

Exam Questions FCSS_EFW_AD-7.6

FCSS - Enterprise Firewall 7.6 Administrator

https://www.2passeasy.com/dumps/FCSS_EFW_AD-7.6/



NEW QUESTION 1

Refer to the exhibit, which shows a partial troubleshooting command output.

```
FortiGate # diagnose vpn tunnel list name Hub2Spoke1

list ipsec tunnel by names in vd 0

...

npu_flag=20 npu_rgwy=10.10.2.2 npu_lgwy=10.10.1.1 npu_selid=1
```

An administrator is extensively using IPsec on FortiGate. Many tunnels show information similar to the output shown in the exhibit. What can the administrator conclude?

- A. IPsec SAs cannot be offloaded.
- B. The two IPsec SAs, inbound and outbound, are copied to the NPU.
- C. Only the outbound IPsec SA is copied to the NPU.
- D. Only the inbound IPsec SA is copied to the NPU.

Answer: B

NEW QUESTION 2

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 3

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

NGFW-2

Dashboard

Network

Security Profiles

WiFi Controller

System

VDOM

Global Resources

Administrators

Admin Profiles

Firmware & Registration

Settings

HA

SNMP

Replacement Messages

+ Create New

Edit

Delete

Switch Management

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

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 5

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?

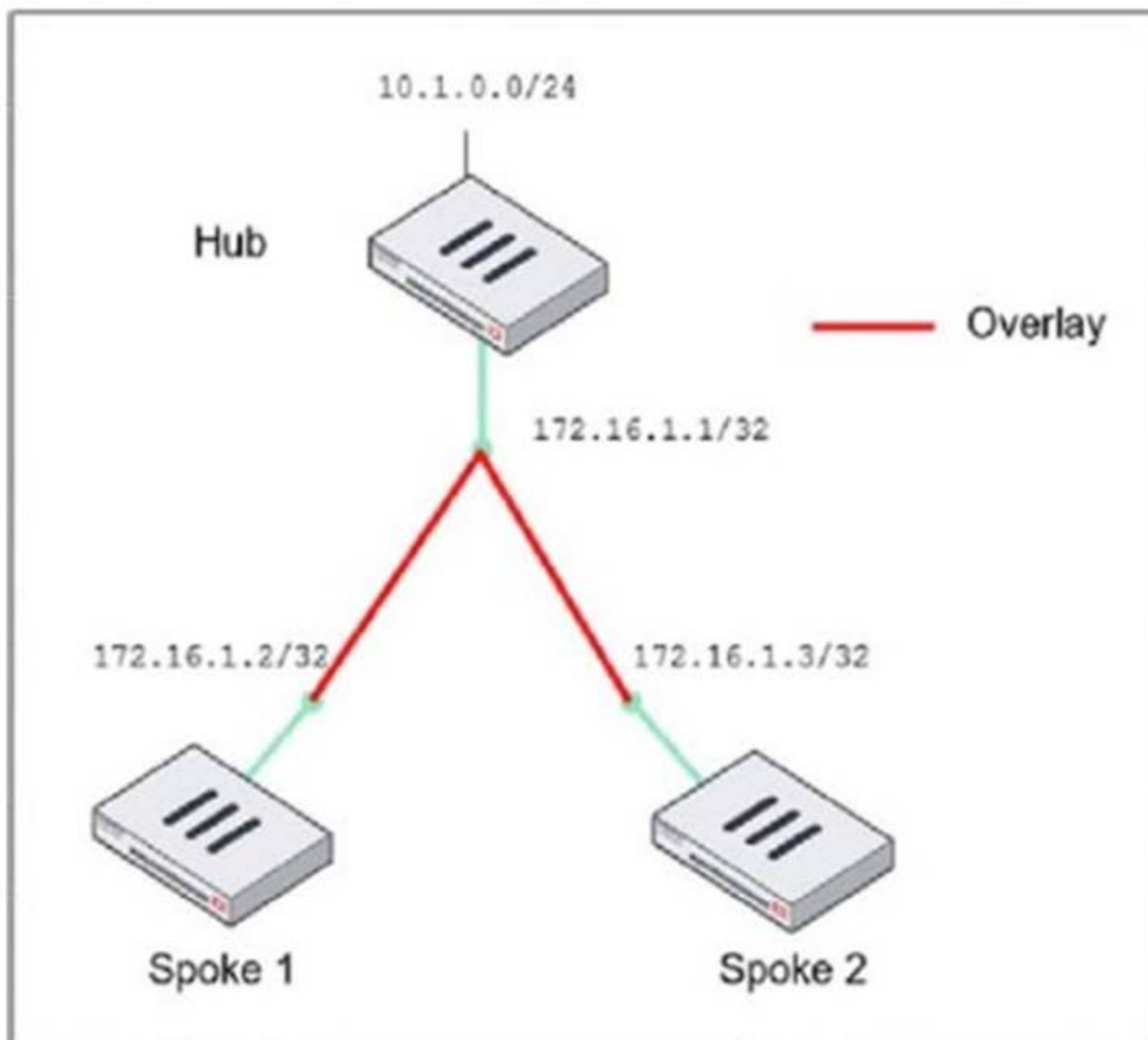
- A. Create an inline-CASB to protect against DNS exfiltration.
- B. Configure a File Filter profile to prevent DNS exfiltration.
- C. Enable DNS Filter to protect against DNS exfiltration.
- D. Use an IPS profile and DNS exfiltration-related signatures.

Answer: D

NEW QUESTION 6

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 7

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?

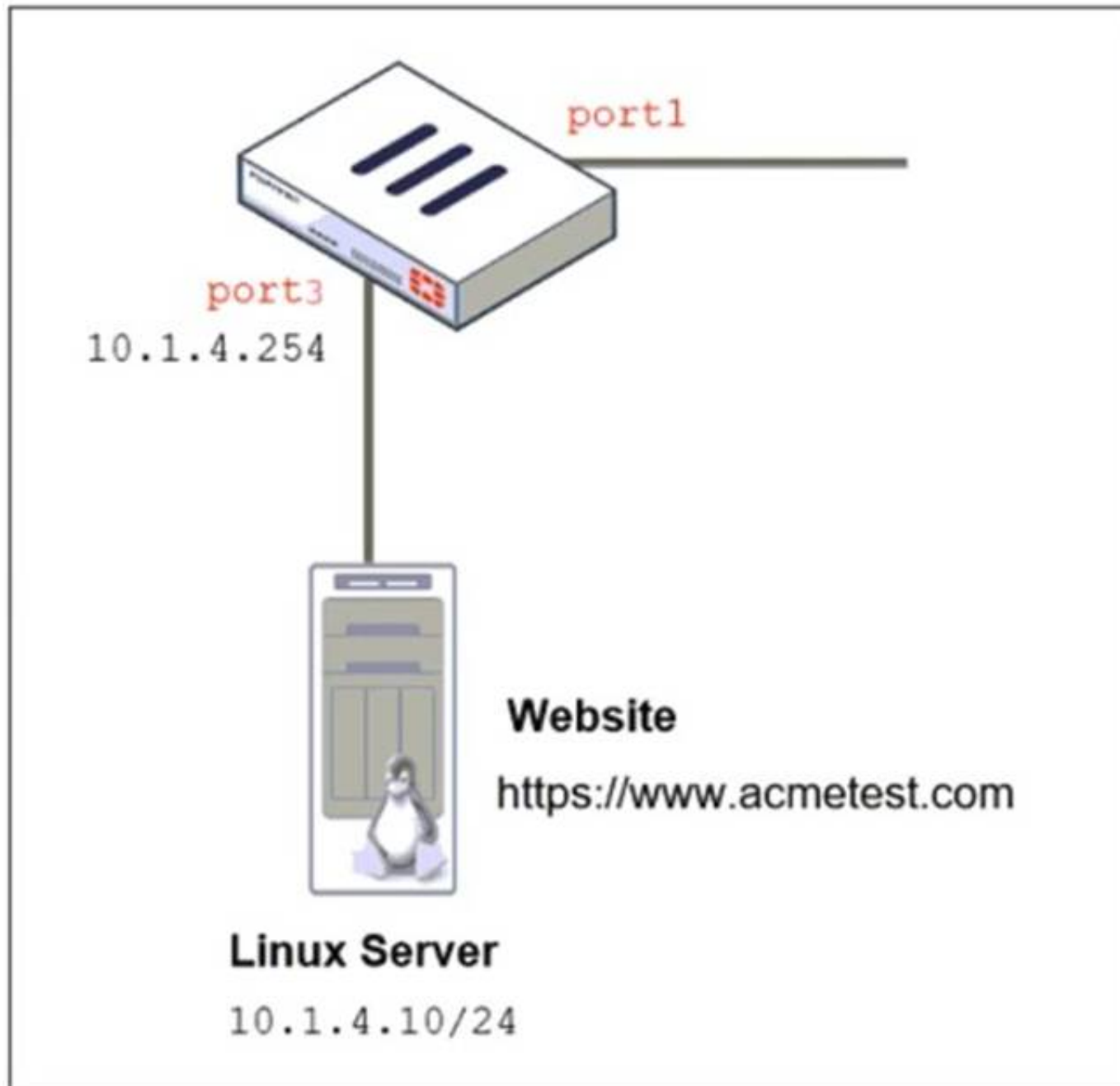
- A. Use IKEv2, which encrypts peer IDs and prevents exposure.
- B. Opt for SSL VPN web mode because it does not use peer IDs at all.
- C. Choose IKEv1 aggressive mode because it simplifies peer identification.
- D. Stick with IKEv1 main mode because it offers better performance.

Answer: A

NEW QUESTION 8

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

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

SMTPS

465

POP3S

995

IMAPS

993

FTPS

990

DNS over TLS

853

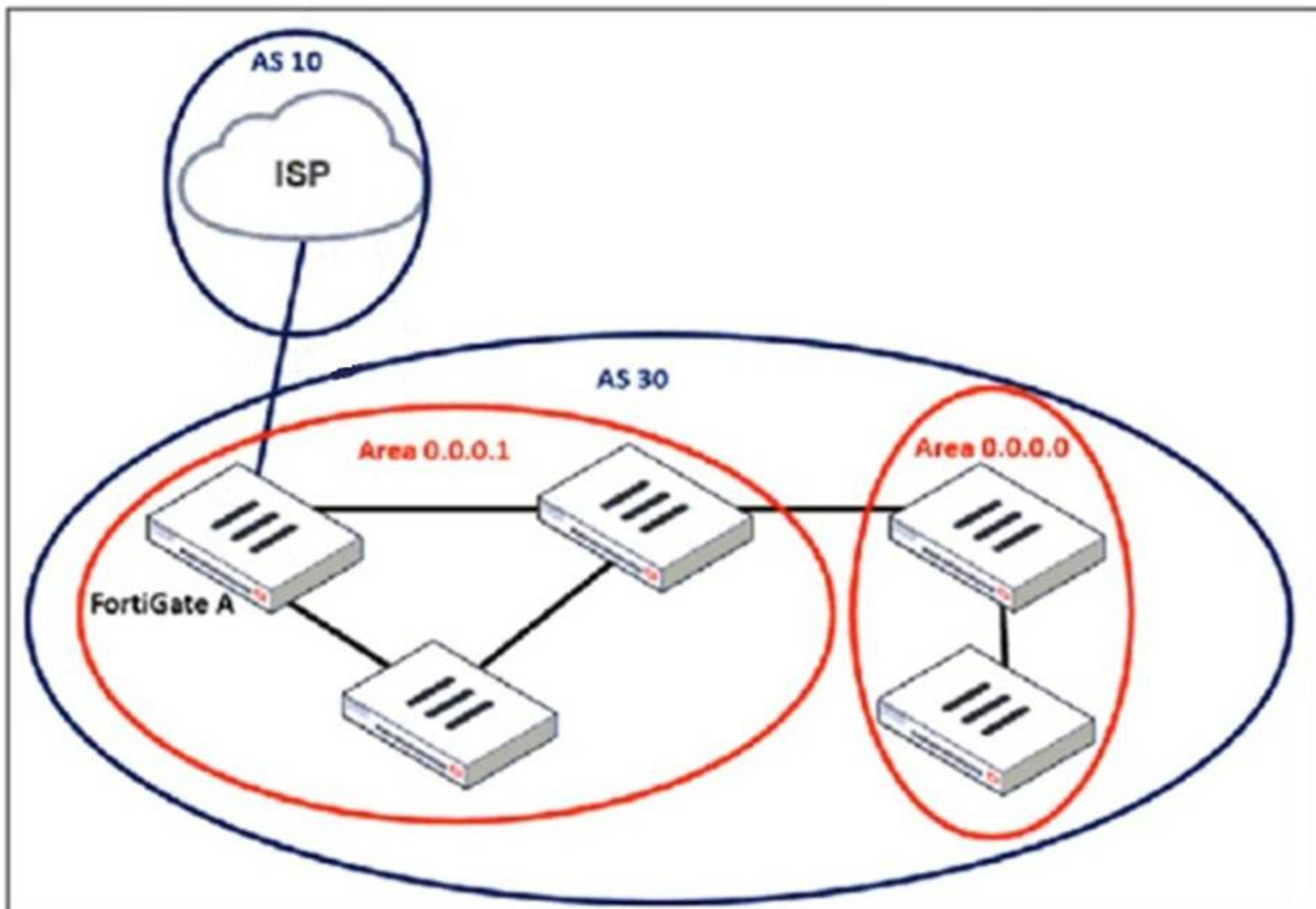
Why is FortiGate unable to detect HTTPS attacks on firewall policy ID 3 targeting the Linux server?

- 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

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

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

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 15

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 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 22

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 27

During the maintenance window, an administrator must sniff all the traffic going through a specific firewall policy, which is handled by NP6 interfaces. The output of the sniffer trace provides just a few packets.

Why is the output of sniffer trace limited?

- A. The traffic corresponding to the firewall policy is encrypted.
- B. auto-asic-off load is set to enable in the firewall policy,

- C. inspection-mode is set to proxy in the firewall policy.
- D. The option npudbg is not added in the diagnose sniff packet command.

Answer: B

NEW QUESTION 32

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.

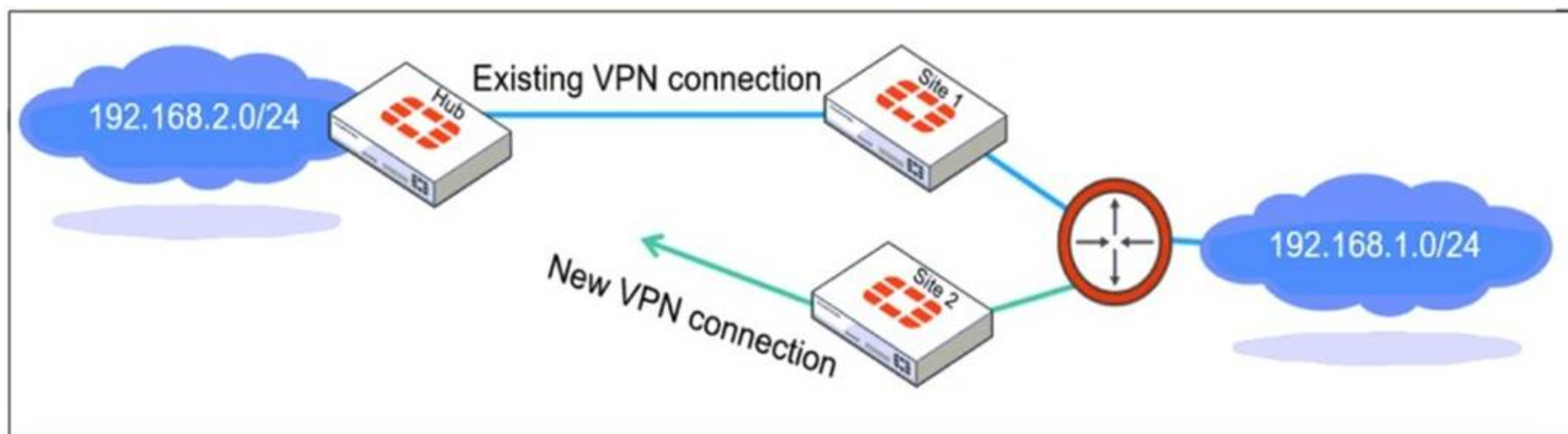
How can an administrator apply IPS in a way that ensures it does not disrupt existing applications in the network?

- 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 36

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.



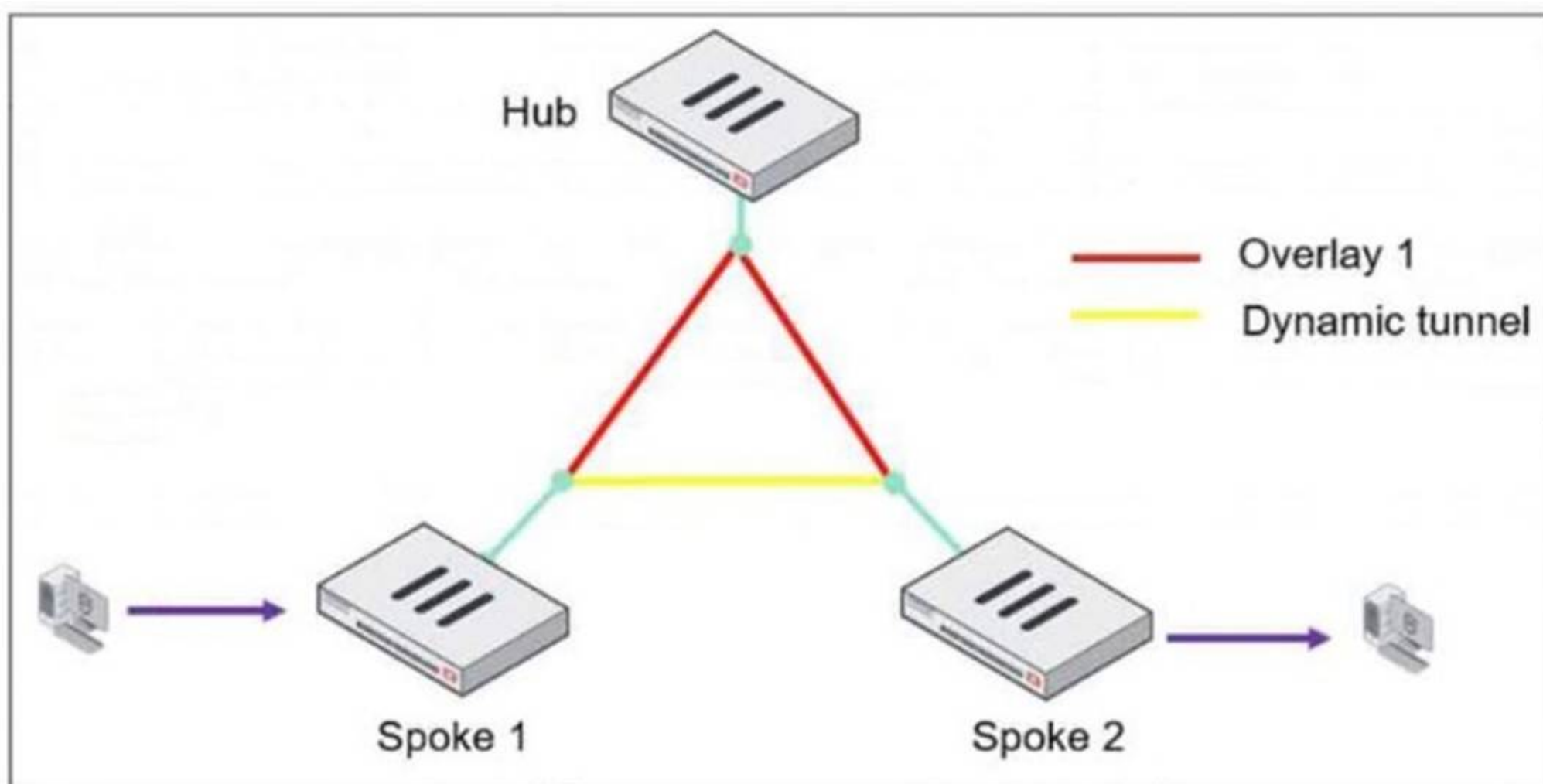
Which IPsec phase 2 configuration must an administrator make on the FortiGate hub to enable equal-cost multi-path (ECMP) routing when multiple remote sites connect with overlapping subnets?

- 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

NEW QUESTION 39

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 43

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 47

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_EFW_AD-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_EFW_AD-7.6 Product From:

https://www.2passeasy.com/dumps/FCSS_EFW_AD-7.6/

Money Back Guarantee

FCSS_EFW_AD-7.6 Practice Exam Features:

- * FCSS_EFW_AD-7.6 Questions and Answers Updated Frequently
- * FCSS_EFW_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_EFW_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_EFW_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year