# Fortinet

## Exam Questions FCSS_SDW_AR-7.6

FCSS - SD-WAN 7.6 Architect

**NEW QUESTION 1**
(Refer to the exhibit.

Refer to the exhibit.

```
config vpn ipsec phase1-interface
    edit "HUB1-VPN1"
        set auto-discovery-shortcuts dependent
        set network-overlay enable
        set network-id 1
    next
    edit "HUB1-VPN2"
        set auto-discovery-shortcuts dependent
        set network-overlay enable
        set network-id 2
    next
    edit
        edit "HUB1-VPN3"
        set auto-discovery-shortcuts dependent
        set network-overlay enable
        set network-id 3
    next
end
```

You update the spokes configuration of an existing auto-discovery VPN (ADVPN) topology by adding the parameters shown in the exhibit.
Which is a valid objective of those settings? Choose one answer.)

A. Enable the tunnels as overlay links.
B. Convert the configuration from ADVPN to ADVPN 2.0.
C. Prevent cross-overlay shortcuts.
D. Prevent multiple shortcuts from being established over the same overlay.

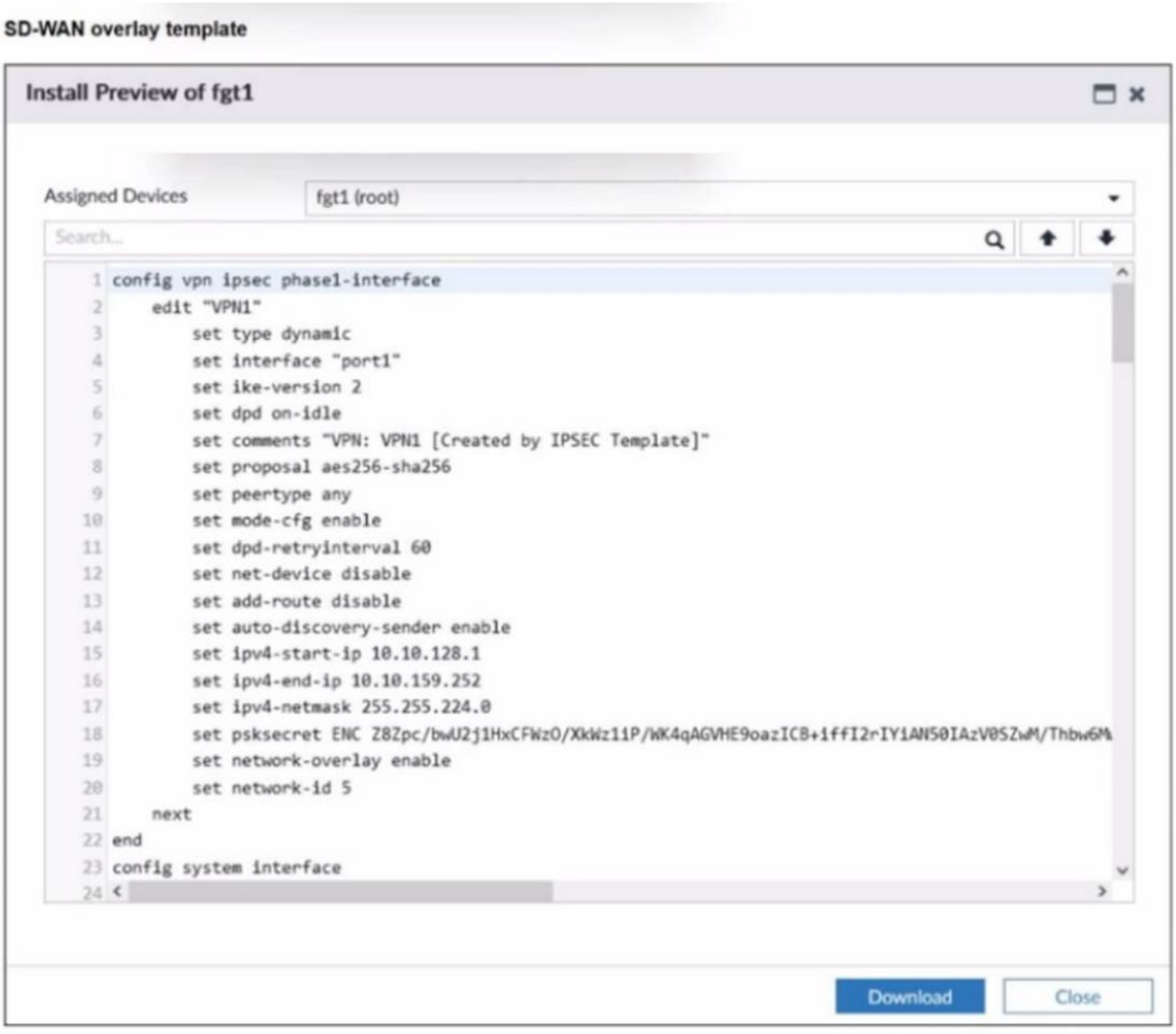
**Answer:** C

**NEW QUESTION 2**
You used the HUB IPsec_Recommended and the BRANCH IPsec_Recommended templates to define the overlay topology. Then, you used the SD-WAN template to define the SD- WAN members, rules, and performance SLAs.
You applied the changes to the devices and want to use the FortiManager monitors menu to get a graphical view that shows the status of each SD-WAN member.
Which statement best explains how to obtain this graphical view?

A. Use the SD-WAN monitor template view to get a map view of the branches, hub, and tunnel status, including the SLA pass or missed status.
B. Use the SD-WAN monitor table view to get a donut view and a table view that shows the status of each SD-WAN member, including the SLA pass or missed status.
C. Use the VPN monitor map view to get a map view of the branches, hub, and tunnel status, including the SLA pass or missed status.
D. Use the SD-WAN monitor asset view to get a donut view and a table view that shows the status of each device and the SLA status of each SD-WAN member.

**Answer:** B

**NEW QUESTION 3**
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 4**
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 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**
(You are configuring SD-WAN to load balance network traffic and you want to take into account the link quality.
Which two facts should you consider? Choose two answers.)

A. When applicable, FortiGate load balances the traffic through all members that meet the SLA target.
B. You can select the best quality strategy and allow SD-WAN load balancing.
C. You can select the lowest cost service level agreement (SLA) strategy and allow SD- WAN load balancing.
D. The best quality strategy supports only the round-robin hash mode.

**Answer:** AC

**NEW QUESTION 8**
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_fgt generates 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:** CD

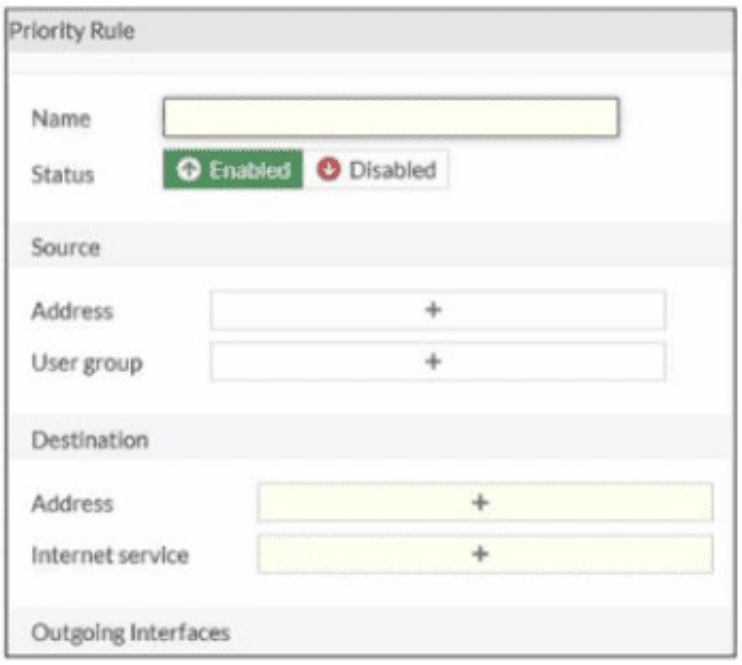
**NEW QUESTION 9**
As an IT manager for a healthcare company, you want to delegate the installation and management of your SD-WAN deployment to a managed security service provider (MSSP). Each site must maintain direct internet access and ensure that it is secure. You expected significant traffic flow 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 best address the customer??s requirements? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 10**
Refer to the exhibit.




An administrator configures SD-WAN rules for a DIA setup using the FortiGate GUI. The page to configure the source and destination part of the rule looks as shown in the exhibit. The GUI page shows no option to configure an application as the destination of the SD- WAN rule Why?

A. You cannot use applications as the destination when FortiGate is used for a DIA setup.
B. FortiGate allows the configuration of applications as the destination of SD-WAN rules only on the CLI.
C. You must enable the feature on the CLI.
D. You must enable the feature first using the GUI menu System > Feature Visibility.

**Answer:** D

**NEW QUESTION 10**
(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 12**
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 15**
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 19**
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 21**
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 22**
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 26**
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 port1 or port2.
D. SD-WAN service rule 4 and interface port2.

**Answer:** D

**NEW QUESTION 31**
(In the context of SD-WAN, the terms underlay and overlay are commonly used to categorize links.
Which two statements about underlay and overlay links are correct? Choose two answers.)

A. A VLAN is a type of overlay link.
B. Overlay links provide routing flexibility.
C. FortiLink interface is considered an underlay link.
D. Wireless connections can be used to build overlay links.
E. Only wired connections can be used as underlay links.

**Answer:** BD

**NEW QUESTION 32**
(When you deploy SD-WAN, you can choose from several common designs. Each design best applies to specific contexts.
Which two statements correctly associate a common SD-WAN design with its main indication or constraint? Choose two answers.)

A. Use a cloud on-ramp topology to improve the performance of cloud applications.
B. Use a standalone design for sites with only one WAN link to the cloud.
C. Use remote breakout to centralize traffic inspection and limit local management requirements.
D. Use a direct internet access (DIA) design to increase the traffic security and allow local devices with limited capabilities.

**Answer:** AC

**NEW QUESTION 33**
Refer to the exhibit.

## Diagnose output

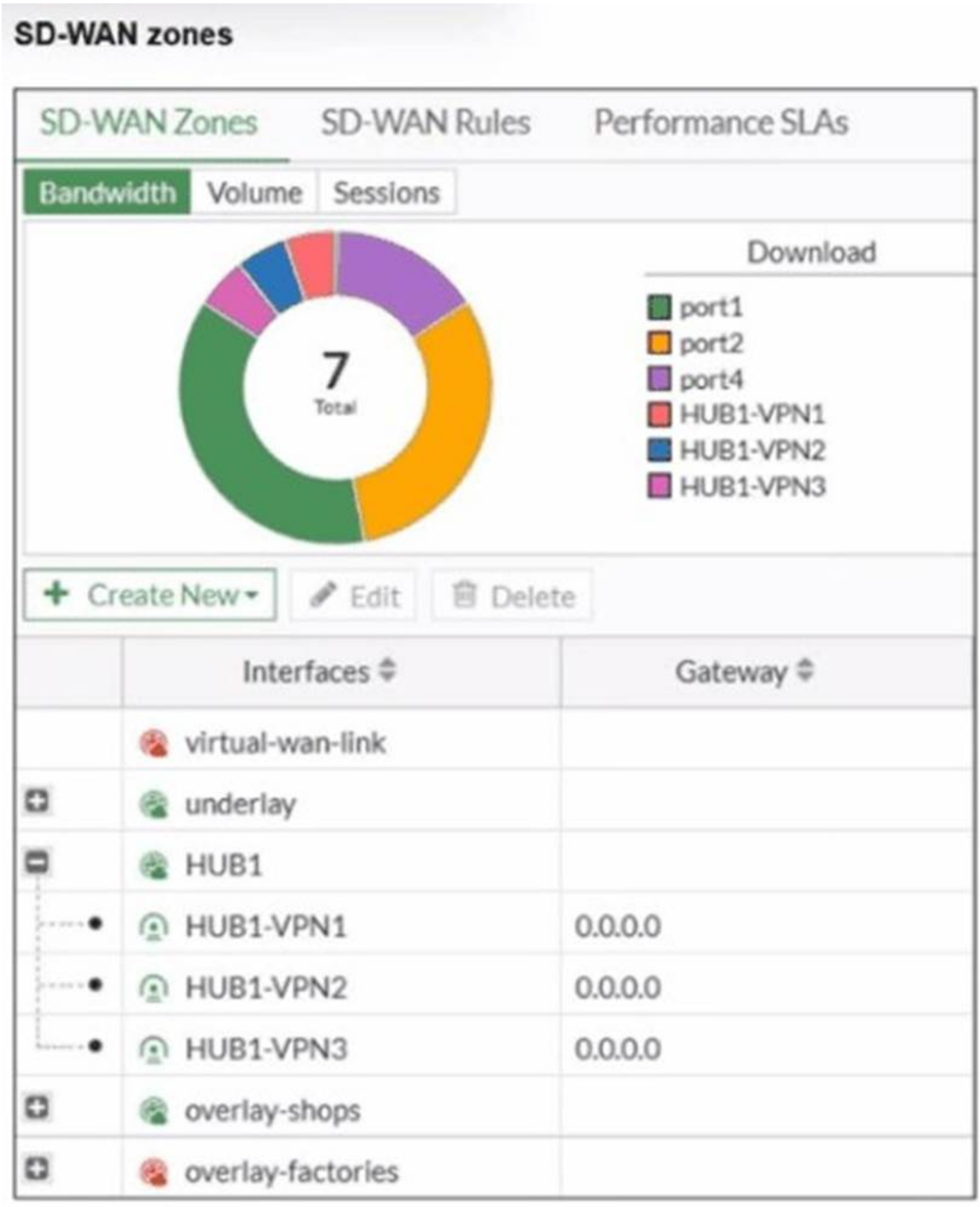
```
fgt_1 # diagnose  sys sdwan service4

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**
Exhibit.




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.

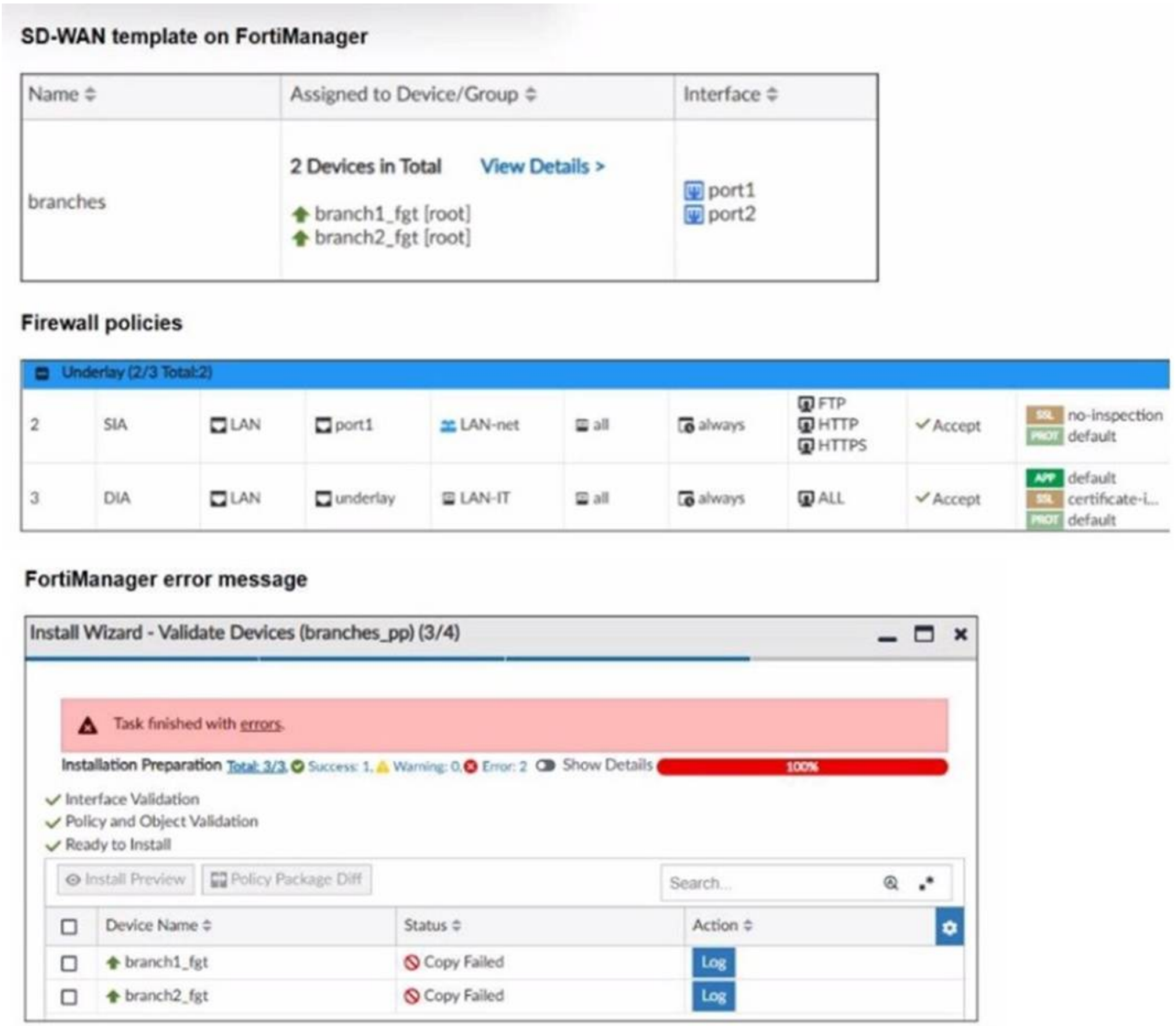
**Answer:** C

**NEW QUESTION 38**
(Which two features must you configure before FortiGate can steer traffic according to SD- WAN rules? Choose two answers.)

A. Security profiles
B. Underlay links
C. Overlay links
D. Traffic shaping
E. Firewall policies

**Answer:** BE

**NEW QUESTION 40**
Refer to the exhibits.




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

A. You must direct SIA traffic to a VPN tunnel.

B. You cannot install firewall policies that reference an SD-WAN zone.
C. You cannot install firewall policies that reference an SD-WAN member.
D. You cannot install SIA and DIA rules on the same device.

**Answer:** C

**NEW QUESTION 41**
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 46**
(Refer to the exhibits.

Extract from Branch-A configuration

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "overlay"
            set advpn-select enable
            set advpn-health-check "HUB1_HC"
        next
    end
    config members
        edit 1
            set interface "T1"
            set zone "overlay"
            set source 10.200.99.1
            set transport-group 1
        next
        edit 2
            set interface "T2"
            set zone "overlay"
            set source 10.200.99.1
            set transport-group 1
        next
        edit 3
            set interface "T3"
            set zone "overlay"
            set source 10.200.99.1
            set transport-group 2
        next
    end
```

Extract from Branch-B configuration

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "overlay"
            set advpn-select enable
            set advpn-health-check "HUB1_HC"
        next
    end
    config members
        edit 1
            set interface "TA"
            set zone "overlay"
            set source 10.200.99.1
            set transport-group 1
        next
        edit 2
            set interface "TB"
            set zone "overlay"
            set source 10.200.99.1
            set transport-group 2
        next
        edit 3
            set interface "TC"
            set zone "overlay"
            set source 10.200.99.1
            set transport-group 3
        next
    end
```

The SD-WAN zones and members configuration of two branch devices are shown. The two branch devices are part of the same hub-and-spoke topology and connect to the same hub. The devices are configured to allow Auto-Discovery VPN (ADVPN). The configuration on the hub allows the initial communication between the two spokes.
When traffic flows require it, between which interfaces can the devices establish shortcuts? Choose one answer.)

A. Any interface in the overlay zones
B. Interface connected to HUB only
C. Between T3 on Branch-A and TC on Branch-B
D. Between T2 on Branch-A and TA on Branch-B

**Answer:** D

**NEW QUESTION 47**
Refer to the exhibit.

**BGP configuration**

```
config router bgp
     set as 65000
     set router-id 10.200.99.253
     set ibgp-multipath enable
     set additional-path enable
     set additional-path-select 3
     config neighbor-group
          edit "VPN1"
               set soft-reconfiguration enable
               set remote-as 65000
          next
          edit "VPN2"
               set soft-reconfiguration enable
               set remote-as 65000
          next
          edit "VPN3"
               set soft-reconfiguration enable
               set remote-as 65000
          next
end
config neighbor-range
     edit 1
          set prefix 192.168.1.0 255.255.255.192
          set neighbor-group "VPN1"
     next
     edit 2
          set prefix 192.168.1.64 255.255.255.192
          set neighbor-group "VPN2"
          next
          edit 3
               set prefix 192.168.1.128 255.255.255.192
               set neighbor-group "VPN3"
          next

     end
     ...
end
```

The exhibit shows the BGP configuration on the hub in a hub-and-spoke topology. The administrator wants BGP to advertise prefixes from spokes to other spokes over the IPsec overlays, including additional paths. However, when looking at the spoke routing table, the administrator does not see the prefixes from other spokes and the additional paths

Which three settings must the administrator configure inside each BGP neighbor group so spokes can learn the prefixes of other spokes and their additional paths? (Choose three.)

A. Set additional-path to send
B. Set additional-path to forward
C. Enable route-reflector-server
D. Enable route-reflector-client.
E. Set adv-additional-path to the number of additional paths to advertise.

**Answer:** ADE

**NEW QUESTION 49**
(Refer to the exhibit. You noticed that one SD-WAN member went down and you immediately collected the session output shown in the exhibit. What can you conclude from this output? Choose one answer.)

```
# diagnose sys session list
session info: proto=6 proto_st=11 duration=90 expire=3511 timeout=3600
refresh dir=both flags=
socktype=0 av
origin-shaper=
class_id=0 ha_i=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may dirty nn-f00 app_valid route_preserve
statisti(bytes/packets/allow_err):org=1995/8/1 reply=1945/7/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=7~3/3->7_0 92.2.0.2/0.0.0
hook=post dir=org act=snat 10.0.1.101:54632->128.66.0.1:22(192.2.0.100:o
hook>pre dir=reply act=dnat 128.66.0.1:22->192.2.0.100:58630(10.0.1.101
(pos/(before, after)/(0,0,0), (0.0.0))
misc=o policy_id=1 pol_uuid_idx=16335 ath_info=0 chk_client_info=0 vd=0
serial=000000c29 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service id=4
rpdb_link_id=f0000004
no_offload_reason: redir-to-ips denied-by-nturbo
total session=1
```

A. FortiGate didn??t receive any traffic related to this session after the interface went down.
B. FortiGate flushed the gateway for the session.
C. FortiGate cannot reevaluate the session.
D. FortiGate already reevaluated this session.

**Answer:** D

**NEW QUESTION 50**
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<br>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<br>Microsoft | | port1<br>port2 | | | any | Enable |
| ☐ | 3 | Corp | LAN-r | Corp-net | | HUB1-VPN1<br>HUB1-VPN2<br>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 51**
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<br>HUB1-VPN2<br>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<br>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 56**
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_1ist=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 61**
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 64**
(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 68**
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?

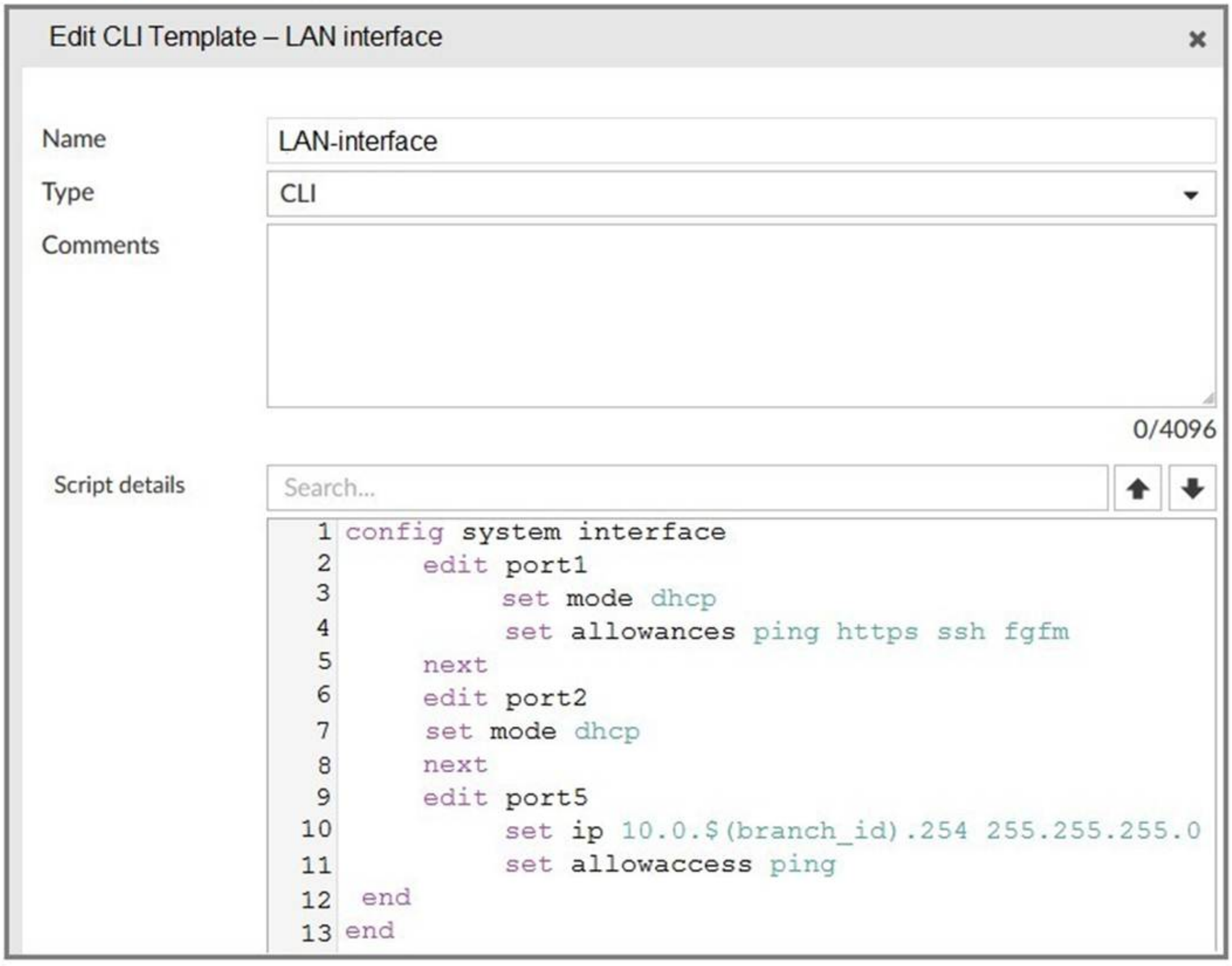
A. You identify sessions steered according to SD-WAN rules with the flag vwl.
B. You cannot identify SD-WAN session
C. You must use the sdwa
D. session filter.
E. You identify sessions steered according to SD-WAN rules with the data vwl_mbr_seq.
F. You identify sessions steered according to SD-WAN rules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

**Answer:** D

**NEW QUESTION 70**
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 72**
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 77**
Refer to the exhibit.

**FortiGate policy route**

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

id=1(0x01) dscp_tag=0xfc flags=0x0 tos=0x0 tos_mask=0x00 protocol=0 port=src(0->0): dst(0->0)
iif=7(port5)
path(1): oif=5(port3) gwy=10.0.1.255
source wildcard(1) : 10.0.1.128/255.255.255.128
destination wildcard(1): 0.0.0.0/0.0.0.0
hit_count=0 rule_last_used=2024-12-13 01:40:44

id=2131427329(0x7f0b0001) vwl_service=1(Critical-DIA), vwl_mbr_seq=2 1 dscp_tag=0xfc 0xfc flags=
0x0 tos=0x0
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(2): oif=4(port2), oif=3(port1)
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) SMTP_Signed.Email(28991,0)
hit_count=732 rule_last_used=2024-12-12 12:30:16

id=2131427329(0x7f070003) vwl_service=3(Corp), vwl_mbr_seq=4 5 6 dscp_tag=0xfc 0xfc flags=0x0
tos=0x0 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(3): oif=20(HUB1-VPN1), oif=21(HUB1-VPN2), oif=22(HUB1-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=2024-12-12 02:29:25

id=2131165188(0x7f070004) vwl_service=4(LAN-to-Corp2), vwl_mbr_seq=1 2 dscp_tag=0xfc 0xfc flags=
0x10 load-balance hash-mode=round-robin tos=0x0 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->
0) iif=0(any)
path(2): oif=3(port1) num_pass=1, oif=4(port2) num_pass=1
source(1) : 10.0.1.0-10.0.1.255
destination (1): 10.66.0.0-10.66.0.255
hit_count=0 rule_last_used=2024-12-13 01:43:31
```

What conclusions can you draw about the traffic received by FortiGate originating from the source LAN device 10.0.1.133 and destined for the company??s SMTP mail server at 10.66.0.125?

A. FortiGate steers the traffic from the LAN device 10.0.1.133 to the company SMTP mail server 10.66 0.125 through port3.
B. ForliGate steers the traffic from the LAN device 10.0.1.133 to the company SMTP mail server 10.66.0.125 through port2.
C. FortiGate steers the traffic from the LAN device 10.0.1.133 to the company SMTP mail server 10.66.0.125 through the SD-WAN member ID 4.
D. FortiGate steers the traffic from the LAN device 10.0.1.133 to the SMTP mail server 10.66.0.125 through the SD-WAN member ID 1 or 2.

**Answer:** D

**NEW QUESTION 79**
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<br>all | all<br>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 82**
Refer to the exhibit.

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

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

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

**Answer:** C

**NEW QUESTION 84**
.....

# 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