

Fortinet

Exam Questions FCSS_EFW_AD-7.6

FCSS - Enterprise Firewall 7.6 Administrator



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.

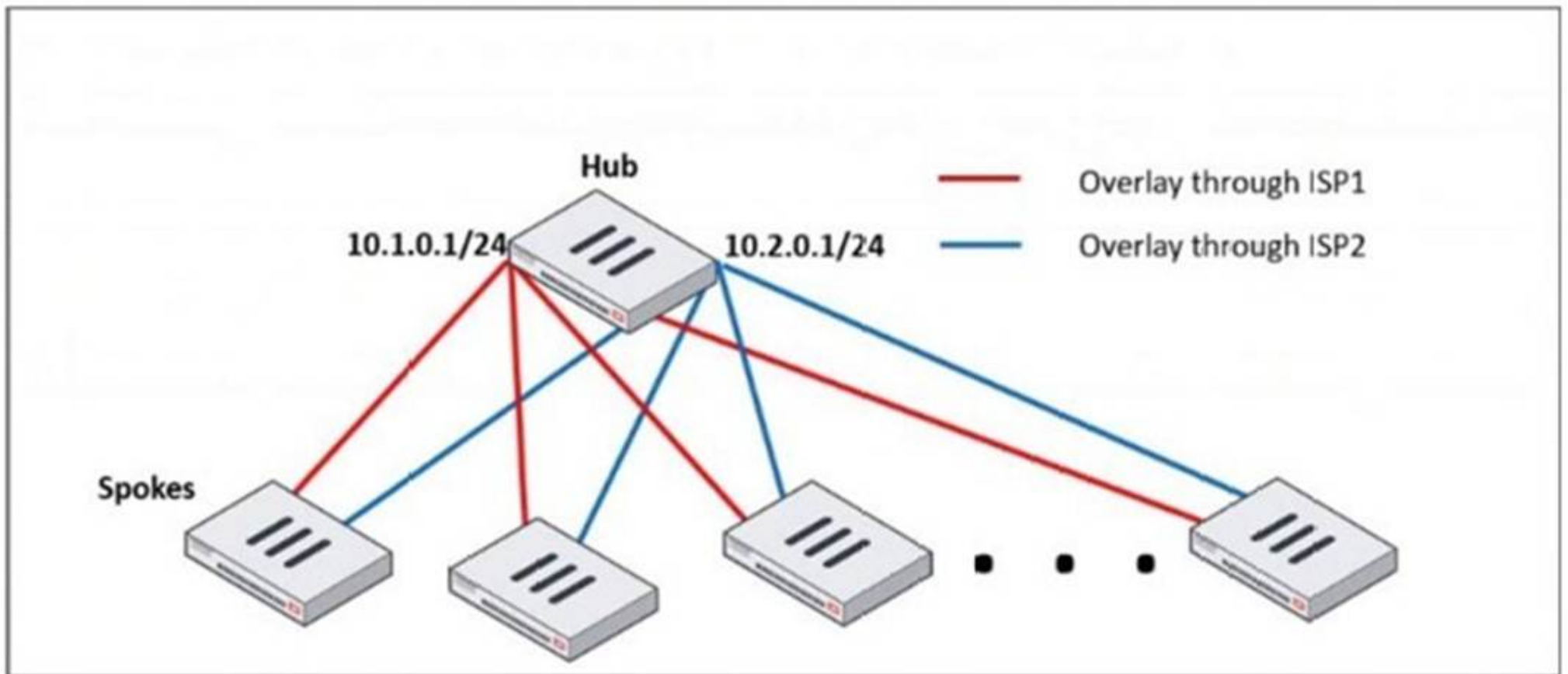
In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

- 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.

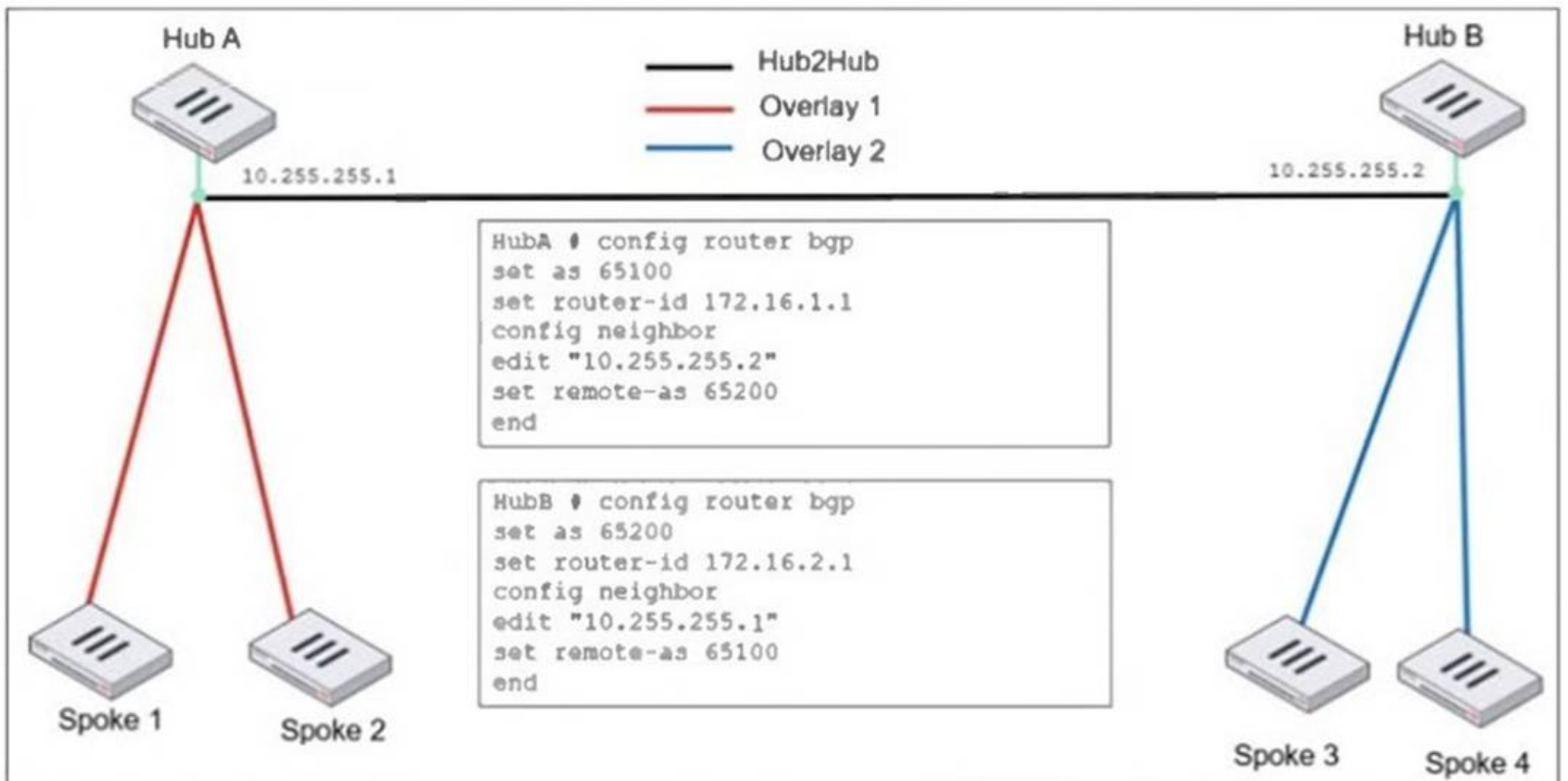
What are two valid approaches to prevent this during future migrations? (Choose two.)

- 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, 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 5

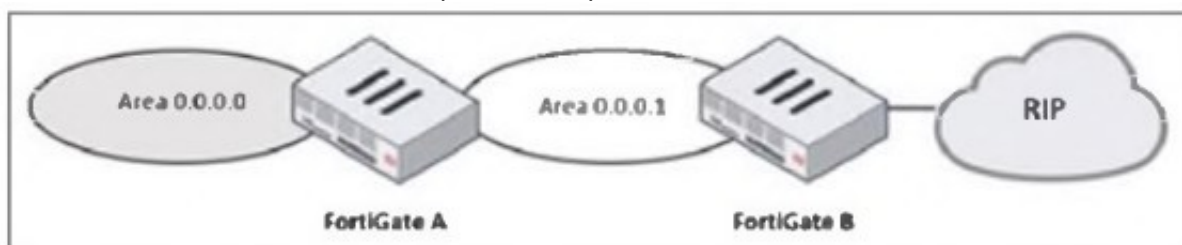
An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection. The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best available connection.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

Normal

Single Sign-On

super_admin_readonly

Default login page

Default admin profile

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 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?

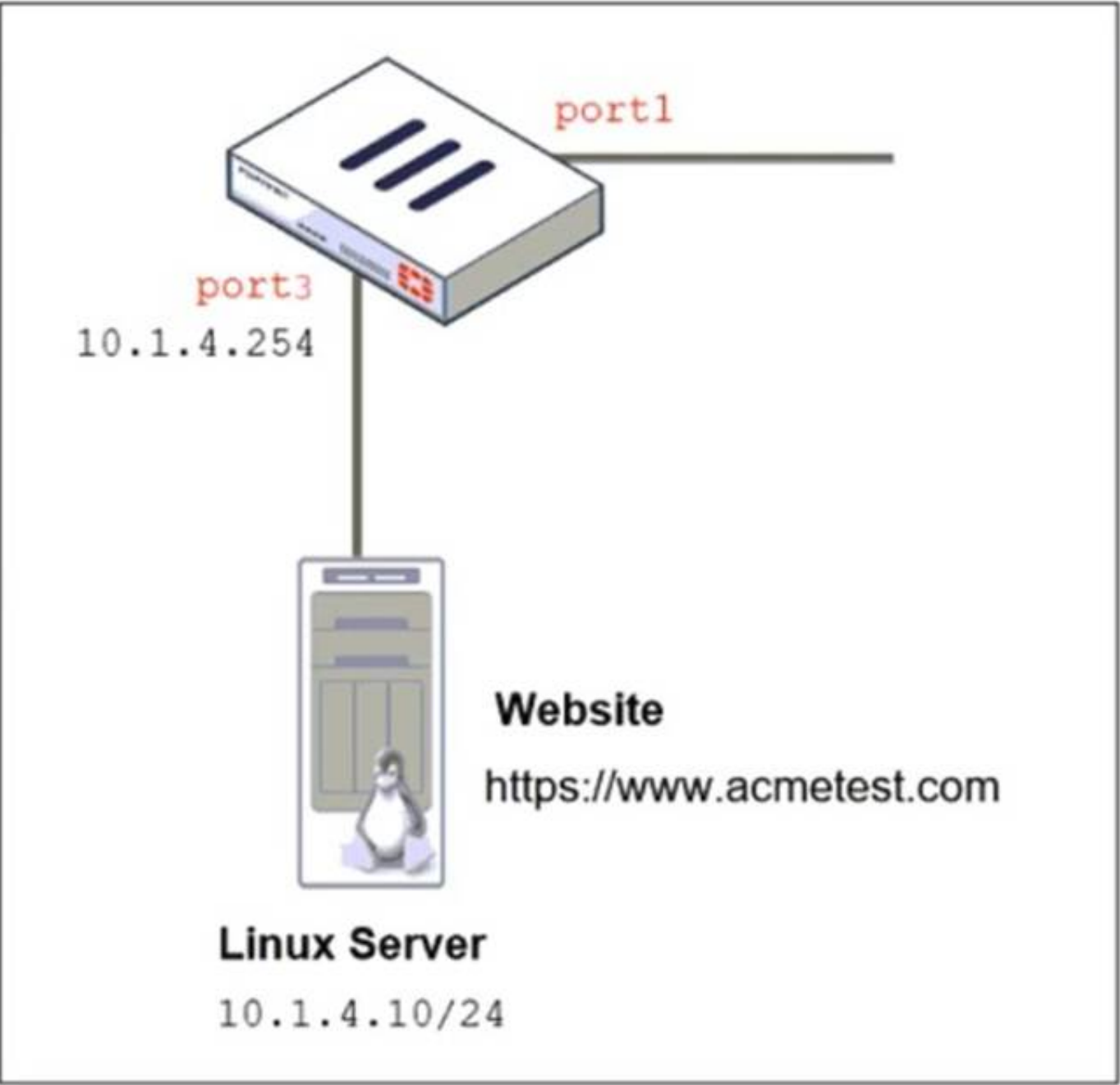
- A. Use IKEv2, which encrypts peer IDs and prevents exposure.
- B. Opt for SSL VPN web mode because it does not use peer IDs at all.
- C. Choose IKEv1 aggressive mode because it simplifies peer identification.
- D. Stick with IKEv1 main mode because it offers better performance.

Answer: A

NEW QUESTION 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

Inspection method

SSL Certificate InspectionFull SSL Inspection

CA certificate

Fortinet_CA_SSL

Download

Blocked certificates

AllowBlock

View Blocked Certificates

Untrusted SSL certificates

AllowBlockIgnore

View Trusted CAs List

Server certificate SNI check

EnableStrictDisable

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 10

Refer to the exhibit.
A pre-run CLI template that is used in zero-touch provisioning (ZTP) and low-touch provisioning (LTP) with FortiManager is shown.

Template Groups	IPsec Tunnel	SD-WAN	System Templates	Static Route	CLI	Feature Visibility
+ Create New Edit Delete Assign to Model Device More						
☐	Name	Type	Assigned to Device/Group		Variables	
Pre-Run CLI Template (4)						
☒	Pre-CLI Template	CLI	0 Devices in Total		GW Hostname IP_port1 IP_port3 IP_port8	

The template is not assigned even though the configuration has already been installed on FortiGate.
What is true about this scenario?

- A. The administrator did not assign the template correctly when adding the model device because pre-CLI templates remain permanently assigned to the firewall
- B. Pre-run CLI templates are automatically unassigned after their initial installation
- C. Pre-run CLI templates for ZTP and LTP must be unassigned manually after the first installation to avoid conflicting error objects when importing a policy package
- D. The administrator must use post-run CLI templates that are designed for ZTP and LTP

Answer: B

NEW QUESTION 11

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 15

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 18

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 19

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 21

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?

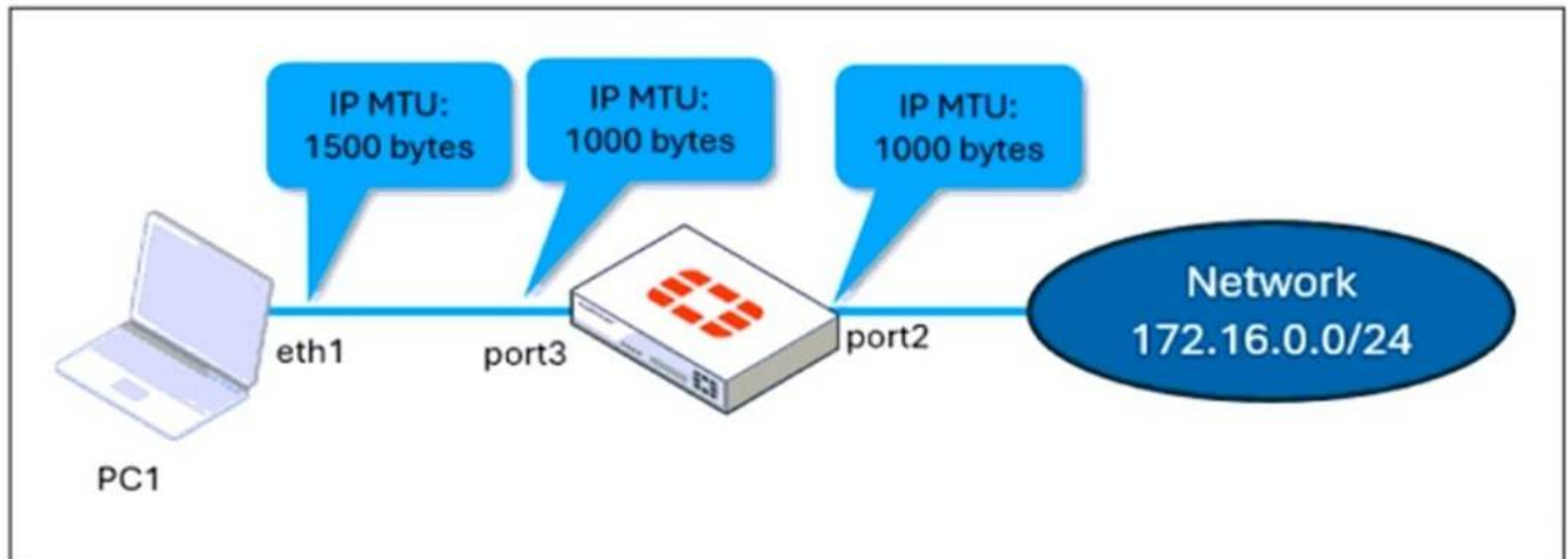
- A. This configuration is the best for networks with regular traffic intervals, providing a balance between connectivity assurance and resource utilization.
- B. Peer IDs are unencrypted and exposed, creating a security risk.
- C. FortiGate will not add a route to its routing or forwarding information 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 25

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.

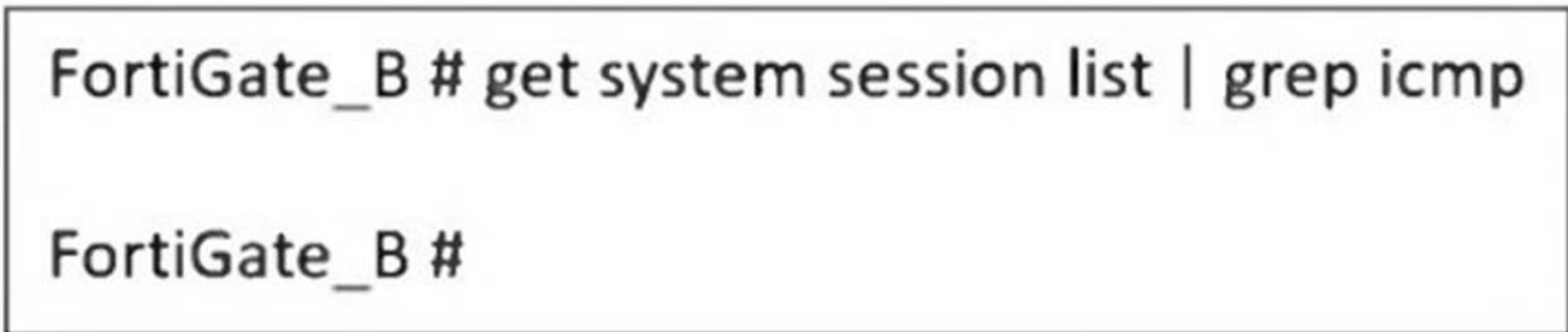
Why is the user in Windows PC1 unable to ping server 172.16.0.254 and is seeing the message: Packet needs to be fragmented but DF set?

- 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 26

Refer to the exhibit, which shows a command output.



FortiGate_A and FortiGate_B are members of an FGSP cluster in an enterprise network. While testing the cluster using the ping command, the administrator monitors packet loss

and found that the session output on FortiGate_B is as shown in the exhibit.

What could be the cause of this output on FortiGate_B?

- A. The session synchronization is encrypted.
- B. session-pickup-connectionless is set to disable on FortiGate_B.
- C. FortiGate_B is configured in passive mode.
- D. FortiGate_A and FortiGate_B have the same standalone-group-id value.

Answer: B

NEW QUESTION 30

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 33

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 36

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 41

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.

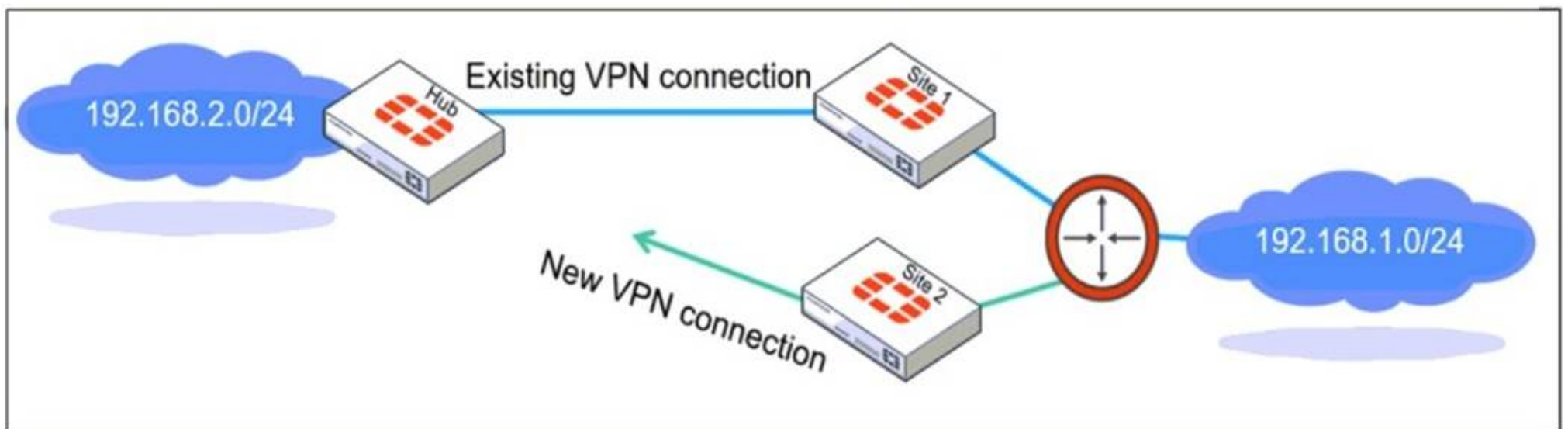
How can an administrator apply IPS in a way that ensures it does not disrupt existing applications in the network?

- 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 48

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.



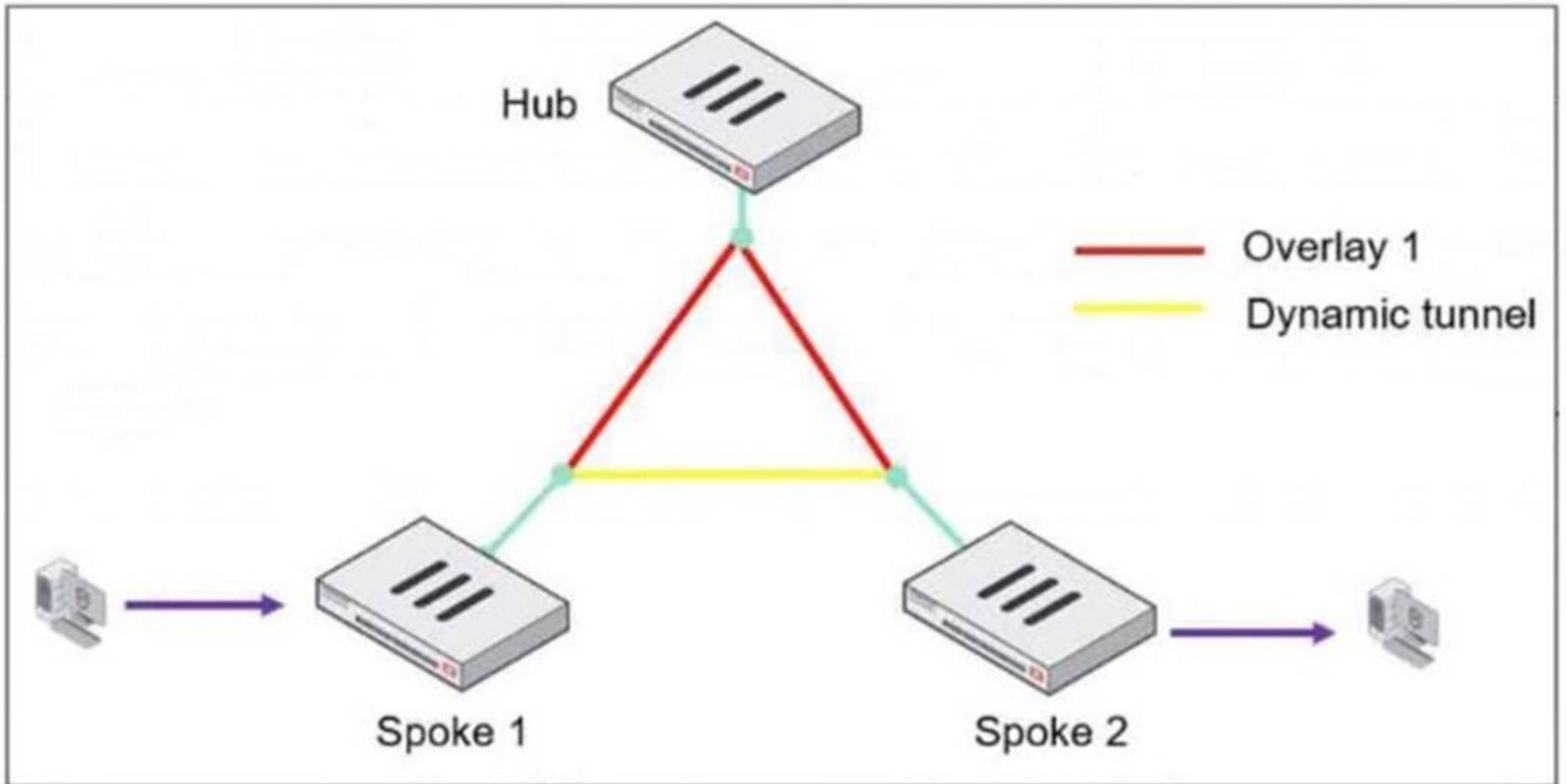
Which IPsec phase 2 configuration must an administrator make on the FortiGate hub to enable equal-cost multi-path (ECMP) routing when multiple remote sites connect with overlapping subnets?

- 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 49

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 51

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 ASBR
```

An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.
 Which statement on this FortiGate device is correct?

- A. The FortiGate device can inject external routing information.
- B. The FortiGate device is in the area 0.0.0.5.
- C. The FortiGate device does not support OSPF ECMP.
- D. The FortiGate device is a backup designated router.

Answer: A

NEW QUESTION 54

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 55

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_EFW_AD-7.6 Practice Test Here](#)