



## 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.

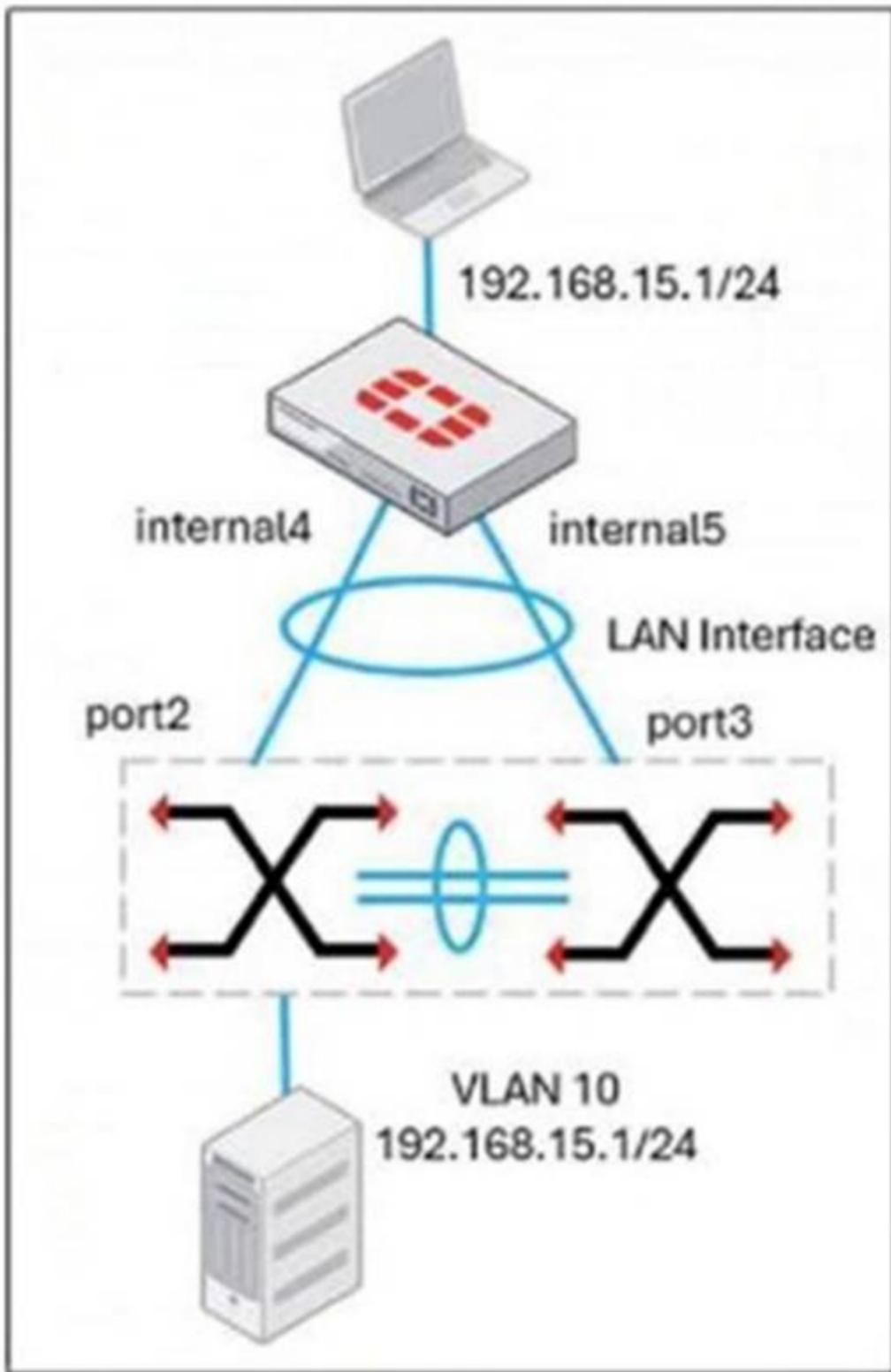
In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

- 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 LAN interface connected from FortiGate to two FortiSwitch devices.



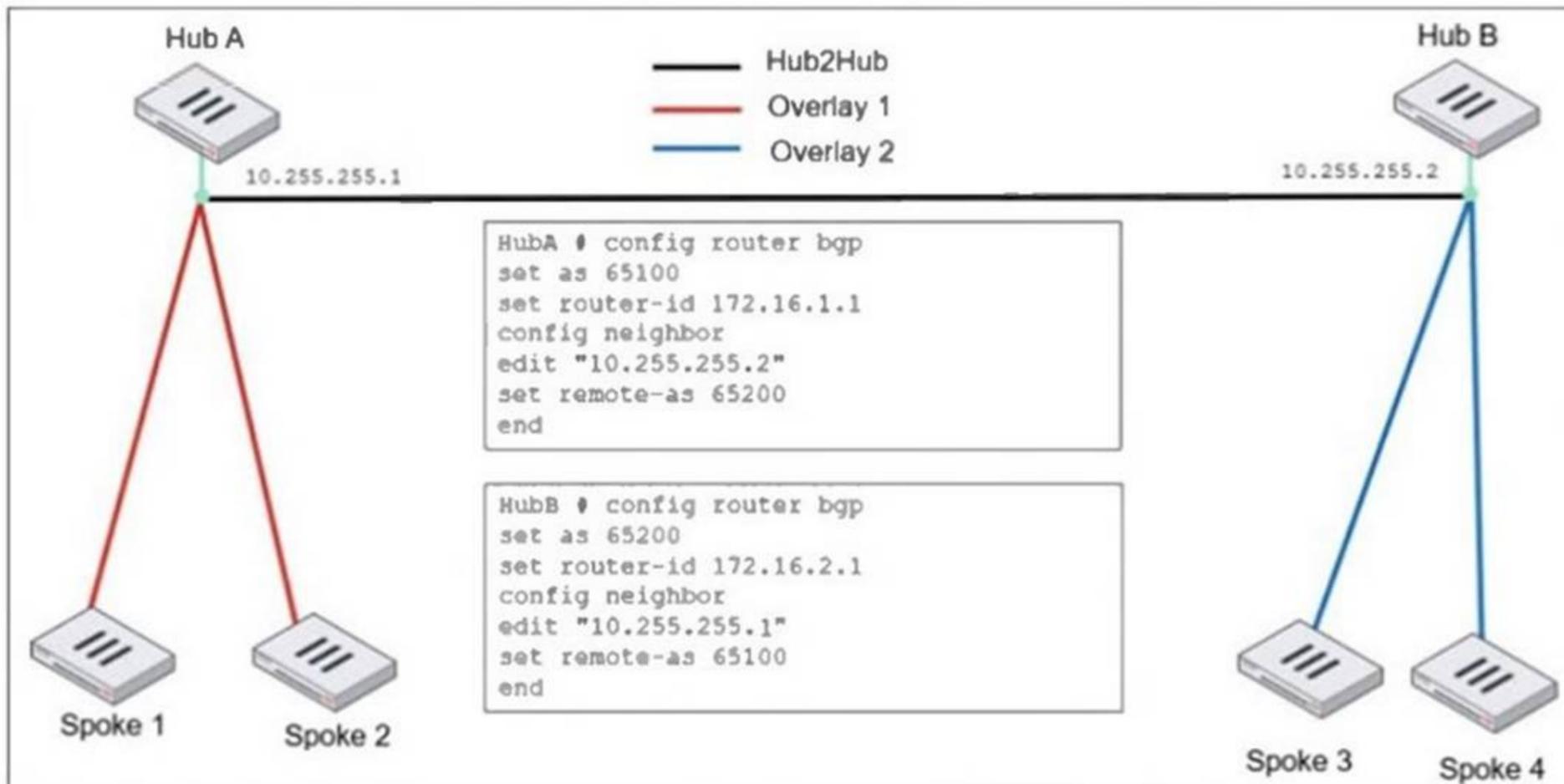
What two conclusions can you draw from the corresponding LAN interface? (Choose two.)

- 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**

Refer to the exhibit, which shows an ADVPN network



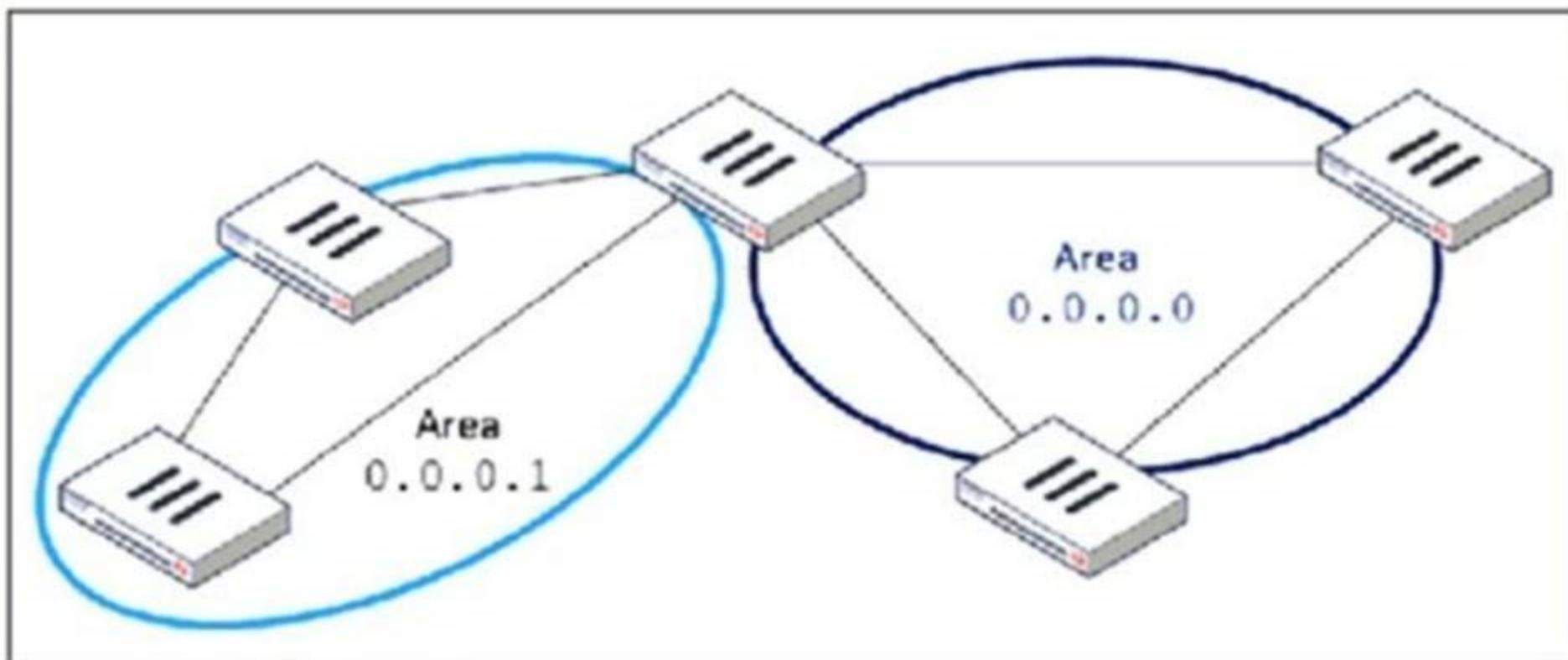
An administrator must configure an ADVPN using IBGP and EBGP to connect overlay network 1 with 2. What two options must the administrator configure in BGP? (Choose two.)

- A. set ebgp-enforce-multihop enable
- B. set next-hop-self enable
- C. set ibgp-enforce-multihop advpn
- D. set attribute-unchanged next-hop

**Answer:** AB

**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 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

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

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

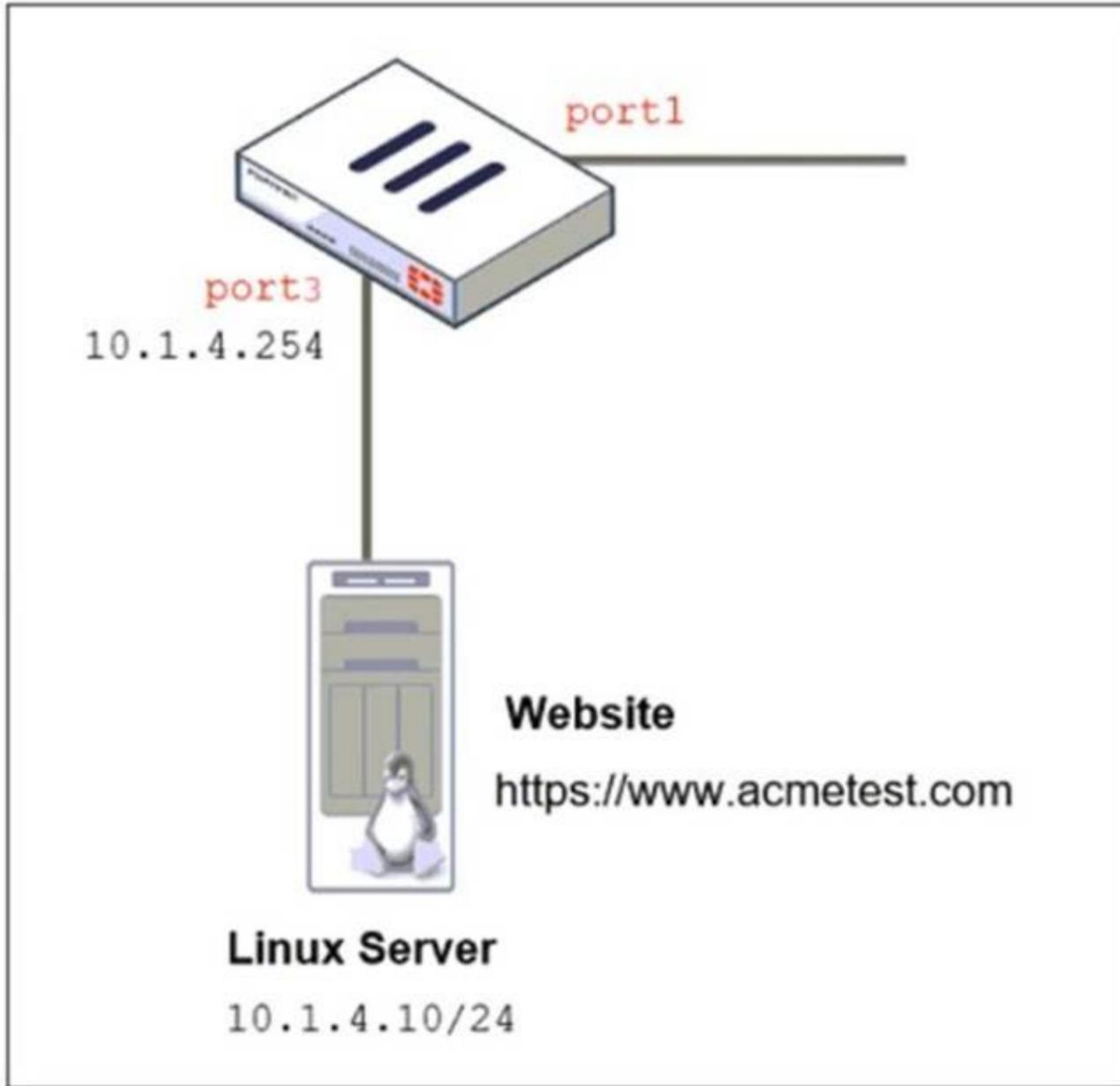
- A. `network-import-check`
- B. `ibgp-enforce-multihop`
- C. `neighbor-group`
- D. `route-reflector-client`

**Answer:** D

#### NEW QUESTION 9

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 Connections Connecting to Multiple Servers

Inspection method Protecting SSL Server

CA certificate ⚠  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	<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 10**

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 10

A company's guest internet policy, operating in proxy mode, blocks access to Artificial Intelligence Technology sites using FortiGuard. However, a guest user accessed a page in this category using port 8443.

Which configuration changes are required for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443 when full SSL inspection is active in the guest policy?

- A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.
- B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.
- C. To analyze nonstandard ports in web filter profiles, use TLSv1.3 in the SSL/SSH Inspection Profile.
- D. Administrators can block traffic on nonstandard ports by enabling the SNI check in the SSL/SSH Inspection Profile.

**Answer:** B

#### NEW QUESTION 15

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 20

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 21

An administrator must minimize CPU and RAM use on a FortiGate firewall while also enabling essential security features, such as web filtering and application control for HTTPS traffic.

Which SSL inspection setting helps reduce system load while also enabling security features, such as web filtering and application control for encrypted HTTPS traffic?

- A. Use full SSL inspection to thoroughly inspect encrypted payloads.
- B. Disable SSL inspection entirely to conserve resources.
- C. Configure SSL inspection to handle HTTPS traffic efficiently.
- D. Enable SSL certificate inspection mode to perform basic checks without decrypting traffic.

Answer: D

**NEW QUESTION 22**

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.

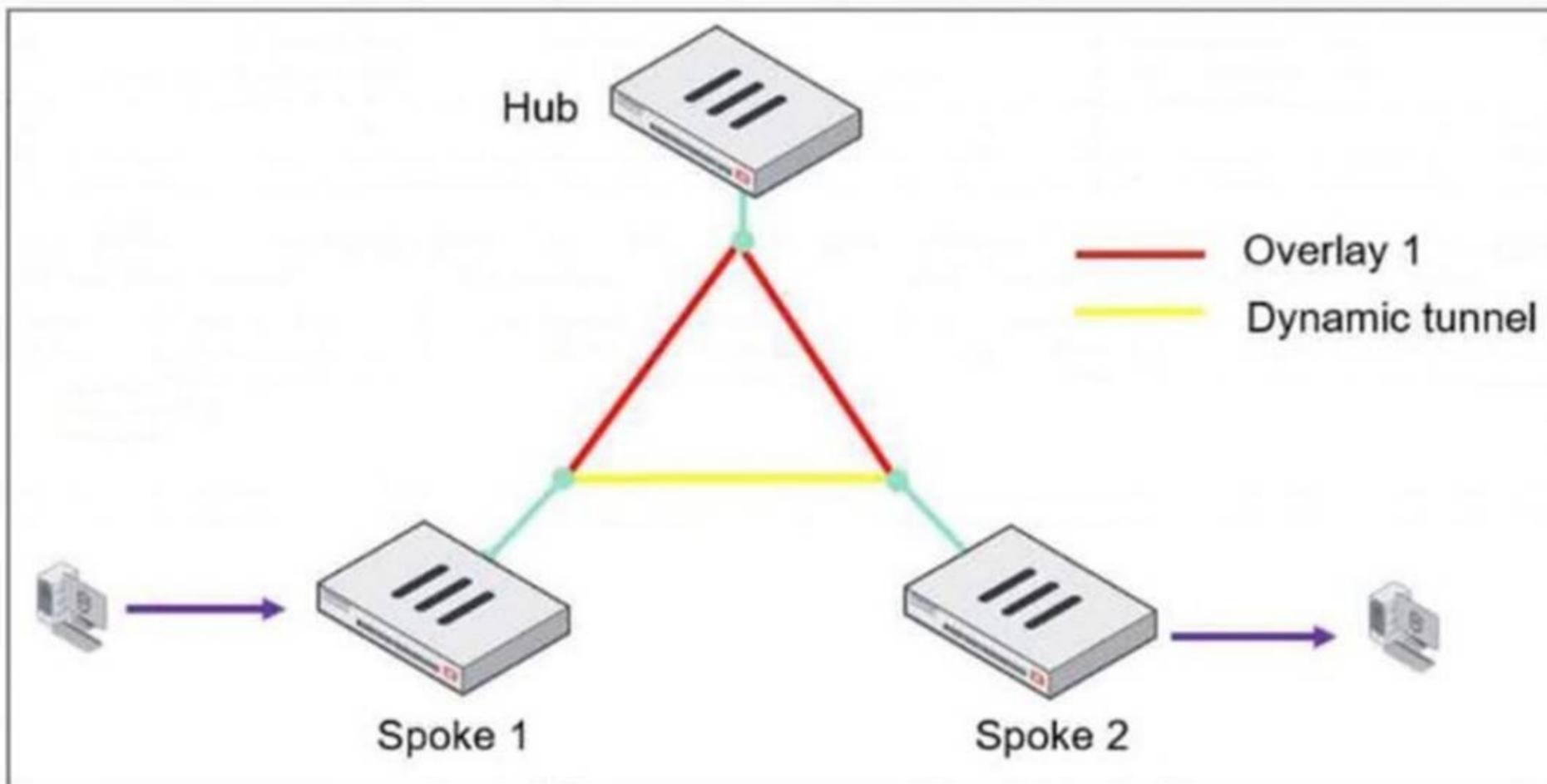
How can an administrator apply IPS in a way that ensures it does not disrupt existing applications in the network?

- 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 23**

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 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**

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 27

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 32**

.....

## 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/](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/>