Fortinet

Exam Questions FCSS_SDW_AR-7.4

FCSS - SD-WAN 7.4 Architect

NEW QUESTION 1
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 2
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 3
What are three key routing principles of SD-WAN? (Choose three.)

A. Directly connected routes have precedence over SD-WAN rules.
B. Policy routes have precedence over SD-WAN rules.
C. SD-WAN rules are skipped if the best route to the destination is a static route
D. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.
E. SD-WAN members are skipped if they do not have a valid route to the destination.

Answer: BDE

NEW QUESTION 4
Refer to the exhibit.

SD-WAN configuration on FortiGate

```
branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [10/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 1d03h58m, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 1d03h58m, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 1d03h58m, [1/0]
C       10.200.99.1/32 is directly connected, Branch-Lo
B       10.2.0.0/16 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 00:03:01, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 00:00:51, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 00:00:51, [1/0]
B       10.2.5.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN3), 00:00:01, [1/0]
...
```

```
branch1_fgt # diag sys sdwan service4

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


Service(4): 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(sla), sla-compare-order
  Members(2):
    1: Seq_num(2 port2 underlay), alive, sla(0x3), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(1 port1 underlay), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.2.0.0-10.2.255.255
```

Which SD-WAN rule and interface uses FortiGate to steer the traffic from the LAN subnet 10.0.1.0/24 to the corporate server 10.2.5.254?

A. SD-WAN service rule 3 and interface HUB1-VPN2.
B. SD-WAN service rule 3 and interface HUB1-VPN3.
C. SD-WAN service rule 4 and port1or port2.
D. SD-WAN service rule 4 and interface port2.

Answer: B

NEW QUESTION 5
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 6
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 7
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 8
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 9
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 10
You have a FortiGate configuration with three user-defined SD-WAN zones and two members in each of these zones. One SD-WAN member is no longer in use in health- check and SD-WAN rules. You want to delete it.
What happens if you delete the SD-WAN member from the FortiGate GUI?

A. FodiGate accepts the deletion and removes routes as required.
B. FortiGate displays an error messag
C. You must use the CLI to delete an SD-WAN member.
D. FortiGate displays an error messag
E. SD-WAN zones must contain at least two members
F. FortiGate accepts the deletion and places the member in the default SD-WAN zone.

Answer: B

NEW QUESTION 10
Exhibit.

SD-WAN rules status and configuration

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(43), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
  link-cost-factor(packet loss), link-cost-threshold(0), heath-check(HUB1_HC)
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, packet loss: 2.000%, selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, packet loss: 4.000%, selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, packet loss: 12.000%, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt (service) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "HUB1_HC"
        set link-cost-factor packet-loss
        set link-cost-threshold 0
        set priority-members 6 4 5
    next
```

Refer to the exhibit, which shows the SD-WAN rule status and configuration.
Based on the exhibit, which change in the measured packet loss will make HUB1-VPN3 the new preferred member?

A. When HUB1-VPN1 has 4% packet loss
B. When HUB1-VPN1 has 12% packet loss
C. When HUB1-VPN3 has 4% packet loss
D. When all three members have the same packet loss

Answer: D

NEW QUESTION 12
The SD-WAN overlay template helps to prepare SD-WAN deployments. To complete the tasks performed by the SD-WAN overlay template, the administrator must perform some post-run tasks. What are two mandatory post-run tasks that must be performed? (Choose two.)

A. Configure routing through the overlay tunnels created by the SD-WAN overlay template.
B. Create policy packages andassign them to the branch devices.
C. Assign a hub id metadata variable to each hub device.
D. Configure SD-WAN rules
E. Assign ansdwan_id metadata variable to each device (branch and hub)

Answer: BD

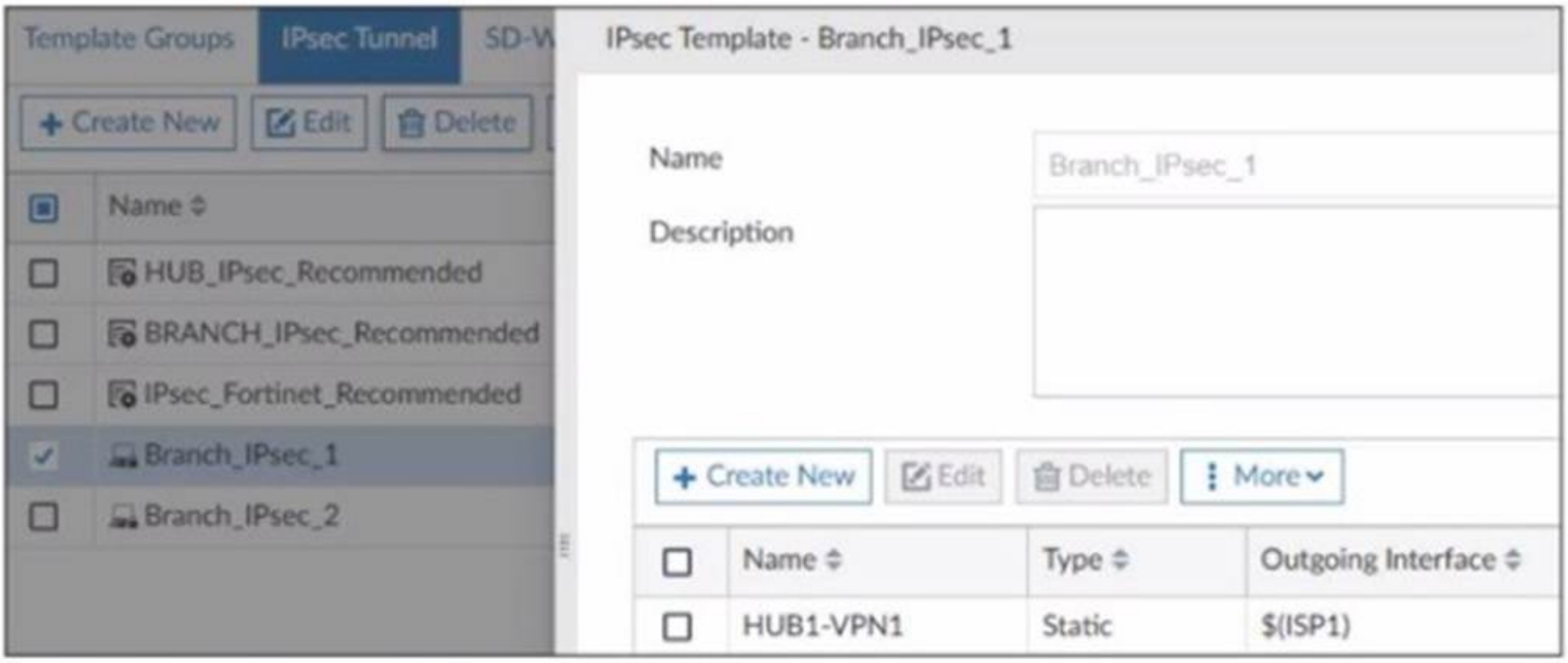
NEW QUESTION 15
When a customer delegate the installation and management of its SD-WAN infrastructure to an MSSP, the MSSP usually keeps the hub within its infrastructure for ease of management and to share costly resources.
In which two situations will the MSSP install the hub in customer premises? (Choose two.)

A. The customer requires SIA with centralized breakout.
B. The administrator expects a large volume of traffic between the branches.
C. The customer expects a large amount of VoIP traffic.
D. The majority of the branch traffic is directed to a corporate data center.

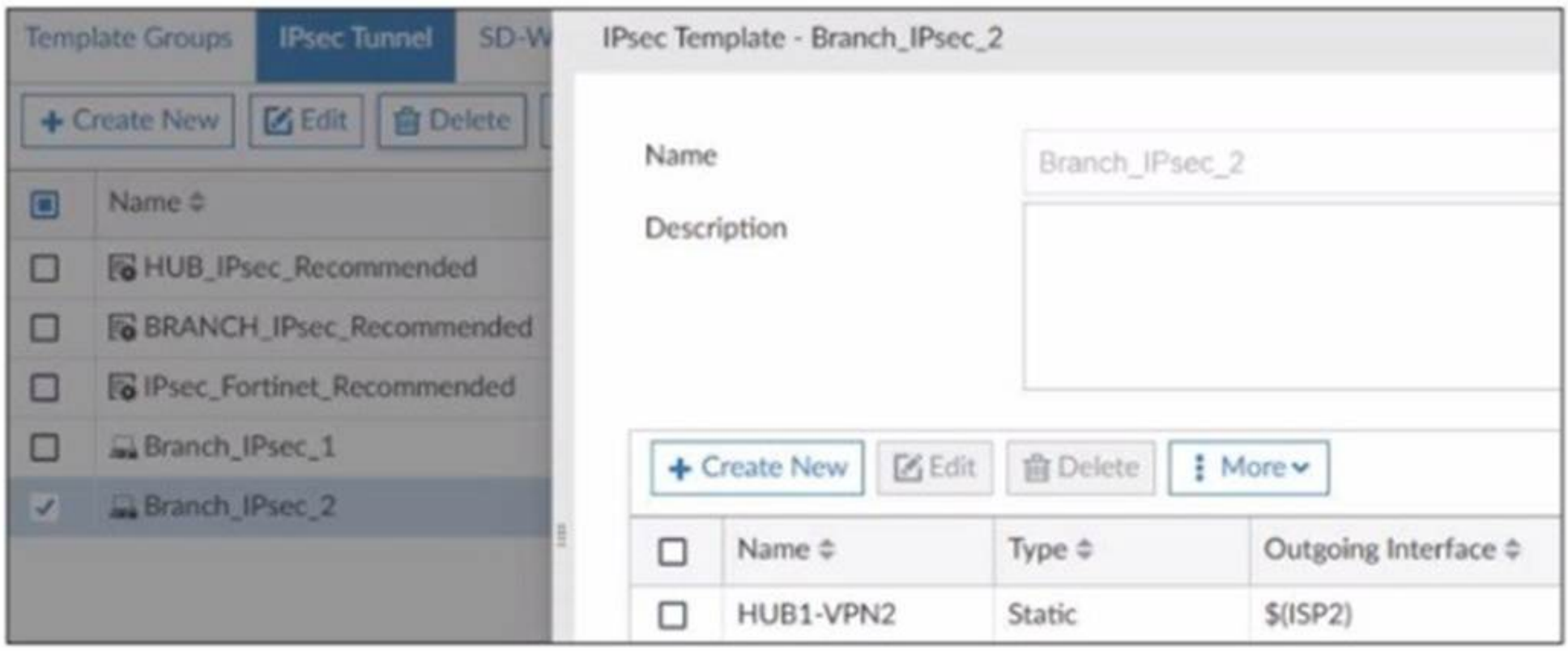
Answer: AB

NEW QUESTION 16
Refer to the exhibits.

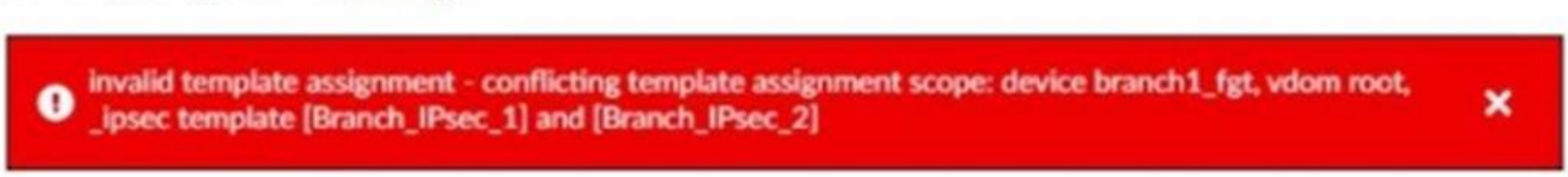
IPsec template for Branch_IPsec_1



IPsec template for Branch_IPsec_2



Error message in FortiManager



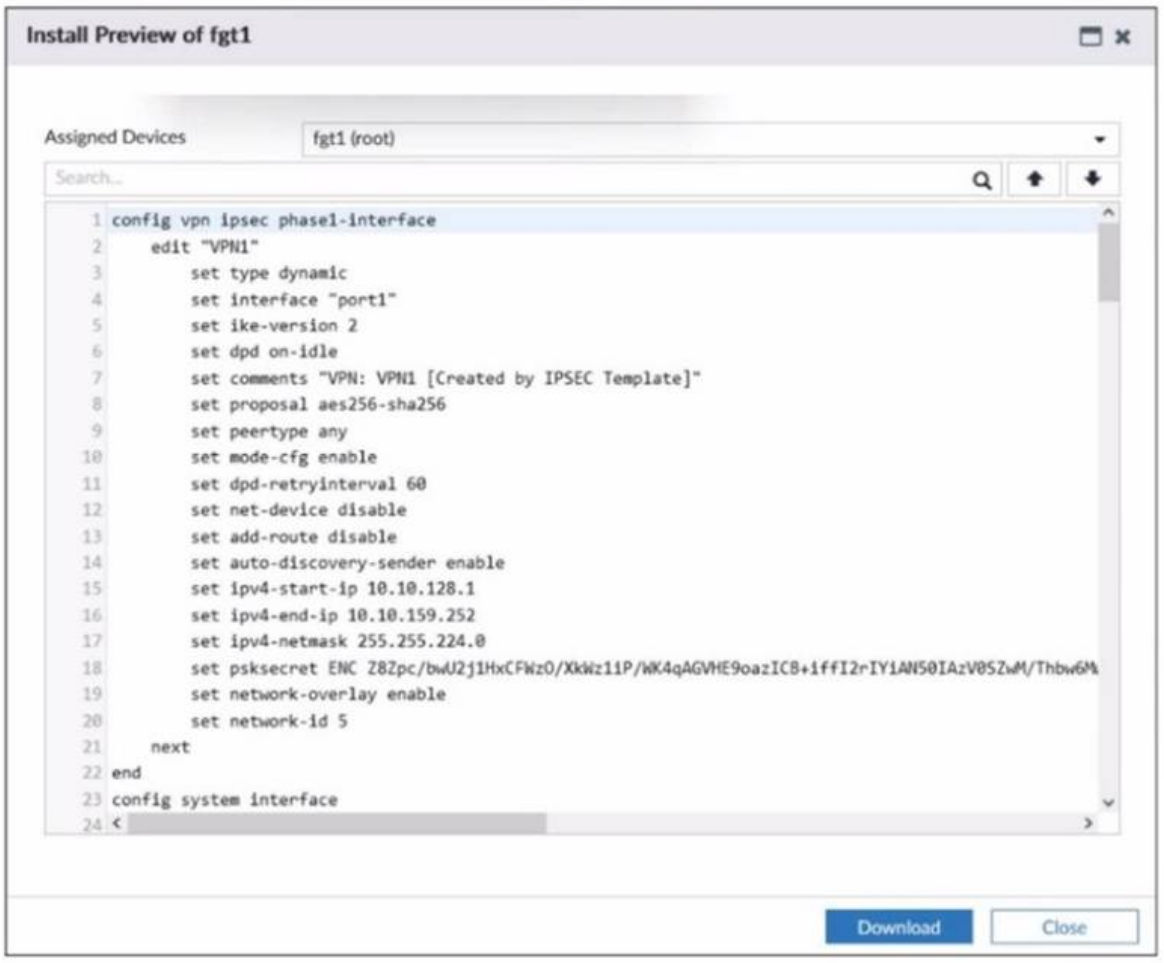
The exhibits show two IPsec templates to define Branch IPsec 1 and Branch_IPsec_2. Each template defines a VPN tunnel. The error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device is also shown.
Which statement best describes the cause 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 18
Refer to the exhibit.

SD-WAN overlay template



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 21
Refer to the exhibit that shows event logs on FortiGate.

Event log on FortiGate

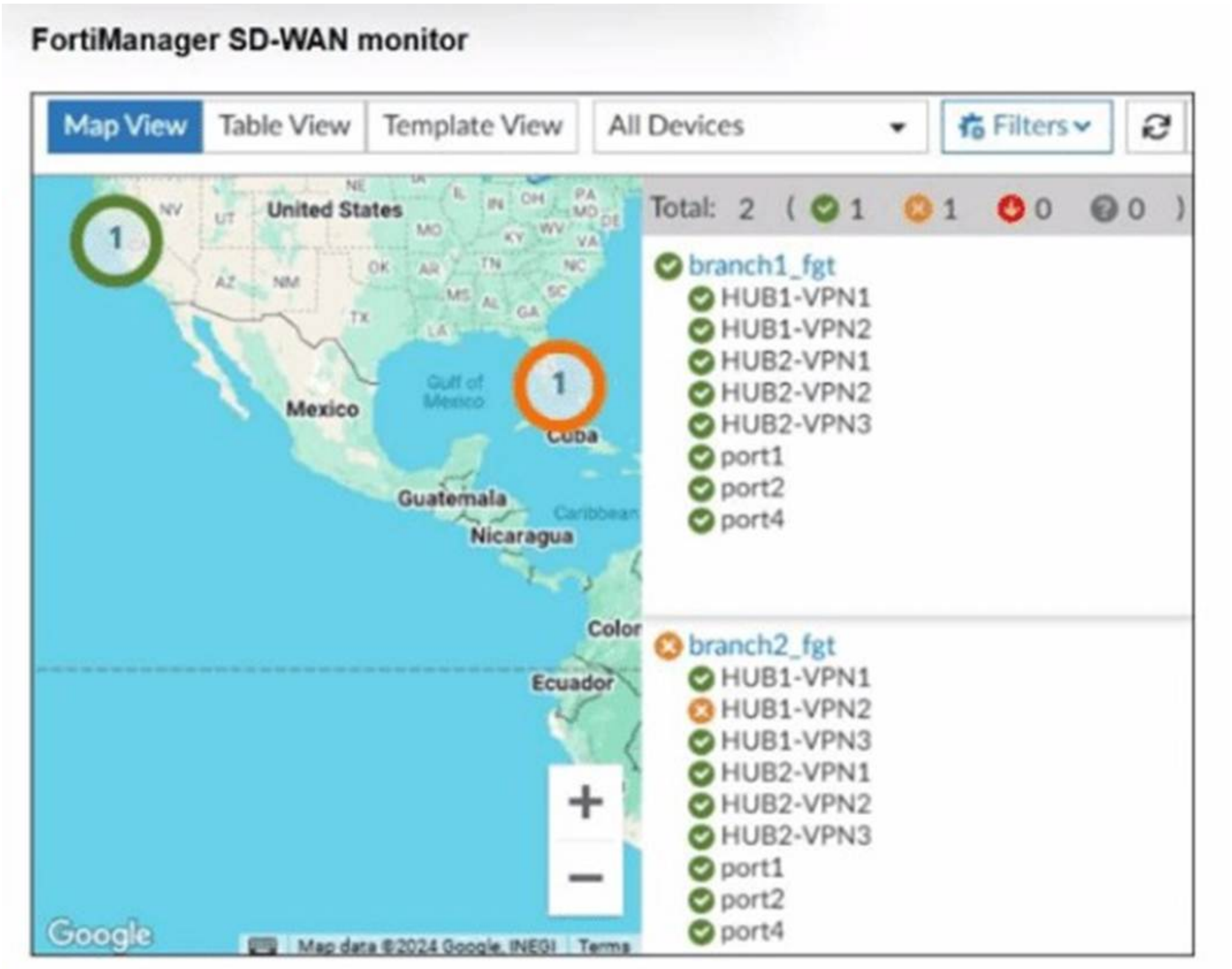
```
6: date=2024-12-18 time=15:15:06 eventtime=1734563705745090691 tz="-0800" logid="0113022925" type="event" subtype="sdwan" leve
l="information" vd="root" logdesc="SDWAN SLA information" eventtype="SLA" healthcheck="HUB1_HC" slatargetid=1 interface="HUB1-
VPN3" status="up" latency="1.001" jitter="0.162" 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 24
Refer to the exhibit.



An administrator checks the status of an SD-WAN topology using the FortiManager SD- WAN monitor menus. All members are configured with one or two SLAs. Which two conclusions can you draw from the output shown? (Choose two.)

A. The template view should be used to see the hub devices.
B. One member of branch2_fgt is missingthe SLAs.
C. branch2_fgt establishes six tunnels to the hubs and they are all up.
D. This SD-WAN topology contains only two branch devices.

Answer: BD

NEW QUESTION 26
.....

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