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 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 4
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 5
Refer to the exhibits.

SD-WAN service details

```
branch1_fgt # diagnose sys sdwan service4

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

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

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

Max_App_Ctrl_Size=32768 Num_App_Ctrl_Entry=6

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

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

n FortiAnalyzer

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

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

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

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

Answer: BD

NEW QUESTION 6
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 7
SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic.
Which three configuration elements that you must configure before FortiGate can steer traffic according to SD-WAN rules? (Choose three.)

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

Answer: ABE

NEW QUESTION 8
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 9
Refer to the exhibits.

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

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

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

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

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

Firewall policy configuration

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

Underlay zone status

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

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

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

Answer: BD

NEW QUESTION 10
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 10
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 11
(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.

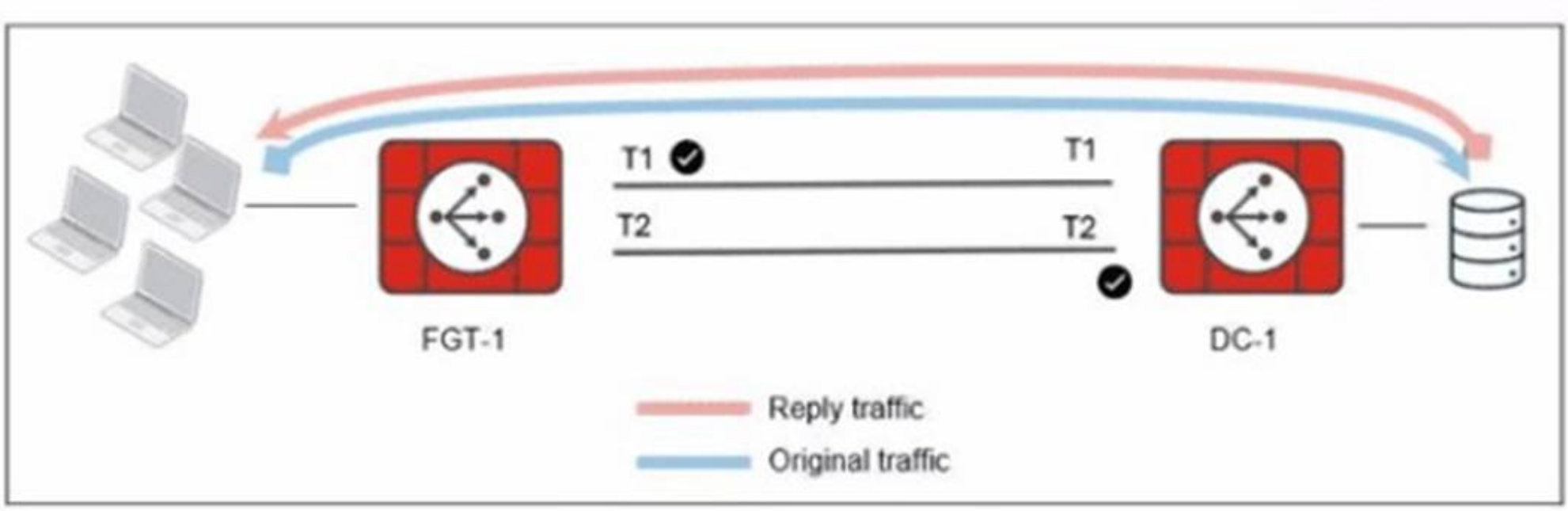
Answer: AC

NEW QUESTION 16
(You want FortiGate to use SD-WAN rules to steer ping local-out traffic. Which two constraints should you consider? Choose two answers.)

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

Answer: AC

NEW QUESTION 19
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 20
(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 23
(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 26
(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 correctly describes the role of the ADVPN device in handling traffic? Choose one answer.)

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

Answer: C

NEW QUESTION 27
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 32
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 36
The administrator uses the FortiManager SD-WAN overlay template to prepare an SD-WAN deployment. Using information provided through the SD-WAN overlay template wizard, FortiManager creates templates ready to install on the spoke and hub devices.
What are the three templates created by the SD-WAN overlay template for a spoke device? (Choose three.)

A. Static route template
B. Rules template
C. CLI template
D. BGP template
E. IPsec tunnel template

Answer: BDE

NEW QUESTION 37
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 41
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 44
(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 45
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 View Details > branch1_fgt[root] branch2_fgt[root] branch3_fgt[root]
6	HUB1-VPN3	0.0.0.0	0	1	Enable	2 Devices in Total View Details > branch2_fgt[root] branch3_fgt[root]

SD-WAN zone HUB2 and SD-WAN member configuration

☐	HUB2						
☐	7	HUB2-VPN1	0.0.0.0	10	1	Enable	3 Devices in Total View Details > branch1_fgt[root] branch2_fgt[root] branch3_fgt[root]
☐	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 49
Refer to the exhibits.

Interface details

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

Static route details

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

Firewall policies on managed FortiGate

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

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

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

Answer: B

NEW QUESTION 50
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

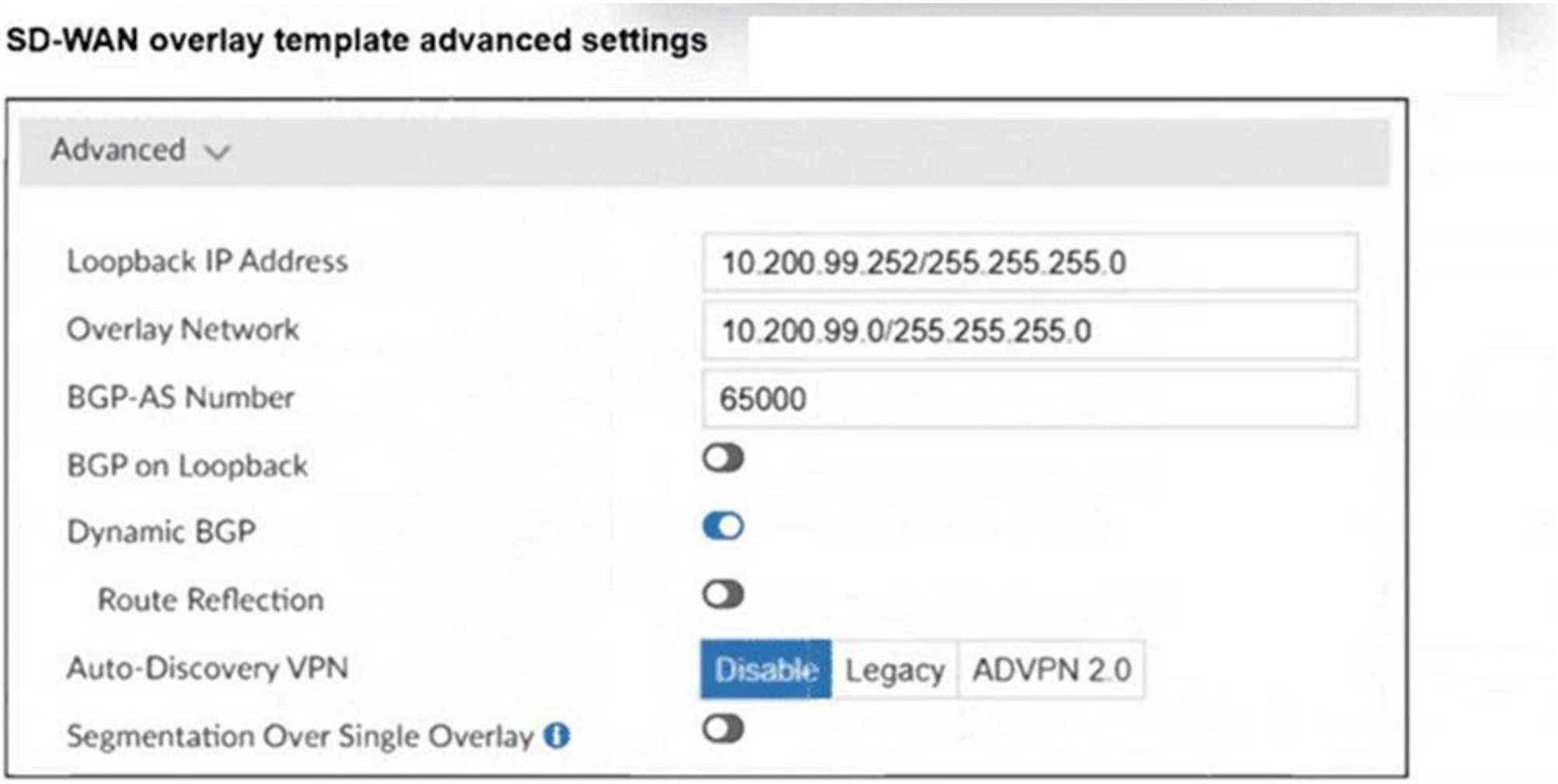
```
branch1_fgt # diagnose sys sdwan service4 3

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 51
(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 55
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 59
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 60
(Refer to the exhibits.

SD-WAN service configuration

```
branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set load-balance enable
        set mode sla
        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 # diag firewall proute list
list route policy info(vf=root):

id=2131034113(0x7f050001) 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=2131034114(0x7f050002) 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=2131034115(0x7f050003) vwl_service=3(Corp) vwl_mbr_seq=5 4 3 dscp_tag=0xfc 0xfc flags=0x10
load-balance hash-mode=round-robin tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(3): oif=21(HUB1-VPN3) num_pass=0, oif=20(HUB1-VPN2) num_pass=0, oif=19(HUB1-VPN1) num_pass=0
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=660 rule_last_used=2025-06-19 04:33:21
```

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 04:34:49.626332 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo request
2025-06-19 04:34:49.626391 HUB1-VPN3 out 10.0.1.101 -> 10.0.2.101: icmp: echo request
2025-06-19 04:34:49.883401 HUB1-VPN3 in 10.0.2.101 -> 10.0.1.101: icmp: echo reply
2025-06-19 04:34:49.883430 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo reply
```

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
```

You collected the output shown in the exhibits and want to know which interface HTTP traffic will flow through from the user device 10.0.1.101 to the corporate web server 10.0.0.126. All SD-WAN links are stable.
Which interface will FortiGate use to steer the traffic? Choose one answer.)

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

Answer: D

NEW QUESTION 62
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

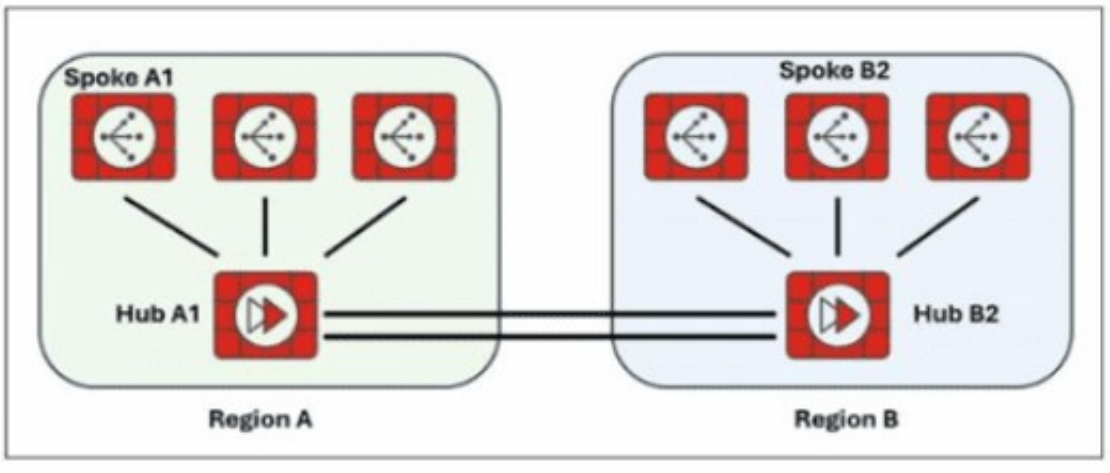
NEW QUESTION 63
When you use the command diagnose sys session list, how do you identify the sessions that correspond to traffic steered according to SD-WAN rules?

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 68

Exhibit.



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

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

Answer: AD

NEW QUESTION 70
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 74
What are three key routing principles of SD-WAN? (Choose three.)

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

Answer: BDE

NEW QUESTION 79
(As an IT manager, you want to delegate the installation and management of your SD- WAN deployment to a managed security service provider (MSSP). Each site must maintain direct internet access and be secure. You expect significant traffic flow between the sites and want to delegate as much of the network administration and management as possible to the MSSP.
Which two MSSP deployment blueprints address your requirements? Choose two answers.)

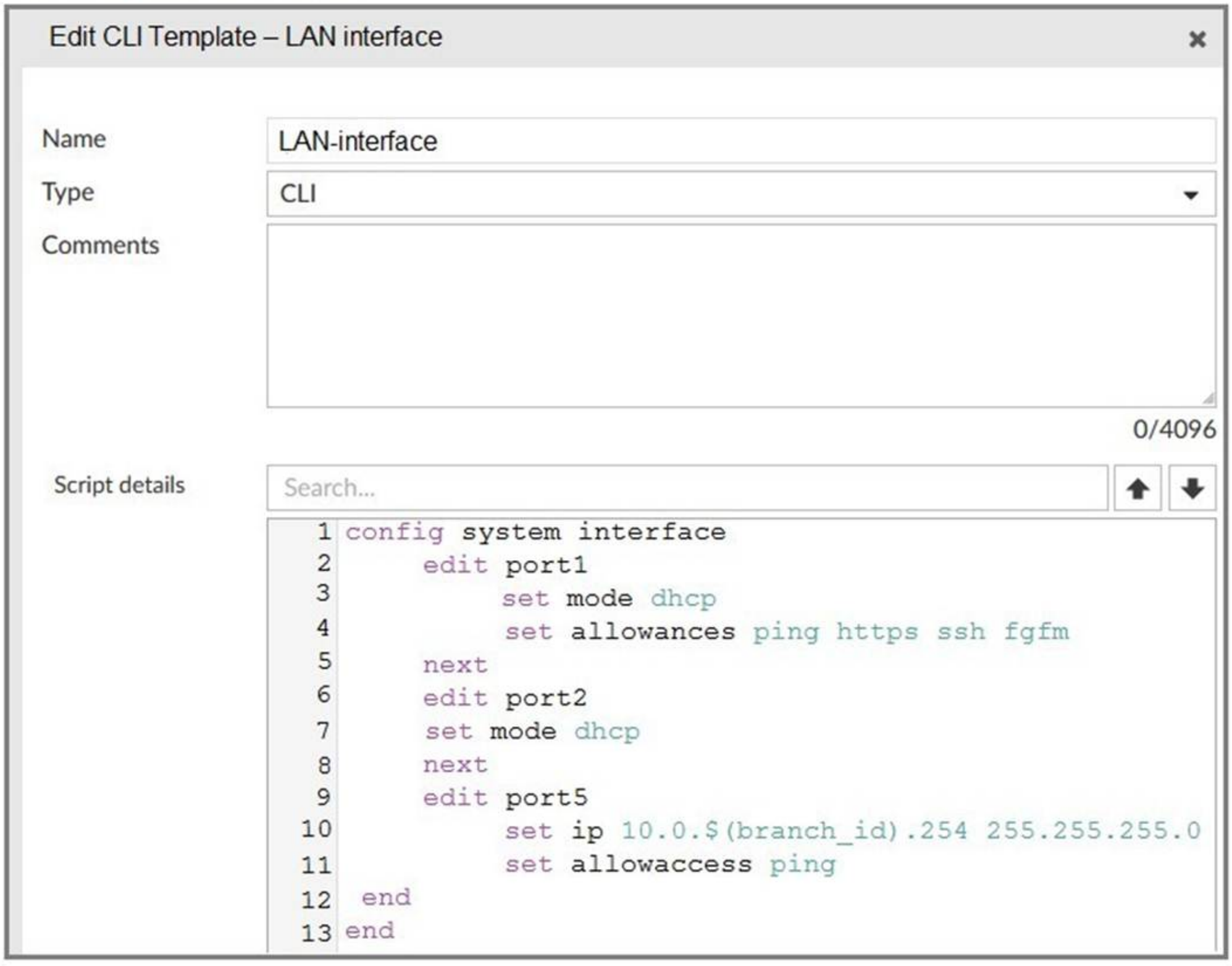
A. Use a shared hub on the MSSP premises and a dedicated hub on the customer premises, and install the spokes on the customer premises.
B. Install a dedicated hub on the MSSP premises for the customer, and install the spokes on the customer premises.
C. Install the hub and spokes on the customer premises,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

Answer: BD

NEW QUESTION 82
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.

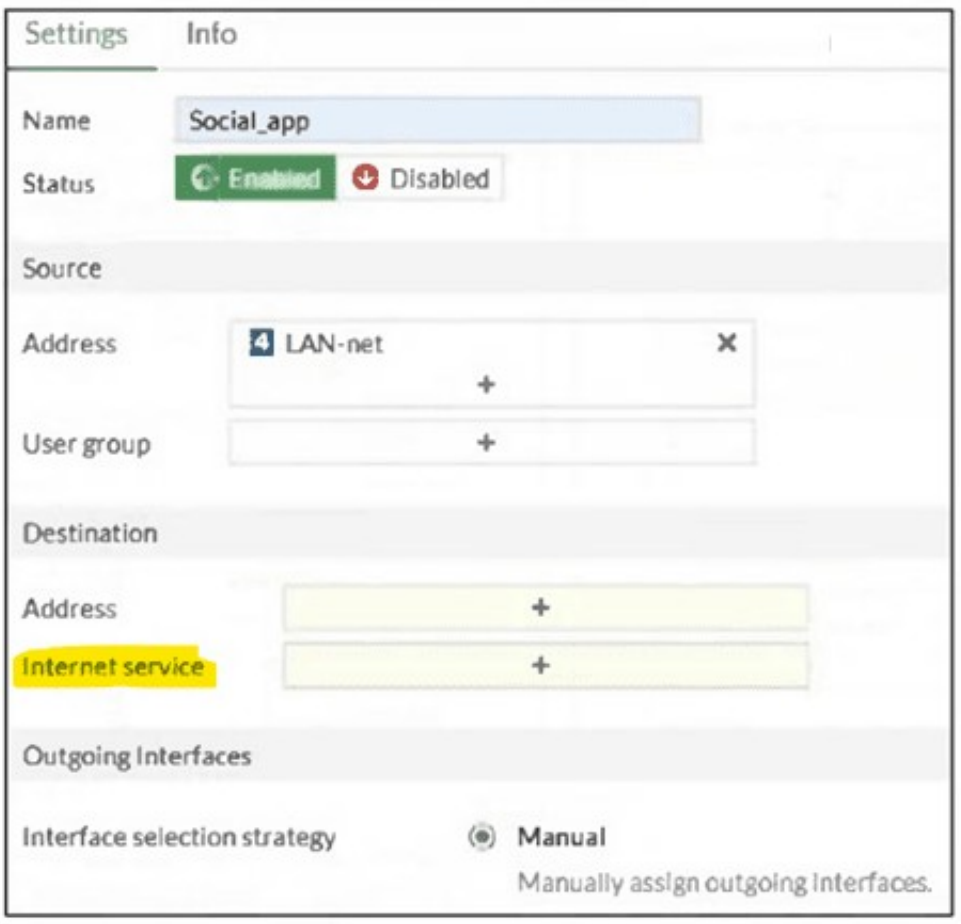
Answer: D

NEW QUESTION 84
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 86
(Refer to the exhibit.



You configure SD-WAN on a standalone FortiGate device.
You want to create an SD-WAN rule that steers traffic related to Facebook and LinkedIn through the less costly internet link.
What must you do to set Facebook and LinkedIn applications as destinations from the GUI? Choose one answer.)

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

Answer: B

NEW QUESTION 89
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
```

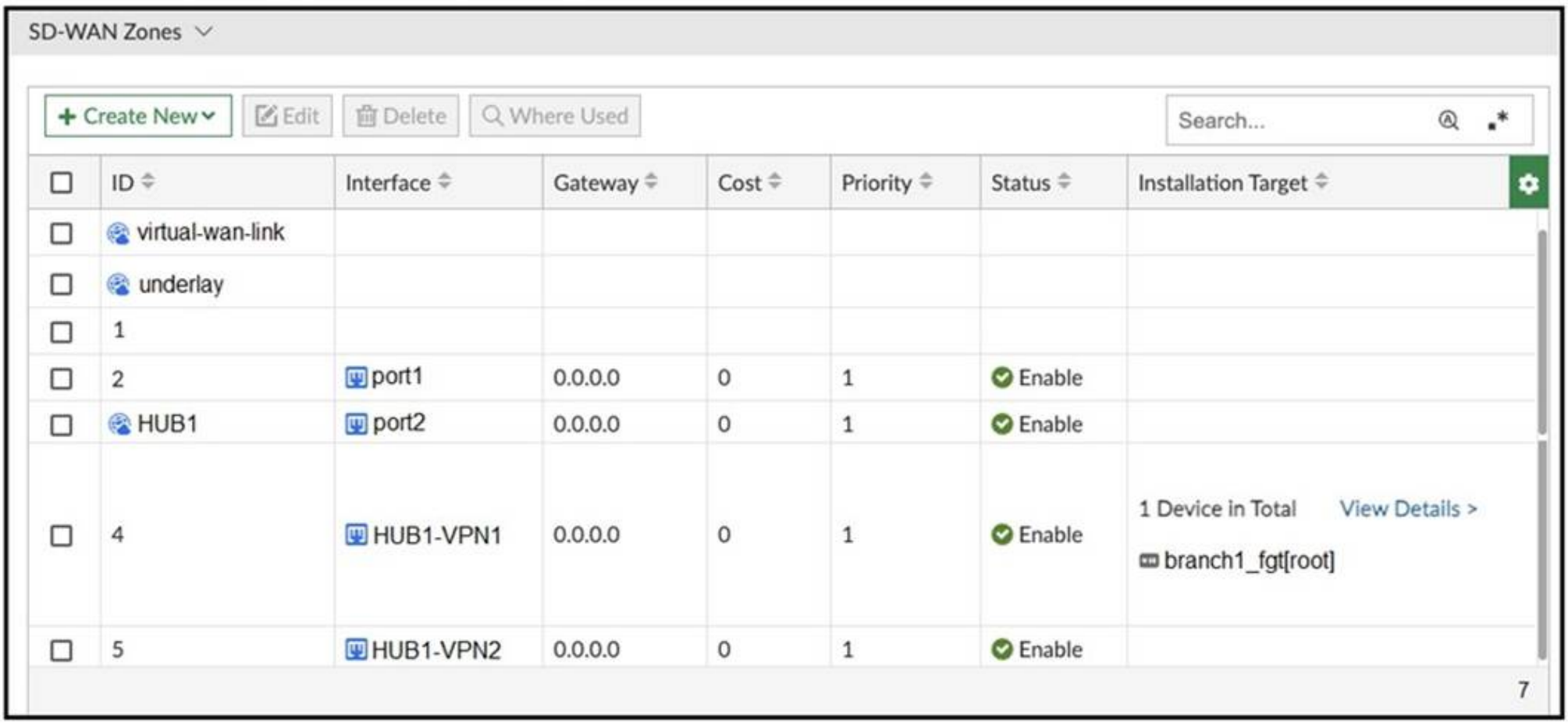
What conclusions can you draw about the traffic received by FortiGate originating from the source LAN device 10.0.1.133 and destined for the company??s SMTP mail server at 10.66.0.125?

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 92
Refer to the exhibits.

SD-WAN zone configuration on FortiManager



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 94
You have configured the performance SLA with the probe mode as Prefer Passive. What are two observable impacts of this configuration? (Choose two.)

A. FortiGate passively monitors the member if TCP traffic is passing through the member.
B. After FortiGate switches to active mode, the SLA performance rule falls back to passive monitoring after 3 minutes.
C. FortiGate passively monitors the member if ICMP traffic is passing through the member.
D. During passive monitoring, the SLA performance rule cannot detect dead members.
E. FortiGate can offload the traffic that is subject to passive monitoring to hardware.

Answer: AD

NEW QUESTION 97
.....

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