Fortinet

Exam Questions FCSS_EFW_AD-7.6

FCSS - Enterprise Firewall 7.6 Administrator

NEW QUESTION 1
Refer to the exhibit, which shows a partial troubleshooting command output.

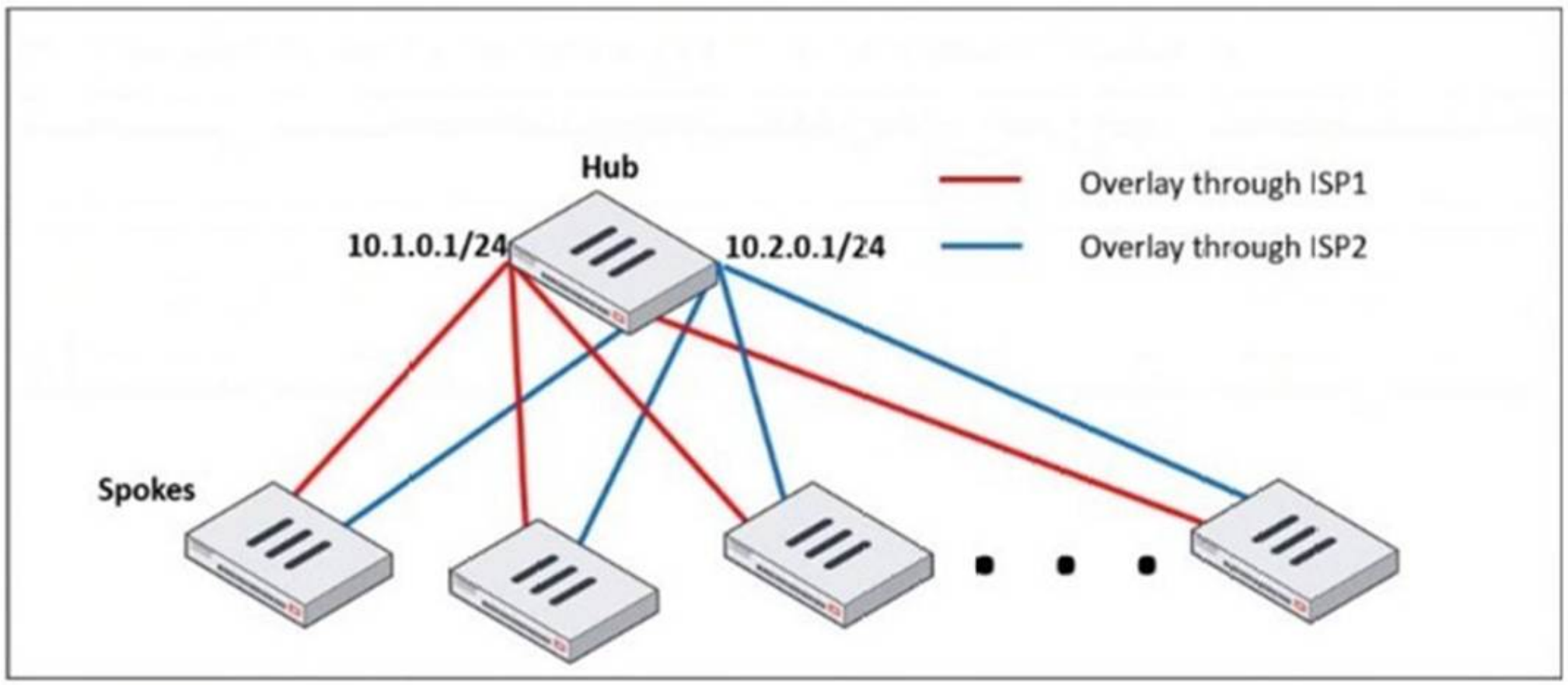
```
FortiGate # diagnose vpn tunnel list name Hub2Spoke1

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
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

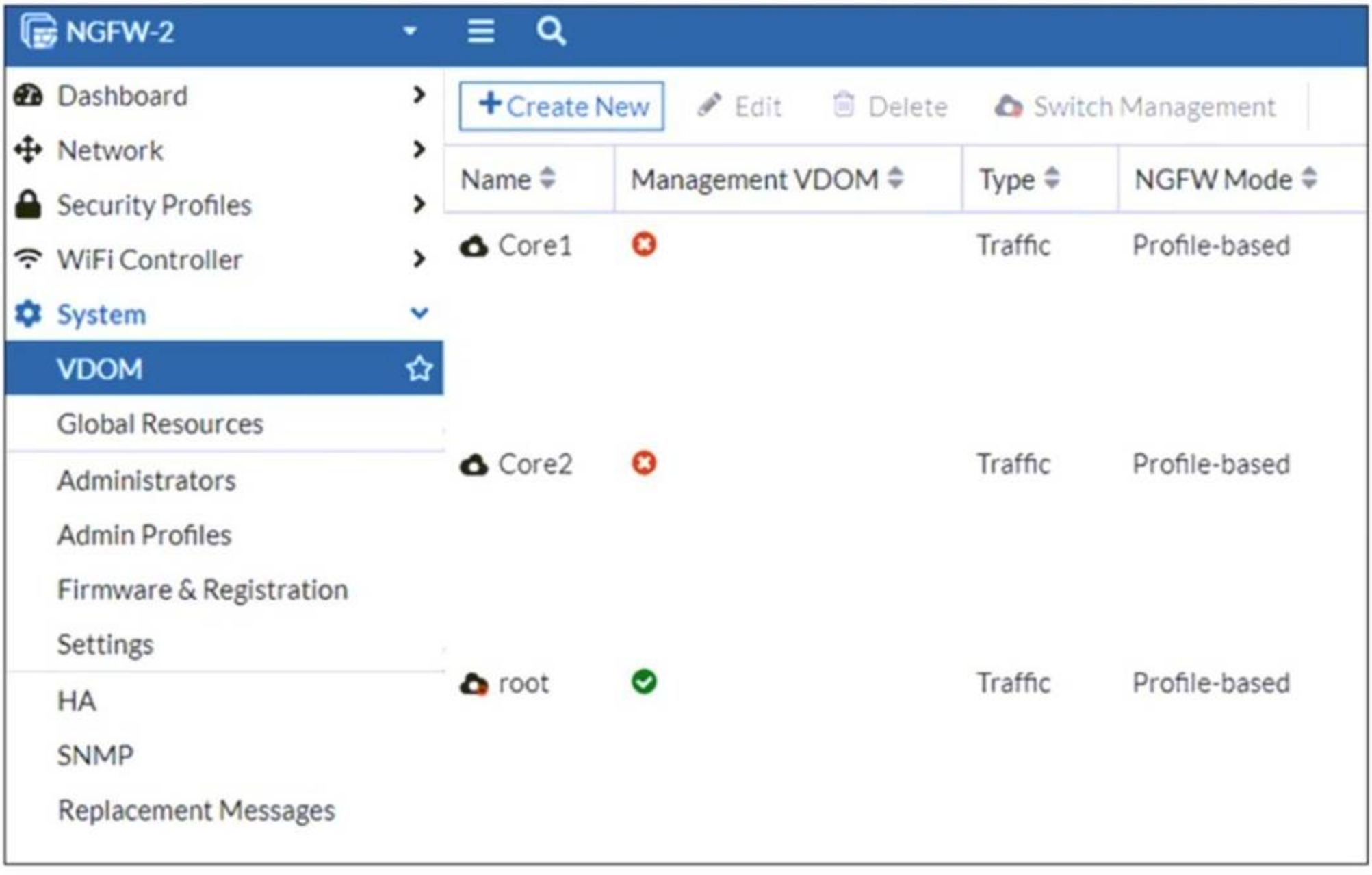
Answer: AC

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 the VDOM section of a FortiGate device.

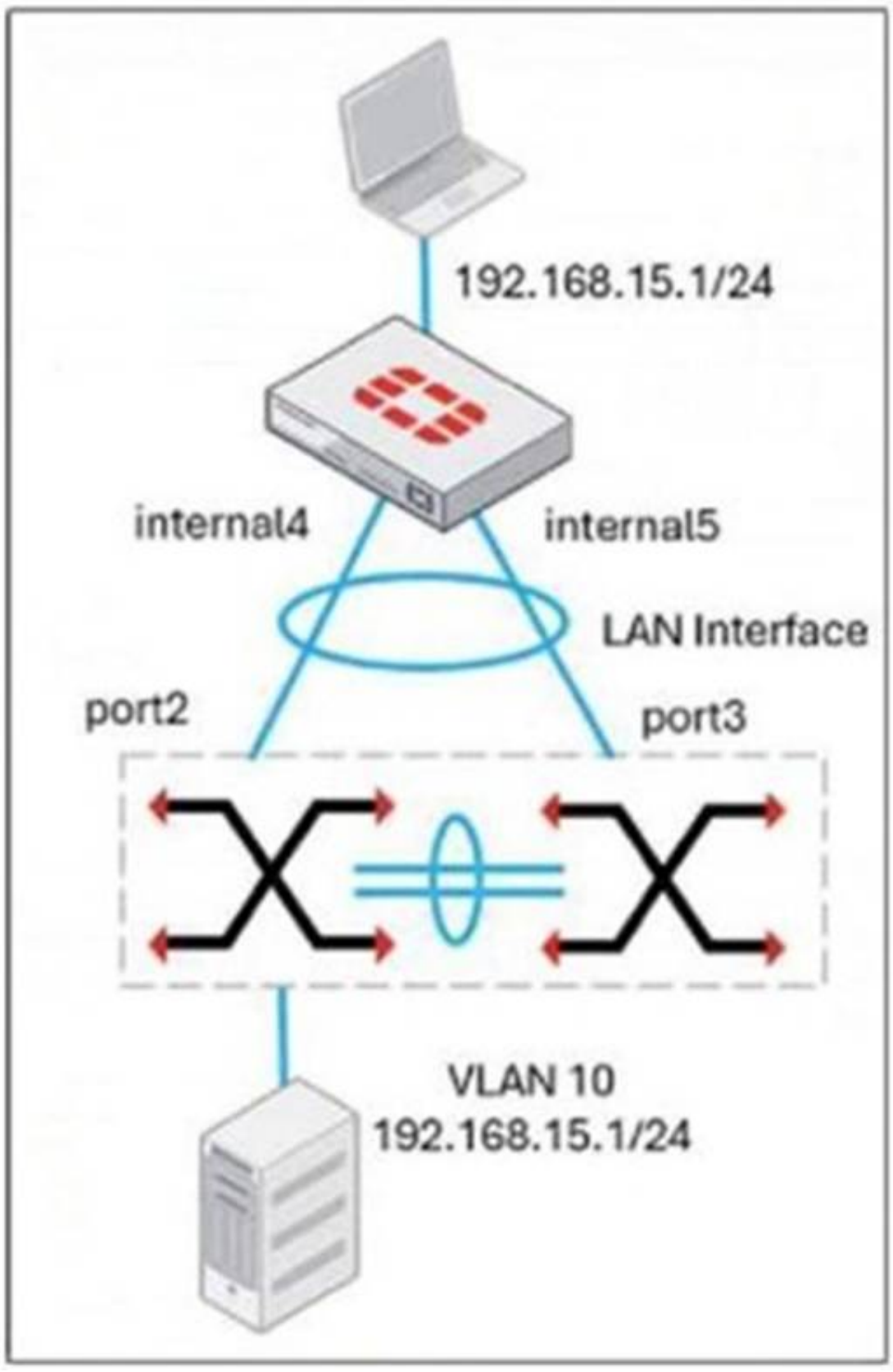


An administrator discovers that webfilter stopped working in Core1 and Core2 after a maintenance window.
Which two reasons could explain why webfilter stopped working? (Choose two.)

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 Corel 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 5
Refer to the exhibit, which shows a LAN interface connected from FortiGate to two FortiSwitch devices.

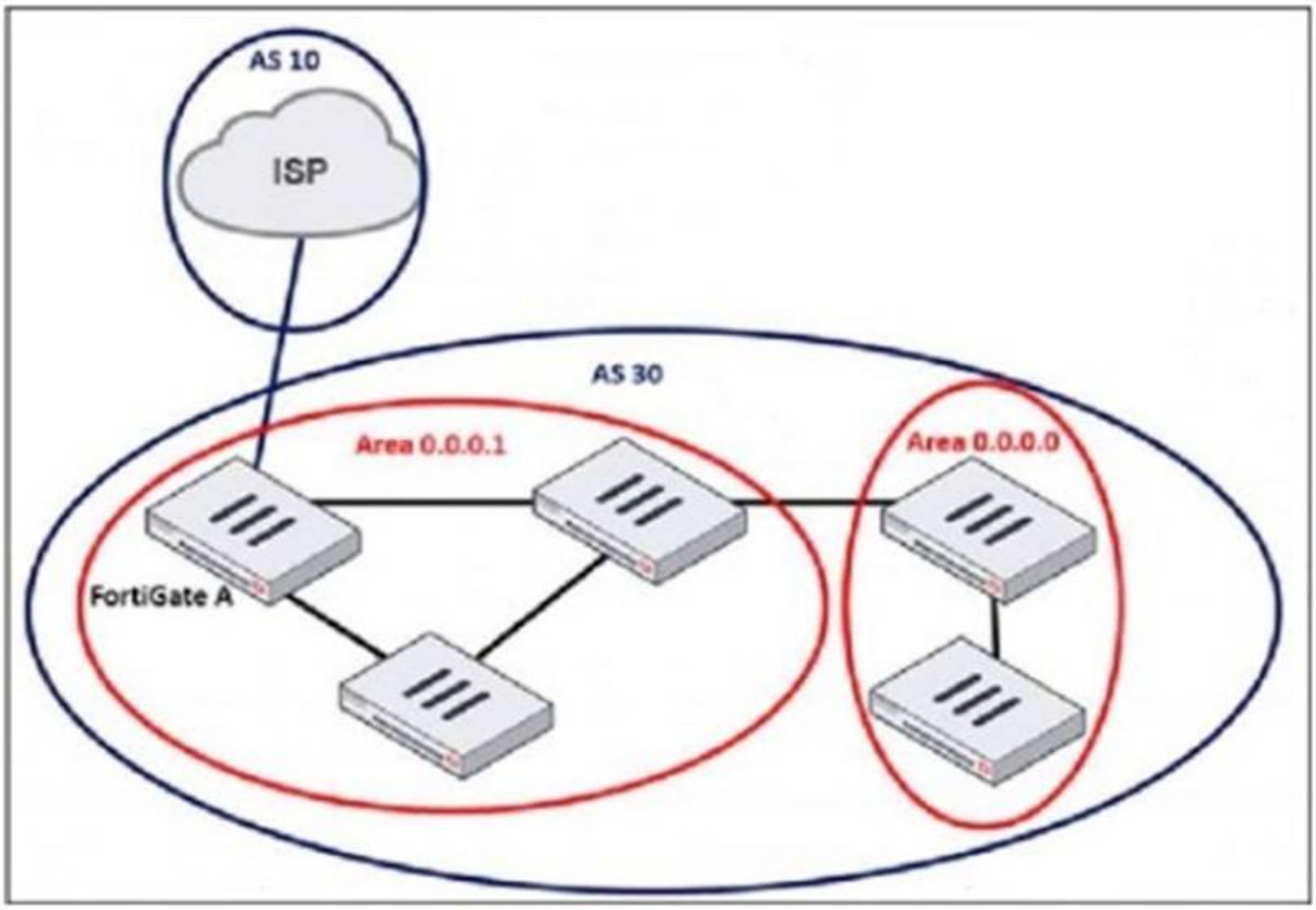


What two conclusions can you draw from the corresponding LAN interface? (Choose two.)

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 6
Refer to the exhibit, which shows an enterprise network connected to an internet service provider.



The administrator must configure the BGP section of FortiGate A to give internet access to the enterprise network.
Which command must the administrator use to establish a connection with the internet service provider?

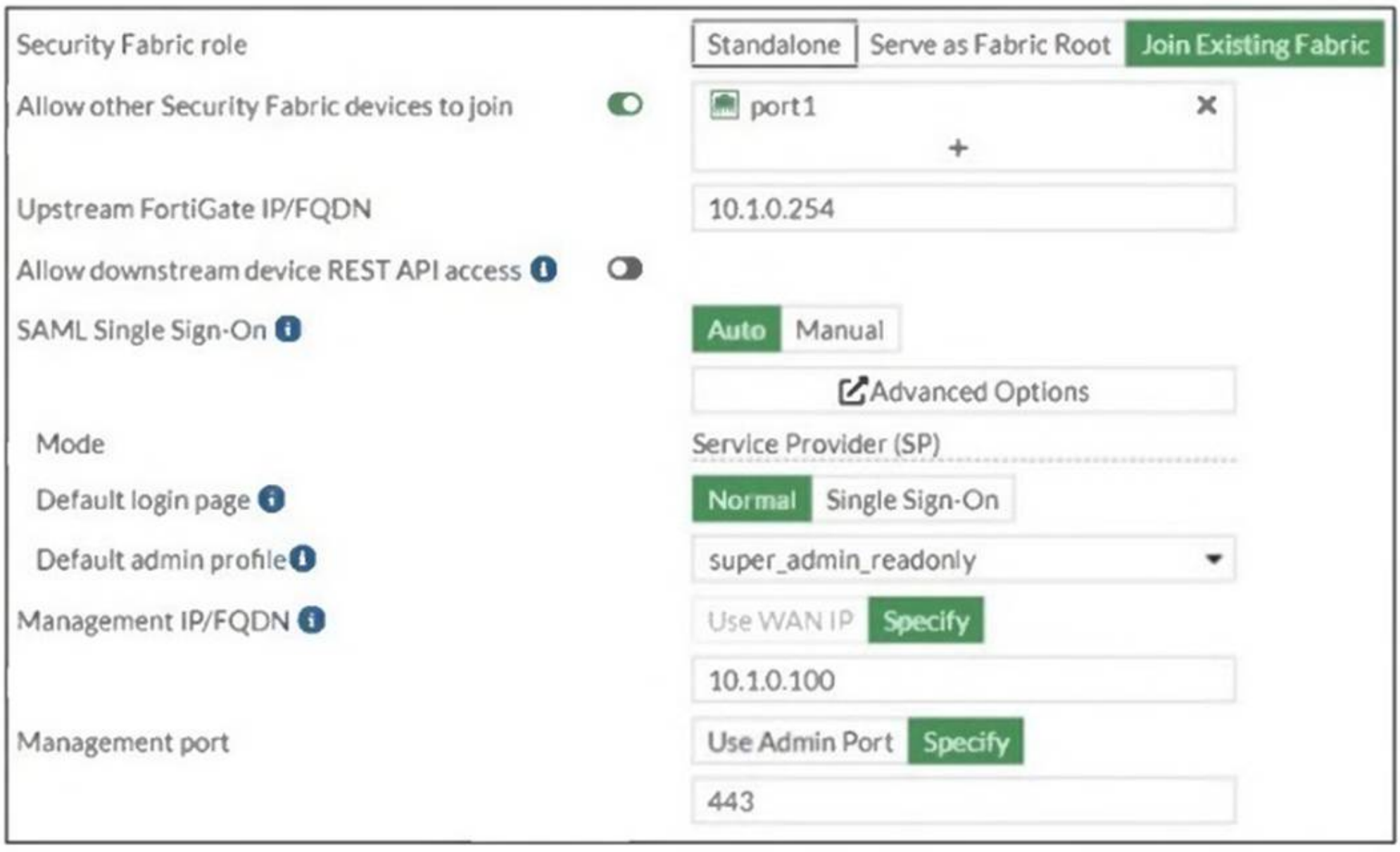
A. config neighbor
B. config redistribute bgp
C. config router route-map
D. config redistribute ospf

Answer: A

NEW QUESTION 7
Refer to the exhibits.

Root FortiGate - System Administrator configuration

System Administrator 2	
admin	super_admin
AdminSSO	super_admin_readonly



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

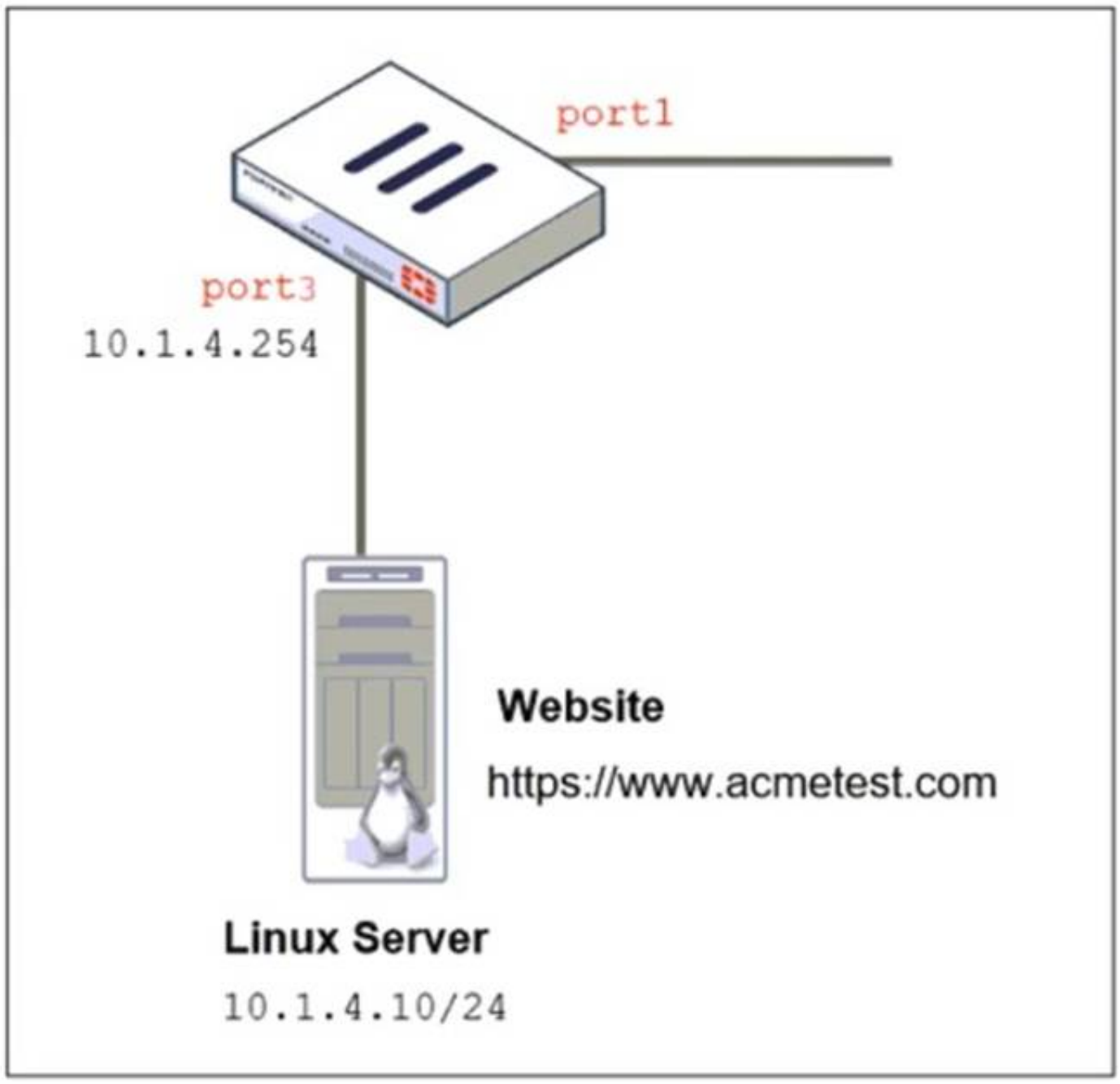
NEW QUESTION 8
What does the command set forward-domain <domain_ID> in a transparent VDOM interface do?

A. It configures the interface to prioritize traffic based on the domain ID, enhancing quality of service for specified VLANs.
B. It isolates traffic within a specific VLAN by assigning a broadcast domain to an interface based on the VLAN ID.
C. It restricts the interface to managing traffic only from the specified VLAN, effectively segregating network traffic.
D. It assigns a unique domain ID to the interface, allowing it to operate across multiple VLANs within the same VDOM.

Answer: B

NEW QUESTION 9
Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

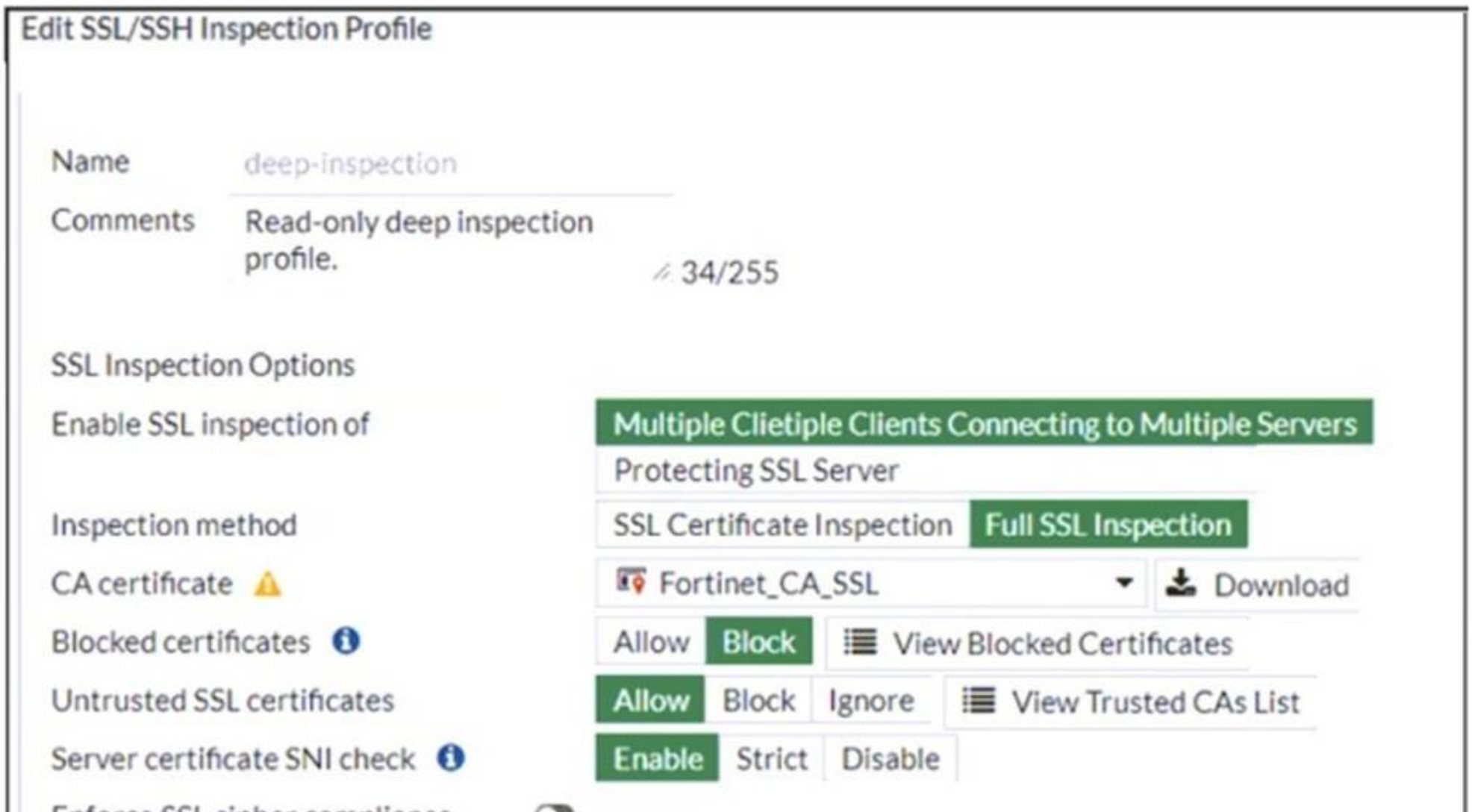
Network Topology



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



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
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.

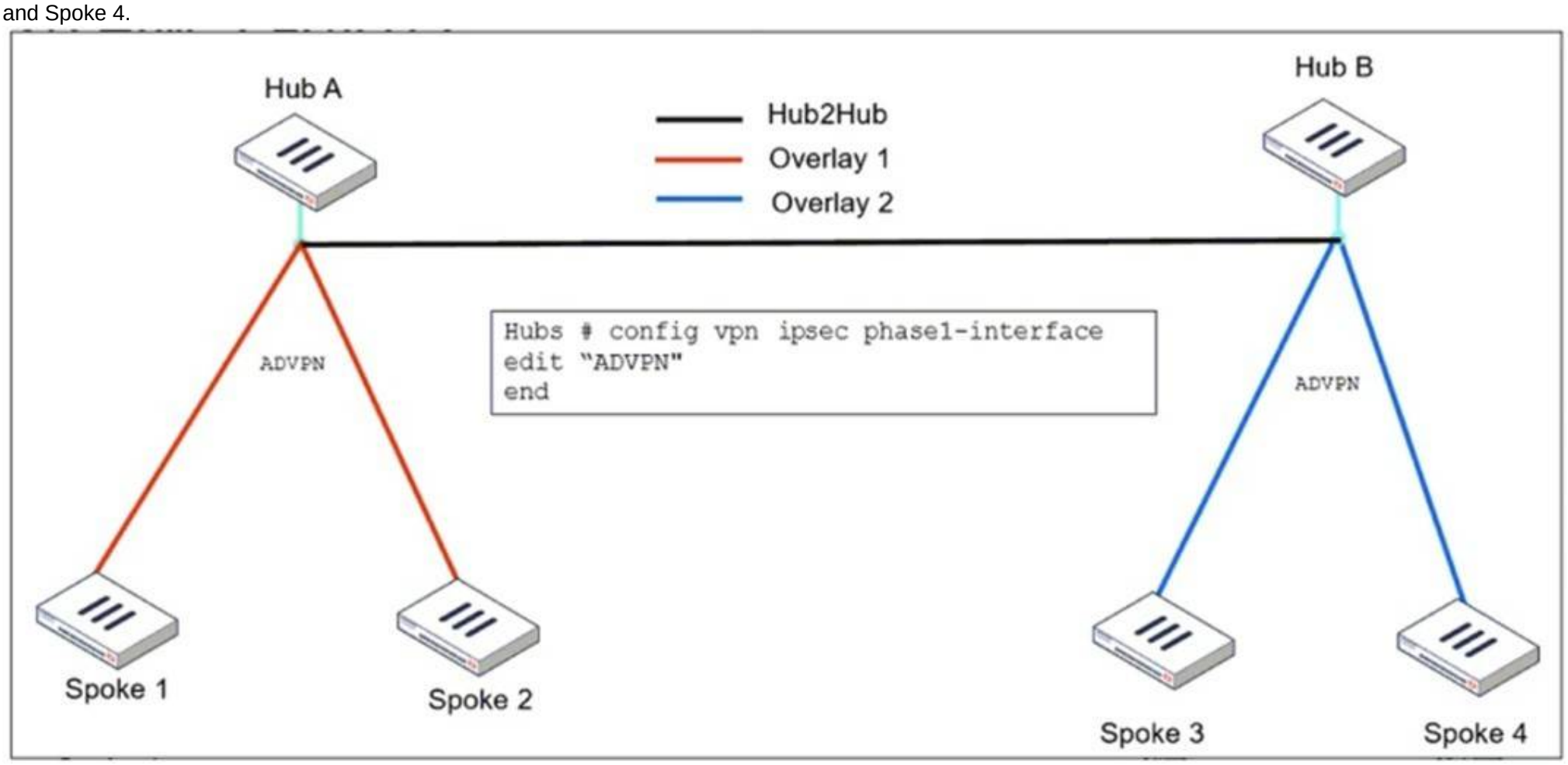
Answer: B

NEW QUESTION 10
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 13
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 14
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 15
Refer to the exhibit, which shows the HA status of an active-passive cluster.

Status	Priority	Hostname	Virtual Domains	Role	System Uptime
Virtual cluster 1 2					
Synchronized	150	FortiGate_A	Core1 root	Primary	4h 52m
Synchronized	100	FortiGate_B	Core1 root	Secondary	4h 52m
Virtual cluster 2 2					
Synchronized	150	FortiGate_A	Core2	Primary	
Synchronized	128	FortiGate_B	Core2	Secondary	

An administrator wants FortiGate_B to handle the Core2 VDOM traffic.
Which modification must the administrator apply to achieve this?

A. The administrator must disable override on FortiGate_A.
B. The administrator must change the priority from 100 to 160 for FortiGate_B.
C. The administrator must change the load balancing method on FortiGate_B.
D. The administrator must change the priority from 128 to 200 for FortiGate_B.

Answer: D

NEW QUESTION 17
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 20
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 25
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 30
Refer to the exhibit, which shows the packet capture output of a three-way handshake between FortiGate and FortiManager Cloud.

Packet capture output of three-way handshake between a FortiGate and a FortiManager Cloud

```
> Frame 35: 1034 bytes on wire (8272 bits), 1034 bytes captured (8272 bits) on interface -, id 0
> Ethernet II, Src: 50:e5:d5:         (50:e5:d5:         ), Dst: Fortinet_         (e0:23:ff:         )
> Internet Protocol Version 4, Src: 192.168.2.60, Dst: 154.52.4.164
> Transmission Control Protocol, Src Port: 16304, Dst Port: 541, Seq: 1, Ack: 1, Len: 980
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 975
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 971
      > Version: TLS 1.2 (0x0303)
        Random: a14f6c4b8f9313bf
        Session ID Length: 32
        Session ID: a0de426e96e83a5
        Cipher Suites Length: 34
      > Cipher Suites (17 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 864
      v Extension: server_name (len=45) name=9398.support.fortinet-ca2.fortinet.com
          Type: server_name (0)
          Length: 45
        v Server Name Indication extension
            Server Name list length: 43
            Server Name Type: host_name (0)
            Server Name length: 40
            Server Name: 9398.support.fortinet-ca2.fortinet.com
      > Extension: ec_point_formats (len=4)
      > Extension: supported_groups (len=22)
      > Extension: session_ticket (len=0)
      > Extension: encrypt_then_mac (len=0)
      > Extension: extended_master_secret (len=0)
      > Extension: signature_algorithms (len=48)
      > Extension: supported_versions (len=9) TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0
      > Extension: psk_key_exchange_modes (len=2)
```

What two conclusions can you draw from the exhibit? (Choose two.)

A. FortiGate will receive a certificate that supports multiple domains because FortiManager operates in a cloud computing environment.
B. FortiGate is connecting to the same IP server and will receive an independent certificatefor its connection between FortiGate and FortiManager Cloud.
C. If the TLS handshake contains 17 cipher suites it means the TLS version must be 1.0 on this three-way handshake.
D. The wildcard for the domain *.fortinet-ca2.support.fortinet.com must be supported by FortiManager Cloud.

Answer: D

NEW QUESTION 34
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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