



Fortinet

Exam Questions FCSS_EFW_AD-7.6

FCSS - Enterprise Firewall 7.6 Administrator

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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.

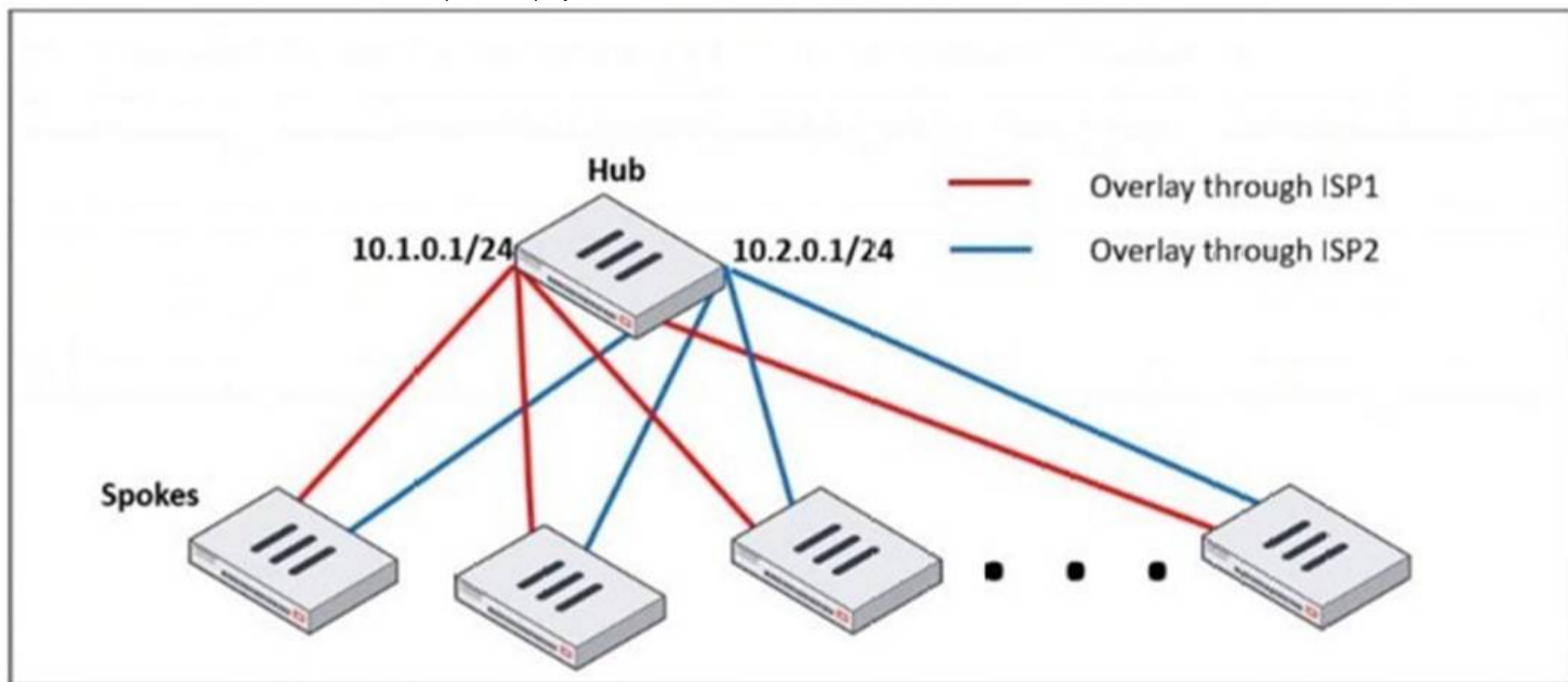
In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

- 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 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 3

Refer to the exhibit, which shows the VDOM section of a FortiGate device.

Name	Management VDOM	Type	NGFW Mode
Core1		Traffic	Profile-based
Core2		Traffic	Profile-based
root		Traffic	Profile-based

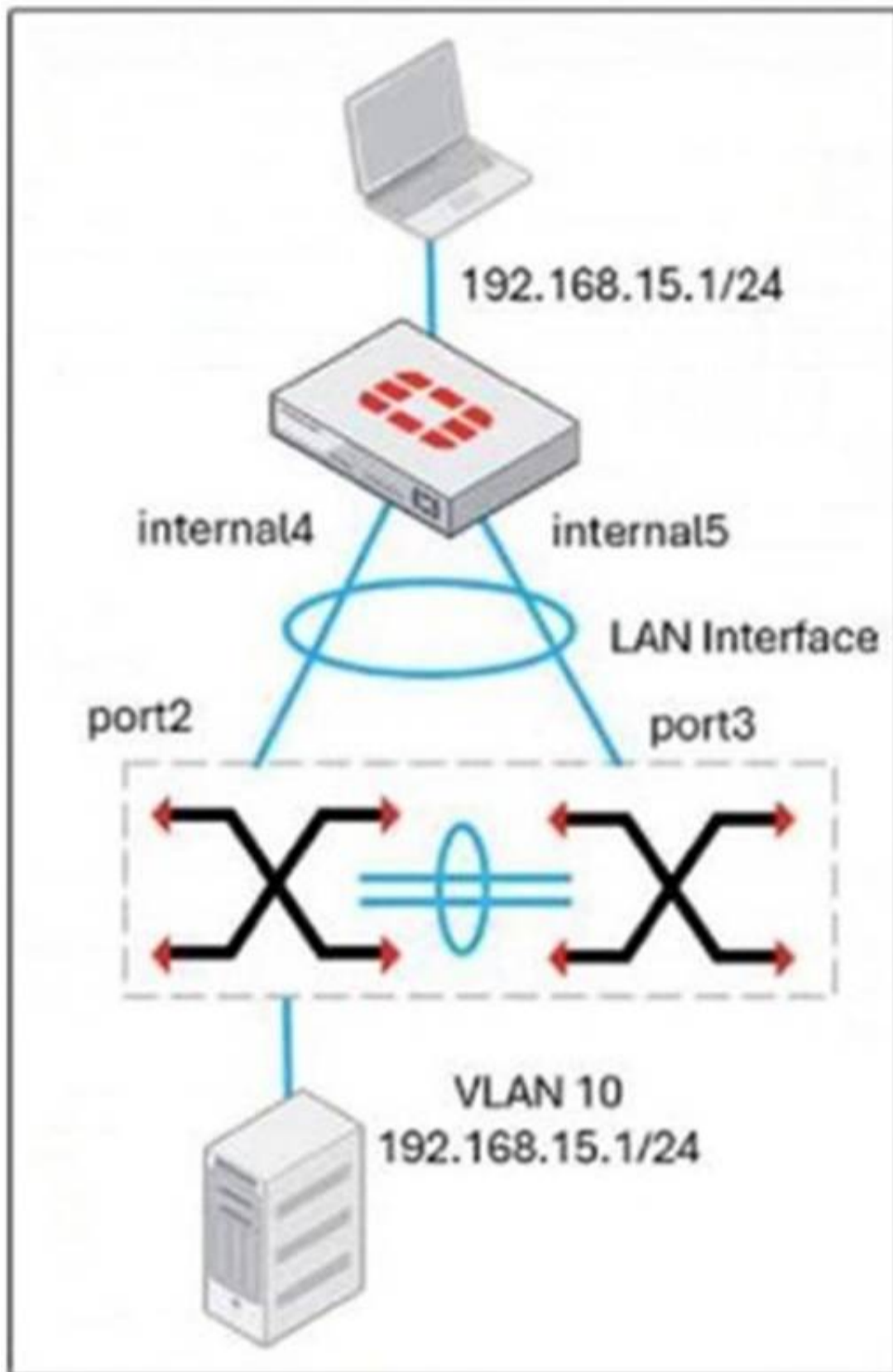
An administrator discovers that webfilter stopped working in Core1 and Core2 after a maintenance window. Which two reasons could explain why webfilter stopped working? (Choose two.)

- 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 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

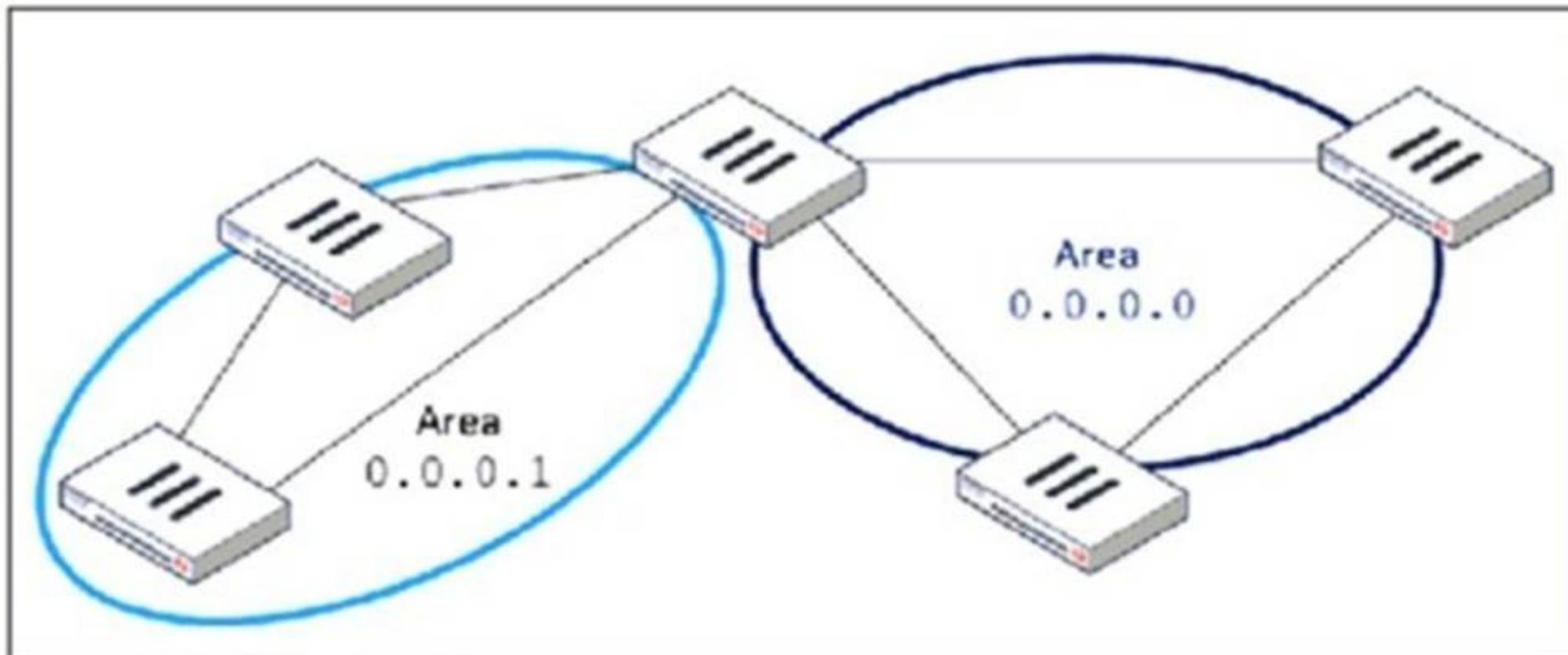
An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection. The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best available connection. 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 6

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 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

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.

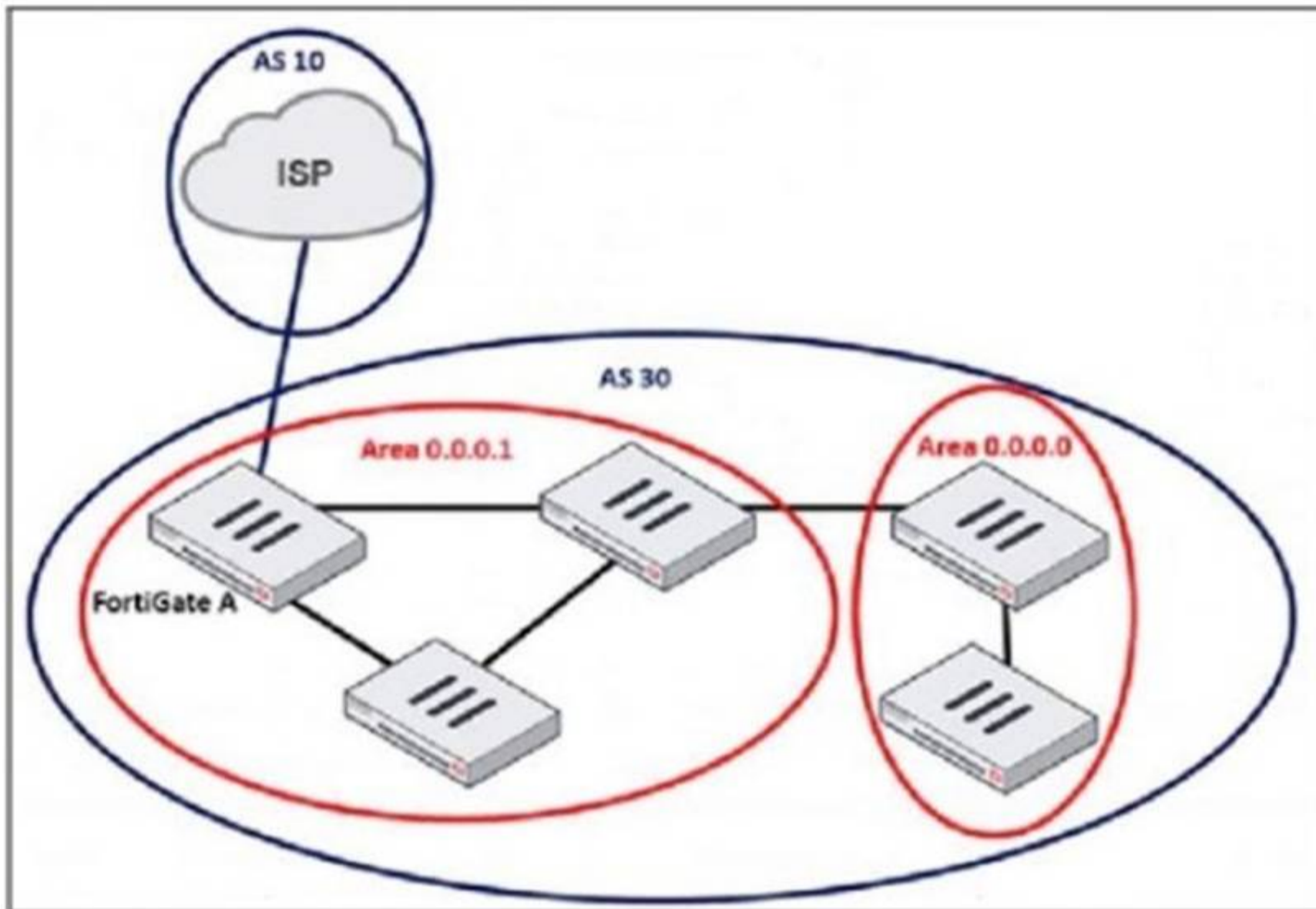
What can the firewall administrator do to block all outdated SSL/TLS versions on any HTTPS web server to prevent possible attacks on user traffic?

- 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 9

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 10

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 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?

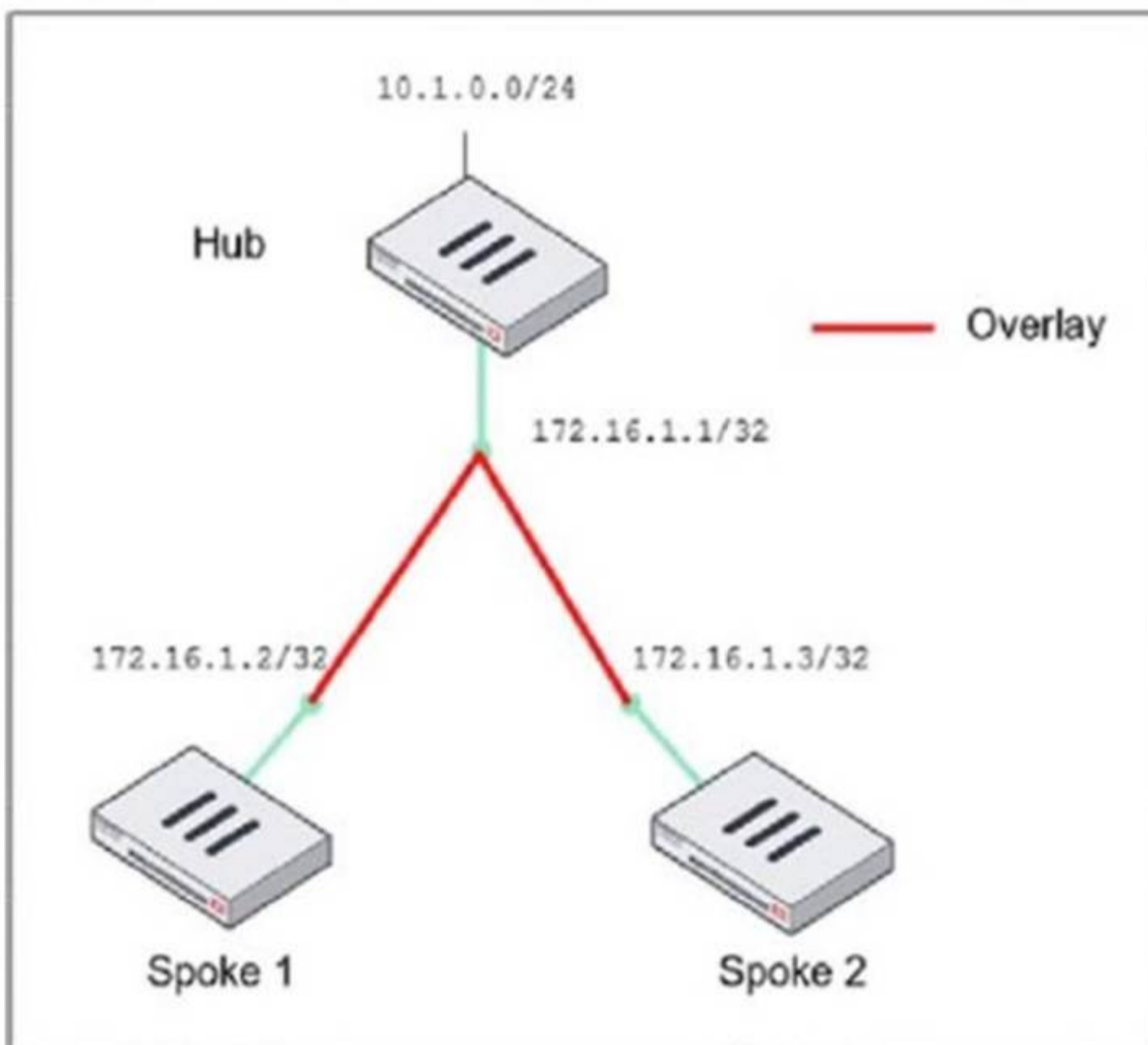
- A. Enable metadata variables to use dynamic configurations in the standard interfaces of FortiManager.
- B. Use the Install On feature in the policy package to automatically assign different interfaces based on the branch.
- C. Create interfaces using device database scripts to use them on the same 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 11

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 16

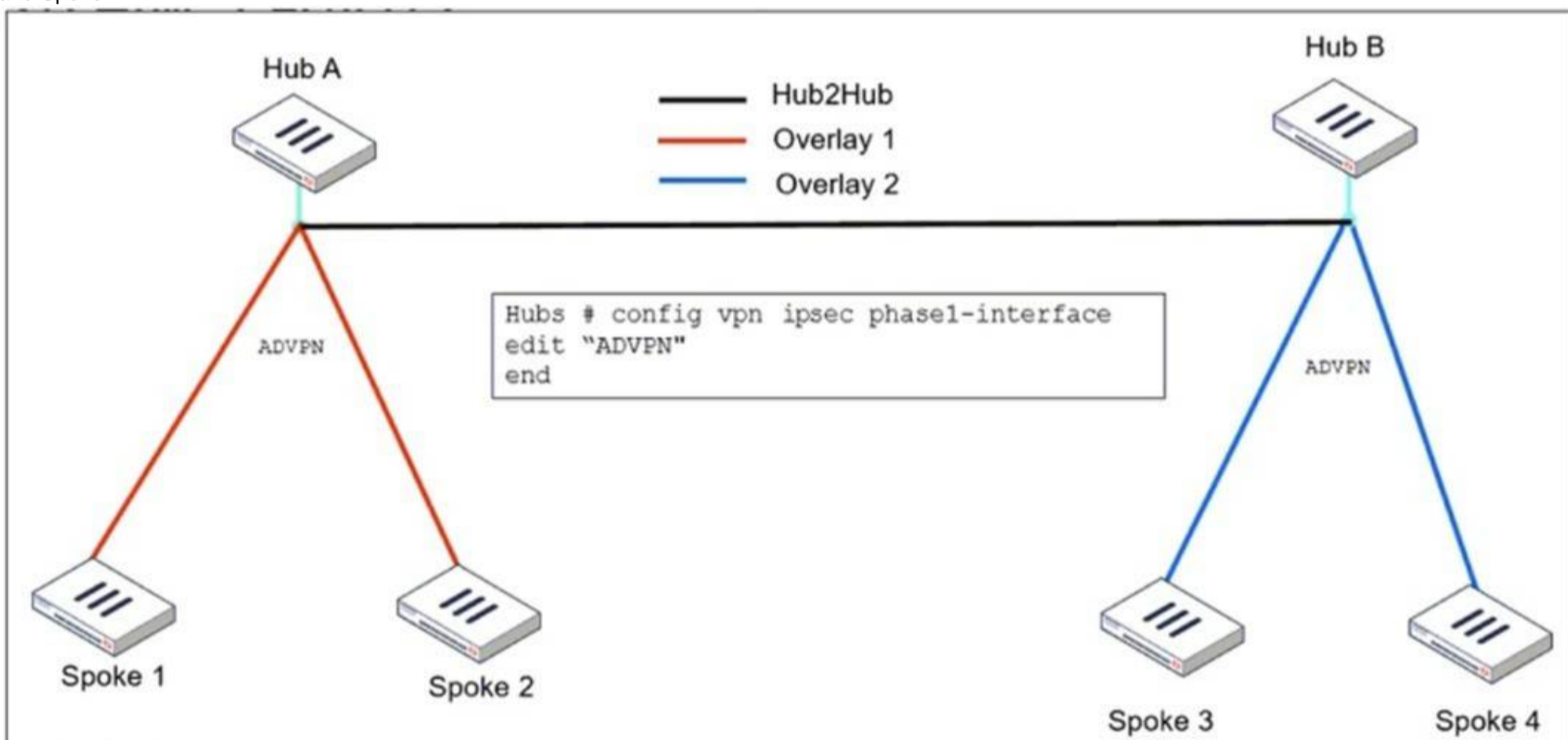
An administrator wants to scale the IBGP sessions and optimize the routing table in an IBGP network. Which parameter should the administrator configure?

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

Answer: D

NEW QUESTION 18

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?

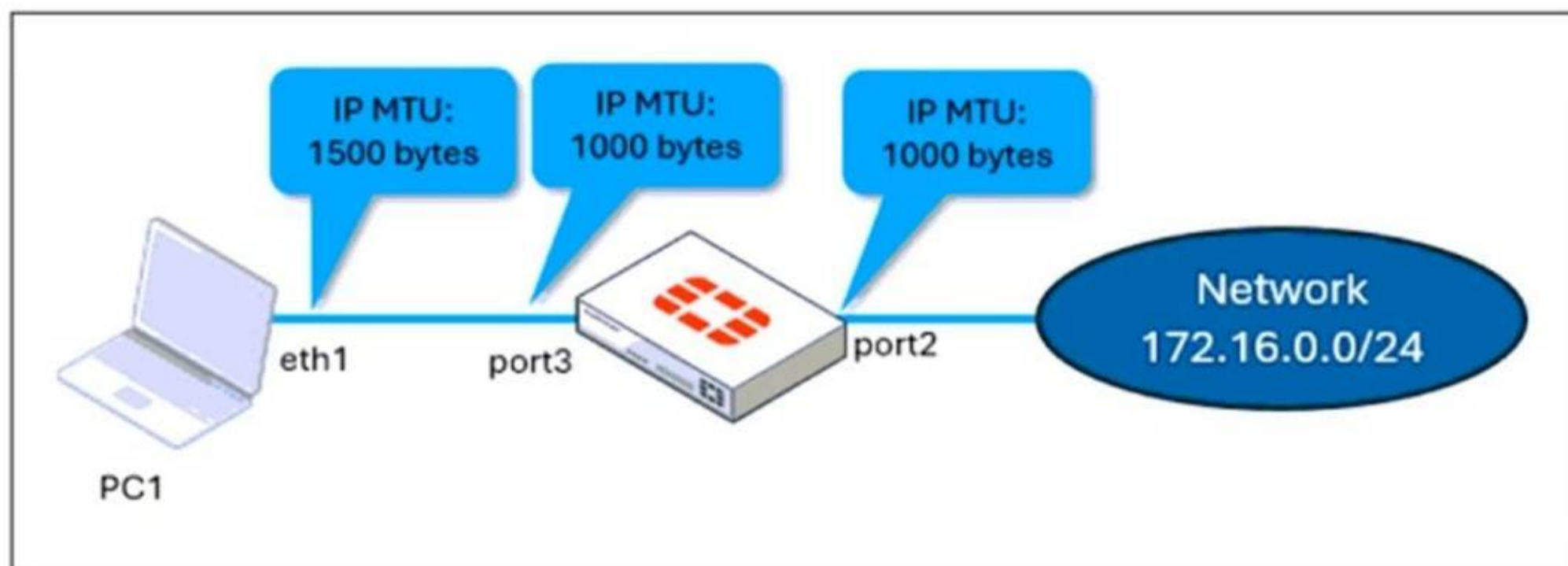
- A. set auto-discovery-sender enable and set network-id x
- B. set auto-discovery-forwarder enable and set remote-as x
- C. set auto-discovery-crossover enable and set enforce-multihop enable
- D. set auto-discovery-receiver enable and set npu-offload enable

Answer: C

NEW QUESTION 20

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 FortiGate
- B. The user has to adjust the ping MTU to 1000 to succeed.
- C. Fragmented packets must be encrypted
- 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 dropped
- 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 24

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 25

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					
Synchronized	150	FortiGate_A	Core1 root	Primary	4h 52m
Synchronized	100	FortiGate_B	Core1 root	Secondary	4h 52m
Virtual cluster 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

NEW QUESTION 28

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 GUI
- 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 33

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 38

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 40

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



The administrator is checking on FortiAnalyzer traffic from the device with IP address 10.1.10.1, 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 action Malware, 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

NEW QUESTION 45

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 50

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 55

.....

Relate Links

100% Pass Your FCSS_EFW_AD-7.6 Exam with Examible Prep Materials

https://www.exambible.com/FCSS_EFW_AD-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>