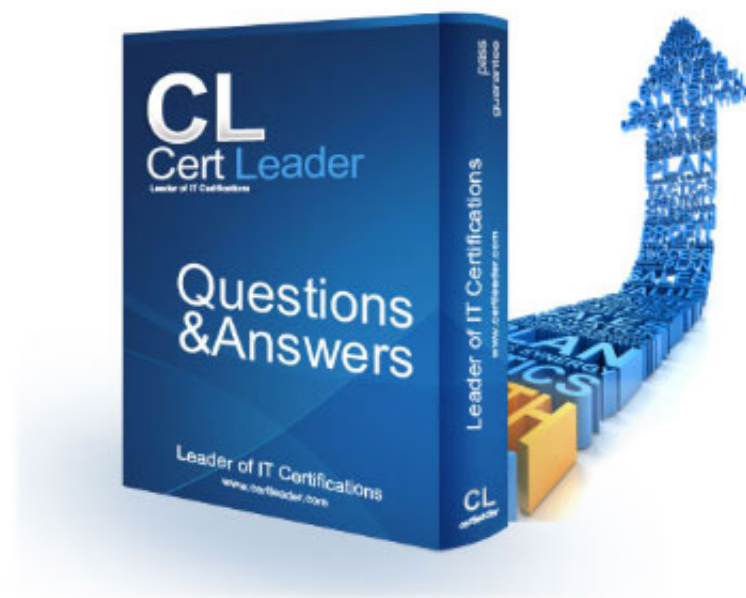


FCSS_EFW_AD-7.6 Dumps

FCSS - Enterprise Firewall 7.6 Administrator

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



NEW QUESTION 1

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.

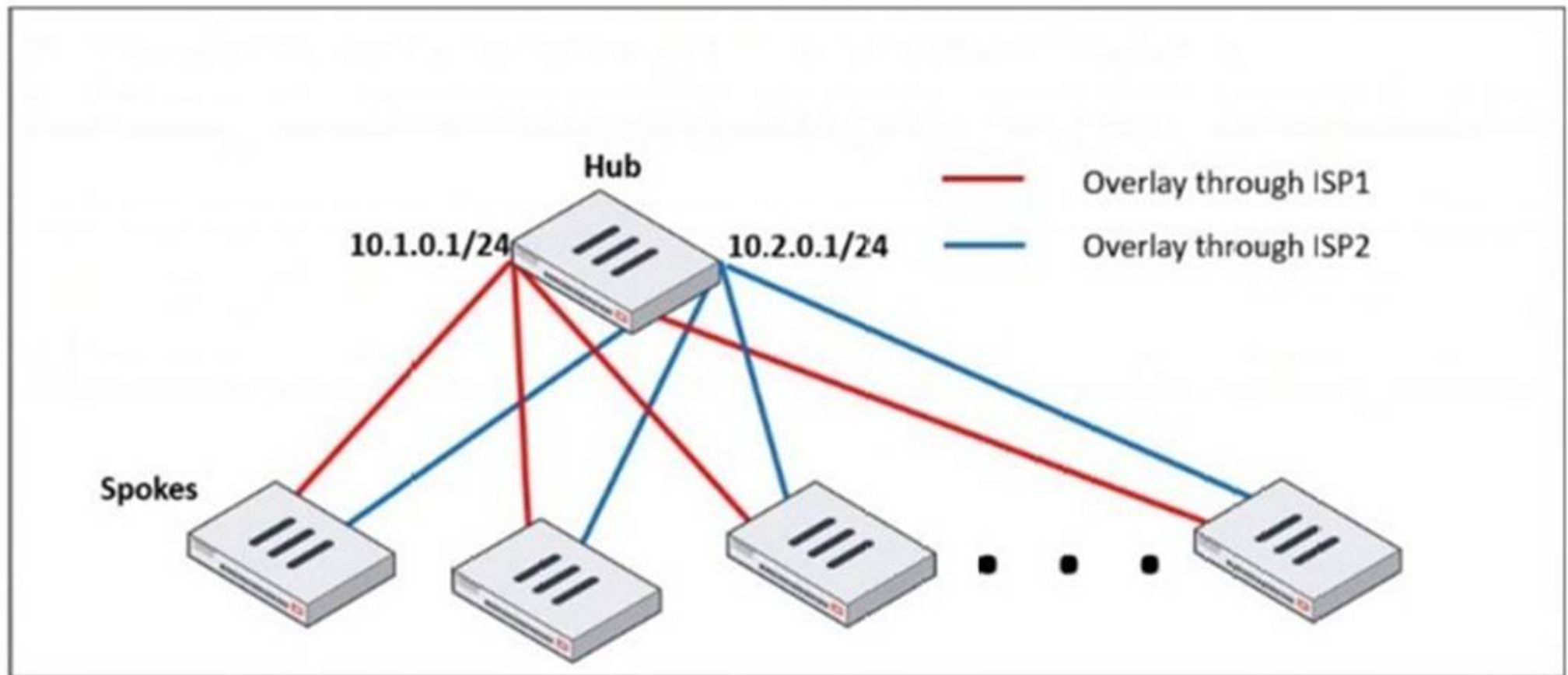
In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

- 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

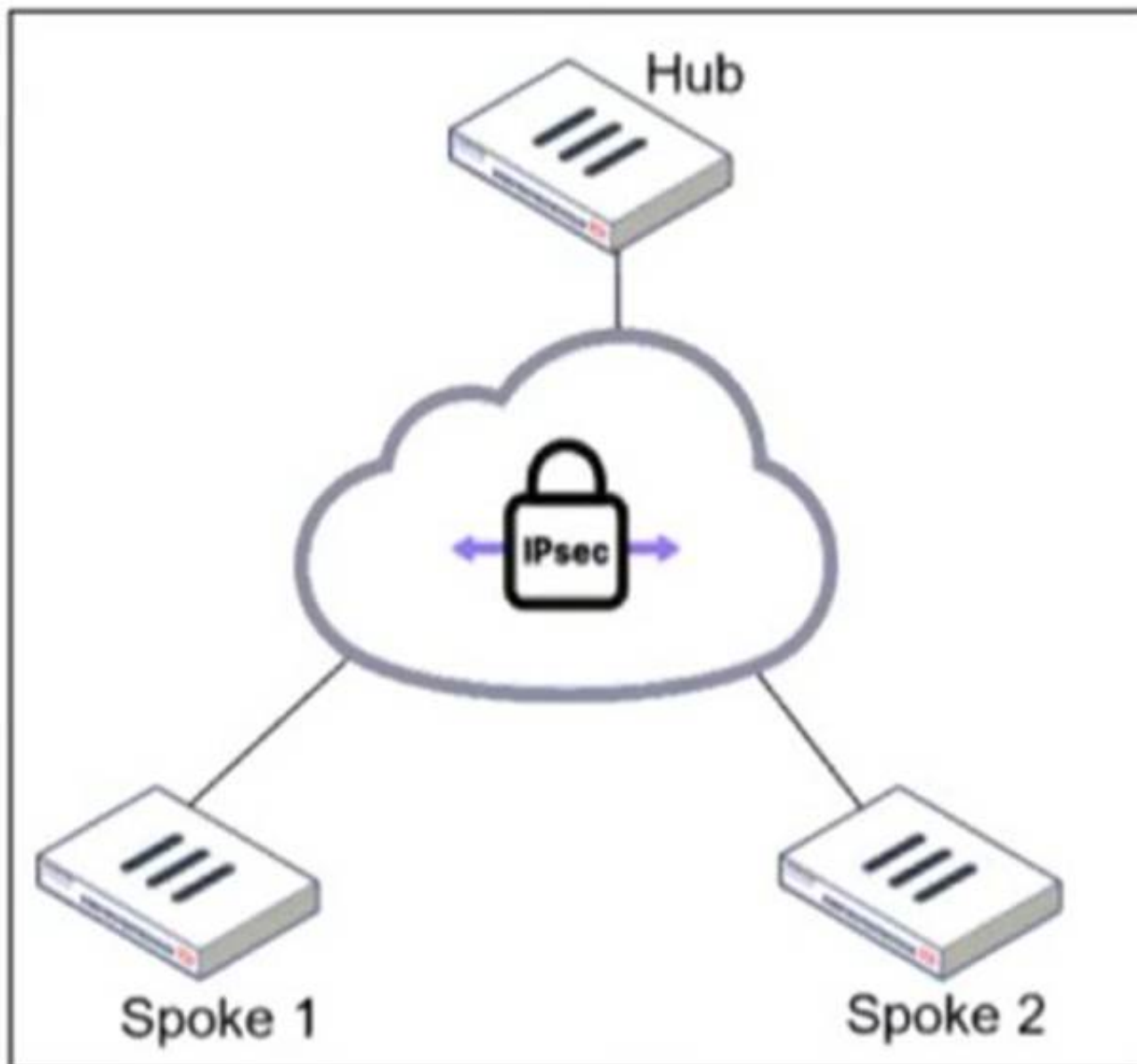
The IT department discovered during the last network migration that all zero phase selectors in phase 2 IPsec configurations impacted network operations. What are two valid approaches to prevent this during future migrations? (Choose two.)

- 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 4

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

NEW QUESTION 5

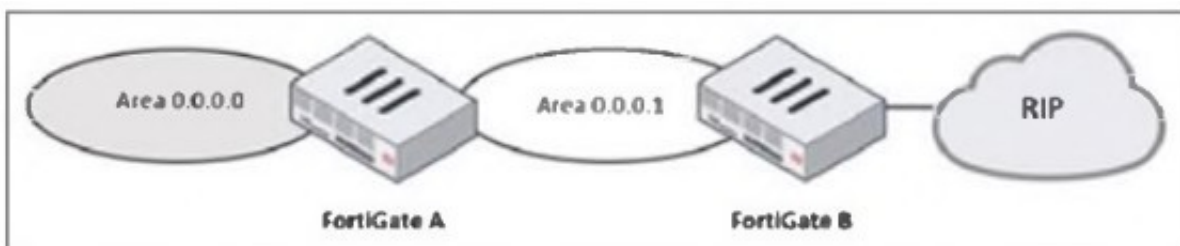
An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection. The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best available connection.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

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 8
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 × +
Upstream FortiGate IP/FQDN	10.1.0.254
Allow downstream device REST API access ⓘ	☐
SAML Single Sign-On ⓘ	☒ Auto ☐ Manual
	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 9

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?

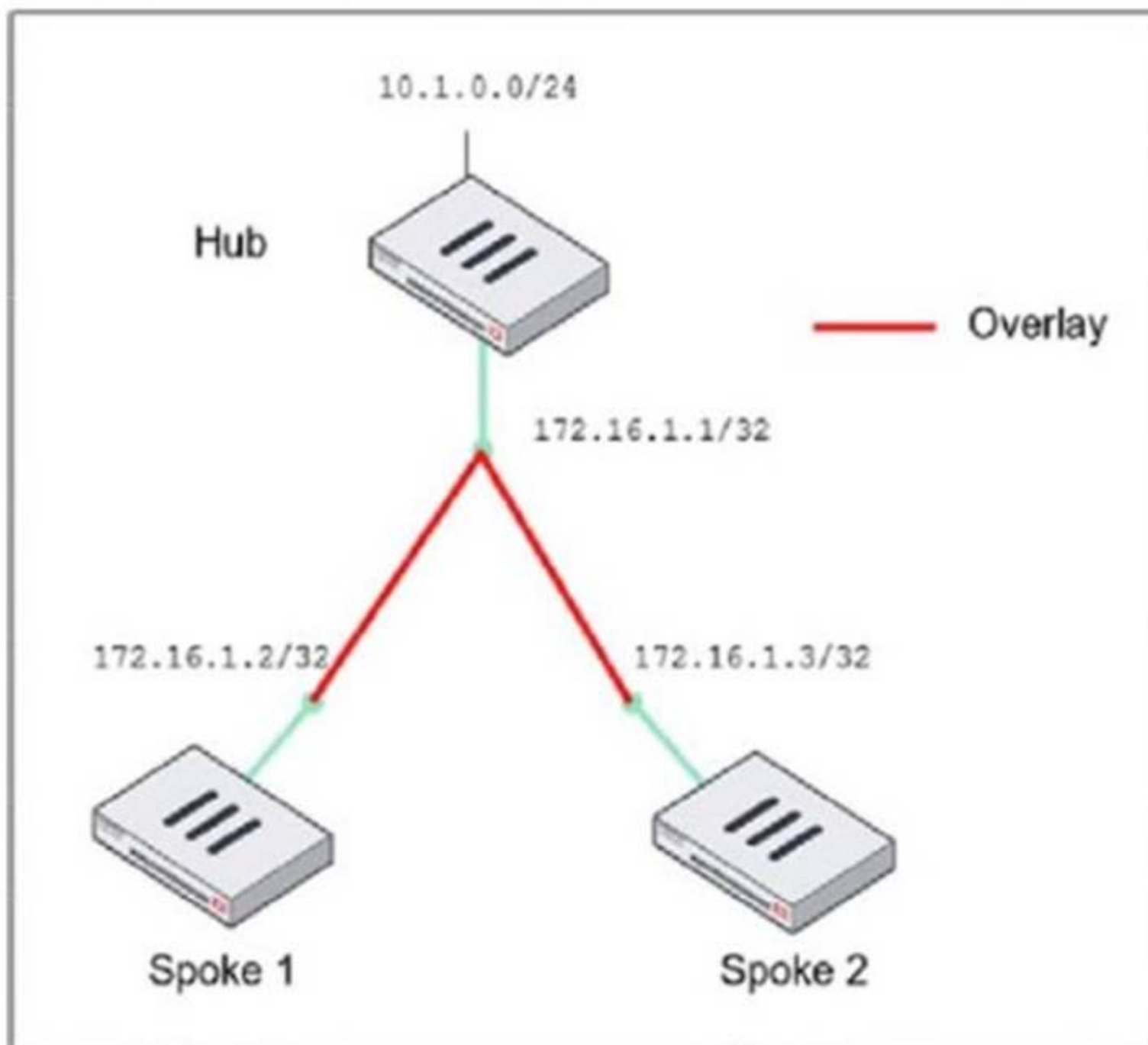
- A. Enable metadata variables to use dynamic configurations in the standard interfaces of FortiManager.
- B. Use the Install On feature in the policy package to automatically assign different interfaces based on the branch.
- C. Create interfaces using device database scripts to use them on the same 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 10

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.)

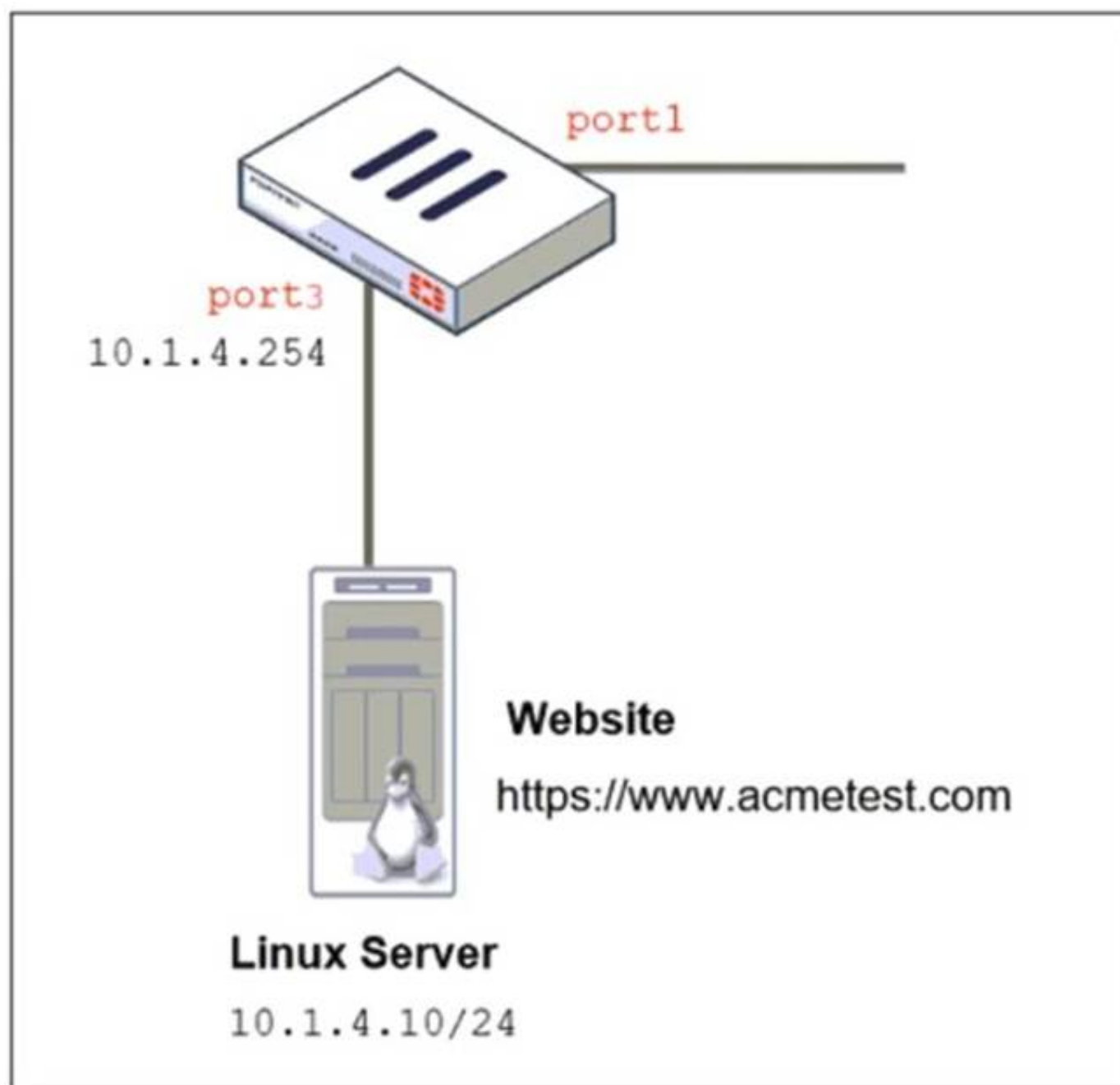
- A. set max-neighbor-num 2
- B. set neighbor-group advpn
- C. set route-reflector-client enable
- D. set prefix 172.16.1.0 255.255.255.0

Answer: BD

NEW QUESTION 10

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

deep-inspection

Comments

Read-only deep inspection profile.

34/255

SSL Inspection Options

Enable SSL inspection of

Multiple Client Clients Connecting to Multiple Servers

Protecting SSL Server

Inspection method

SSL Certificate Inspection

Full SSL Inspection

CA certificate

Fortinet_CA_SSL

Download

Blocked certificates

Allow

Block

View Blocked Certificates

Untrusted SSL certificates

Allow

Block

Ignore

View Trusted CAs List

Server certificate SNI check

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

SMTPTS

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

NEW QUESTION 12

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
```

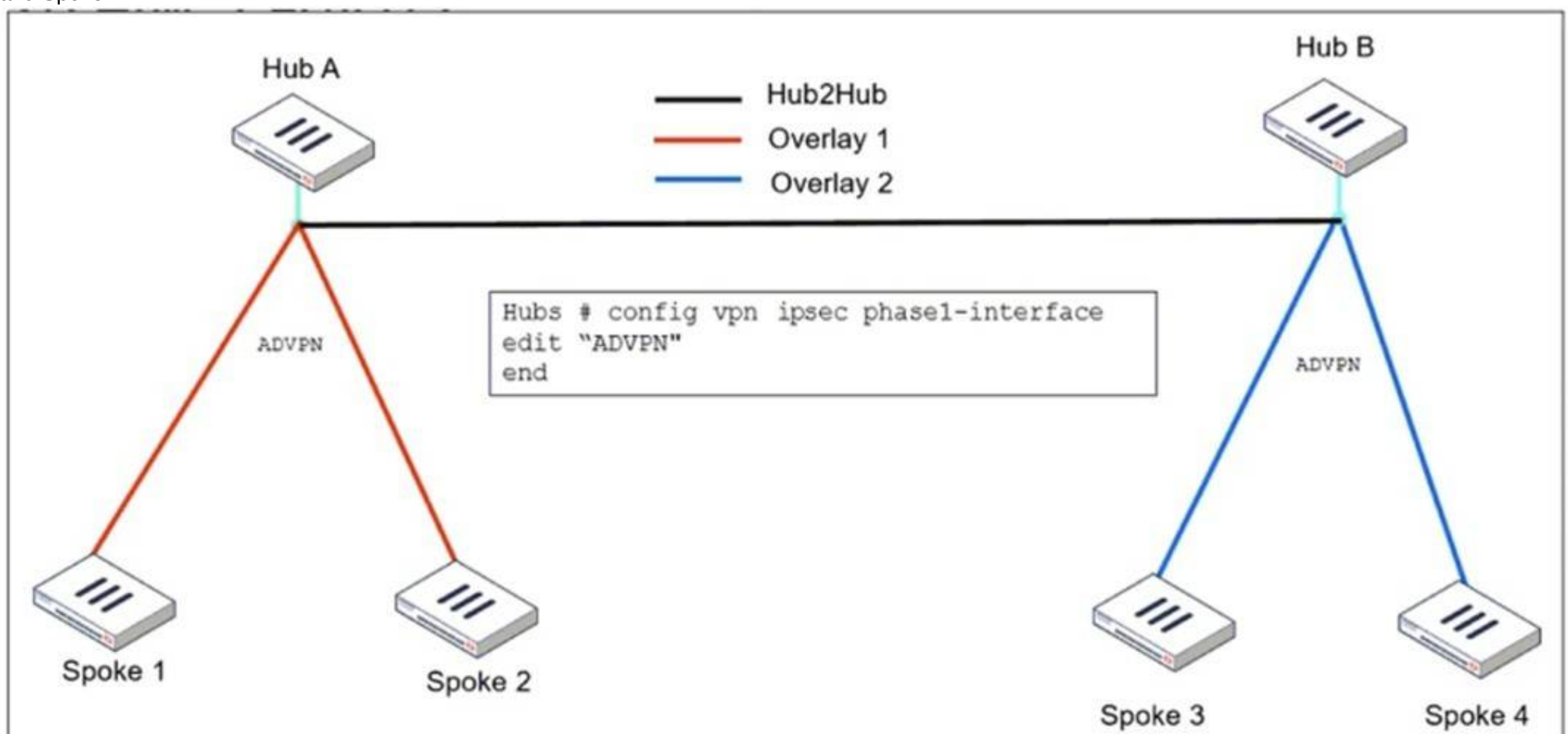
What can you conclude from this VPN IPsec phase 1 configuration?

- 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

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

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 24

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 25

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 29

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 30

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

Configuration Revision History					
View ConfigView Install LogRevision DiffRetrieve ConfigMoreSearch...					
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 32

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 34

.....

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