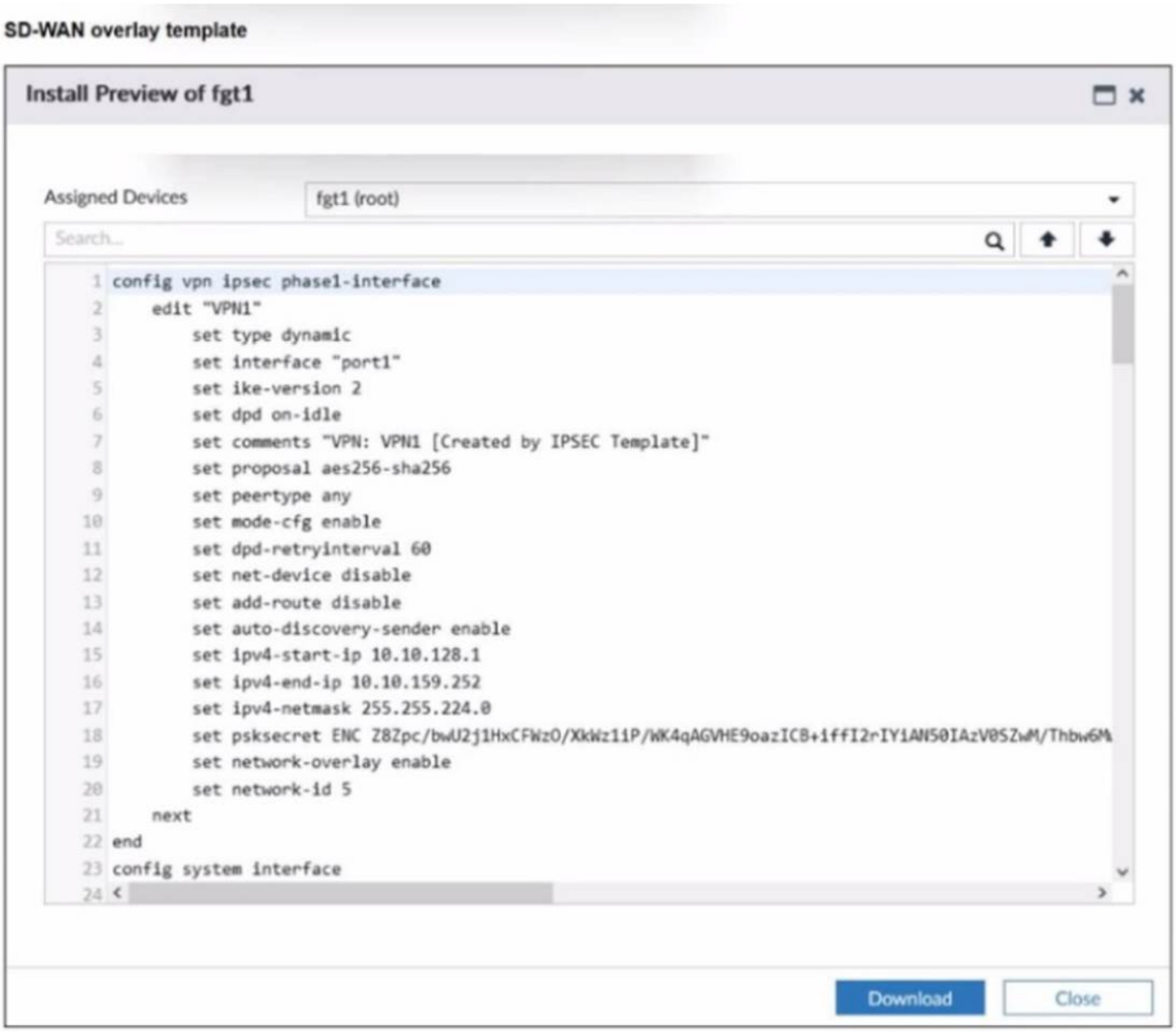
Fortinet

Exam Questions FCSS_SDW_AR-7.6

FCSS - SD-WAN 7.6 Architect

NEW QUESTION 1
Refer to the exhibit.



The administrator used the SD-WAN overlay template to prepare an IPsec tunnels configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the FortiManager installation preview for one FortiGate device.
Based on the exhibit, which statement best describes the configuration applied to the FortiGate device?

A. It is a spoke device that establishes dynamic IPsec tunnels to the hu
B. The local subnet range is 10.10.128.0/23.
C. It is a hub devic
D. It can send ADVPN shortcut offers.
E. It is a hub devic
F. It will automatically discover the spoke devices and add them to the SD-WAN topology.
G. It is a spoke device that establishes dynamic IPsec tunnels to the hub It can send ADVPN shortcut requests.

Answer: B

NEW QUESTION 2
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: C

NEW QUESTION 3
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 4
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

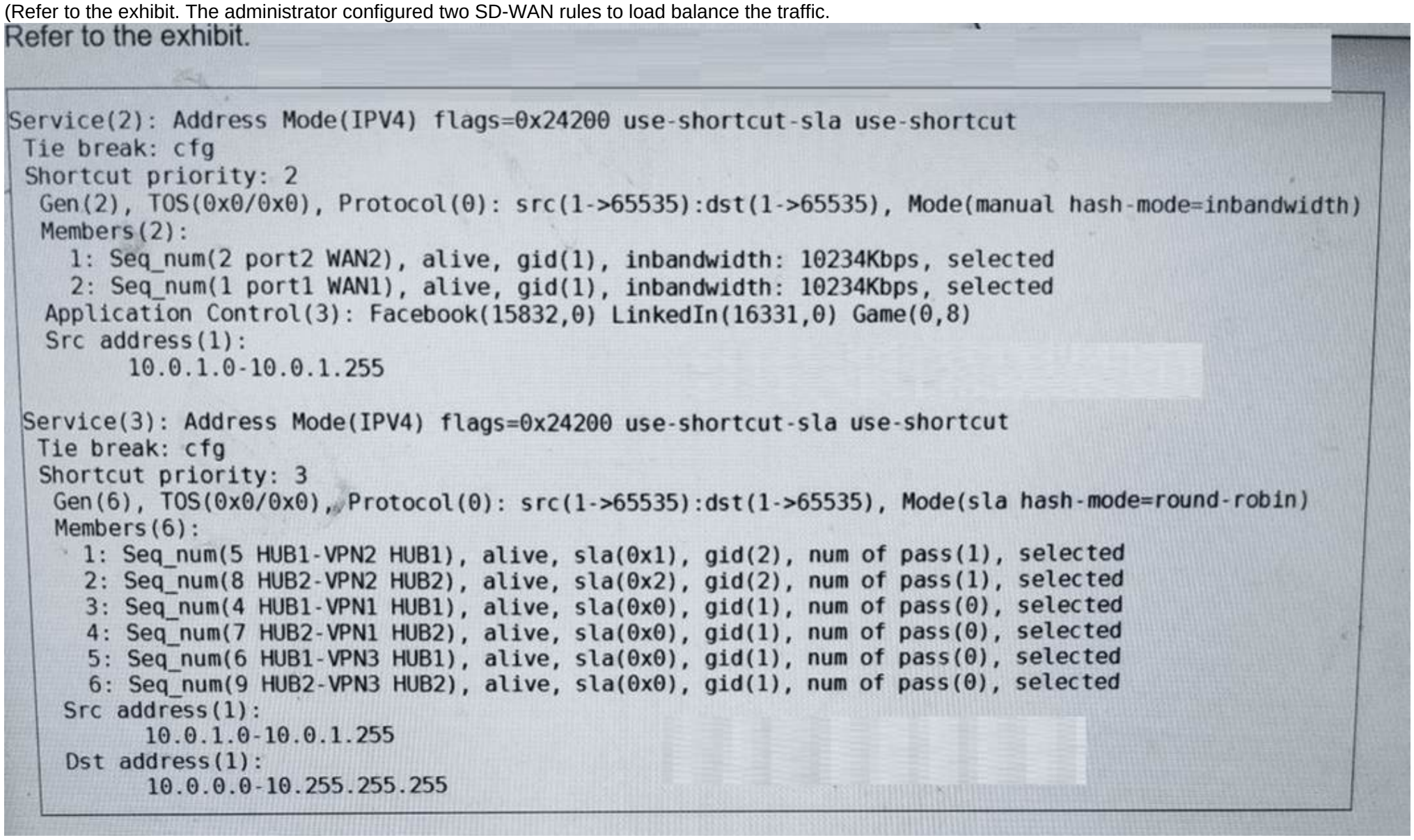
- Security
  - APP Count
  - Level: notice
- General
  - Log ID: 0000000013
  - Session ID: 769
  - Tran Display: snat
  - Virtual Domain: root
- Source
  - Country: Reserved
  - Device ID: FGVM01TM22000077
  - Device Name: branch1_fgt
  - IP: 10.0.1.101
  - Interface: port5
  - Interface Role: undefined
  - 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: BD

NEW QUESTION 5
(Refer to the exhibit. The administrator configured two SD-WAN rules to load balance the traffic.



Which interfaces does FortiGate use to steer the traffic from 10.0.1.124 to 10.0.0.254? Choose one answer.)

A. HUB2-VPN2
B. HUB1-VPN2 or HUB2-VPN2
C. port1 or port2
D. Any interface in the HUB1 or HUB2 zones

Answer: B

NEW QUESTION 6
You want FortiGate to use SD-WAN rules to steer local-out traffic. Which two constraints should you consider? (Choose two.)

A. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.
B. By default, local-out traffic does not use SD-WAN.
C. You can steer local-out traffic only with SD-WAN rules that use the manual strategy.
D. You must configure each local-out feature individually to use SD-WAN.

Answer: BD

NEW QUESTION 7
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: BD

NEW QUESTION 8
An SD-WAN member is no longer used to steer SD-WAN traffic. The administrator updated the SD-WAN configuration and deleted the unused member. After the configuration update, users report that some destinations are unreachable. You confirm that the affected flow does not match an SD-WAN rule.
What could be a possible cause of the traffic interruption?

A. FortiGate, with SD-WAN enabled, cannot route traffic through interfaces that are not SD-WAN members.
B. FortiGate can remove some static routes associated with an interface when the member is removed from SD-WAN.
C. FortiGate removes the layer 3 settings for interfaces that are removed from the SD-WAN configuration.
D. FortiGate administratively brings down interfaces when they are removed from the SD- WAN configuration.

Answer: B

NEW QUESTION 9
(You are using the FortiManager SD-WAN monitor menus to check the status of an SD- WAN topology. When you place the mouse next to branch1_fgt, you receive the output shown in the exhibit.

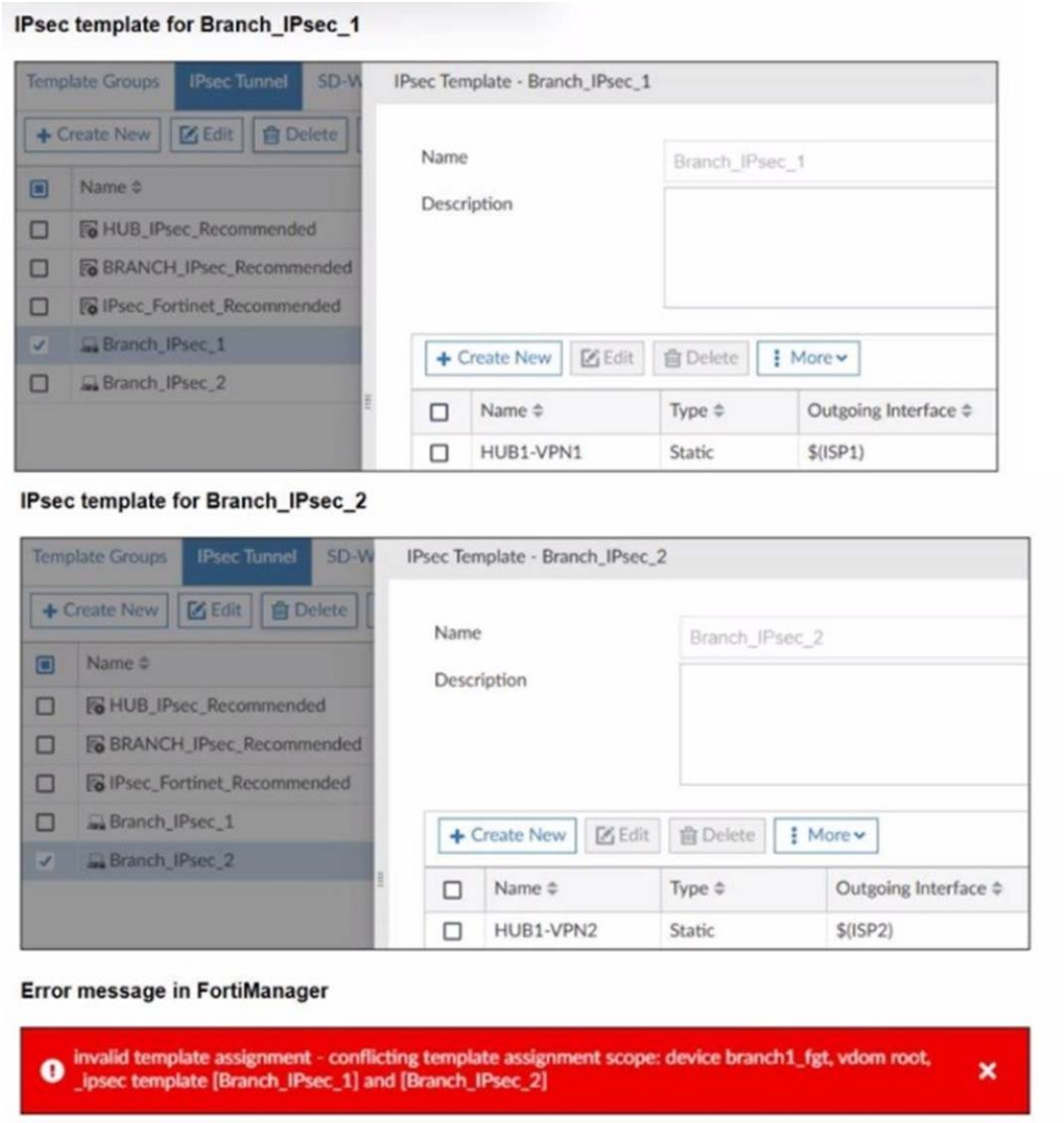
Which two conclusions can you draw from the output shown in the exhibit? Choose two answers.)

A. Three spokes have tunnels that are out of SLA.

B. The template Corp-SOT defines a dual-hub topology.
C. branch3_fgt is configured with three SD-WAN overlay tunnels and one is down.
D. branch1_fgt is configured with six SD-WAN overlay tunnels and three are down.

Answer: AC

NEW QUESTION 10
Refer to the exhibits.



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 10
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: C

NEW QUESTION 12
You manage an SD-WAN topology. You will soon deploy 50 new branches.
Which three tasks can you do in advance to simplify this deployment? (Choose three.)

A. Update the DHCP server configuration.
B. Create model devices.
C. Create a ZTP template.
D. Define metadata variables value for each device.
E. Create policy blueprint.

Answer: BCE

NEW QUESTION 17
Refer to the exhibits.

Interface details

	Name	Type	Members	IP/Netmask
⊟	Physical Interface 13			
⊞	port1	Physical Interface		192.2.0.1/255.255.255.248
⊞	port2	Physical Interface		192.2.0.9/255.255.255.248
	port3	Physical Interface		0.0.0.0/0.0.0.0
⊞	port4	Physical Interface		172.16.0.1/255.255.255.248
	port5	Physical Interface		10.0.1.254/255.255.255.0
	port6	Physical Interface		0.0.0.0/0.0.0.0
	port7	Physical Interface		0.0.0.0/0.0.0.0
	port8	Physical Interface		0.0.0.0/0.0.0.0
	port9	Physical Interface		0.0.0.0/0.0.0.0
	port10	Physical Interface		192.168.0.31/255.255.255.0
	T_shop_1(port9)	Physical interface		0.0.0.0/0.0.0.0
⊟	SD-WAN Zone 3			
	HUB1	SD-WAN Zone	HUB1-VPN1 HUB1-VPN2 HUB1-VPN3	0.0.0.0/0.0.0.0
	Test	SD-WAN Zone	port2	0.0.0.0/0.0.0.0
	virtual-wan-link	SD-WAN Zone		0.0.0.0/0.0.0.0

Static route details

Destination	Gateway IP	Interface	Status
192.168.1.0/24	192.2.0.254	port1	Enabled
168.1.1.0/24	192.2.0.4	port1	Enabled

Firewall policies on managed FortiGate

	Policy	From	To	Source	Destination	Service
☐	Corp(5)	port1	port5	Corp-net	LAN-net	HTTP HTTPS
☐	DIA(1)	port5	port1	LAN-net	all	ALL

The interface details, static route configuration, and firewall policies on the managed FortiGate device are shown.
You want to configure a new SD-WAN zone, named Underlay, that contains the interfaces port1 and port2.
What must be your first action?

A. Define port1 as an SD-WAN member.
B. Delete the static routes.
C. Delete the SD-WAN Zone Test.
D. Delete the firewall policies.

Answer: B

NEW QUESTION 20
Refer to the exhibit.

```
ike V=root:0:HUB1-VPN1:0: received informational request
ike V=root:0:HUB1-VPN1:0: processing notify type SHORTCUT_QUERY
ike V=root:0:HUB1-VPN1: recv shortcut-query 16573251835242579210
cff150ded109a548/0000000000000000 192.2.0.1 10.0.1.101:2048->
10.0.3.101:0 0 psk 64 ppk 0 ttl 31 nat 0 ver 2 mode 0 network-id 1
ike V=root:0:HUB1-VPN1: iif 20 10.0.1.101->10.0.3.101 0 route lookup
oif 7 port5 gwy 0.0.0.0
ike V=root:0:HUB1-VPN1: shortcut-query received from 192.2.0.1:500,
local-nat=yes, peer-nat=no
ike V=root:0:HUB1-VPN1: NAT hole punching for peer at 192.2.0.1:4500
```

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

A. This is a spoke that has received a direct shortcut query from a remote spoke.
B. This is a hub, and two spokes, 192.2.0.1 and 10.0.3.101, establish a shortcut.
C. This is a hub that has received a shortcut query from a spoke and has forwarded it to another spoke.
D. This is a spoke that has received a shortcut query from a remote hub.

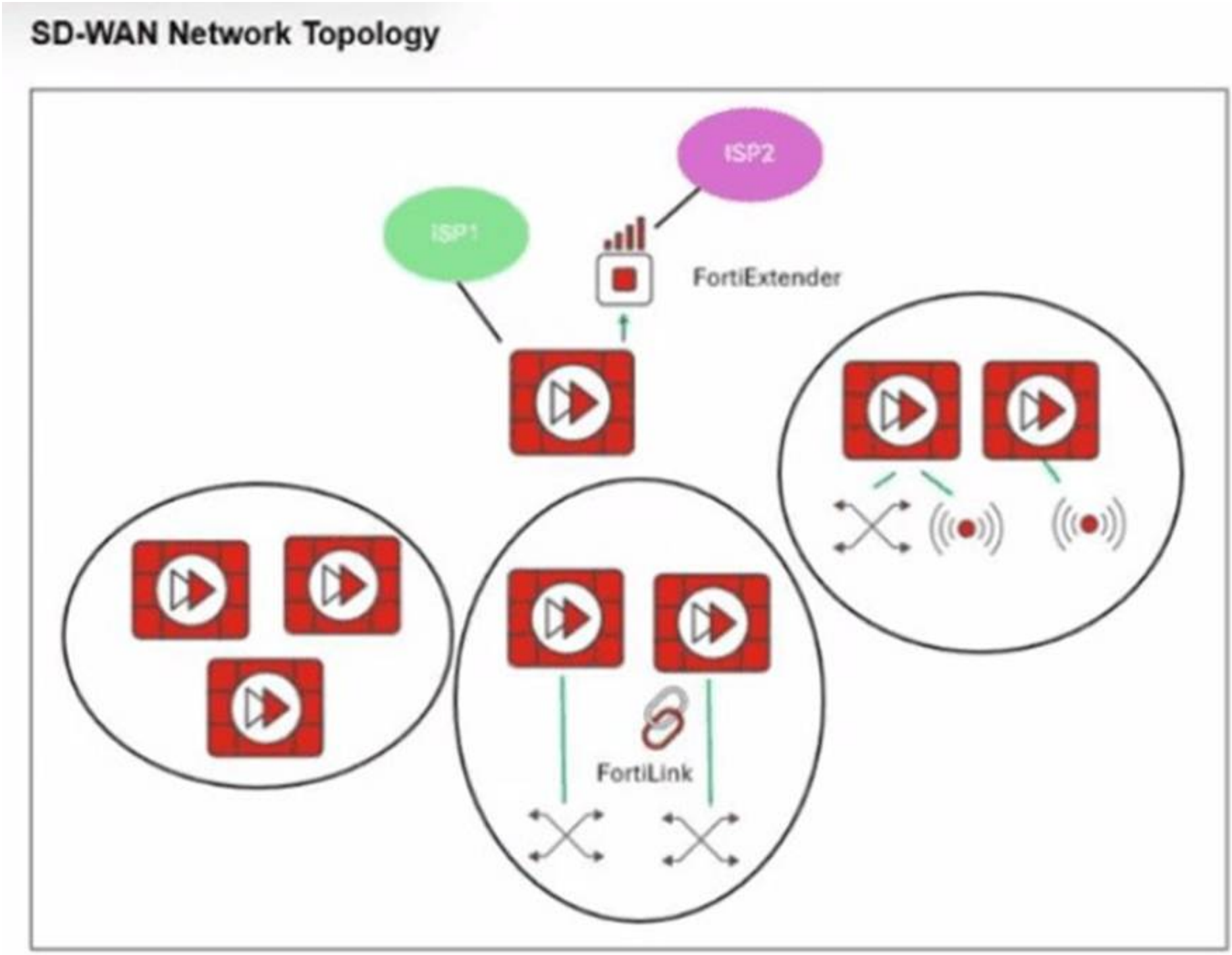
Answer: B

NEW QUESTION 23
(You want to configure two static routes: one that references an SD-WAN zone and a second one that references an SD-WAN member that belongs to that zone. Which statement about this scenario is true? Choose one answer.)

A. You cannot create static routes for individual SD-WAN members.
B. You cannot create static routes that reference an SD-WAN zone.
C. The destination subnets must be different.
D. The source subnets must be different.

Answer: C

NEW QUESTION 24
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 27
(As an IT manager, you want to delegate the installation and management of your SD- WAN deployment to a managed security service provider (MSSP). Each site must maintain direct internet access and be secure. You expect significant traffic flow between the sites and want to delegate as much of the network administration and management as possible to the MSSP.
Which two MSSP deployment blueprints address your requirements? Choose two answers.)

A. Use a shared hub on the MSSP premises and a dedicated hub on the customer premises, and install the spokes on the customer premises.
B. Install a dedicated hub on the MSSP premises for the customer, and install the spokes on the customer premises.
C. Install the hub and spokes on the customer premises, and enable the MSSP to manage the SD-WAN deployment using FortiManager with a dedicated ADOM.
D. Use a shared hub on the MSSP premises with a dedicated VDOM for the customer, and install the spokes on the customer premises.

Answer: BD

NEW QUESTION 28
(You configure the overlay tunnels for an SD-WAN hub-and-spoke topology defined with IPsec tunnels, BGP on loopback, and dynamic BGP.
Which are two recommended IPsec settings for this topology? Choose two answers.)

A. On the spoke, set the parameter net-device to enable.
B. On the spoke, configure the parameter localid.
C. On the hub, set the parameter mode-cfg to enable.
D. On the hub, set the tunnel type to static.

Answer: AB

NEW QUESTION 31

.....

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-7.6 Practice Exam Features:

* FCSS_SDW_AR-7.6 Questions and Answers Updated Frequently

* FCSS_SDW_AR-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_SDW_AR-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_SDW_AR-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year