



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

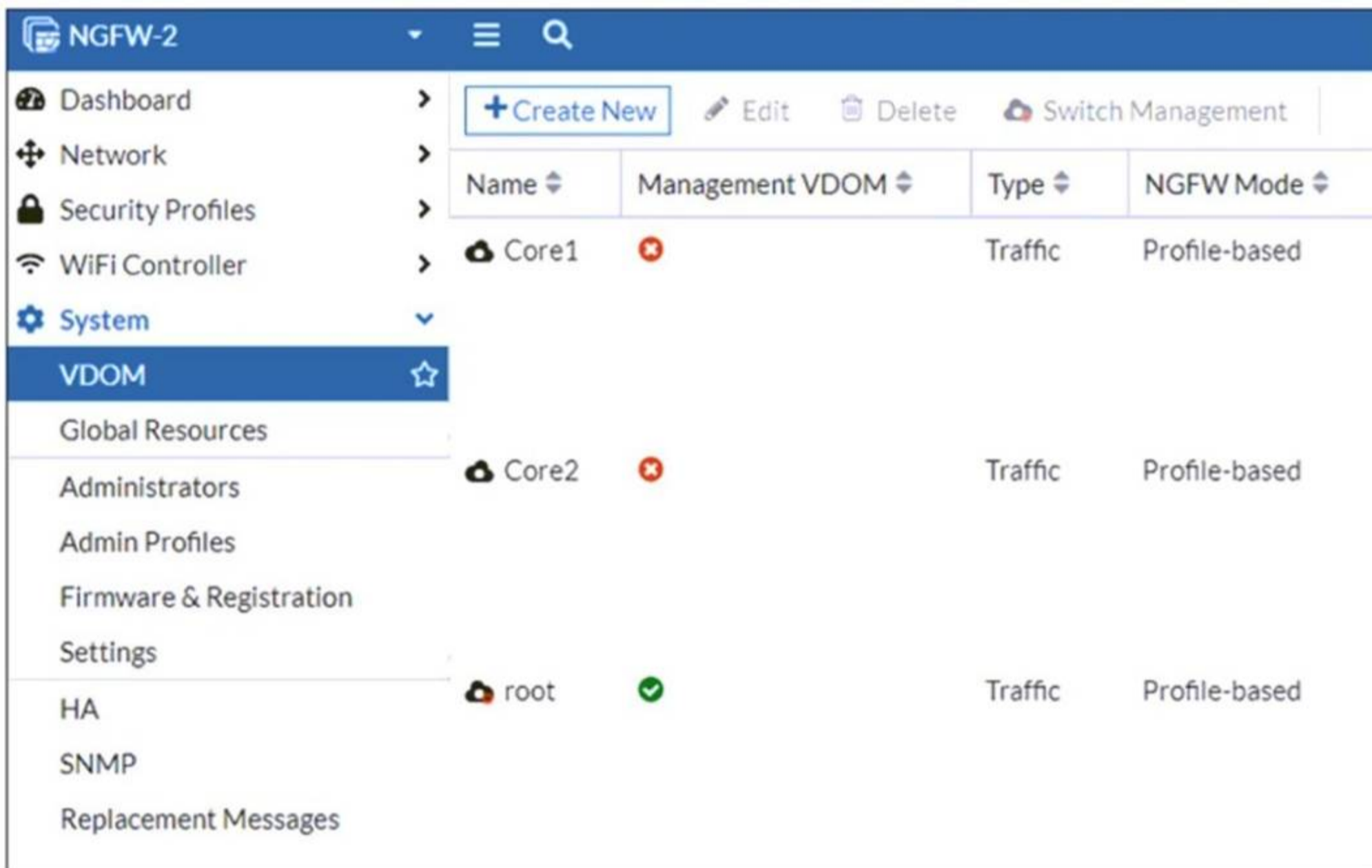
The IT department discovered during the last network migration that all zero phase selectors in phase 2 IPsec configurations impacted network operations. What are two valid approaches to prevent this during future migrations? (Choose two.)




- 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 2

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

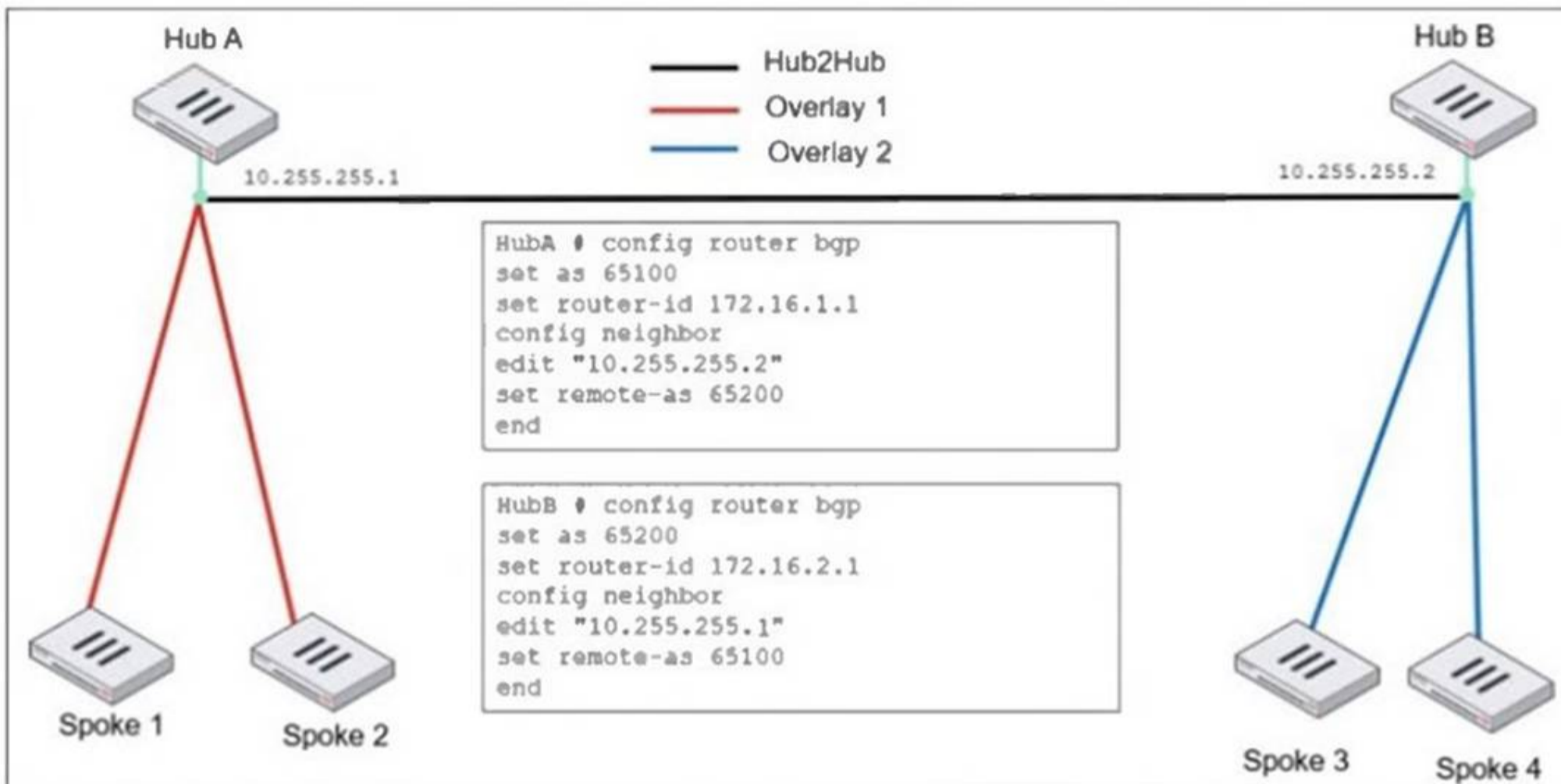
An administrator discovers that webfilter stopped working in Core1 and Core2 after a maintenance window. Which two reasons could explain why webfilter stopped working? (Choose two.)

- 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 3

Refer to the exhibit, which shows an ADVPN network



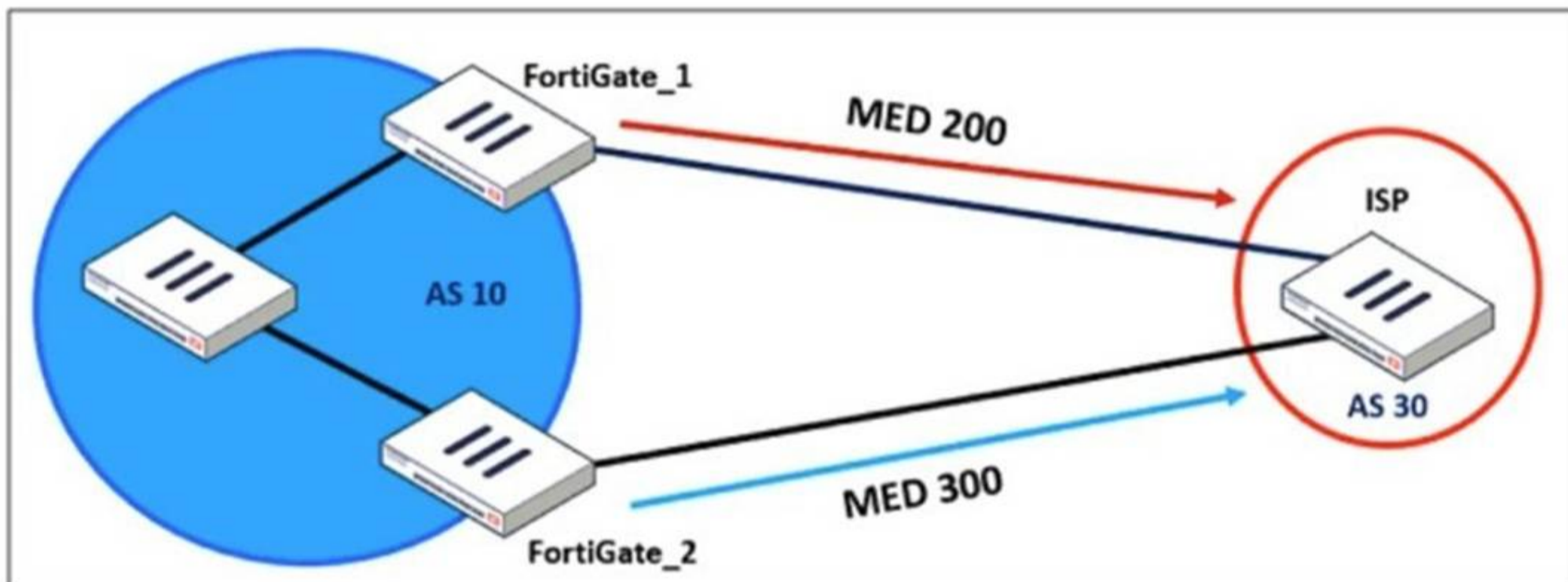
An administrator must configure an ADVPN using IBGP and EBGP to connect overlay network 1 with 2. What two options must the administrator configure in BGP? (Choose two.)

- 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 a network diagram.



An administrator would like to modify the MED value advertised from FortiGate_1 to a BGP neighbor in the autonomous system 30. What must the administrator configure on FortiGate_1 to implement this?

- A. route-map-out
- B. network-import-check
- C. prefix-list-out
- D. distribute-list-out

Answer: A

NEW QUESTION 5

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 6

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		
<input type="checkbox"/>	Name	Type	Assigned to Device/Group		Variables		
Pre-Run CLI Template (4)							
<input checked="" type="checkbox"/>	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 7

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 8

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 9

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 10

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 10

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 12

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 15

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 16

A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on the policy.
 How can an administrator ensure that FortiGate can analyze encrypted HTTPS traffic on a website?

- A. The administrator must enable reputable websites to allow only SSL/TLS websites rated by FortiGuard web filter.
- B. The administrator must enable URL extraction from SNI on the SSL certificate inspection to ensure the TLS three-way handshake is correctly analyzed by FortiGate.
- C. The administrator must enable DNS over TLS to protect against fake Server Name Indication (SNI) that cannot be analyzed in common DNS requests on HTTPS websites.
- D. The administrator must enable full SSL inspection in the SSL/SSH Inspection Profile to decrypt packets and ensure they are analyzed as expected.

Answer: D

NEW QUESTION 18

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 23

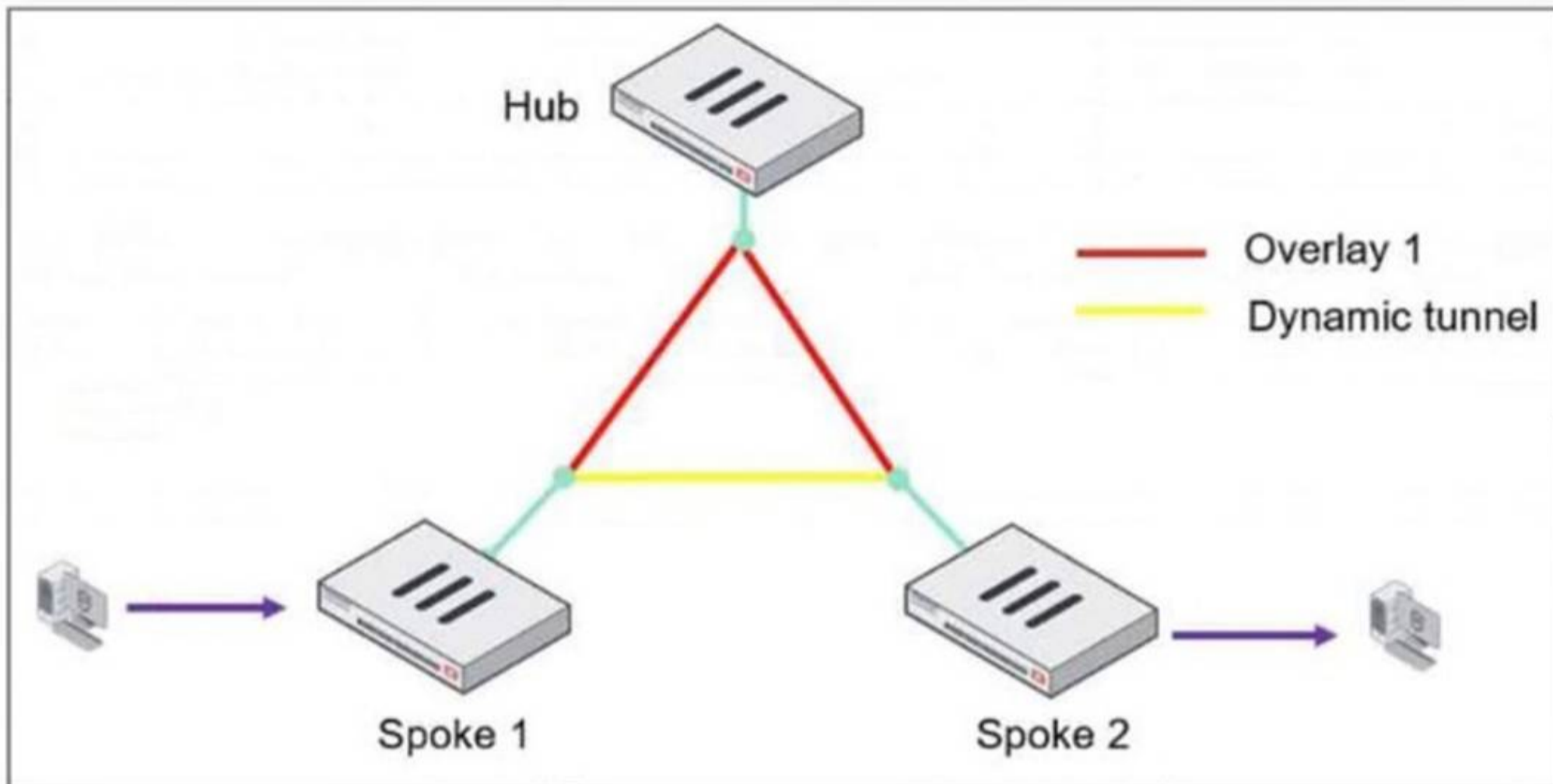
A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices.
 Which three approaches can the company take to successfully deploy advanced initial configurations on remote branches? (Choose three.)

- A. Use metadata variables to dynamically assign values according to each FortiGate device.
- B. Use provisioning templates and install configuration settings at the device layer.
- C. Use the Global ADOM to deploy global object configurations to each FortiGate device.
- D. Apply Jinja in the FortiManager scripts for large-scale and advanced deployments.
- E. Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices.

Answer: ABE

NEW QUESTION 28

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 29

.....

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/>