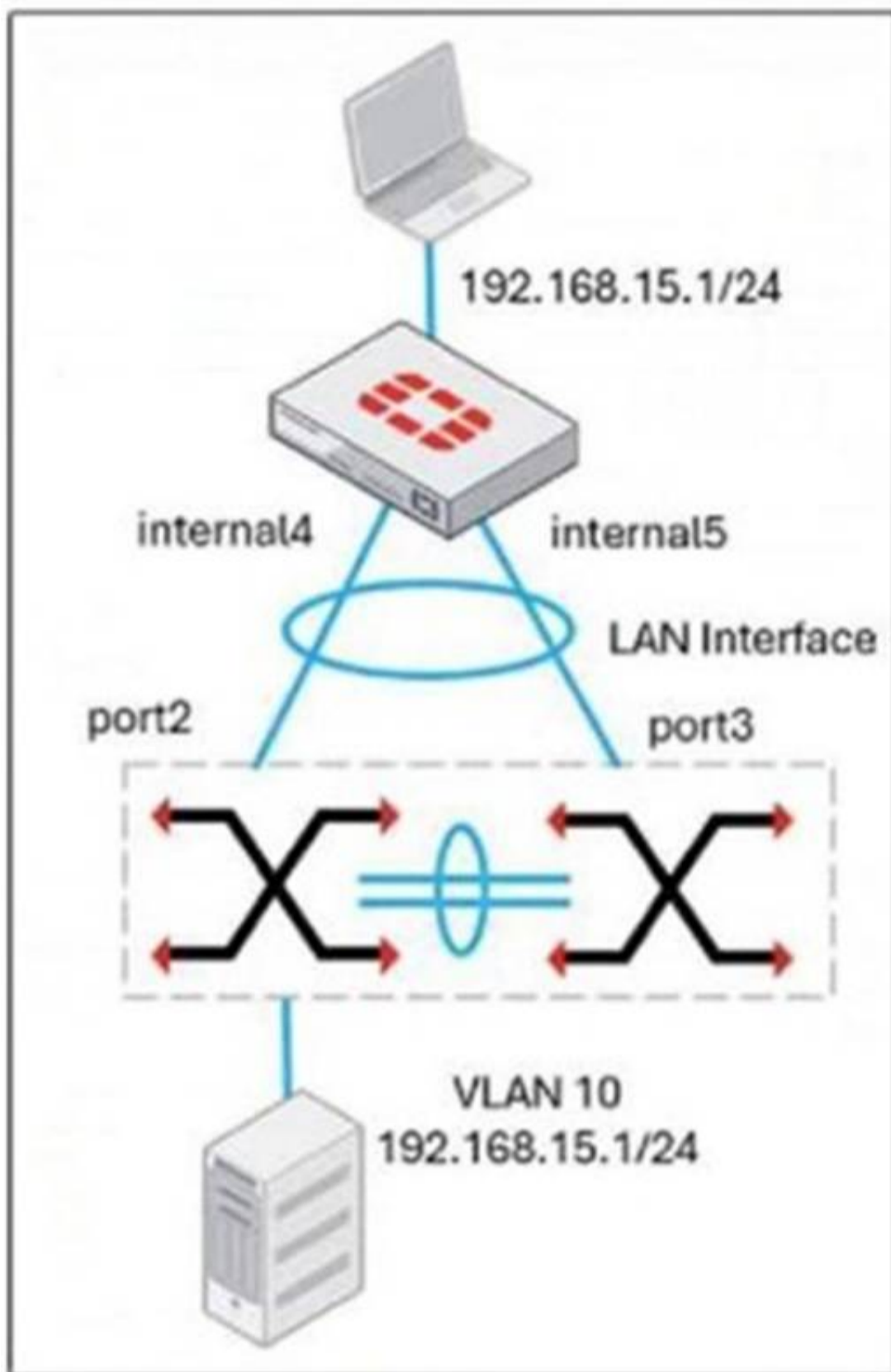
An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub. Which two commands allow the administrator to minimize the configuration? (Choose two.)

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

Answer: AC

NEW QUESTION 2

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



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

- A. You must enable STP or RSTP on FortiGate and FortiSwitch to avoid layer 2 loopbacks.
- B. The LAN interface must use a 802.3ad type interface.
- C. This connection is using a FortiLink to manage VLANs on FortiGate.
- D. FortiGate is using an SD-WAN-type interface to connect to a FortiSwitch device with MCLAG.

Answer: BC

NEW QUESTION 3

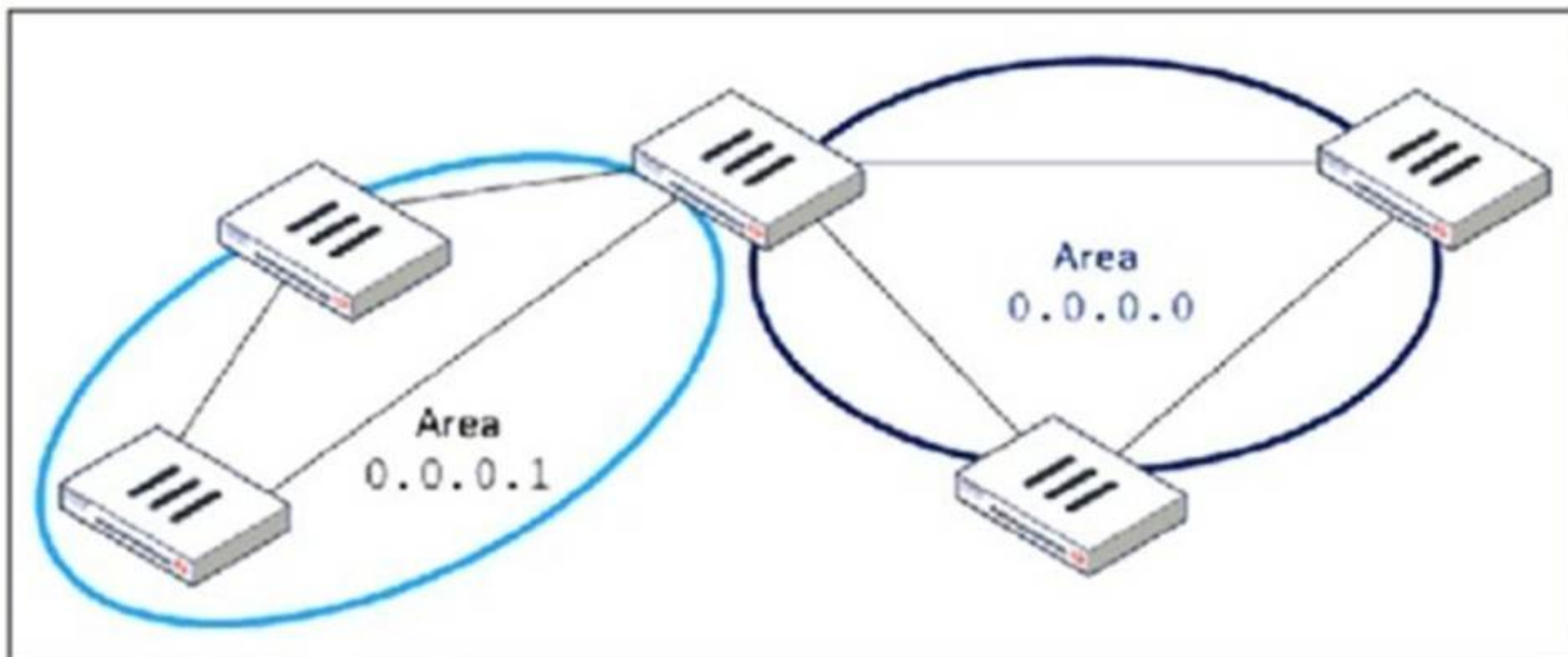
An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection. The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best available connection. 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 4

Refer to the exhibit, which shows an OSPF network.



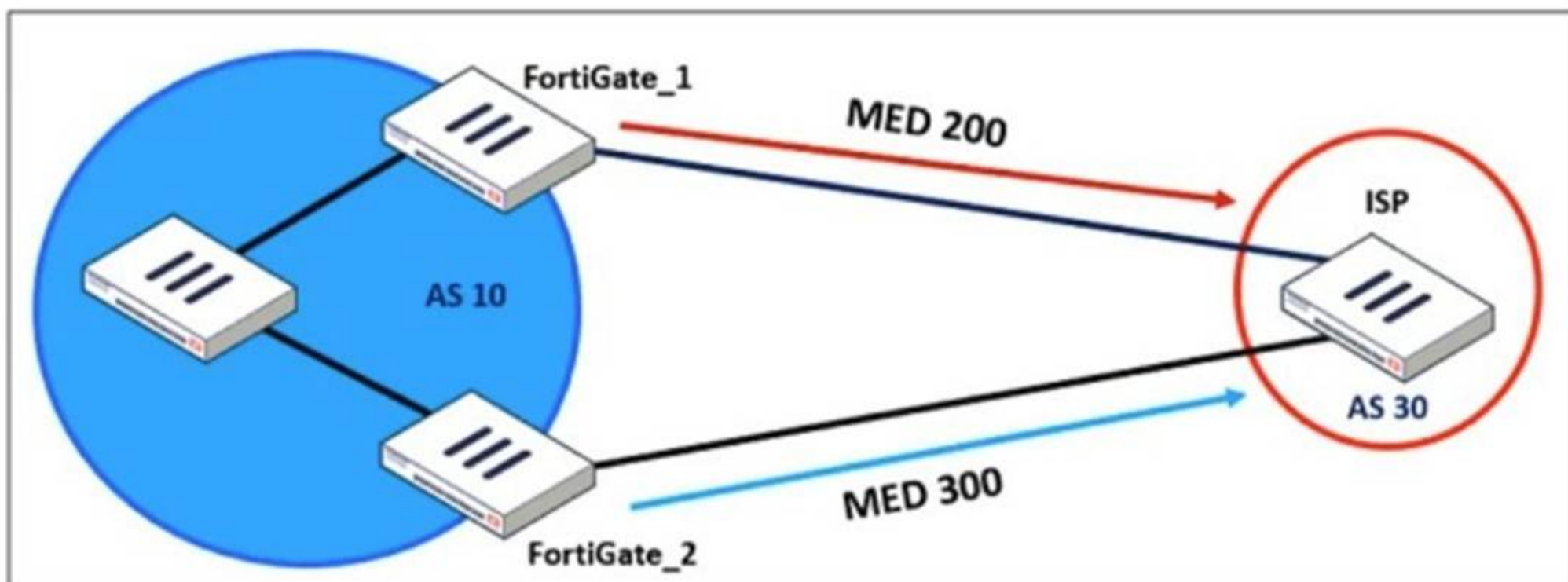
Which configuration must the administrator apply to optimize the OSPF database?

- 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 5

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 6

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 7

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?

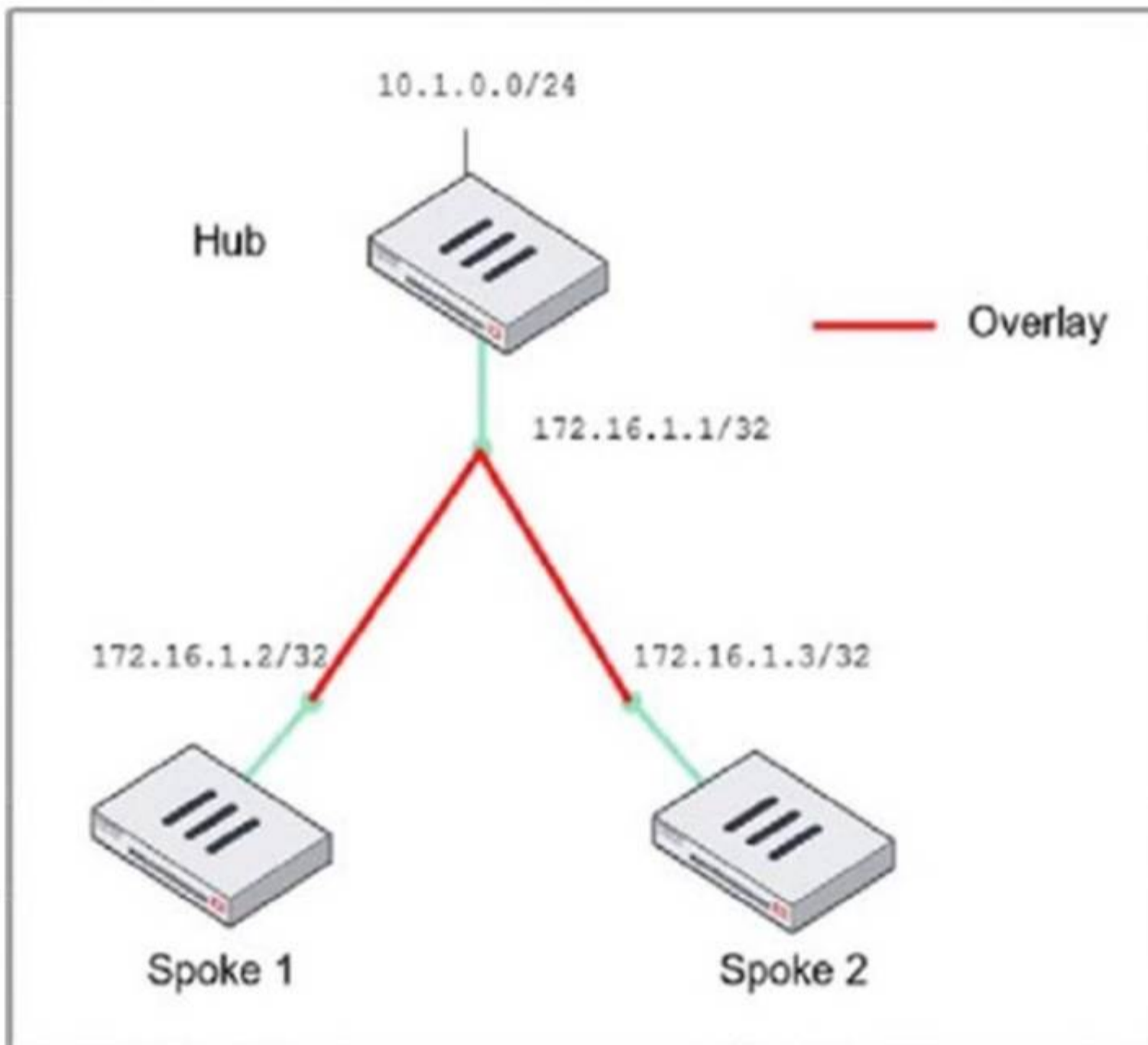
- A. Create an inline-CASB to protect against DNS exfiltration.
- B. Configure a File Filter profile to prevent DNS exfiltration.
- C. Enable DNS Filter to protect against DNS exfiltration.
- D. Use an IPS profile and DNS exfiltration-related signatures.

Answer: D

NEW QUESTION 8

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
```

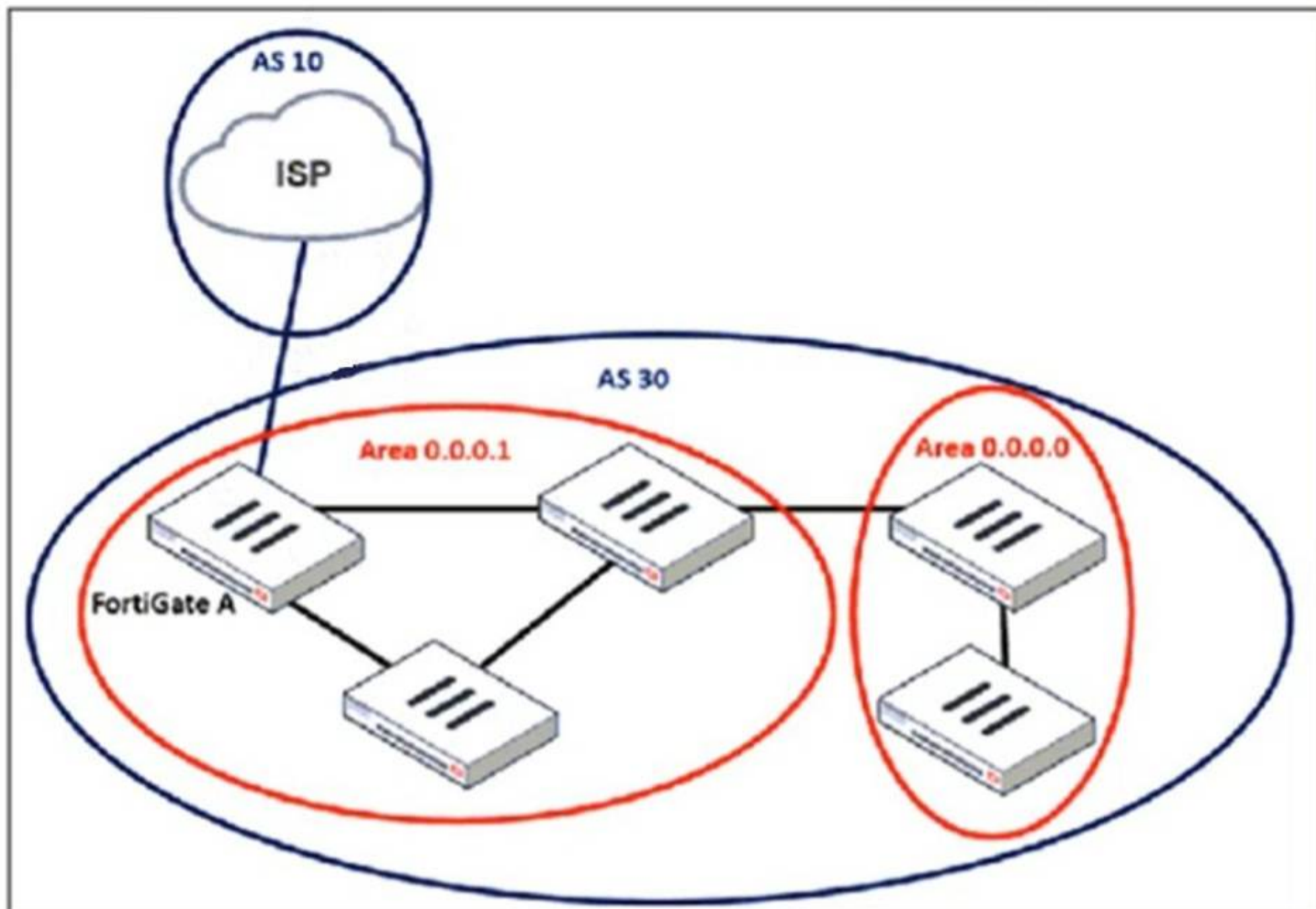
Which two parameters must an administrator configure in the config neighbor range for spokes shown in the exhibit? (Choose two.)

- 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 9

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 10

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

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

Answer: B

NEW QUESTION 10

Why does the ISDB block layers 3 and 4 of the OSI model when applying content filtering? (Choose two.)

- A. FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard.
- B. The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard.
- C. The ISDB works in proxy mode, allowing the analysis of packets in layers 3 and 4 of the OSI model.
- D. The ISDB limits access by URL and domain.

Answer: AB

NEW QUESTION 14

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 17

An administrator is designing an ADVPN network for a large enterprise with spokes that have varying numbers of internet links. They want to avoid a high number of routes and peer connections at the hub.

Which method should be used to simplify routing and peer management?

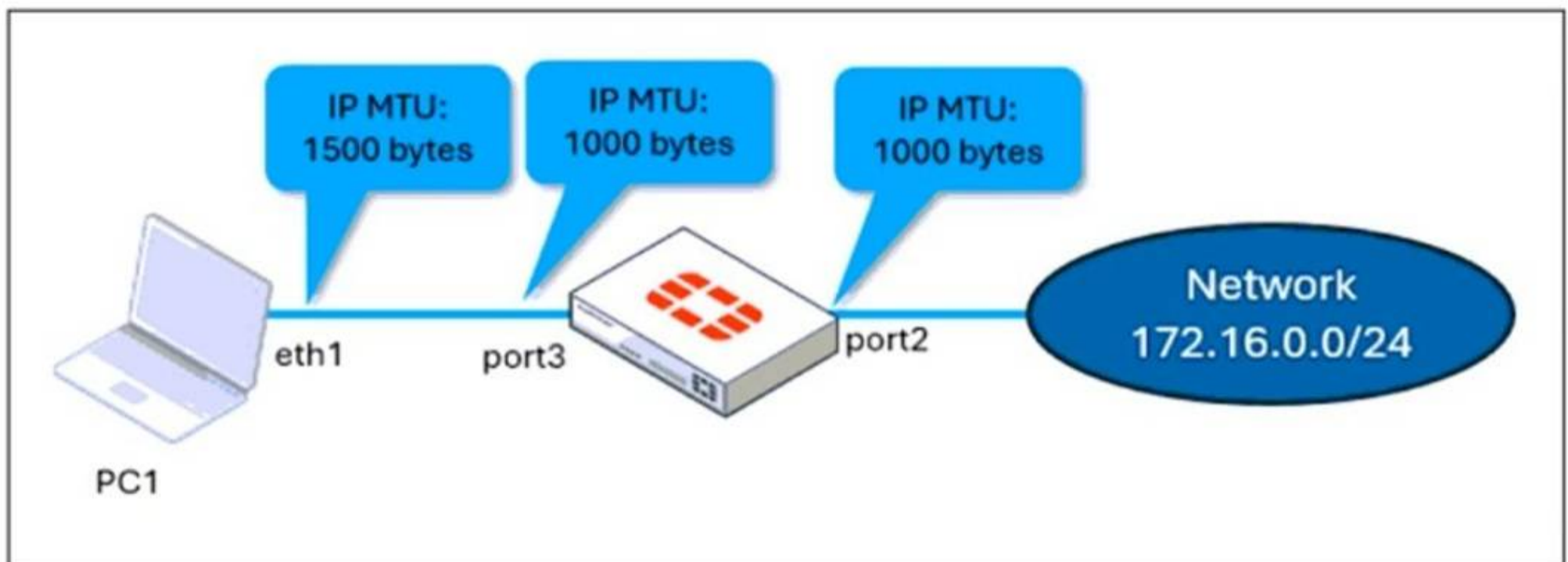
- A. Deploy a full-mesh VPN topology to eliminate hub dependency.
- B. Implement static routing over IPsec interfaces for each spoke.
- C. Use a dynamic routing protocol using loopback interfaces to streamline peers and routes.
- D. Establish a traditional hub-and-spoke VPN topology with policy routes.

Answer: C

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 23

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 25

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 26

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCSS_EFW_AD-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_EFW_AD-7.6-dumps.html