Fortinet

Exam Questions FCSS_SDW_AR-7.6

FCSS - SD-WAN 7.6 Architect

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
Refer to the exhibit.

```
config system sdwan
    config health_check
        edit "DNS"
            set server "4.2.2.1" "4.2.2.2"
            set detect-mode active
            set protocol ping
            set embed-measured-health enable
            set members 3 4
            config sla
                edit 1
                set link-cost-factor latency
                set latency-threshold 100
            end
        next
    end
end
```

The exhibit shows the health-check configuration on a FortiGate device used as a spoke. You notice that the hub FortiGate doesn??t prioritize the traffic as expected.
Which two configuration elements should you check on the hub? (Choose two.)

A. The performance SLA has the parameter priority-out-sla configured.
B. This performance SLA uses the same members.
C. The performance SLA uses the same criteria.
D. The performance SLA is configured with set embedded-measure accept.

Answer: CD

NEW QUESTION 2
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: D

NEW QUESTION 3
Refer to the exhibits.
You use FortiManager to configure SD-WAN on three branch devices.

SD-WAN template zones and rules configuration

SD-WAN Zones

Create New | Edit | Delete | Where Used | Search

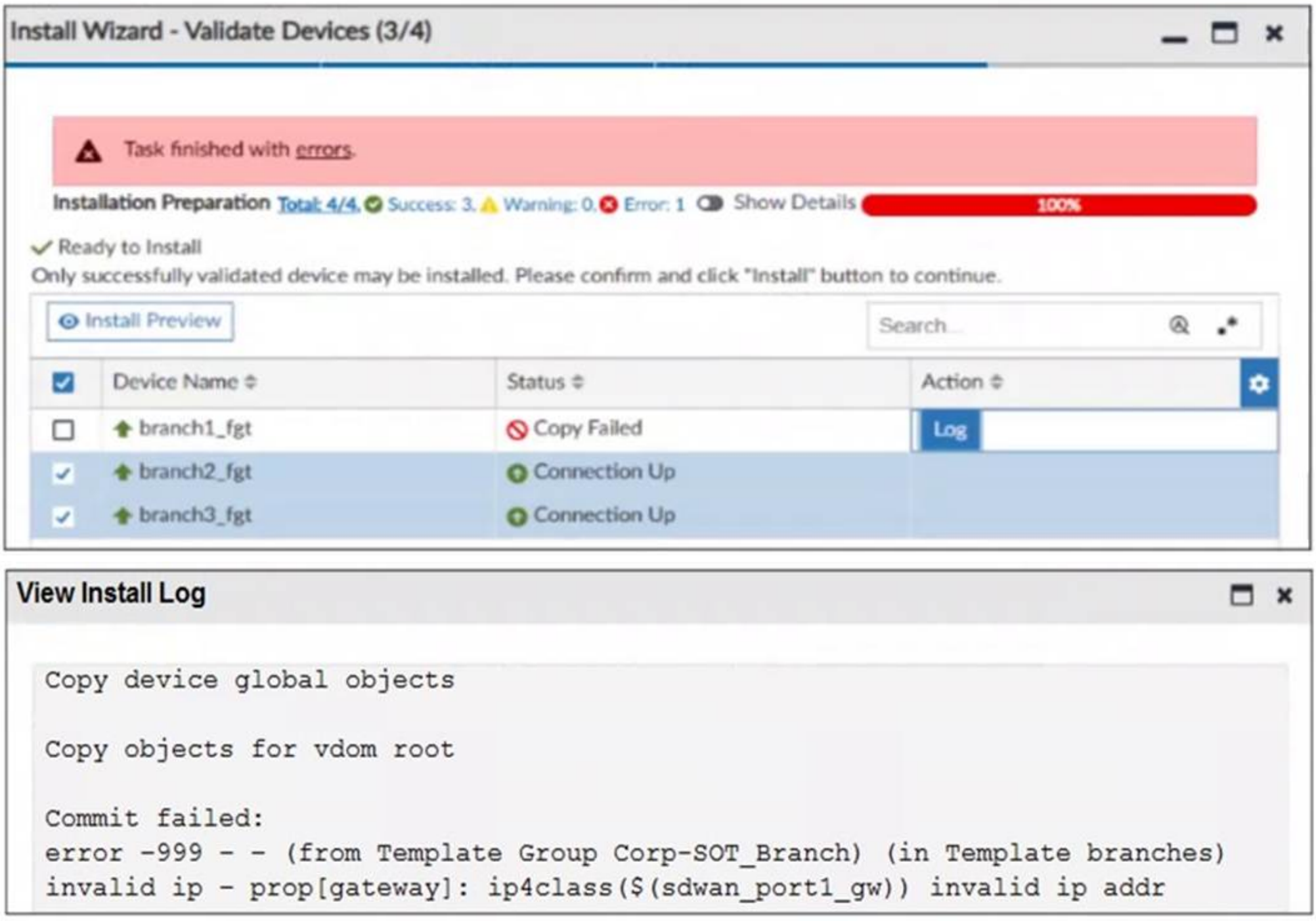
	ID	Interface	Gateway	Cost	Priority	Status	Installation Target
	virtual-wan-link						
	underlay						
	1	port1	$(sdwan_port1_gw)	0	1	Enable	
	2	port2	0.0.0.0	0	1	Enable	
	WAN3						
	3	port4	$(sdwan_port4_gw)	0	1	Enable	1 Device in Total branch1_fgt [root]
	HUB1						
	4	HUB1-VPN1	0.0.0.0	0	1	Enable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

	1	Critical-DIA	LAN-r	Salesforce Microsoft		port1 port2		any	Enable
	2	Non-Critical-DIA	LAN-r	Facebook LinkedIn Game		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



When you install the device settings, FortiManager prompts you with the error ??Copy Failed?? for the device branch1_fgt. When you click the log button, FortiManager displays the message shown in the exhibit.
There are two different ways to resolve this issue. Based on the exhibits, which methods could you use? (Choose two.)

A. Update the management IP address of branch1_fgt.
B. Specify the gateway of the SD-WAN member port1 with an IP address or use the default value.
C. Do not define installation targets for SD-WAN members.
D. Review the per-device mapping configuration for metadata variables

Answer: BD

NEW QUESTION 4
Refer to the exhibits.

Global System configuration

```
config system global
    set snat-route-change enable
end
```

Interface port2 configuration

```
config system interface
    [...]
    edit "port2"
        set vdom "root"
        set mode dhcp
        set allowaccess ping
        set type physical
        set snmp-index 2
    next
    [...]
```

Routing Table on FortiGate

```
branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port2, [1/0]
                  [1/0] via 192.2.0.10, port1 [10/0]
...
```

The exhibits show the source NAT (SNAT) global setting. port2 interface settings, and the routing table on FortiGate.
The administrator increases the member priority on port2 to 20.
Upon configuration changes and the receipt of new packets, which two actions does FortiGate perform on existing sessions established over port2? (Choose two.)

A. FortiGate continues routing all existing sessions over port2.
B. FortiGate routes only new sessions over port2.
C. FortiGate flags the SNAT session as dirty only if the administrator has assigned an IP pool to the firewall policies with NAT.
D. FortiGate flags the sessions as dirty.
E. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: DE

NEW QUESTION 5
Within the context of SD-WAN, what does SIA correspond to?

A. Remote Breakout
B. Local Breakout
C. Software Internet Access
D. Secure Internet Authorization

Answer: B

NEW QUESTION 6
Refer to the exhibit.

FortiGate router policy and diagnose output

```
branch1_fgt # show router policy
config router policy
     edit 1
          set src "10.0.1.128/255.255.255.128"
          set dst "128.66.0.0/255.255.255.0"
          set action deny
     next
end

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(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst
(1->65535), Mode(priority),
          link-cost-factor(latency), link-cost-threshold(10),
health-check(Corp_HC)
          Members(2):
               1: Seq_num(2 port2 underlay), alive, latency:
0.769, selected
               2: Seq_num(1 port1 underlay), alive, latency:
71.022, 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(4): Address Mode(IPV4) flags=0x24200 use-shortcut-sla
use-shortcut
     Tie break: cfg
     Shortcut priority: 2
          Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst
(1->65535), Mode(sla hash-mode=round-robin),
          Members(2):
               1: Seq_num(1 port1 underlay), alive sla(0x1),
gid(2), num of pass(1), selected
               2: Seq_num(2 port2 underlay), alive sla(0x1),
gid(2), num of pass(1), selected
          Src address(1):
               10.0.1.0-10.0.1.255

          Dat address(1):
               128.66.0.0-128.66.255.255
```

How does FortiGate handle the traffic with the source IP 10.0.1.130 and the destination IP 128.66.0 125?

A. FortiGate drops the traffic flow.
B. FortiGate routes the traffic flow according to the forwarding information base (FIB).
C. FortiGate load balances the traffic flow through port7 and port8.
D. FortiGate steers the traffic flow through port7.

Answer: C

NEW QUESTION 7
(Refer to the exhibit. The administrator configured two SD-WAN rules to load balance the traffic.

Refer to the exhibit.

```
Service(2): Address Mode(IPV4) flags=0x24200 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 hash-mode=inbandwidth)
  Members(2):
    1: Seq_num(2 port2 WAN2), alive, gid(1), inbandwidth: 10234Kbps, selected
    2: Seq_num(1 port1 WAN1), alive, gid(1), inbandwidth: 10234Kbps, selected
  Application Control(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
  Src address(1):
        10.0.1.0-10.0.1.255

Service(3): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 3
  Gen(6), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla hash-mode=round-robin)
  Members(6):
    1: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(2), num of pass(1), selected
    3: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(1), num of pass(0), selected
    4: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x0), gid(1), num of pass(0), selected
    5: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x0), gid(1), num of pass(0), selected
    6: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x0), gid(1), num of pass(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        10.0.0.0-10.255.255.255
```

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 8
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 9
(You plan a large SD-WAN deployment for a global company. You want to divide the network architecture into five geographical regions and install two hubs in each region for increased redundancy. You expect a significant amount of traffic within each region and limited traffic flow between spokes in different regions. You plan to connect the small branch sites to only the closest hub in their regions and the large branch sites to the two hubs in the regions.
Which statement about your plan is true? Choose one answer.)

A. It is possibl
B. You should use eBGP as the routing protocol between the regions.
C. It is not possibl
D. FortiOS 7.6 supports multihub topologies with up to four hubs.
E. It is possibl
F. You should use FortiManager and the overlay orchestrator multihub topology to simplify the deployment.
G. It is not possibl
H. In a region, all spokes must have either single-hub or dual-hub connectivity.

Answer: A

NEW QUESTION 10
Refer to the exhibit.

Session details

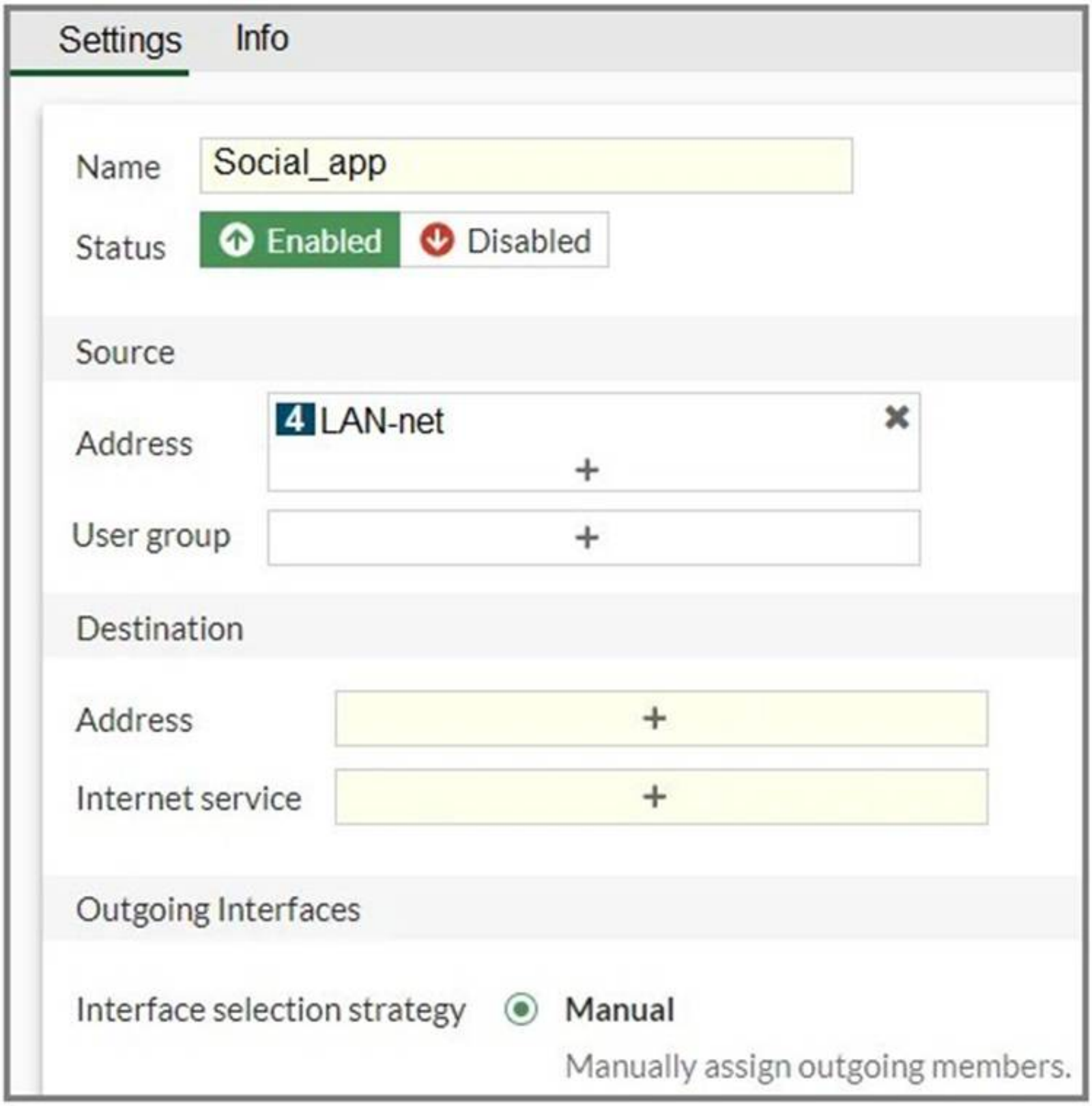
```
# diagnose sys session list

session info: proto=6 proto_state=01 duration=39 expire=3593 timeout=3600
flags=00000000
socktype=0 sockport=0 av_idxe=0 use=4
state=may dirty npu
orgin->sink: org pre->post, reply pre->post dev=7->5/5->7 gwy=
10.10.10.1/10.9.31.160
hook=pre dir=org act=noop 10.9.31.160:7932->10.0.1.7:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.0.1.7:22->10.9.31.160:7932(0.0.0.0:0)
pos/ (before, after) 0/(0,0), 0/ (0,0)
misc=0 policy id=1 auth_info=0 chk _client_info=0 vd=0
serial=00045e02 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=1 sdwan_servic_id=1
rpdb_link_id=800000000 rpdb_svc_id=0 ngfwid=n/a
npu_state= x4000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=64/76, ipid=
76/64,
vian=0x0000/0x0000
vlifid=76/64, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0,
qid=2/2
reflect info 0:
dev=7->6/6->7
npu_state=0x4000800
npu info: flag=0x00/0x81, offload=0/8, ips_offload-0/0, epid-0/76, ipid=
0/65, vlan=0x0000/0x0000
vlifid=0/65, vtag_in=0x0000/0x0000 in_npu=0/1, out_npu=0/1, fwd_en=0/0,
qid=0/2
total reflect session num: 1
total session 1

# diagnose netlink interface list

if=port1 family=00 type=1 index=5 mtu=1500 link=0 master=0
if=port2 family=00 type=1 index=6 mtu=1500 link=0 master=0
if=port3 family=00 type=1 index=7 mtu=1500 link=0 master=0
```

The exhibit shows the details of a session and the index numbers of some relevant interfaces on a FortiGate device that supports hardware offloading.
Based on the information shown in the exhibits, which two conclusions can you draw? (Choose two.)

A. By default, FortiGate offloads symmetric and asymmetric flows.
B. The original direction of the symmetric traffic flows from port3 to port2.
C. The reply direction of the asymmetric traffic flows from port2 to port3.
D. The auxiliary session can be offloaded to hardware.

Answer: BC

NEW QUESTION 10
Refer to the exhibit.



You configure SD-WAN on a standalone FortiGate device. You want to create an SD-WAN rule that steers Facebook and Linkedin traffic through the less costly internet link. The FortiGate GUI page appears as shown in the exhibit.
What should you do to set Facebook and LinkedIn as destinations?

A. Install a license to allow applications as destinations of SD-WAN rules.
B. In the Internet service field, select Facebook and LinkedIn.
C. Enable the applications as destinations of the SD-WAN rule feature visibility.
D. You cannot configure applications as destinations of an SD-WAN rule on a standalone FortiGate device.

Answer: B

NEW QUESTION 15
Which three characteristics apply to provisioning templates available on FortiManager? (Choose three.)

A. A template group can include a system template and an SD-WAN template.
B. Each template group can contain up to three IPsec tunnel templates.
C. CLI templates are applied in order, from top to bottom
D. A CLI template group can contain CLI templates of both types.
E. A CLI template can be of type CLI script or Perl script.

Answer: ACD

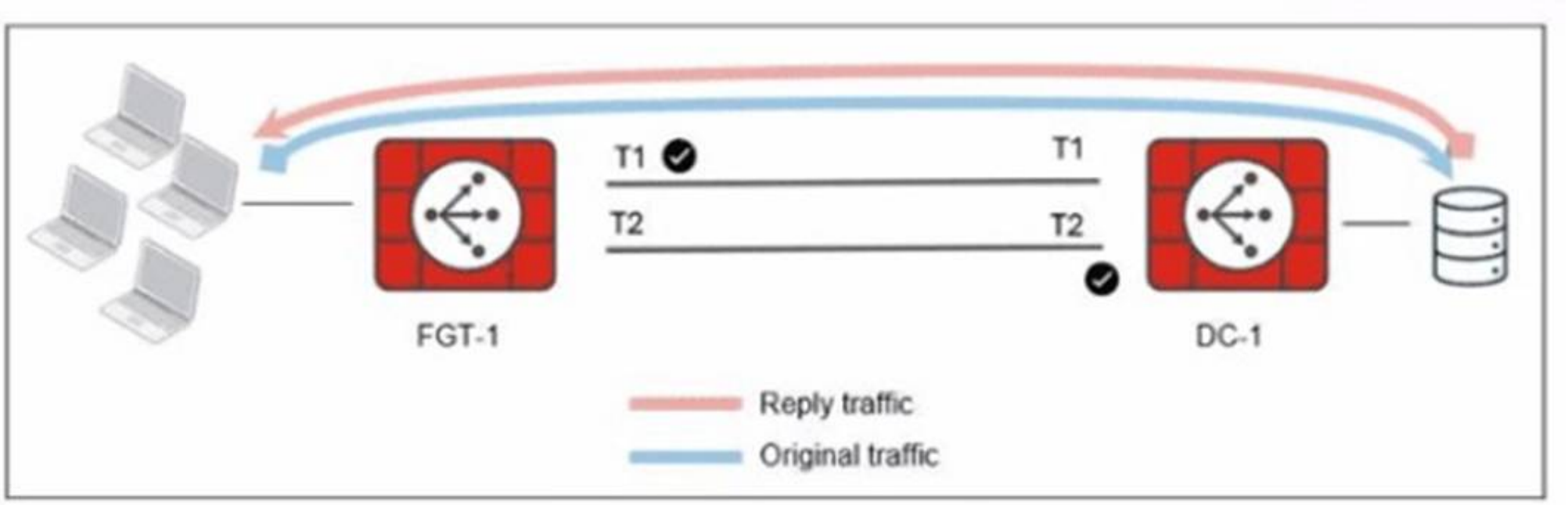
NEW QUESTION 16
(You are using the FortiManager SD-WAN monitor menus to check the status of an SD- WAN topology. When you place the mouse next to branch1_fgt, you receive the output shown in the exhibit.

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 17
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: B

NEW QUESTION 22
(Refer to the exhibits.

SD-WAN event logs

Identity

Device ID	FGVM02TM25002088
Device Name	branch1_fgt

Type

Sub Type	sdwan
Type	event

Alerts

Action	
Level	notice

General

Log Description	SDWAN status
Log ID	0113022923
Member	1
Message	Member status changed. Member out-of-sla.
Virtual Domain	root

Others

Date	2025-07-01
Date/Time	2025-07-01 05:00:25
Destination End User ID	3
Destination Endpoint ID	3
Destination Geo ID	0
Device Time	2025-07-01 05:00:25
Device Time Zone	-0700
Event Time	2025-07-01 05:00:25
Event Type	Health Check
Health Check	Corp_HC
Log Flag	0
New Value	1
Old Value	2
SLA Target ID	1
Source City	Sunnyvale

SD-WAN rule configuration

```
branch1_fgt (service) # show
config service
    edit 1
        set name "Critical-DIA"
        set mode sla
        set src "LAN-net"
        set internet-service enable
        set internet-service-app-ctrl 16920 41469
        set internet-service-app-ctrl-category 28
        config sla
            edit "Corp_HC"
                set id 1
            next
        end
        set priority-members 1 2
    next
```

SD-WAN health-check configuration

```
branch1_fgt (health-check) # show
config health-check
    edit "Corp_HC"
        set server "198.18.1.1" "198.18.1.2"
        set member 1 2
        config sla
            edit 1
                set latency-threshold 150
                set jitter-threshold 50
                set packetloss-threshold 5
            next
        end
    end
```

SD-WAN member status

```
branch1_fgt # diagnose sys sdwan member
Member(1): type: 0, transport-group: 0, interface: port1, flags=0x0,
gateway: 192.2.0.2, source 192.2.0.1, priority: 1 1024, weight: 0
Member(2): type: 0, transport-group: 0, interface: port2, flags=0x0,
gateway: 192.2.0.10, source 192.2.0.9, priority: 1 1024, weight: 0
Member(3): type: 0, transport-group: 0, interface: port4, flags=0x0,
source 172.16.0.1, priority: 1 1024, weight: 0
```

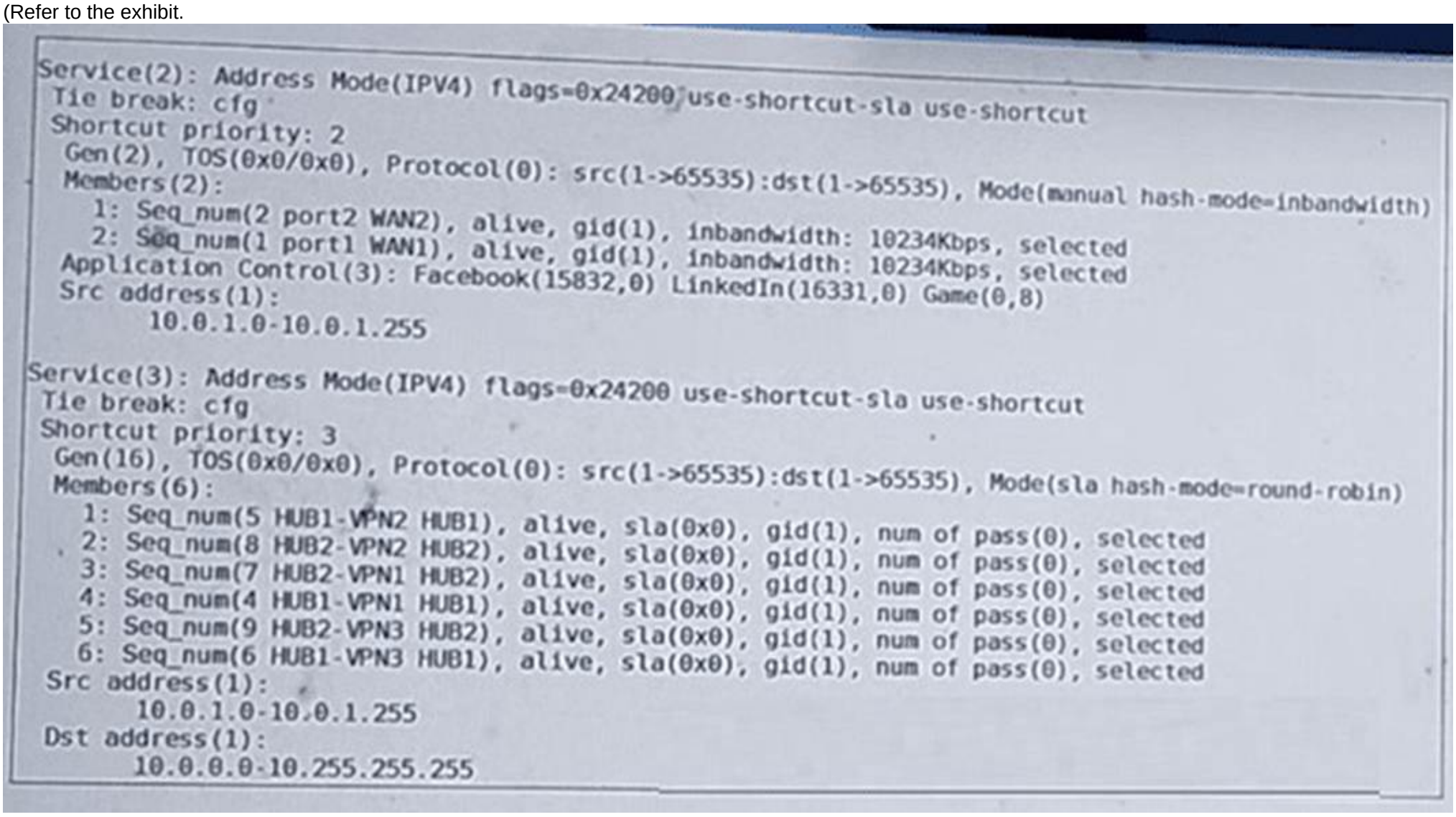
Two SD-WAN event logs, the member status, the SD-WAN rule configuration, and the health-check configuration for a FortiGate device are shown.
Immediately after the log messages are displayed, how will the FortiGate steer the traffic based on the information shown in the exhibits? Choose one answer.)

A. FortiGate skips SD-WAN rule ID 1.

B. FortiGate uses port2 to steer the traffic for SD-WAN rule ID 1.
C. FortiGate uses port1 to steer the traffic for SD-WAN rule ID 1.
D. FortiGate uses port1 or port2 to steer the traffic for SD-WAN rule ID 1.

Answer: B

NEW QUESTION 23
(Refer to the exhibit.



The administrator configured two SD-WAN rules to load balance traffic.
Which interfaces does FortiGate use to steer the traffic from 10.0.1.124 to 10.0.0.254? Choose one answer.)

A. port1 or port2
B. FortiGate routes the traffic according to the FIB.
C. HUB1-VPN2
D. Any interface in the HUB1 or HUB2 zones

Answer: B

NEW QUESTION 25
You configured an SD-WAN rule with the best quality strategy and selected the predefined health check, Default_FortiGuard, to check the link performances against FortiGuard servers.
For the quality criteria, you selected Custom-profile-1.
Which factors does FortiGate use, and in which order. to determine the link that it should use to steer the traffic?

A. Latency – Member configuration order – Link cost threshold
B. Link quality index – Member configuration order – Link cost threshold
C. Links that meet the SLA targets – Member configuration order – Member local cost
D. Latency – Jitter - Packet loss – Bibandwidth – Member configuration order

Answer: C

NEW QUESTION 30
Refer to the exhibit.

Diagnose output

```
fgt_1 # diagnose  sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
 link-cost-factor(latency), link-cost-threshold(10), heath-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.906, selected
    2: Seq_num(1 port1 underlay), alive, latency: 1.079, selected
  Application Control(2): Microsoft.Portal(41469,0) Business(0,29)
  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(1), 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(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
 link-cost-factor(latency), link-cost-threshold(10), heath-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.906, selected
    2: Seq_num(1 port1 underlay), alive, latency: 1.079, selected
  Application Control(2): Microsoft.Portal(41469,0) Business(0,29)
  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(1), 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(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla
hash-mode=round-robin)
  Members(3):
    1: Seq_num(4 HQ_T1 overlay), alive, sla(0x3), gid(0), cfg_order(0),
local cost(0), selected
    2: Seq_num(5 HQ_T2 overlay), alive, sla(0x3), gid(0), cfg_order(1),
local cost(0), selected
    3: Seq_num(6 HQ_T3 overlay), alive, sla(0x3), gid(0), cfg_order(2),
local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

The exhibit shows output of the command diagnose sys adwan aervice4 collected on a FortiGate device.
The administrator wants to know through which interface FortiGate will steer traffic from local users on subnet 10.0.1.0/255.255.255.192 and with a destination of the social media application Facebook.
Based on the exhibits, which two statements are correct? (Choose two.)

A. When FortiGate cannot recognize the application of the flow, it steers the traffic through the preferred member of rule 3, HQ_T1.
B. There is no service defined for the Facebook application, so FortiGate appliesservice rule 3 and directs the traffic to headquarters.
C. FortiGate steers traffic for social media applications according to the service rule 2 and steers traffic through port2.
D. When FortiGate cannot recognize the application of the flow, it load balances the traffic through the tunnels HQ_T1. HQ_T2. HQ_T3.

Answer: CD

NEW QUESTION 35
(Refer to the exhibit.

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." Brave-Dumps.com "

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
```

The event log on a FortiGate device is shown.
Based on the output shown in the exhibit, what can you conclude about the tunnels on this device? (Choose one answer))

A. There is one shortcut tunnel built from the master tunnel VPN4.
B. The voice traffic is steered through the VPN tunnel HUB1-VPN3.
C. The VPN tunnel HUB1-VPN1_0 is a shortcut tunnel.
D. The master tunnel HUB2-VPN3 cannot accept Auto-Discovery VPN (ADVPN) shortcuts.

Answer: C

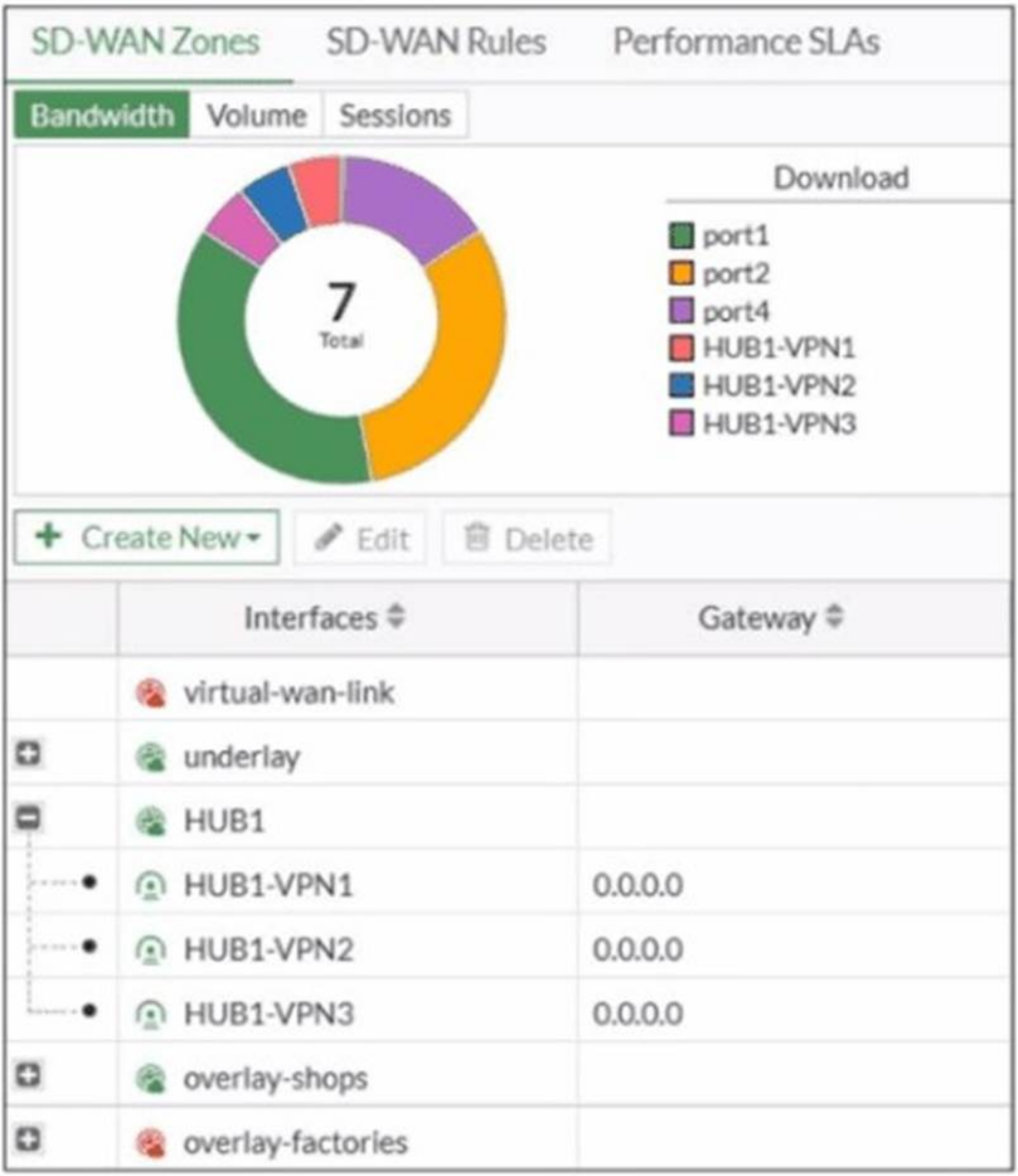
NEW QUESTION 37
An administrator is configuring SD-WAN to load balance their network traffic. Which two things should they consider when setting up SD-WAN? (Choose two.)

A. You can select the outbandwidth hash mode with all strategies that allow load balancing.
B. Only the manual and best-quality strategies allow SD-WAN load balancing.
C. When applicabl
D. FortiGate load balances the traffic through all members that meet the SLA target.
E. SD-WAN load balancing is possible only using the best quality and lowest cost (SLA) strategies.

Answer: AC

NEW QUESTION 41
Exhibit.

SD-WAN zones



Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI. What can you conclude about the zone and member configuration on this device?

A. The underlay zone contains three members.
B. You can delete the virtual-wan-link zones.
C. The overlay-factories zone contains no member.
D. You can move HUB1-VPN3 from the HUB1 zone to the overlay-shops zone.

Answer: C

NEW QUESTION 42
Refer to the exhibits.

Network Properties

Service	Critical-DIA
Identity	
Device ID	FGVM01TM22000077
Device Name	branch1_fgt
Type	
Sub Type	sdwan
Type	event
Alerts	
Level	notice
General	
Log Description	SDWAN status
Log ID	0113022923
Message	Service prioritized by performance metric will be redirected in sequence order
Sequence Number	2.1
Virtual Domain	root
Others	
Date	2024-12-12
Date/Time	2024-12-12 09:09:30
Destination End User ID	3
Destination Endpoint ID	3
Device Time	2024-12-12 09:09:30
Device Time Zone	–0800
Event Time	1734023370180275742
Event Type	Service
Metric	latency
Service ID	1
Time	09:09:30
UEBA Endpoint ID	3
UEBA User ID	3

SD-WAN member status

```
branch1_fgt # diagnose sys sdwan member
Member(1): transport-group: 0, interface: port1, flags=0x0,
gateway: 192.2.0.2, source 192.2.0.1, priority: 1 1024, weight: 0
Member(2): transport-group: 0, interface: port2, flags=0x0,
gateway: 192.2.0.10, source 192.2.0.9, priority: 10 1024, weight: 0
```

SD-WAN rule configuration

```
config service
     edit 1
          set name "Critical-DIA"
          set mode priority
          set src "LAN-net"
          set internet-service enable
          set internet-service-app-ctrl 41469 16920
          set internet-service-app-ctrl-category 28
          set health-check "Corp_HC"
          set priority-members 1 2
     next
end
```

The exhibits show an SD-WAN event log, the member status, and the SD-WAN rule configuration.
Which two conclusions can you draw from the information shown? (Choose two.)

A. The administrator configured the service ID 1 with the highest priority member for port2.
B. Port2 has a lower latency than port1.
C. FortiGate updated the outgoing interface list on the rule so it prefers port2.
D. The administrator configured the SD-WAN rule ID 1 with the default strategy mode.

Answer: BC

NEW QUESTION 46
Exhibit.

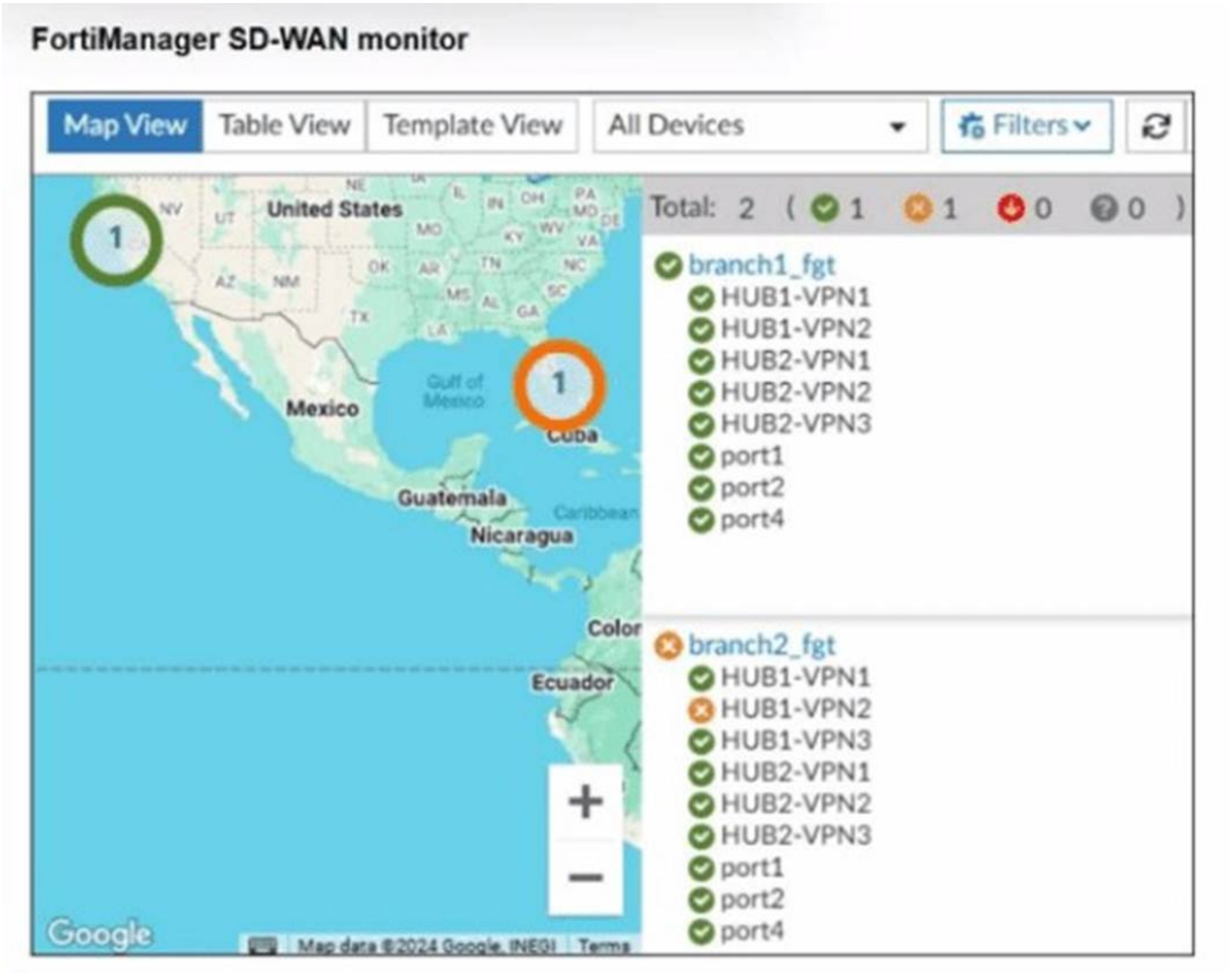
```
config system sdwan
    set fail-detect enable
    set fail-alert-interfaces "port5"
    config health-check
        edit "Level3_DNS"
            set update-cascade-interface enable
            set members 1 2
        next
        edit "HQ"
            set update-cascade-interface enable
            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 51
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 missing the 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 56
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 60
(In which order does FortiGate consider the following elements during the route lookup process? Choose one answer.)

A. SD-WAN rules, ISDB routes, policy routes, BGP routes
B. Policy routes, SD-WAN rules, Internet Service Database (ISDB) routes, BGP routes
C. SD-WAN rules, policy routes, static routes, ISDB routes
D. Policy routes, ISDB routes, SD-WAN rules, static routes

Answer: D

NEW QUESTION 61

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 and assign them to the branch devices.
C. Assign a hub id metadata variable to each hub device.
D. Configure SD-WAN rules
E. Assign an sdwan_id metadata variable to each device (branch and hub)

Answer: BD

NEW QUESTION 64
Refer to the exhibits.

SD-WAN zone HUB1 and SD-WAN member configuration

SD-WAN Zones

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

	ID	Interface	Gateway	Cost	Priority	Status	Installation Target
	HUB1						
	4	HUB1-VPN1	0.0.0.0	0	1	Enable	
	5	HUB1-VPN2	0.0.0.0	0	1	Enable	3 Devices in Total branch1_fgt[root] branch2_fgt[root] branch3_fgt[root] View Details >
	6	HUB1-VPN3	0.0.0.0	0	1	Enable	2 Devices in Total branch2_fgt[root] branch3_fgt[root] View Details >

SD-WAN zone HUB2 and SD-WAN member configuration

	HUB2						
	7	HUB2-VPN1	0.0.0.0	10	1	Enable	3 Devices in Total branch1_fgt[root] branch2_fgt[root] branch3_fgt[root] View Details >
	8	HUB2-VPN2	0.0.0.0	10	1	Enable	
	9	HUB2-VPN3	0.0.0.0	10	1	Enable	

Output of command `diagnose sys sdwan member`

```
     _fgt # diagnose sys sdwan member
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xd
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xd
Member(7): transport-group: 0, interface: HUB2-VPN1, flags=0xd
Member(8): transport-group: 0, interface: HUB2-VPN2, flags=0xd
Member(9): transport-group: 0, interface: HUB2-VPN3, flags=0xd
```

The first exhibit shows the SD-WAN zone HUB1 and SD-WAN member configuration from an SD-WAN template, and the second exhibit shows the output of command diagnose sys sdwan member collected on a FortiGate device.
Which statement best describes what the diagnose output shows?

A. The diagnose output shows that HUB1-VPN1 and all HUBx-VPNy members are dead.
B. The diagnose output does not correspond to a device configured with the SD-WAN template shown in the exhibit.
C. The diagnose output was collected on the device branch2_fgt.
D. The diagnose output was collected on the device branch1_fgt

Answer: D

NEW QUESTION 67
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 combine metadata variable and installation targets.
C. Gateways for all 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: D

NEW QUESTION 71
Refer to the exhibits, which show the configuration of an SD-WAN rule and the corresponding rule status and routing table.

SD-WAN rule

```
branch_fgt (3) # show
config service
     edit 3
          set name "Corp"
          set mode sla
          set dst "LAN-net"
          set src "LAN-net"
          config sla
               edit "HUB1_HC"
                    set id 1
               next
               edit "HUB1_HTTP"
                    set id 1
               next
          end
          set priority-members 4 5 6
     next
end
```

SD-WAN rule status and routing table

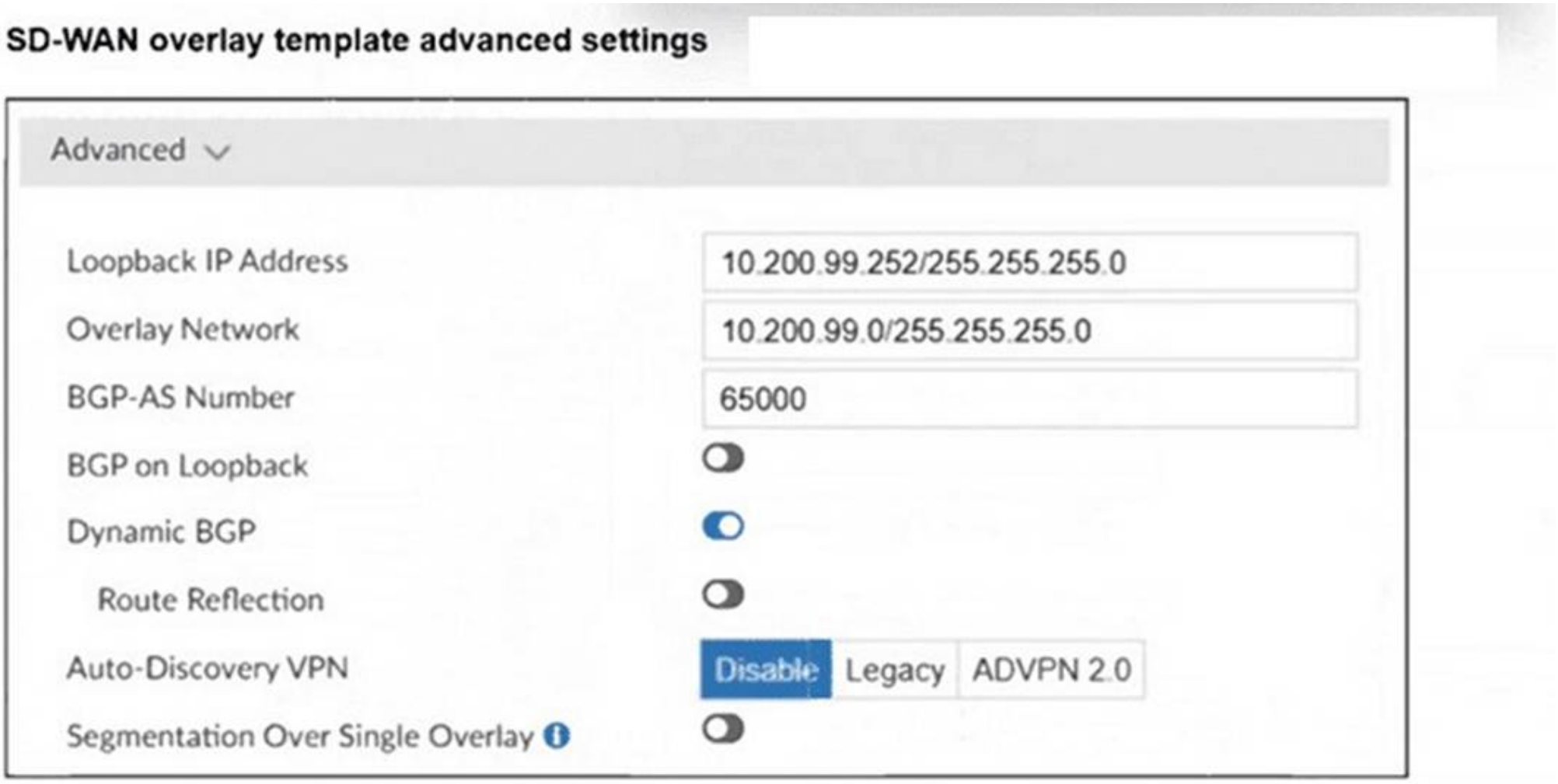
```
branch1_fgt # diagnose sys sdwan service4 3

Service (3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority: 2
          Gen(3), TOS(0x0/0x0), Protocol (0): src(1->65535):dst (1->65535),
     Mode(sla), sla-compare-order
          Members (3):
          1: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x3), gid(0), cfg order(2),
     local cost (0), selected
          2: Seq num(5 HUB1-VPN2  HUB1), alive, sla(0x2), gid(0), cfg order
     (1), local cost (0), selected
          3: Seq num(4 HUB1-VPN1 HUB1), alive, s1a(0x0), gid(0), cfg order
     (0), local cost (0), selected
          Src address(1):
               10.0.1.0-10.0.1.255

          Dst address (1):
               10.1.0.0-10.1.255.255

branch1_fgt # get router info routing-table all | grep HUB1
B    10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected,
HUB1-VPN1), 00:20:06, [1/0]
                [200/0] via 192.168.1.125 (recursive is directly connected,
          HUB1-VPN2), 00:20:06, [1/0]
B    10.2.0.0/24 [200/0] via 192.168.1.189 (recursive is directly connected,
HUB1-VPN3), 00:20:06, [1/0]
C    192.168.1.0/26 is directly connected, HUB1-VPN1
C    192.168.1.1/32 is directly connected, HUB1-VPN1
C    192.168.1.64/26 is directly connected, HUB1-VPN2
C    192.168.1.65/32 is directly connected, HUB1-VPN2
C    192.168.1.128/26 is directly connected, HUB1-VPN3
C    192.168.1.129/32 is directly connected, HUB1-VPN3
```

The administrator wants to understand the expected behavior for traffic matching the SD- WAN rule.
Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

A. The traffic will be routed over HUB1-VPN3.
B. The traffic will be routed over HUB1-VPN2
C. The traffic will be routed over HUB1-VPN1.
D. The traffic will be load balanced across all three overlays

Answer: B

NEW QUESTION 72
(Refer to the exhibits.



The SD-WAN overlay template advanced settings and the underlay and network advertisement settings are shown. These are the configurations for the secondary hub of a dual-hub SD-WAN topology created with the FortiManager SD-WAN overlay orchestrator.
Which two conclusions can you draw from the information shown in the exhibits? Choose two answers.)

A. FortiManager will define port2 as a BGP neighbor.
B. FortiManager will create an overlay tunnel on the port2 interface.
C. FortiManager will create an overlay tunnel on the port1 interface.
D. FortiManager will define port5 as a BGP neighbor.

Answer: BC

NEW QUESTION 76
Refer to the exhibit.

```
# diagnose sys session list
session info: proto=6 prote_state=11 duration=180 expire=3424 timeout=3600
refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may dirty ndr f00 app_valid route preserve
statistic (bytes/packets/allow_err): org=3369/19/1 reply=3881/19/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=192.2.0.2/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:58630->128.66.0.1:22(192.2.0.100:58630)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.100:58360(10.0.1.101:58360)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:58630(0.0.0.0:0)
pos/ (before, after) 0/(0,0), 0/(0,0)
misc=0 policy id=1 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=00000c0c tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service id=4
rpdb_link_id=ff000004 ngfwid=n/a
npu_stave=0x001108
no_offoad_reason: redir-to-ips denied-by-nturbo
```

The administrator configured the SD-WAN rule ID 4 with two members (port1 and port2) and strategy lowest cost (SLA).
What are the two characteristics of the session shown in the exhibit? (Choose two.)

A. FortiGate steered this flow according to an SD-WAN rule 4.
B. FortiGate will never re-evaluate this session.
C. FortiGate steered this flow according to the application detected and the outgoing interface is port3.
D. FortiGate will re-evaluate this session if the outgoing interface goes down.

Answer: AD

NEW QUESTION 78
Refer to the exhibit, which shows the SD-WAN rule status and configuration.

SD-WAN rule 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(10), heath-check(HUB1_HC)
     Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, latency: 96.349, selected
          2: Seq_num(5 HUB1-VPN2 HUB1), alive, latency: 141.278, selected
          3: Seq_num(6 HUB1-VPN3 HUB1), alive, latency: 190.984, 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 4 5 6
     next
```

Based on the exhibit, which change in the measured latency will first make HUB1-VPN3 the new preferred member?

A. When HUB1-VPN3 has a lower latency than HUB1-VPN1 and HUB1-VPN2
B. When HUB1-VPN3 has a latency of 80 ms
C. When HUB1-VPN3 has a latency of 90 ms
D. When HUB1-VPN1 has a latency of 200 ms

Answer: D

NEW QUESTION 80
(Refer to the exhibit.

Refer to the exhibit.

```
London_1 # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 3
  Gen(33), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Member sub interface(9):
    4: seq_num(4), interface(HUB1-VPN1):
       1: HUB1-VPN1_0(30)
       2: HUB1-VPN1_1(35)
    5: seq_num(5), interface(HUB1-VPN2):
       1: HUB1-VPN2_0(31)
  Members(9):
    1: Seq_num(4 HUB1-VPN1_1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(4 HUB1-VPN1_0 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    3: Seq_num(5 HUB1-VPN2_0 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    4: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    5: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    6: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    7: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
    8: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(0), cfg_order(4), local cost(10), selected
    9: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x2), gid(0), cfg_order(5), local cost(10), selected
  Src address(2):
        10.0.0.0-10.255.255.255
        10.0.1.0-10.0.1.255
  Dst address(2):
        10.0.1.0-10.0.1.255
        10.0.0.0-10.255.255.255
```

What can you conclude from the output shown? Choose one answer.)

A. It is a spoke devic
B. SD-WAN rule 3 is configured with nine members.
C. It is a spoke devic
D. The members of SD-WAN rule 3 are grouped into two zones.
E. It is a hub devic
F. It allowed the establishment of three auto-discovery VPN (ADVPN) shortcuts.
G. It is a spoke devic
H. SD-WAN rule 4 allows three shortcut tunnels.

Answer: A

NEW QUESTION 81
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 84
When you use the command diagnose sys session list, how do you identify the sessions that correspond to traffic steered according to SD-WAN rules?

A. You identify sessions steered according to SD-WAN rules with the flag vwl.
B. You cannot identify SD-WAN session
C. You must use the sdwa
D. session filter.
E. You identify sessions steered according to SD-WAN rules with the data vwl_mbr_seq.
F. You identify sessions steered according to SD-WAN rules with the data 3dwan_service_id.

Answer: D

NEW QUESTION 87
The FortiGate devices are managed by ForliManager, and are configured for direct internet access (DIA). You confirm that DIA is working as expected for each branch, and check the SD-WAN zone configuration and firewall policies shown in the exhibits.

SD-WAN zones

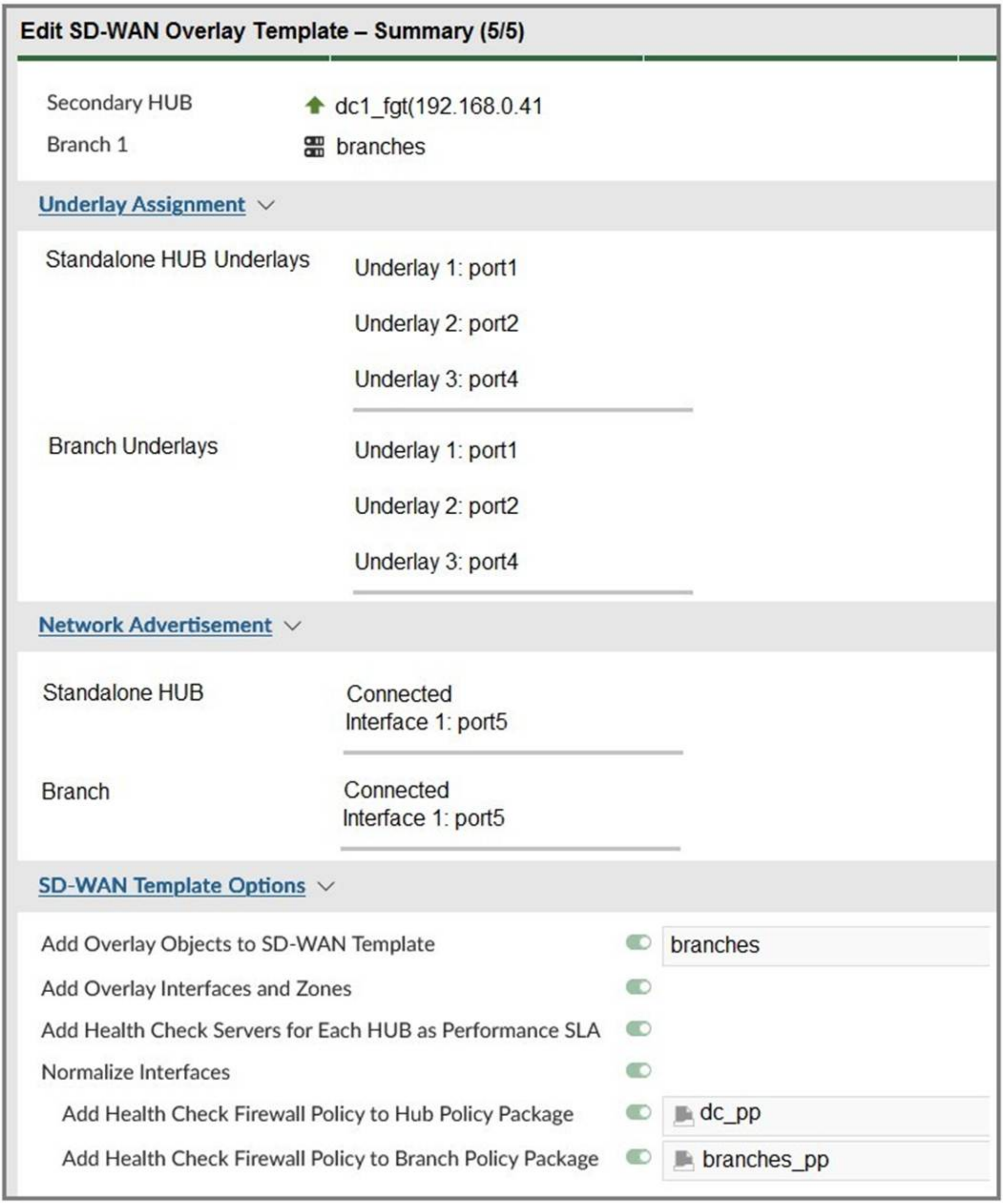
SD-WAN Zones

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

ID	Interface	Gateway	Cost	Priority	Status
virtual-wan-link					
underlay					
1	port1	$(sdwan_port1_gw)	0	1	Enable
2	port2	$(sdwan_port2_gw)	0	1	Enable

Firewall Policy

ID	Name	From	To	Source	Destination	Service	Action	Schedule
1	DIA	LAN	underlay	LAN-net	all	All	Accept	always



Then, you use the SD-WAN overlay template to configure the IPsec overlay tunnels. You create the associated SD-WAN rules to connect existing branches to the company hub device and apply the changes on the branches.
After those changes, users complain that they lost internet access. DIA is no longer working.
Based on the exhibit, which statement best describes the possible root cause of this issue?

A. The SD-WAN overlay template defines a zone for each underlay interface and moves the interfaces into those zones.
B. The SD-WAN overlay template didn??t configure a firewall policy to allow traffic through the overlay.
C. The SD-WAN overlay template redefines the interface gateway addresses if they are defined with metadata variables.
D. The SD-WAN overlay template updates the SD-WAN template and the rules.

Answer: A

NEW QUESTION 89

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 90
(Refer to the exhibits. You collected the output shown in the exhibits and want to know which interface TCP traffic will flow through from the user device 10.0.1.101 to the corporate file server 10.0.0.125. All SD-WAN links are stable.

SD-WAN rule configuration

```
config service
    edit 3
        set name "Corp"
        set load-balance enable
        set mode sla
        set minimum-sla-meet-members 2
        set hash-mode source-ip-based
        set dst "Corp-net"
        set src "LAN-net"
        config sla
            edit "HUB1_HC"
                set id 1
            next
            edit "HUB1_HTTP"
                set id 1
            next
        end
        set priority-members 3 4 5
    next
end
```

Proute list

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

id=2130968577(0x7f040001) 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=0 rule_last_used=2025-06-19 03:14:42

id=2130968578(0x7f040002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=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(1): 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(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
hit_count=0 rule_last_used=2025-06-19 03:14:42

id=2130968579(0x7f040003) vwl_service=3(Corp) vwl_mbr_seq=3 4 5 dscp_tag=0xfc 0xfc flags=0x10
load-balance hash-mode=source-ip-based tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0)
iif=0(any)
path(3): oif=19(HUB1-VPN1) num_pass=2, oif=20(HUB1-VPN2) num_pass=2, oif=21(HUB1-VPN3) num_pass=1
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=473 rule_last_used=2025-06-19 04:04:40
```

Sniffer trace

```
branch1_fgt # diagnose sniffer packet any "host 10.0.1.101 and icmp" 4 0 1
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.1.101 and icmp]
2025-06-19 04:08:12.140250 port5 in 10.0.1.101 -> 10.0.3.101: icmp: echo request
2025-06-19 04:08:12.140322 HUB1-VPN2 out 10.0.1.101 -> 10.0.3.101: icmp: echo request
2025-06-19 04:08:13.152744 port5 in 10.0.1.101 -> 10.0.3.101: icmp: echo request
2025-06-19 04:08:13.152764 HUB1-VPN2 out 10.0.1.101 -> 10.0.3.101: icmp: echo request
```

Routing table

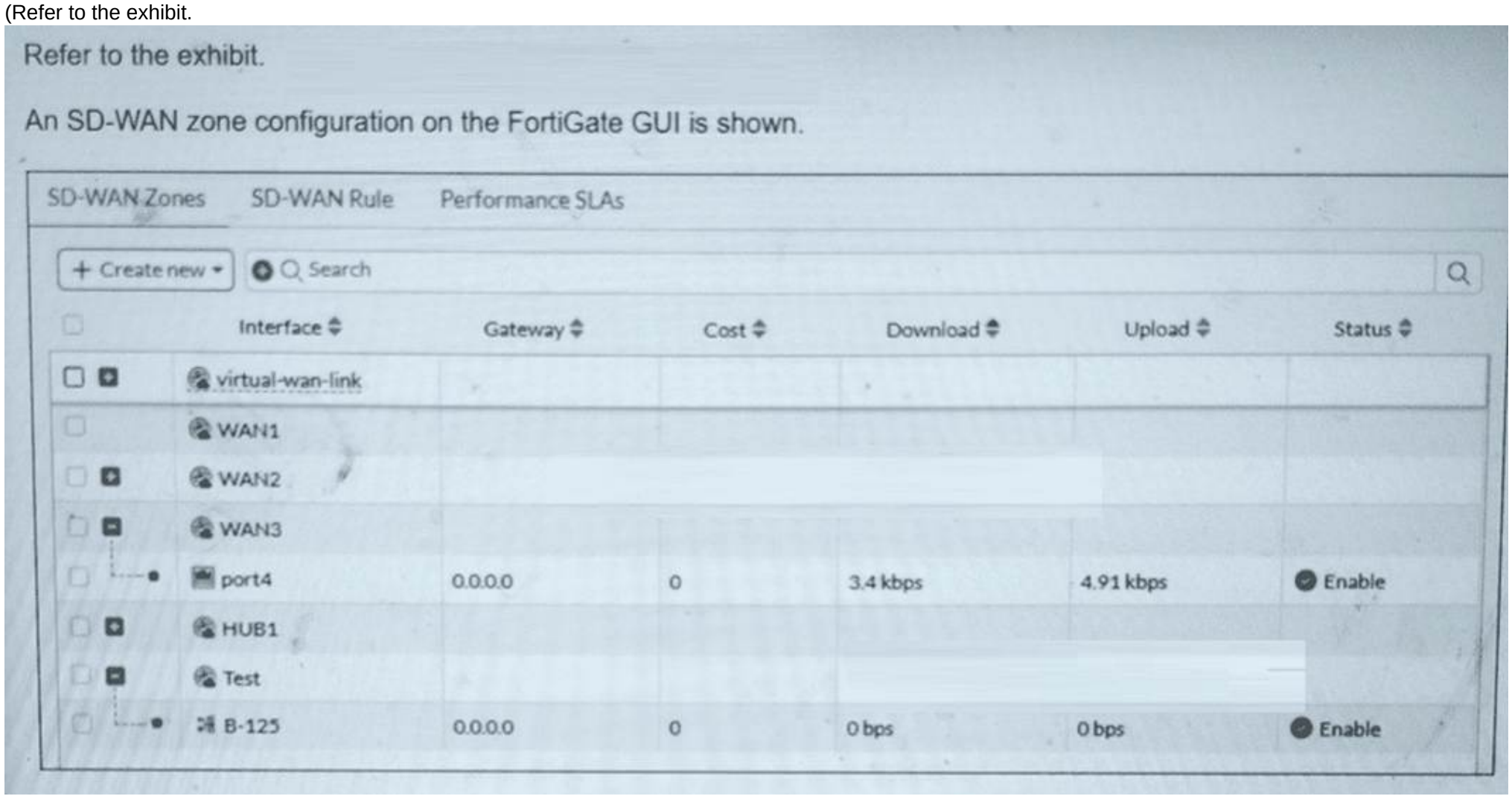
```
branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [1/0]
S       10.0.0.0/8 [10/0] via HUB1-VPN1 tunnel 100.64.1.1, [1/0]
                   [10/0] via HUB1-VPN2 tunnel 100.64.1.9, [1/0]
                   [10/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
C       10.0.1.0/24 is directly connected, port5
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10
```

Which interface will FortiGate use to steer the traffic? Choose one answer.)

A. Only HUB1-VPN1
B. Either HUB1-VPN1 or HUB1-VPN2
C. Only HUB1-VPN2
D. Either HUB1-VPN1, HUB1-VPN2, or HUB1-VPN3

Answer: B

NEW QUESTION 92
(Refer to the exhibit.



An SD-WAN zone configuration on the FortiGate GUI is shown.
What can you conclude about the zone and member configuration on this device? Choose one answer.)

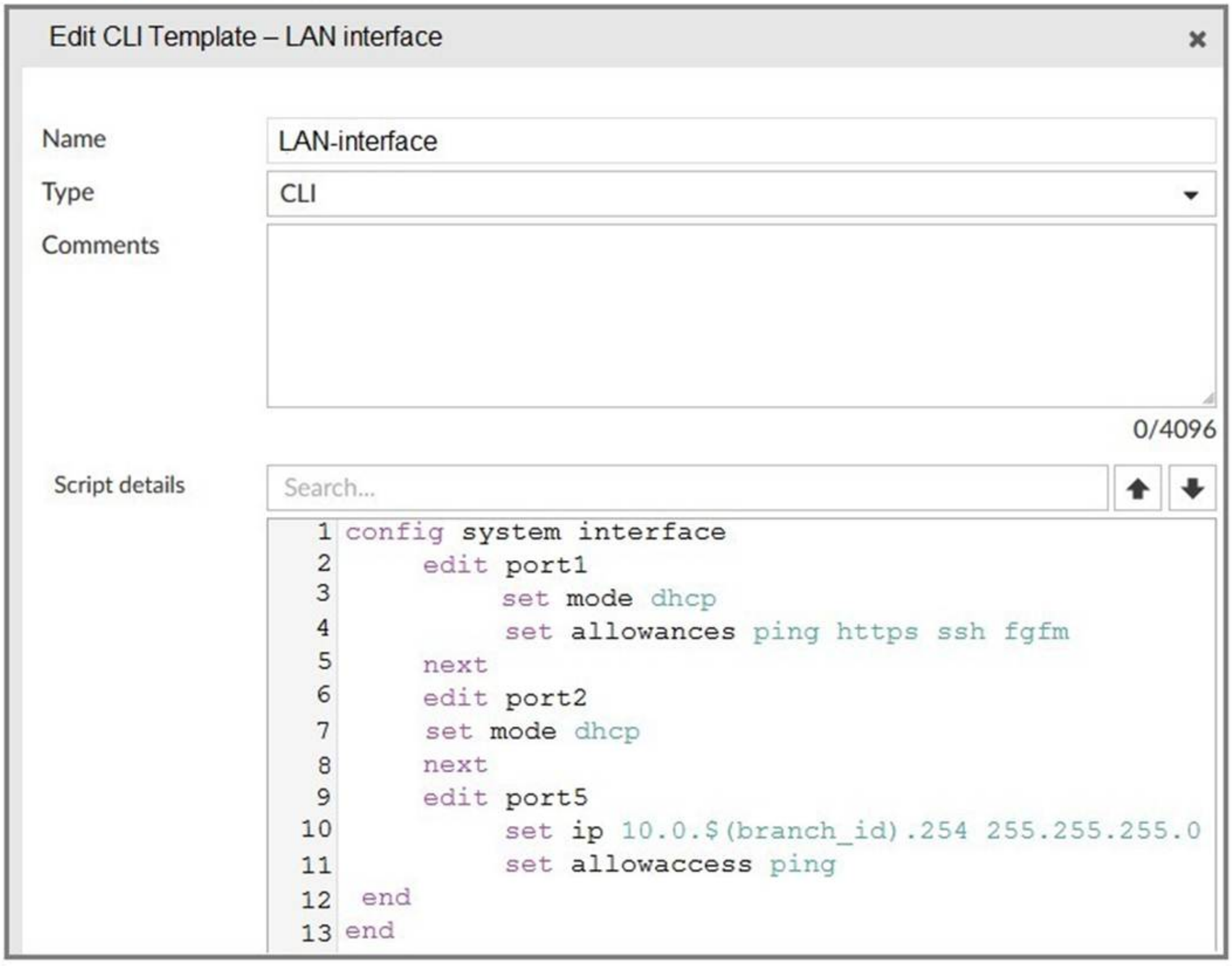
A. You can delete the virtual-wan-link zone.
B. The WAN2 zone contains no member.
C. You can delete the WAN1 zone.
D. You can add the member B-125 to the WAN3 zone and keep it as a member of the Test zone.

Answer: B

NEW QUESTION 95
Refer to the exhibits.

Device blueprint

CLI script LAN-interface



The administrator configured a device blueprint and CLI scripts as shown in the exhibits, to prepare for onboarding FortiGate devices in the company??s stores. Later, a technician prepares a FortiGate 51G with a basic configuration and connects it to the network. The basic configuration contains the port1 configuration and the minimal configuration required to allow the device to connect to FortiManager.
After the device first connects to FortiManager, FortiManager updates the device configuration.
Based on the exhibits, which actions does FortiManager perform?

A. FortiManager updates the device configuration according to the selected template
B. It applies the corp_st template first.
C. FortiManager does not update the port1 configuration because FortiManager does not change the configuration of interfaces with fgfm access.
D. FortiManager updates access rights only for port1. FortiManager cannot update the IP address because it was already set manually.
E. FortiManager updates the configuration of port1, port2, and port5. The three ports might get new IP addresses.

Answer: D

NEW QUESTION 98
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: BD

NEW QUESTION 100
Which statement describes FortiGate behavior when you reference a zone in a static route?

A. FoftiGate installs ECMP static routes for the first two members of the zone.
B. FortiGate ignores the static routes defined through members referenced in the zone.
C. FortiGate routes the traffic through the best performing member of the zone.
D. FortiGate installs a static route for each member in the zone.

Answer: D

NEW QUESTION 101
Refer to the exhibits.

SD-WAN zone configuration on FortiManager

SD-WAN Zones

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

	ID	Interface	Gateway	Cost	Priority	Status	Installation Target
	virtual-wan-link						
	underlay						
	1						
	2	port1	0.0.0.0	0	1	Enable	
	HUB1	port2	0.0.0.0	0	1	Enable	
	4	HUB1-VPN1	0.0.0.0	0	1	Enable	1 Device in Total View Details > branch1_fgt[root]
	5	HUB1-VPN2	0.0.0.0	0	1	Enable	

7

Policy package configuration

#	Name	From	To	Source	Destination	Install On
Corp-SOT_BBLK(1/1 Total:1)						
2	DIA	LAN	underlay	LAN-net	all	Installation Targets
3	To Hub-Overlay	LAN	HUB1-VPN1	all	all	Installation Targets
Implicit(4/4 Total:1)						
4	Implicit Deny	any	any	all all	all all	

The exhibits show the SD-WAN zone configuration of an SD-WAN template prepared on FortiManager and the policy package configuration.
When the administrator tries to install the configuration changes, FortiManager fails to commit.
What should the administrator do to fix the issue?

A. Configure branch1_fgt as the installation target for policy 3.
B. Configure HUB1 as the destination of policy 3.
C. Configure a normalized interface for the IPsec tunnel HUB1-VPN1.
D. Configure both HUB1-VPN1 and HUB1-VPN2 as the destination of policy 3

Answer: B

NEW QUESTION 106
.....

Relate Links

100% Pass Your FCSS_SDW_AR-7.6 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_SDW_AR-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/