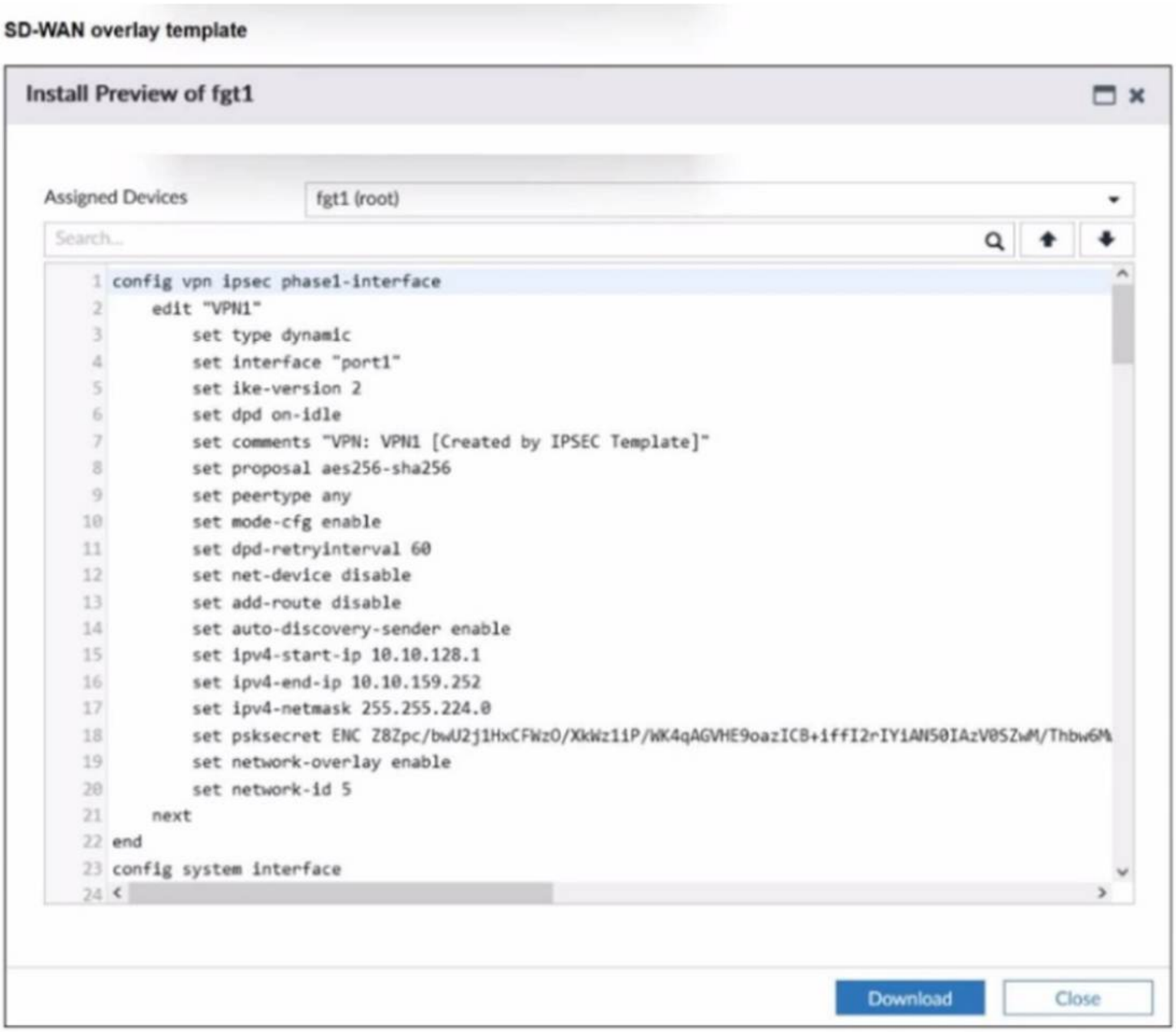
Fortinet

Exam Questions FCSS_SDW_AR-7.6

FCSS - SD-WAN 7.6 Architect

NEW QUESTION 1
Refer to the exhibit.



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

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

Answer: B

NEW QUESTION 2
Refer to the exhibit that shows event logs on FortiGate.

Event log on FortiGate

```
6: date=2024-12-18 time=15:15:06 eventtime=1734563705745090691 tz="-0800" logid="0113022925" type="event" subtype="sdwan" leve
l="information" vd="root" logdesc="SDWAN SLA information" eventtype="SLA" healthcheck="HUB1_HC" slatargetid=1 interface="HUB1-
VPN3" status="up" latency="1.001" jitter="0.162" packetloss="0.000" moscodec="g711" mosvalue="4.404" inbandwidthavailable="10.
00Gbps" outbandwidthavailable="10.00Gbps" bibandwidthavailable="20.00Gbps" inbandwidthused="0kbps" outbandwidthused="0kbps" bi
bandwidthused="0kbps" slamap="0x1" msg="Health Check SLA status."

7: date=2024-12-18 time=15:14:26 eventtime=1734563666333265394 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=120.64.1.1 loci
p=192.2.0.1 remport=500 locport=500 outintf="port1" srccountry="Reserved" cookies="50b8a3684ddfd2cb/af3f725d883c5585" user="10
0.64.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=172.168.1.1 vpntunnel="VPN4_0" tunnelip=N/A t
unnelid=3050027470 tunneltype="ipsec" duration=2968 sentbyte=245849 rcvdbyte=246456 nextstat=600 fctuid="N/A" advpnsc=0

8: date=2024-12-18 time=15:04:26 eventtime=1734563066334261977 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.33.1 loc
ip=192.2.0.1 remport=4500 locport=4500 outintf="port1" srccountry="Reserved" cookies="cff150ded109a548/165f413d17cecc49" user=
"Branch3" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="HUB1-VPN1_0" tunnelip=192.168.1.4
 tunnelid=3050027486 tunneltype="ipsec" duration=1122 sentbyte=92064 rcvdbyte=0 nextstat=600 fctuid="N/A" advpnsc=1

9: date=2024-12-18 time=15:04:26 eventtime=1734563066334252138 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.1.1 loci
p=172.16.0.1 remport=500 locport=500 outintf="port4" srccountry="Reserved" cookies="ce1c2c62ecc04871/a4d93a059b8df005" user="1
72.16.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=192.168.1.193 vpntunnel="HUB2-VPN3" tunnelip=N/
A tunnelid=3050027467 tunneltype="ipsec" duration=2367 sentbyte=195836 rcvdbyte=196492 nextstat=600 fctuid="N/A" advpnsc=0
```

Based on the output shown in the exhibit, what can you say about the tunnels on this device?

A. The master tunnel HU82-VPN3 cannot accept ADVPN shortcuts.
B. The device steers voice traffic through the VPN tunnel HUB1-VPN3.
C. The VPN tunnel HUB1-VPN1_0 is a shortcut tunnel.
D. There is one shortcut tunnel built from master tunnel VPN4.

Answer: C

NEW QUESTION 3
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 4
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

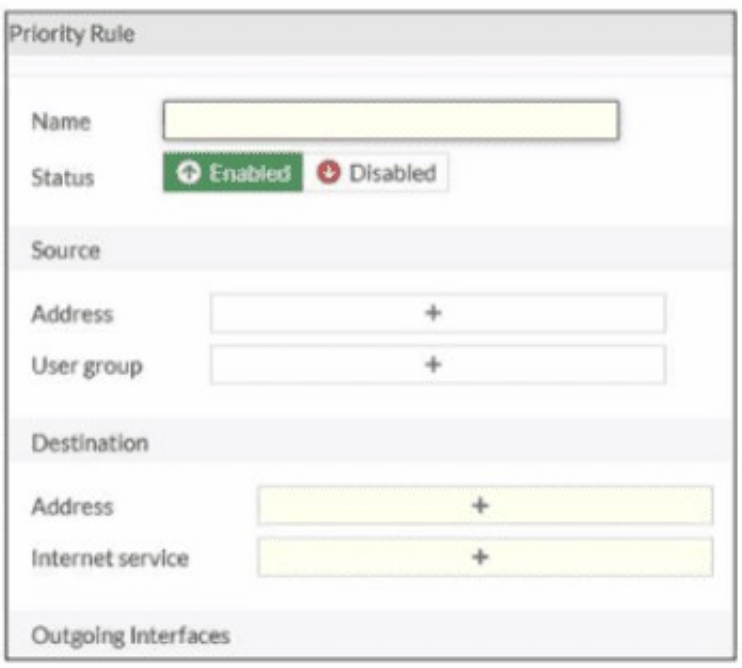
Answer: ABE

NEW QUESTION 5
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 6
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 7
(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 8
Your FortiGate is in production. To optimize WAN link use and improve redundancy, you enable and configure SD-WAN.
What must you do as part of this configuration update process?

A. Replace references to interfaces used as SD-WAN members in the routing configuration.
B. Purchase and install the SD-WAN license, and reboot the FortiGate device.
C. Replace references to interfaces used as SD-WAN members in the firewall policies.
D. Disable the interface that you want to use as an SD-WAN member.

Answer: C

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

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

Answer: A

NEW QUESTION 10
(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 15

(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 19
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 20
Exhibit.

```
config system sdwan
    set fail-detect enable
    set fail-alert-interfaces "port5"
    config health-check
        edit "Level3_DNS"
            set update-cascade-interface enable
            set members 1 2
        next
        edit "HQ"
            set update-cascade-interface enable
            set members 3
        next
    end
end
```

Which action will FortiGate take if it detects SD-WAN members as dead?

A. FoftiGate bounces port5 after it detects all SD-WAN members as dead.
B. FortiGate fails over to the secondary device after it detects port5 as dead.
C. FortiGate sends alert messages through poft5 when it detects all SD-WAN members as dead
D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

Answer: C

NEW QUESTION 23
(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 24
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 27
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 28
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 30
(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 31
(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 34
(Refer to the exhibits. You collected the output shown in the exhibits and want to know which interface TCP traffic will flow through from the user device 10.0.1.101 to the corporate file server 10.0.0.125. All SD-WAN links are stable.

SD-WAN rule configuration

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

Proute list

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

id=2130968577(0x7f040001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xfc 0xfc flags=0x0
tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(2): oif=3(port1), oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(2): Salesforce(16920,0) Microsoft.Portal(41469,0)
hit_count=0 rule_last_used=2025-06-19 03:14:42

id=2130968578(0x7f040002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xfc 0xfc flags=0x0
tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
hit_count=0 rule_last_used=2025-06-19 03:14:42

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

Sniffer trace

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

Routing table

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

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

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

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

Answer: B

NEW QUESTION 37
Exhibit.

Serial Number	name	branch_id	admin_gw	sdwan_port1_gw	sdwan_port2_gw	lan_interface_ip	latitude	longitude
FGVM01TM22000077	branch1_fgt	1	172.16.0.2	192.2.0.2	192.2.0.10	10.0.1.254	37.37610911	-122.0260914
FGVM01TM22000078	branch2_fgt	2	172.16.0.10	203.0.11.2	203.0.113.10	10.0.2.254	25.77404351	-80.20508525
FGT40FTK20000624	shop1_fgt	11		198.0.1.1		10.10.1.254		
FGT40FTK20003026	shop2_fgt	12				10.10.2.254	48.88941	2.25125
FGVM02TM24010735		3	172.16.0.10	100.64.33.2	100.64.33.10	10.0.3.254	45.32482	-75.8359

For your ZTP deployment, you review the CSV file shown in exhibit and note that it is missing important information. Which two elements must you change before you can import it into FortiManager? (Choose two.)

A. You must associate a device blueprint with each device
B. You must define a name for each device
C. You must define a value for each device and each metadata variable that defines an IP address.
D. You must define a value for each device and each user-defined metadata variable.

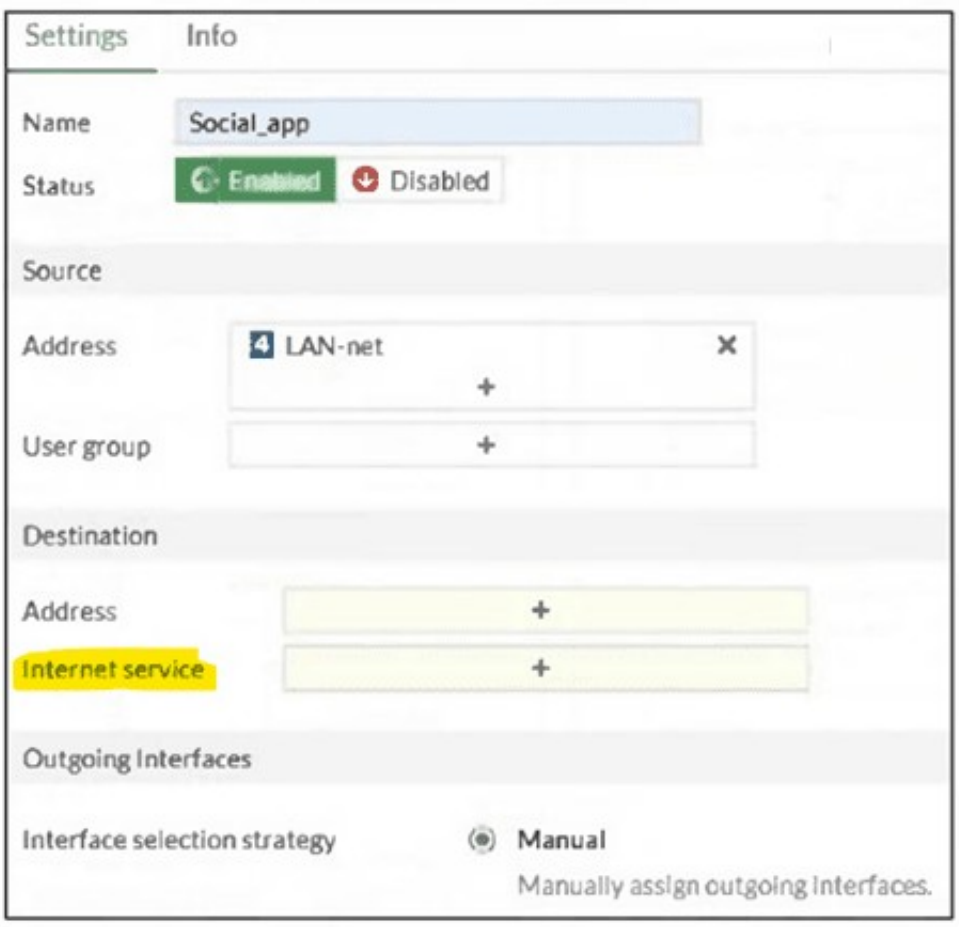
Answer: AB

NEW QUESTION 38
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 39
(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 40
As an MSSP administrator, you are asked to configure ADVPN on an existing SD-WAN topology. FortiManager manages the customer devices in a dedicated ADOM. The previous administrator used the SD-WAN overlay topology.
Which two statements apply to this scenario? (Choose two.)

A. You can activate auto-discovery VPN in the SD-WAN overlay template only if it is a single hub topology.
B. When auto-discovery VPN is enabled, FortiManager updates the IPsec and BGP templates in the hub.
C. After you enable auto-discovery VPN in the overlay template, you must select between ADVPN 2.0 and ADVPN 1.0.
D. You can activate auto-discovery VPN in the SD-WAN overlay template for any type of topology, including a primary-primary dual-hub topology.

Answer: BD

NEW QUESTION 43
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 47
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 51
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The FCSS_SDW_AR-7.6 Practice Test Here