Fortinet

Exam Questions FCSS_SDW_AR-7.4

FCSS - SD-WAN 7.4 Architect

NEW QUESTION 1
Refer to the exhibits.

Ping result

```
root@branch1-client-cli# ping facebook.com
PING facebook.com (157.240.19.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35): icmp_seq=1 ttl=56 time=33.4 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35): icmp_seq=2 ttl=56 time=32.5 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35): icmp_seq=3 ttl=56 time=32.5 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35): icmp_seq=4 ttl=56 time=32.6 ms
```

Diagnose output

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1(0x01) dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=21(HUB1-VPN2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 10.1.0.7/255.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:44

id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(2): oif=3(port1), oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(2): Salesforce(16920,0) Microsoft.Portal(41469,0)
hit_count=13 rule_last_used=2025-01-06 01:55:12

id=2130903043(0x7f030003) vwl_service=3(Corp) vwl_mbr_seq=4 5 6 7 8 9 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(6): oif=20(HUB1-VPN1), oif=21(HUB1-VPN2), oif=22(HUB1-VPN3), oif=23(HUB2-VPN1), oif=24(HUB2-VPN2),
oif=25(HUB2-VPN3)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:49

id=2130903045(0x7f030005) vwl_service=5(Internet) vwl_mbr_seq=3 2 1 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(3): oif=6(port4), oif=4(port2) path_last_used=2025-01-06 02:12:08, oif=3(port1)
source(1): 10.0.1.0-10.0.1.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=27 rule_last_used=2025-01-06 02:12:08
```

Diagnose output

```
branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list
List App Ctrl Database Entry(IPv4) in Kernel:

Max_App_Ctrl_Size=32768 Num_App_Ctrl_Entry=8

Facebook(15832 23): IP=157.240.19.35 6 443

Addicting.Games(30156 8): IP=172.64.80.1 6 443

Microsoft.Portal(41469 28): IP=184.27.181.201 6 443

LinkedIn(16331 23): IP=13.107.42.14 6 443

MSN.Game(16135 8): IP=13.107.246.35 6 443

Salesforce(16920 29): IP=23.222.17.73 6 443

Salesforce(16920 29): IP=23.222.17.76 6 443

Facebook(15832 23): IP=31.13.80.36 6 443
```

You connect to a device behind a branch FortiGate device and initiate a ping test. The device is part of the LAN subnet and its IP address is 10.0.1.101.
Based on the exhibits, which interface uses branch 1_fgt to steer the test traffic?

A. port4
B. HUB1-VPN1
C. port1

D. port2

Answer: B

NEW QUESTION 2
Refer to the exhibits.

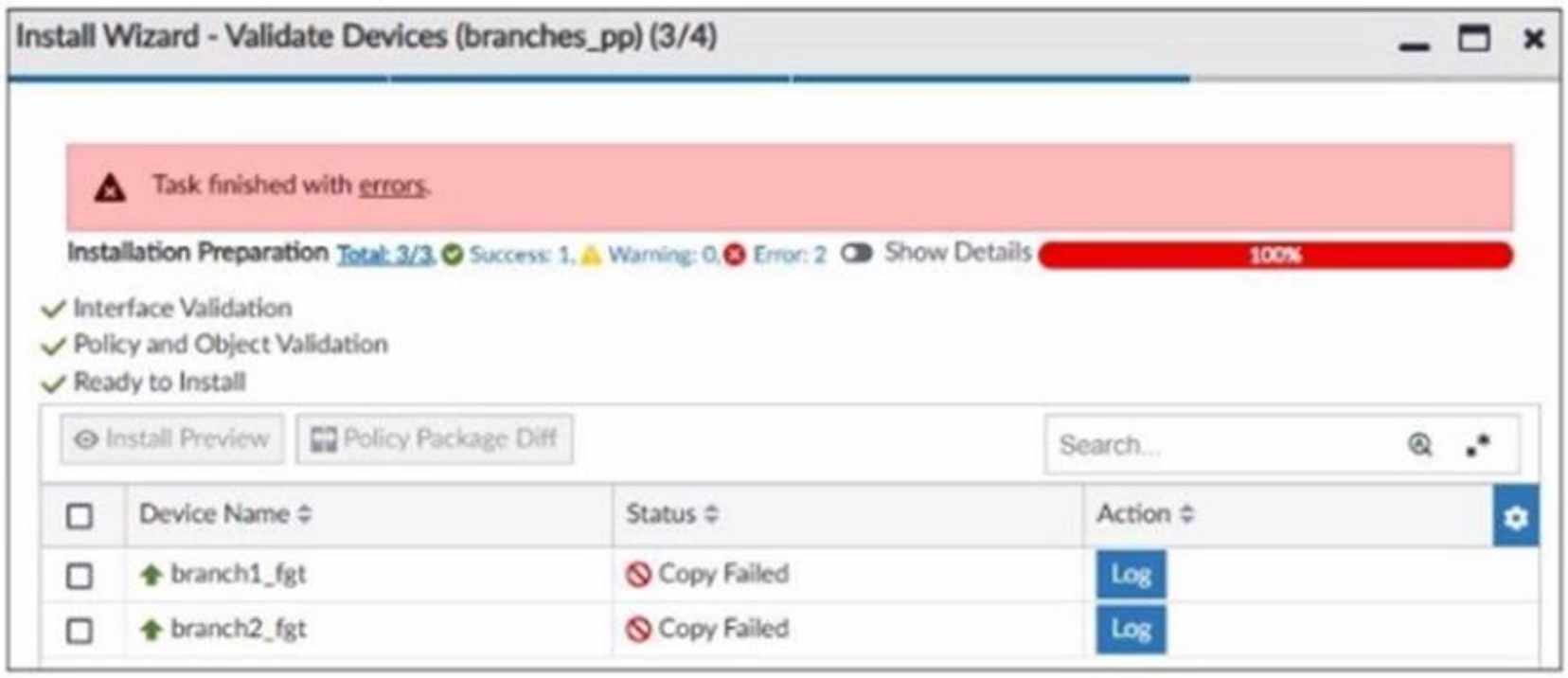
SD-WAN template on FortiManager

Name	Assigned to Device/Group	Interface
branches	2 Devices in Total View Details > branch1_fgt [root] branch2_fgt [root]	port1 port2

Firewall policies

Underlay (2/3 Total:2)									
2	SIA	LAN	port1	LAN-net	all	always	FTP HTTP HTTPS	Accept	SSL no-inspection PROT default
3	DIA	LAN	underlay	LAN-IT	all	always	ALL	Accept	APP default SSL certificate-i... PROT default

FortiManager error message



You use FortiManager to manage the branch devices and configure the SD-WAN template. You have configured direct internet access (DIA) for the IT department users. Now. you must configure secure internet access (SIA) for all local LAN users and have set the firewall policies as shown in the second exhibit.
Then, when you use the install wizard to install the configuration and the policy package on the branch devices, FortiManager reports an error as shown in the third exhibit.
Which statement describes why FortiManager could not install the configuration on the branches?

A. You must direct SIA traffic to a VPN tunnel.
B. You cannot install firewall policies that reference an SD-WAN zone.
C. You cannot install firewall policies that reference an SD-WAN member.
D. You cannot install SIA and DIA rules on the same device.

Answer: C

NEW QUESTION 3
SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic.
Which three configuration elements that you must configure before FortiGate can steer traffic according to SD-WAN rules? (Choose three.)

A. Firewall policies
B. Interfaces
C. Security profiles
D. Traffic shaping
E. Routing

Answer: ABE

NEW QUESTION 4
Refer to the exhibit.

Diagnose output

```
fgt_A # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


fgt_A # diagnose sys sdwan member | grep HUB1
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xd  may_child, gateway: 100.64.1.1,
peer: 192.168.1.29, source 192.168.1.1, priority: 15 1024, weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xd  may_child, gateway: 100.64.1.9,
peer: 192.168.1.61, source 192.168.1.33, priority: 10 1024, weight: 0
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xd  may_child, gateway: 172.16.1.5,
peer: 192.168.1.93, source 192.168.1.65, priority: 1 1024, weight: 0


fgt_A # get router info routing-table all | grep HUB1
S       10.0.0.0/8 [10/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 04:11:41, [1/0]
                    [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 04:11:41, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 04:11:42, [1/0]
                    [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 04:11:42, [1/0]
                    [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 04:11:42, [1/0]
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1_fgtgenerates traffic to the 10.0.0.0/8 network.
The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over HUB1- VPN1. However, the traffic is routed over HUB1-VPN3.
Based on the output shown in the exhibit, which two reasons, individually or together, could explain the observed behavior? (Choose two.)

A. HUB1-VPN3 has a higher member configuration priority than HUB1-VPN1.
B. The traffic matches a regular policy route configured with HUB1-VPN3 as the outgoing device
C. HUB1-VPN1 does not have a valid route to the destination
D. HUB1-VPN3 has a lower route priority value (higher priority) than HUB1-VPN1.

Answer: AD

NEW QUESTION 5
Which two statements correctly describe what happens when traffic matches the implicit SD-WAN rule? (Choose two.)

A. The session information output displays no SD-WAN service id.
B. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.
C. The traffic is distributed, regardless of weight, through all available static routes.
D. Traffic does not match any of the entries in the policy route table.
E. FortiGate flags the session with may_dirty and vwl_def ault.

Answer: AD

NEW QUESTION 6
Exhibit.

```
config system sdwan
    set fail-detect enable
    set fail-alert-interfaces "port5"
    config health-check
        edit "Level3_DNS"
            set update-cascade-interface enable
            set members 1 2
        next
        edit "HQ"
            set update-cascade-interface enable
            set members 3
        next
    end
end
```

Which action will FortiGate take if it detects SD-WAN members as dead?

A. FoftiGate bounces port5 after it detects all SD-WAN members as dead.
B. FortiGate fails over to the secondary device after it detects port5 as dead.
C. FortiGate sends alert messages through poft5 when it detects all SD-WAN members as dead
D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

Answer: D

NEW QUESTION 7
You are planning a new SD-WAN deployment with the following criteria:
- Two regions
- Most of the traffic is expected to remain within its region
- No requirement for inter-region ADVPN
To remain within the recommended best practices, which routing protocol should you select for the overlays?

A. OSPF for the routing within each region and EBGP between the regions.
B. IBGP with BGP on loopback within each region and EBGP between the regions.
C. IBGP with BGP per overlays within each region and IBGP with BGP on loopback between the regions.
D. IBGP within each region and between the regions.

Answer: B

NEW QUESTION 8
Refer to the exhibits.

SD-WAN template zones and rules configuration

SD-WAN Zones

Create New | Edit | Delete | Where Used | Search...

ID	Interface	Gateway	Cost	Priority	Status	Installation Target
virtual-wan-link						
underlay						
1	port1	$(sdwan_port1_gw)	0	1	Enable	
2	port2	0.0.0.0	0	1	Enable	
WAN3						
3	port4	$(sdwan_port4_gw)	0	1	Enable	1 Device in Total branch1_fgt [root]
HUB1						
4	HUB1-VPN1	0.0.0.0	0	1	Enable	
5	HUB1-VPN2	0.0.0.0	0	1	Enable	
6	HUB1-VPN3	0.0.0.0	0	1	Enable	

SD-WAN Rules

Create New | Edit | Delete | More | Search...

ID	Name	Source	Destination	Criteria	Members	Performance SLA	Port	Protocol	Status
1	Critical-DIA	LAN-r	Salesforce Microsoft		port1 port2			any	Enable
3	Corp	LAN-r	Corp-net		HUB1-VPN1 HUB1-VPN2 HUB1-VPN3			any	Enable
	sd-wan	All	All	Source IP	All			any	

FortiManager error message

Install Wizard - Validate Devices (3/4)

Task finished with errors.

Installation Preparation Total: 4/4. Success: 3. Warning: 0. Error: 1 Show Details 100%

Ready to Install

Only successfully validated device may be installed. Please confirm and click "Install" button to continue.

Install Preview | Search...

Device Name	Status	Action
branch1_fgt	Copy Failed	Log
branch2_fgt	Connection Up	
branch3_fgt	Connection Up	

View install log in FortiManager

View Install Log

```
Copy device global objects

Copy objects for vdom root

Commit failed:
error -999 -  - (from Template Group Corp-SOT_BRANCH) (in Template branches) invalid ip - prop[gateway]: ip4class($(sdwan_port1_gw)) invalid ip addr
```

You use FortiManager to configure SD-WAN on three branch devices.
When you install the device settings. FortiManager prompts you with the error "Copy Failed" for the device branch1_fat When you click the log button.
FortiManager displays the message shown in the exhibit.

A. Based on the exhibits, which statement best describes the issue and how you can resolve it?
B. Remove the installation target for the SD-WAN member port4. You cannot combinemetadata variable and installation targets.
C. Gateways forall members in a zone must be defined the same wa
D. Specify the gateway of the SD-WAN member port! without metadata variables.
E. Check the metadata variable definitions, and review the per-device mapping configuration.
F. Check the connection between branch1_fgt and FortiManager

Answer: A

NEW QUESTION 9
You are planning a large SD-WAN deployment with approximately 1000 spokes and want to allow ADVPN between the spokes. Some remote sites use FortiSASE to connect to the company's SD-WAN hub. Which overlay routing configuration should you use?

A. BGP on loopback with dynamic BGP for ADVPN shortcut routing.
B. BGP on loopback with IPsec phase2 selectors for ADVPN shortcut routing.
C. BGP per overlay with dynamic BGP for ADVPN shortcut routing.
D. BGP per overlay with BGP next-hop convergence for ADVPN shortcut routing.

Answer: A

NEW QUESTION 10
You are tasked with configuring ADVPN 2.0 on an SD-WAN topology already configured for ADVPN. What should you do to implement ADVPN 2.0 in this scenario?

A. Update the IPsec tunnel configurations on the hub.
B. Update the SD-WAN configuration on the branches.
C. Update the IPsec tunnel configuration on the branches.
D. Delete the existing ADVPN configuration and configure ADVPN 2.0.

Answer: B

NEW QUESTION 10
Refer to the exhibits.

Configuration for SD-WAN performance SLA, SD-WAN rule configuration, and application IDs YouTube.

```
config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end

config system sdwan
    config service
        edit 1
            set name "Facebook-YouTube"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 31077
            set health-check "Passive"
            set priority-member 3 4
            set passive-measurement enable
        next
    end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077
```

Firewall policy configuration

```
config firewall policy
    edit 1
        set name "DIA"
        set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end
```

Underlay zone status

```
branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
        members(2): 3(port1) 4(port2)
```

The exhibits show the configuration for SD-WAN performance. SD-WAN rule, the application IDs of Facebook and YouTube along with the firewall policy configuration and the underlay zone status.
Which two statements are true about the health and performance of SD-WAN members 3 and 4? (Choose two.)

A. Only related TCP traffic is used for performance measurement.
B. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
C. Encrypted traffic is not used for the performance measurement.
D. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.

Answer: AB

NEW QUESTION 14
Refer to the exhibit.

```
ike V=root:0:VPN1_0:9: received informational request
ike V=root:0:VPN1_0:9: processing notify type SHORTCUT_QUERY
ike V=root:0:VPN1_0: recv shortcut-query 5752810260829471092 6d5cdb5ceab1874d
/0000000000000000 192.2.0.1 10.0.1.101:2048->10.0.3.101:0 0 psk 64 ppk 0 ttl
32 nat 0 ver 2 mode 0 network-id 1
ike V=root:0:VPN1: iif 20 10.0.1.101->10.0.3.101 0 route lookup oif 20 VPN1
gwy 192.168.1.4
ike V=root:0: shared dev tunnel lookup, tun-id=192.168.1.4
ike V=root:0:VPN1_3: forward shortcut-query 5752810260829471092 6d5cdb5ceab18
74d/0000000000000000 192.2.0.1 10.0.1.101->10.0.3.101 0 psk 64 ppk 0 ttl 31
ver 2 mode 0, ext-mapping 192.2.0.1:0, network-id 1
```

Which statement best describe the role of the ADVPN device in handling traffic?

A. This is a hub that has received a query from a spoke and has forwarded it to another spoke.
B. This is a hub in a dual-region topolog
C. The remote hub tunnel ID is 10.0.2.101.
D. This is a spoke that has received a shortcut query from another spoke and has forwarded the response to its hub.
E. This is a spok
F. The kernel received a shortcut request and forwards the query to another spoke.

Answer: C

NEW QUESTION 18
Refer to the exhibits.

SD-WAN service details

```
branch1_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port1 underlay), alive, selected
    2: Seq_num(2 port2 underlay), alive, selected
  Application Control(3): Microsoft.Portal(41469,0) Salesforce(16920,0) Collaboration(0,28)
  Src address(1):
10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
  Src address(1):
10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list
List App Ctrl Database Entry(IPv4) in Kernel:

Max_App_Ctrl_Size=32768 Num_App_Ctrl_Entry=6

Microsolf.Portal (41469 28): IP=184.27.181.201 6 443
MSN.Game(16135 8): IP=13.107.246.36 6 443
Salesforce(16920 29): IP=23.205.255.92 6 443
GoToMeeting (16354 28): IP=23.205.106.86 6 443
GoToMeeting (16354 28): IP=23.212.249.144 6 443
Facebook(15832 23): IP=31.13.80.36 6 443

branch1_fgt # get router info routing-table all
...
```

n FortiAnalyzer

Application	Security Event List	SD-WAN Rule Name	Destination Interface
GoToMeeting	APP 2		port2
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2		port2
GoToMeeting	APP 2		port2
GoToMeeting	APP 2		port2

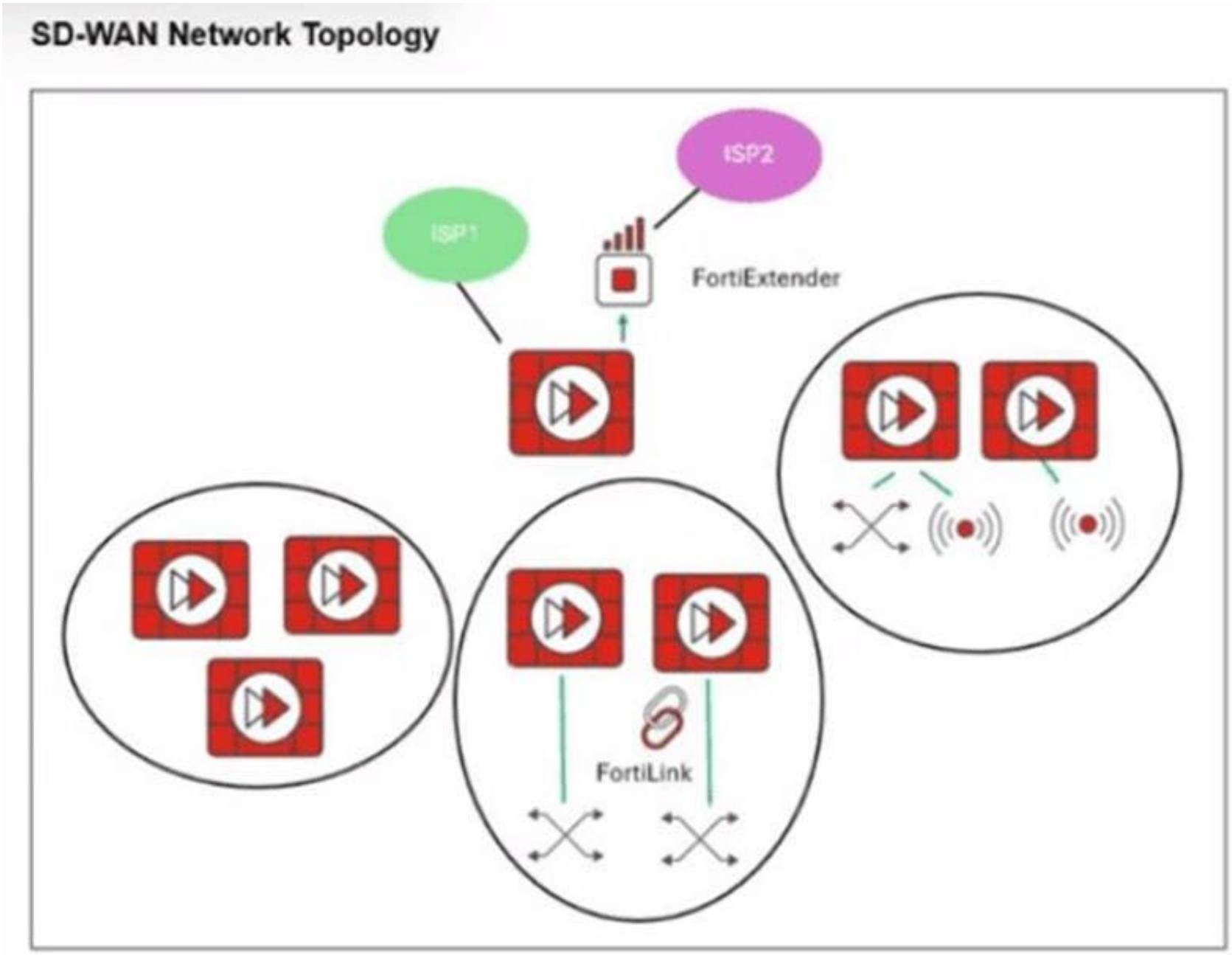
- Security
  - APP Count: 2
  - Level: notice
- General
  - Log ID: 0000000013
  - Session ID: 769
  - Tran Display: snat
  - Virtual Domain: root
- Source
  - Country: Reserved
  - Device ID: FGVM01TM22000077
  - Device Name: branch1_fgt
  - IP: 10.0.1.101
  - Interface: port5
  - Interface Role: undefined
  - NAT IP: 192.2.0.9
  - NAT Port: 51042
  - Port: 51042
  - Source: 10.0.1.101
  - UEBA Endpoint ID: 1025
  - UEBA User ID: 3
- Destination
  - Country: United States
  - End User ID: 3
  - Endpoint ID: 101
  - Host Name: www.gotomeeting.com
  - IP: 23.212.248.205
  - Interface: port2

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in the first exhibit. After generating GoToMeeting test traffic, the administrator examined the corresponding traffic log on FortiAnalyzer, which is shown in the second exhibit.
The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1.
Which two reasons explain why some log messages show that the traffic matched the implicit SD-WAN rule? (Choose two.)

A. Full SSL inspection is not enabled on the matching firewall policy.
B. The session 3-tuple did not match any of the existing entries in the ISDB application cache.
C. FortiGate could not refresh the routing information on the session after the application was detected.
D. No configured SD-WAN rule matches the traffic related to the collaboration application GoToMeeting

Answer: BC

NEW QUESTION 20
Refer to the exhibit.



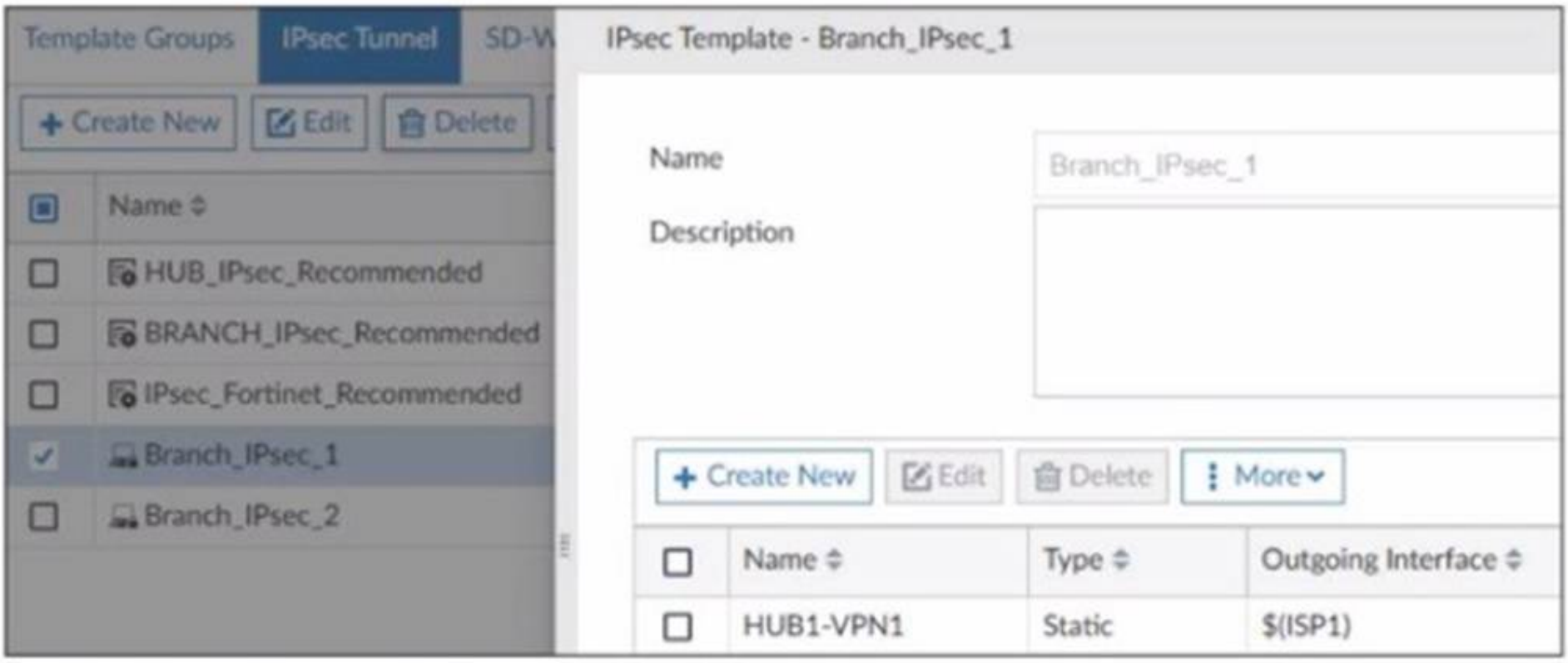
You want to configure SD-WAN on a network as shown in the exhibit.
The network contains many FortiGate devices. Some are used as NGFW, and some are installed with extensions such as FortiSwitch. FortiAP. or Forti Ex tender.
What should you consider when planning your deployment?

A. You can build an SD-WAN topology that includes all device
B. The hubs can be FortiGate devices with Forti Extender.
C. You can build an SD-WAN topology that includes all device
D. The hubs must be devices without extensions.
E. You must use FortiManager to manage your SD-WAN topology.
F. You must build multiple SD-WAN topologie
G. Each topology must contain only one type of extension.

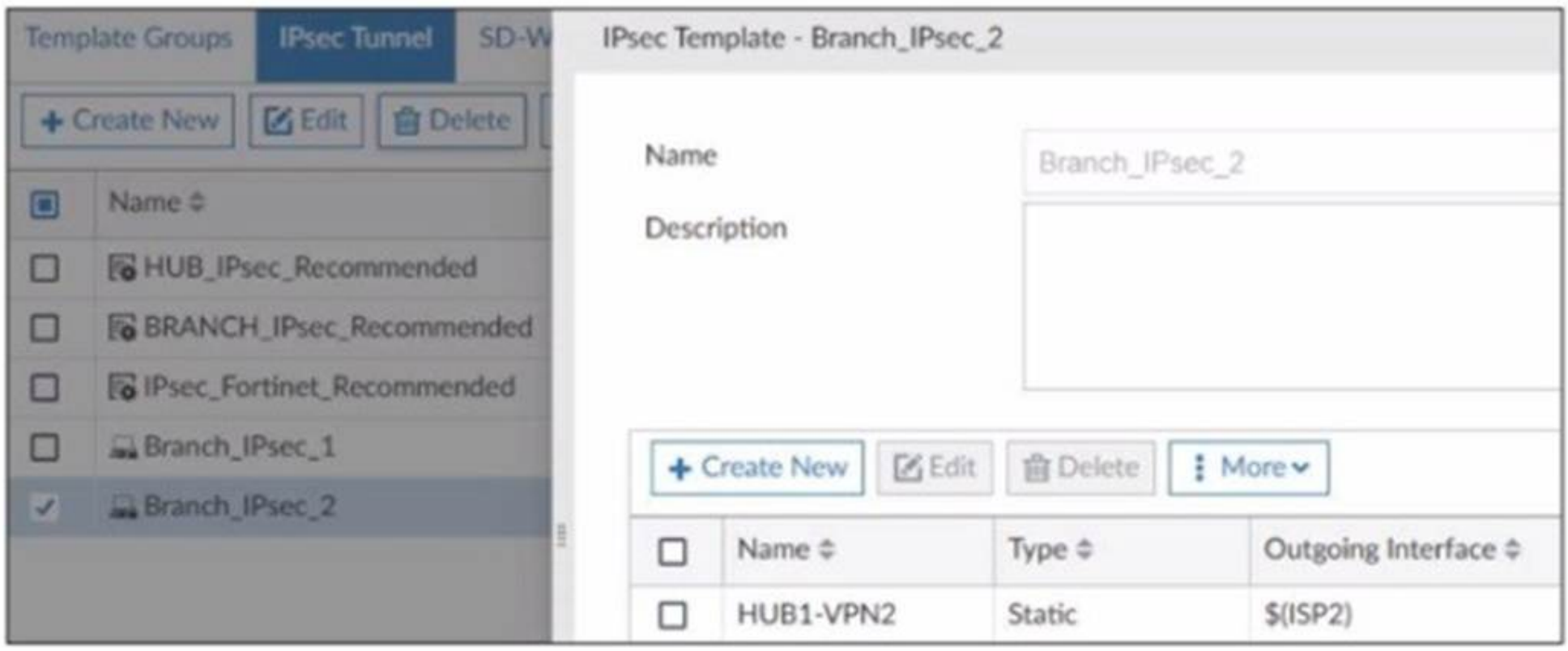
Answer: B

NEW QUESTION 25
Refer to the exhibits.

IPsec template for Branch_IPsec_1



IPsec template for Branch_IPsec_2



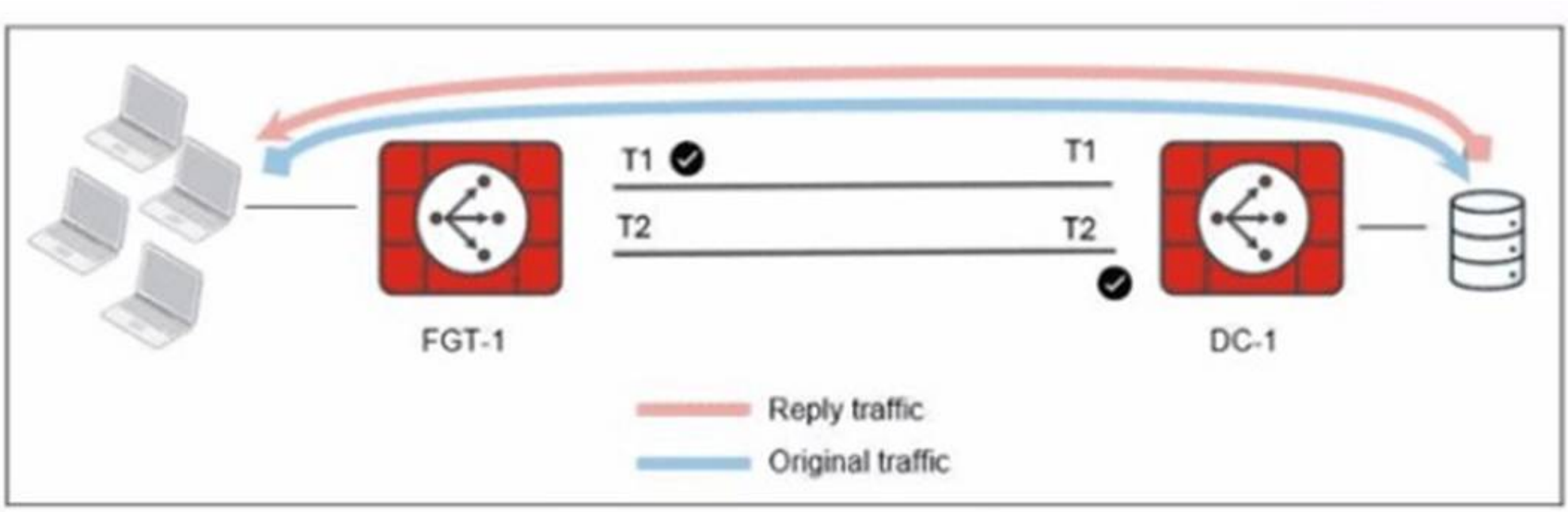
Error message in FortiManager

The exhibits show two IPsec templates to define Branch IPsec 1 and Branch_IPsec_2. Each template defines a VPN tunnel. The error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device is also shown.
Which statement best describes the cause of the issue?

A. You can assign only one template with a tunnel type of static to each FortiGate device.
B. You can assign only one IPsec template to each FortiGate device.
C. You should review the branch1_fgt configuration for configured tunnels in the rootVDOM.
D. You should use the same outgoing interface of both templates.

Answer: B

NEW QUESTION 28
Refer to the exhibit.



The administrator analyzed the traffic between a branch FortiGate and the server located in the data center, and noticed the behavior shown in the diagram. When the LAN clients located behind FGT1 establish a session to a server behind DC-1, the administrator observes that, on DC-1, the reply traffic is routed overT2. even though T1 is the preferred member in
the matching SD-WAN rule.
What can the administrator do to instruct DC-1 to route the reply traffic through the member with the best performance?

A. Enable snat-route-change under config system global.
B. Enable reply-session under config system sdwan.
C. Enable auxiliary-session under config system settings.
D. FortiGate route lookup for reply traffic only considers routes over the original ingress interface.

Answer: C

NEW QUESTION 33
Refer to the exhibit that shows event logs on FortiGate.

Event log on FortiGate

```
6: date=2024-12-18 time=15:15:06 eventtime=1734563705745090691 tz="-0800" logid="0113022925" type="event" subtype="sdwan" leve
l="information" vd="root" logdesc="SDWAN SLA information" eventtype="SLA" healthcheck="HUB1_HC" slatargetid=1 interface="HUB1-
VPN3" status="up" latency="1.001" jitter="0.162" packetloss="0.000" moscodec="g711" mosvalue="4.404" inbandwidthavailable="10.
00Gbps" outbandwidthavailable="10.00Gbps" bibandwidthavailable="20.00Gbps" inbandwidthused="0kbps" outbandwidthused="0kbps" bi
bandwidthused="0kbps" slamap="0x1" msg="Health Check SLA status."

7: date=2024-12-18 time=15:14:26 eventtime=1734563666333265394 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=120.64.1.1 loci
p=192.2.0.1 remport=500 locport=500 outintf="port1" srccountry="Reserved" cookies="50b8a3684ddfd2cb/af3f725d883c5585" user="10
0.64.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=172.168.1.1 vpntunnel="VPN4_0" tunnelip=N/A t
unnelid=3050027470 tunneltype="ipsec" duration=2968 sentbyte=245849 rcvdbyte=246456 nextstat=600 fctuid="N/A" advpnsc=0

8: date=2024-12-18 time=15:04:26 eventtime=1734563066334261977 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.33.1 loc
ip=192.2.0.1 remport=4500 locport=4500 outintf="port1" srccountry="Reserved" cookies="cff150ded109a548/165f413d17cecc49" user=
"Branch3" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="HUB1-VPN1_0" tunnelip=192.168.1.4
 tunnelid=3050027486 tunneltype="ipsec" duration=1122 sentbyte=92064 rcvdbyte=0 nextstat=600 fctuid="N/A" advpnsc=1

9: date=2024-12-18 time=15:04:26 eventtime=1734563066334252138 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.1.1 loci
p=172.16.0.1 remport=500 locport=500 outintf="port4" srccountry="Reserved" cookies="ce1c2c62ecc04871/a4d93a059b8df005" user="1
72.16.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=192.168.1.193 vpntunnel="HUB2-VPN3" tunnelip=N/
A tunnelid=3050027467 tunneltype="ipsec" duration=2367 sentbyte=195836 rcvdbyte=196492 nextstat=600 fctuid="N/A" advpnsc=0
```

Based on the output shown in the exhibit, what can you say about the tunnels on this device?

A. The master tunnel HU82-VPN3 cannot accept ADVPN shortcuts.
B. The device steers voice traffic through the VPN tunnel HUB1-VPN3.
C. The VPN tunnel HUB1-VPN1_0 is a shortcut tunnel.
D. There is one shortcut tunnel built from master tunnel VPN4.

Answer: B

NEW QUESTION 35
Exhibit.

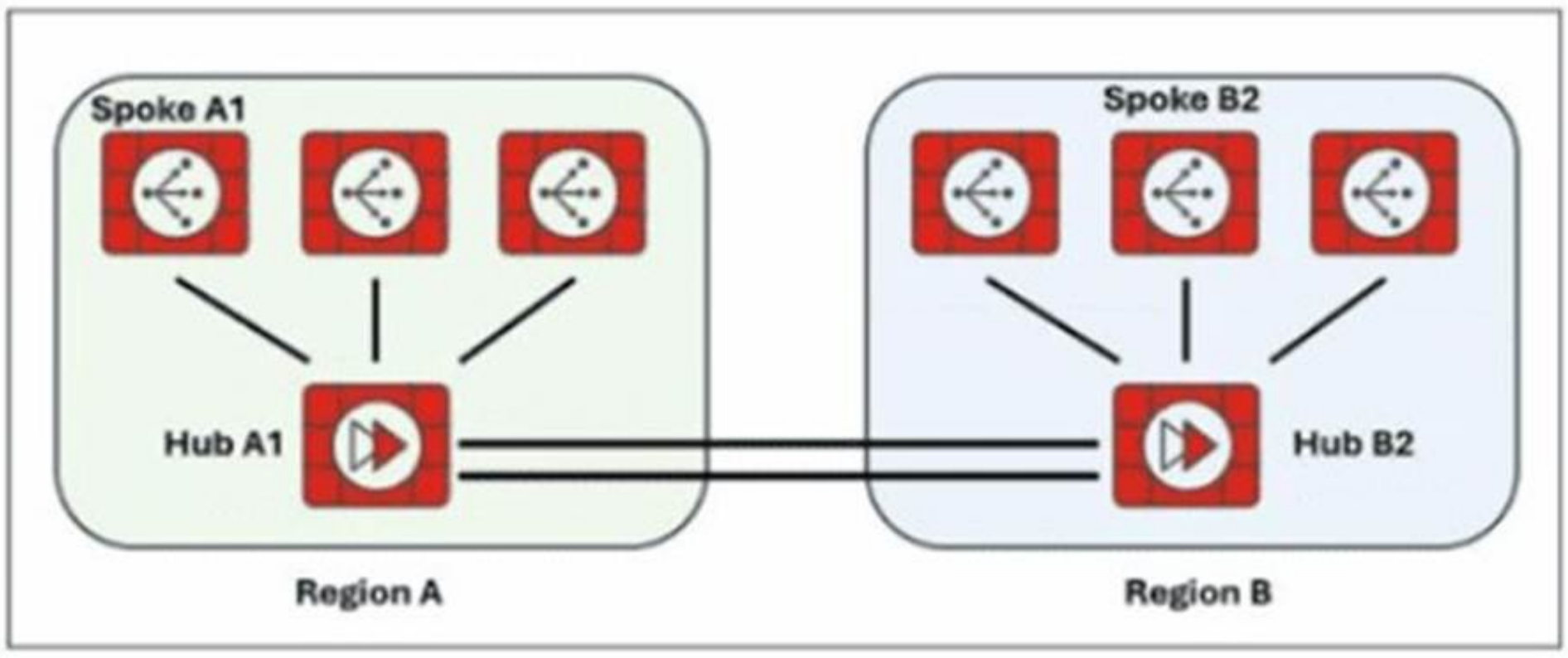
```
config vpn ipsec phase1-interface
    edit "VPN1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set exchange-interface-ip enable
        set mode-cfg disable
        set proposal aes256-sha256
        ...
    end
end
```

The administrator configured the IPsec tunnel VPN1 on a FortiGate device with the parameters shown in exhibit.
Based on the configuration, which three conclusions can you draw about the characteristics and requirements of the VPN tunnel? (Choose three.)

A. The tunnel interface IP address on the spoke side is provided by the hub.
B. The remote end can be a third-party IPsec device.
C. The administrator must manually assign the tunnel interface IP address on the hub side
D. The remote end must support IKEv2.
E. This configuration allows user-defined overlay IP addresses.

Answer: BCE

NEW QUESTION 37
Exhibit.



Two hub-and-spoke groups are connected through redundant site-to-site IPsec VPNs between Hub 1 and Hub 2
Which two configuration settings are required for the spoke A1 to establish an ADVPN shortcutwith the spoke B2? (Choose two.)

A. On hubs, auto-discovery-forwarder must be enabled on the IPsec VPNs to hubs.
B. On hubs, auto-discovery-receiver must be enabled on the IPsec VPNs to spokes.
C. On hubs, auto-discovery-forwarder must be enabled on the IPsec VPNs to spokes.
D. On hubs, auto-diacovery-sender must be enabled on the IPsec VPNs to spokes

Answer: AD

NEW QUESTION 41
.....

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_SDW_AR-7.4 Practice Exam Features:

* FCSS_SDW_AR-7.4 Questions and Answers Updated Frequently

* FCSS_SDW_AR-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_SDW_AR-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_SDW_AR-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year