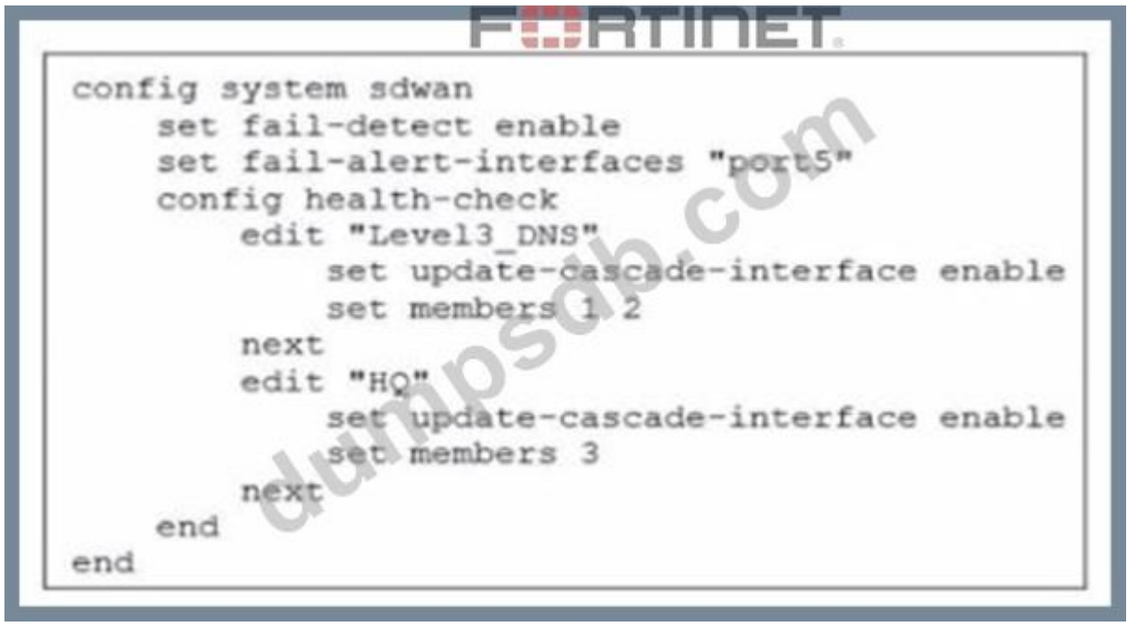
Fortinet.FCSS_SDW_AR-7.4.v2026-03-03.q77

Exam Code:	FCSS_SDW_AR-7.4
Exam Name:	FCSS - SD-WAN 7.4 Architect
Certification Provider:	Fortinet
Free Question Number:	77
Version:	v2026-03-03
# of views:	129
# of Questions views:	770
https://www.dumpsdb.com/dumps/Fortinet/FCSS_SDW_AR-7.4/Fortinet.FCSS_SDW_AR-7.4.v2026-03-03.q77	

NEW QUESTION: 1
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 accepts the deletion and places the member in the default SD-WAN zone.
C. FortiGate displays an error message. SD-WAN zones must contain at least two members
D. FortiGate displays an error message. You must use the CLI to delete an SD-WAN member.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Exhibit.



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 brings down port5 after it detects all SD-WAN members as dead.

D. FortiGate sends alert messages through poft5 when it detects all SD-WAN members as dead

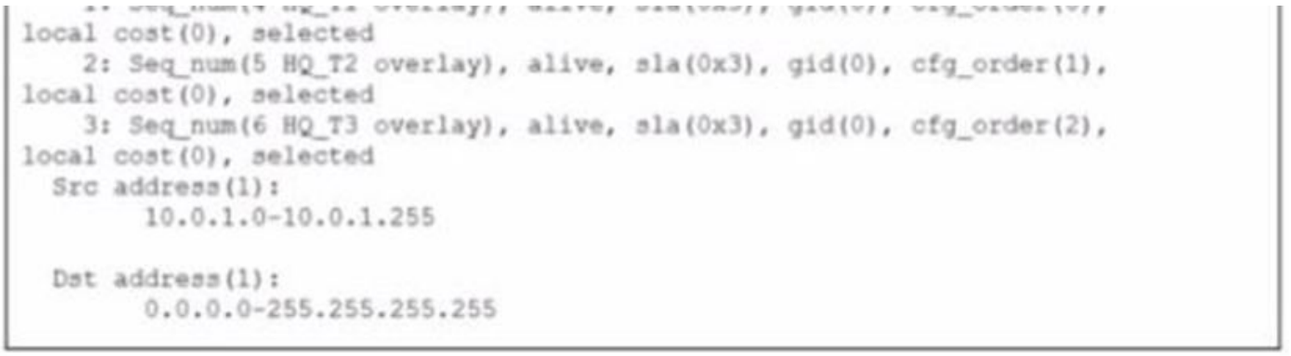
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3

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),
```



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. FortiGate steers traffic for social media applications according to the service rule 2 and steers traffic through port2.

B. When FortiGate cannot recognize the application of the flow, it load balances the traffic through the tunnels HQ_T1. HQ_T2. HQ_T3.

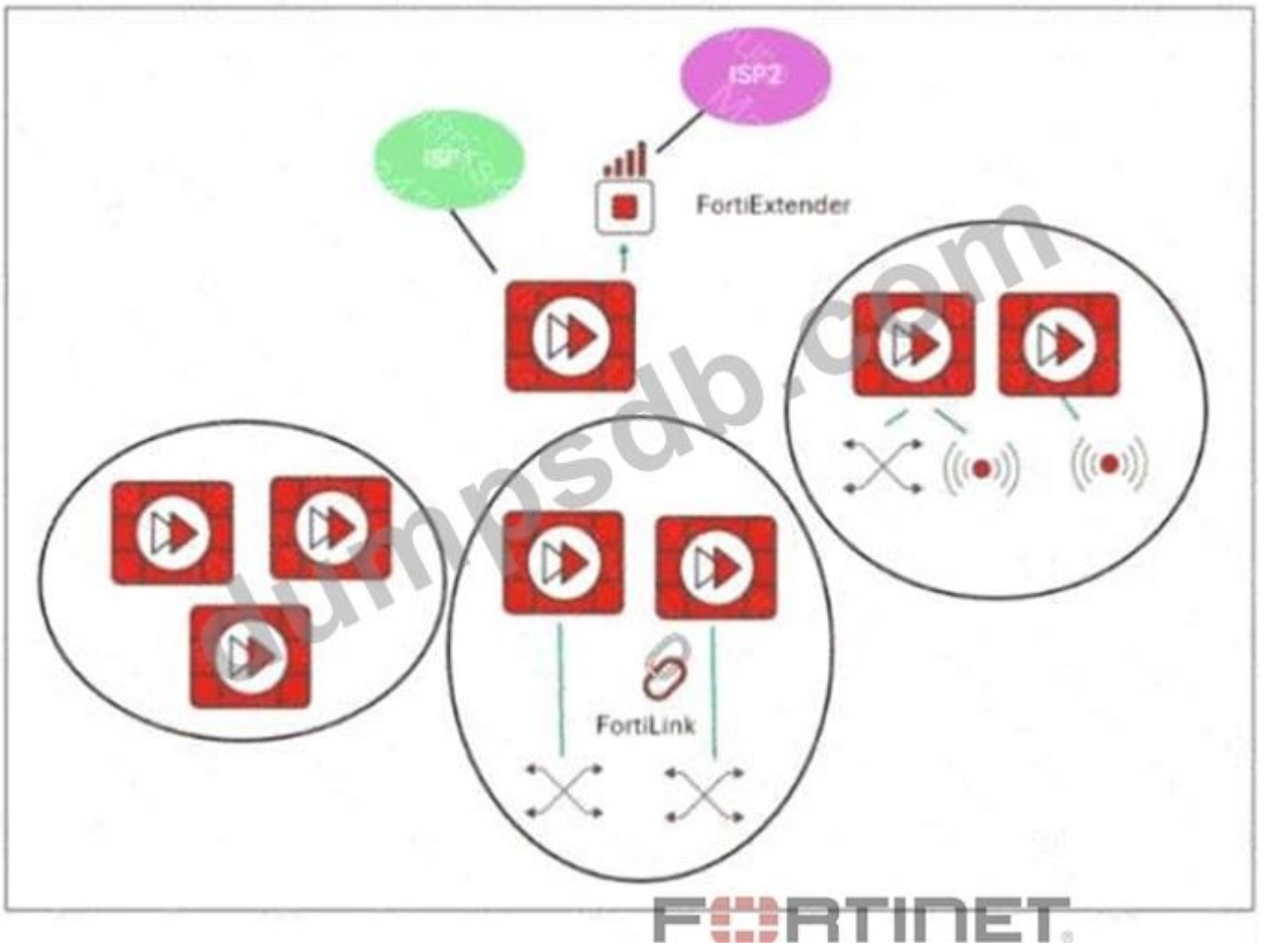
C. When FortiGate cannot recognize the application of the flow, it steers the traffic through the preferred member of rule 3, HQ_T1.

D. There is no service defined for the Facebook application, so FortiGate appliesservice rule 3 and directs the traffic to headquarters.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 4

SD-WAN Network Topology



Refer to the exhibit.

You want to configure SD-WAN on a network as shown in the exhibit.
The network contains many FortiGate devices. Some are used as NGFW, and some are installed with extensions such as FortiSwitch. FortiAP. or Forti Ex tender.

What should you consider when planning your deployment?

A. You can build an SD-WAN topology that includes all devices. The hubs can be FortiGate devices with Forti Extender.

B. You can build an SD-WAN topology that includes all devices. The hubs must be devices without extensions.

C. You must use FortiManager to manage your SD-WAN topology.

D. You must build multiple SD-WAN topologies. Each topology must contain only one type of extension.

Answer: B (LEAVE A REPLY)

In Fortinet SD-WAN, hubs should not have extensions like FortiSwitch, FortiAP, or FortiExtender installed, as these can affect hub functionality and scalability. While all device types can be included in the topology, the hubs must be "clean" FortiGate devices without such extensions to ensure proper ADVPN and overlay management.

References:

[FCSS_SDW_AR-7.4 1-0.docx Q3]

Fortinet SD-WAN Reference Architecture Guide 7.4 - Hub requirements

NEW QUESTION: 5

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: (SHOW ANSWER)
Interfaces must be defined and added as SD-WAN members to participate in traffic steering.
Routing is required so FortiGate knows how to reach destinations through SD-WAN paths.
Firewall policies are needed to permit traffic and allow SD-WAN rules to take effect.

NEW QUESTION: 6
In which SD-WAN template field can you use a metadata variable?
A. You can use metadata variables only to define interface members and the gateway IP.
B. Any field identified with a dollar sign (S) in a magnifying glass.
C. All SD-WAN template fields support metadata variables.
D. Any field identified with an "M" in a circle.
Answer: D (LEAVE A REPLY)

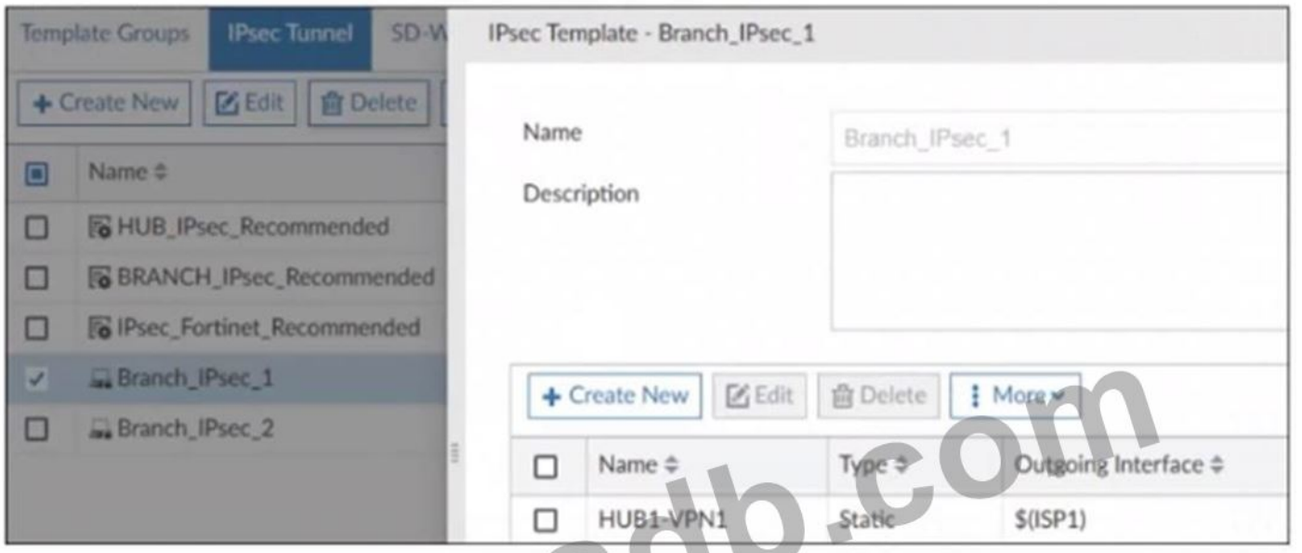
NEW QUESTION: 7
Which three characteristics apply to provisioning templates available on FortiManager? (Choose three.)
A. You cannot apply a system template and CLI template to the same FortiGate device.
B. A template group can include a system template and an SD-WAN template.
C. A CLI template can be of type CLI script or Perl script.
D. A CLI template group can contain CLI templates of both types.
E. CLI templates are applied in order, from top to bottom.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
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 expects a large amount of VoIP traffic.
B. The customer requires SIA with centralized breakout.
C. The majority of the branch traffic is directed to a corporate data center.
D. The administrator expects a large volume of traffic between the branches.
Answer: B,D (LEAVE A REPLY)

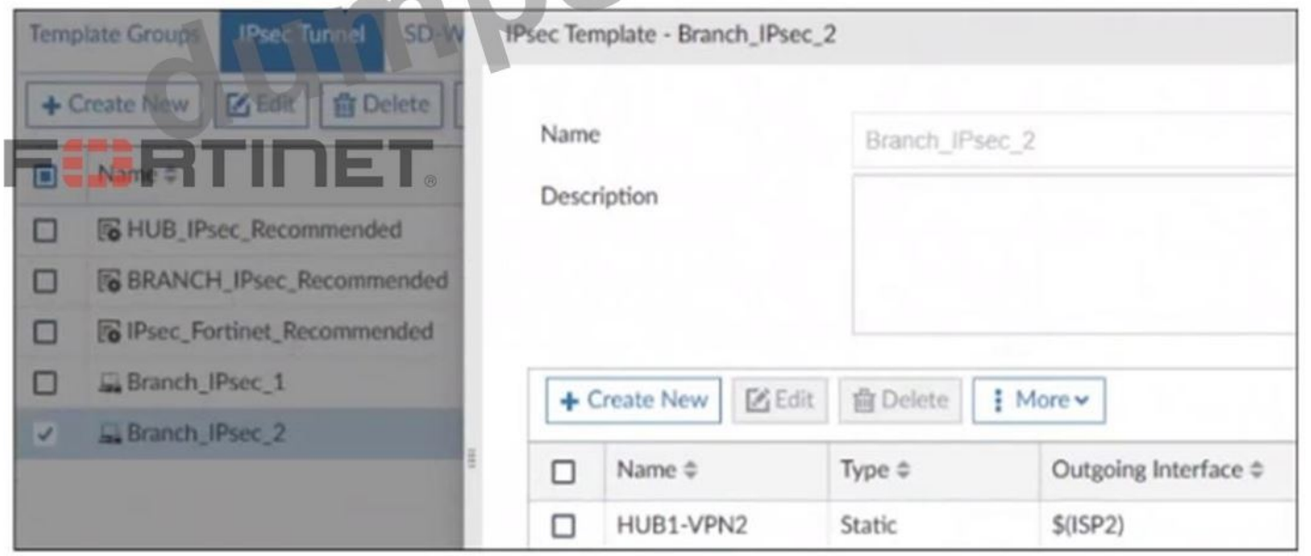
NEW QUESTION: 9

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

IPsec template for Branch_IPsec_1



IPsec template for Branch_IPsec_2



Error message in FortiManager

A. You can assign only one template with a tunnel type of static to each FortiGate device.

B. You can assign only one IPsec template to each FortiGate device.

C. You should review the branch1_fgt configuration for configured tunnels in the rootVDOM.

D. You should use the same outgoing interface of both templates.

Answer: (SHOW ANSWER)

FortiManager allows only one IPsec template to be assigned per FortiGate device. The error indicates a conflicting template assignment, meaning assigning both Branch_IPsec_1 and Branch_IPsec_2 to the same device (branch1_fgt) is not permitted.

NEW QUESTION: 10

Refer to the exhibits. 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 membercollected on a FortiGate device.

Which statement best describes what the diagnose output shows?

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
```

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 (LEAVE A REPLY)

The diagnose output lists SD-WAN members 4(HUB1-VPN1), 5(HUB1-VPN2), 7(HUB2-VPN1), 8(HUB2-VPN2), and 9(HUB2-VPN3). It does not include member 6 (HUB1-VPN3). From the template, HUB1-VPN3 is installed only on branch2_fgt and branch3_fgt - not on branch1_fgt.

Therefore, the output must be from branch1_fgt.

NEW QUESTION: 11

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 (LEAVE A REPLY)

When referencing a zone in a static route, FortiGate's behavior is described as:

"Referencing a zone in a static route causes FortiGate to install a static route for each member interface of the zone. This enables ECMP (Equal-Cost Multi-Path) and load balancing where supported and ensures that traffic can be steered over any valid zone member according to SD-WAN rules or standard routing." This mechanism is fundamental to Fortinet's implementation of SD-WAN and simplifies large, multi- interface deployments.

References:

[FCSS_SDW_AR-7.4 1-0.docx Q21]

FortiOS 7.4 Routing Guide, "Zone-based Routing and ECMP Behavior"

NEW QUESTION: 12

Exhibit.

SD-WAN rules status and configuration

```
branch1_fgt # diagnose sys sdwan service4 3

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

  Dst address(1):
        10.0.0.0-10.255.255.255


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

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

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

A. When HUB1-VPN1 has 4% packet loss

B. When HUB1-VPN1 has 12% packet loss

C. When HUB1-VPN3 has 4% packet loss

D. When all three members have the same packet loss

Answer: D (LEAVE A REPLY)

NEW QUESTION: 13

Which three factors about SLA targets and SD-WAN rules should you consider when configuring SD-WAN rules? (Choose three.)

A. Member metrics are measured only if a rule uses the SLA target.

B. SLA targets are used only by SD-WAN rules that are configured with a Lowest Cost (SLA) strategy.

C. SD-WAN rules can use SLA targets to check whether the preferred members meet the SLA requirements.

D. When configuring an SD-WAN rule, you can select multiple SLA targets if they are from the same performance SLA.

E. When configuring an SD-WAN rule, you can select multiple SLA targets from different performance SLAs.

Answer: B,C,E (LEAVE A REPLY)
The use of SLA targets is specific to certain SD-WAN strategies. The "Lowest Cost (SLA)" and "Maximize Bandwidth (SLA)" strategies are explicitly designed to use the configured SLA targets to make routing decisions. The "Best Quality" strategy uses performance metrics but does not necessarily require or reference SLA targets in the same way, while "Manual" does not use metrics at all for path selection.
This is a core function of SD-WAN rules with SLA targets. The purpose of configuring an SLA target with specific thresholds for latency, jitter, and packet loss is to define what is considered "acceptable" performance for an application. SD-WAN rules then use these targets to check if the members (interfaces) meet these requirements before a flow is steered over them, ensuring that a preferred path still offers a good user experience.
FortiGate allows for a single SD-WAN rule to reference multiple, different performance SLAs. This is crucial for complex deployments where a single SD-WAN rule needs to handle traffic for multiple applications that have distinct performance requirements. For example, a single rule might direct VoIP traffic based on one performance SLA with strict latency/jitter targets, while simultaneously handling general web traffic using another performance SLA with more lenient requirements.

NEW QUESTION: 14
An administrator is configuring SD-WAN to load balance their network traffic. Which two things should they consider when setting up SD-WAN? (Choose two.)
A. SD-WAN load balancing is possible only using the best quality and lowest cost (SLA) strategies.
B. When applicable. FortiGate load balances the traffic through all members that meet the SLA target.
C. Only the manual and best-quality strategies allow SD-WAN load balancing.
D. You can select the outbandwidth hash mode with all strategies that allow load balancing.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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: B,D (LEAVE A REPLY)
When you enable ADVPN (auto-discovery VPN) in the overlay template, FortiManager automatically updates both the IPsec and BGP templates on the hub so that shortcut tunnels can be established dynamically.
ADVPN can be activated in the SD-WAN overlay template for any supported topology, including dual-hub primary-primary, not just single hub.
NEW QUESTION: 16

Refer to the exhibit. The exhibit shows the details of a session and the index numbers of some relevant interfaces on a FortiGate device that supports hardware offloading.

Based on the information shown in the exhibits, which two conclusions can you draw? (Choose two.)

Session details

```
# diagnose sys session list

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

# diagnose netlink interface list

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


A. By default, FortiGate offloads symmetric and asymmetric flows.

B. The original direction of the symmetric traffic flows from port3 to port2.

C. The reply direction of the asymmetric traffic flows from port2 to port3.

D. The auxiliary session can be offloaded to hardware.

Answer: B,C (LEAVE A REPLY)

The session details show the symmetric flow's original direction as port3 → port2.

The asymmetric flow's reply direction is listed as port2 → port3.

NEW QUESTION: 17
What is true about SD-WAN multiregion topologies?
A. Each region has its own SD-WAN topology.
B. Routing between the hub and spokes must be BGP.
C. It is not compatible with ADVPN.
D. Regions must correspond to geographical areas.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
The FortiGate devices are managed by ForliManager, and are configured for direct internet access (DIA). You confirm that DIA is working as expected for each branch, and check the SD- WAN zone configuration and firewall policies shown in the exhibits.

SD-WAN Zones

Firewall Policy

Then, you use the SD-WAN overlay template to configure the IPsec overlay tunnels. You create the associated SD-WAN rules to connect existing branches to the company hub device and apply the changes on the branches. After those changes, users complain that they lost internet access. DIA is no longer working.

Based on the exhibit, which statement best describes the possible root cause of this issue?

A. The SD-WAN overlay template defines a zone for each underlay interface and moves the interfaces into those zones.

B. The SD-WAN overlay template didn't configure a firewall policy to allow traffic through the overlay.
C. The SD-WAN overlay template redefines the interface gateway addresses if they are defined with metadata variables.
D. The SD-WAN overlay template updates the SD-WAN template and the rules.
Answer: A (LEAVE A REPLY)
The SD-WAN overlay template defines a zone for each underlay interface and moves the interfaces into those zones. This statement perfectly describes the likely sequence of events. The template, when applied, re-organizes the interfaces and zones, causing the existing firewall policy that relies on the old zone configuration to fail. This is the most plausible root cause.

NEW QUESTION: 19
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 (LEAVE A REPLY)
The SD-WAN monitor's table view in FortiManager provides a donut visualization plus a detailed table that shows each SD-WAN member's status and SLA pass/miss, giving the per-member health view you're after.

NEW QUESTION: 20
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 expects a large amount of VoIP traffic.
B. The majority of the branch traffic is directed to a corporate data center.
C. The administrator expects a large volume of traffic between the branches.
D. The customer requires SIA with centralized breakout.
Answer: (SHOW ANSWER)

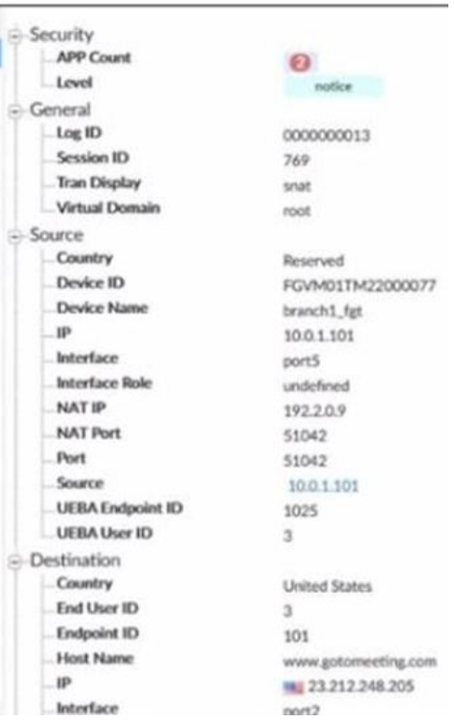
NEW QUESTION: 21
Refer to the exhibits.

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
...
```

on FortiAnalyzer

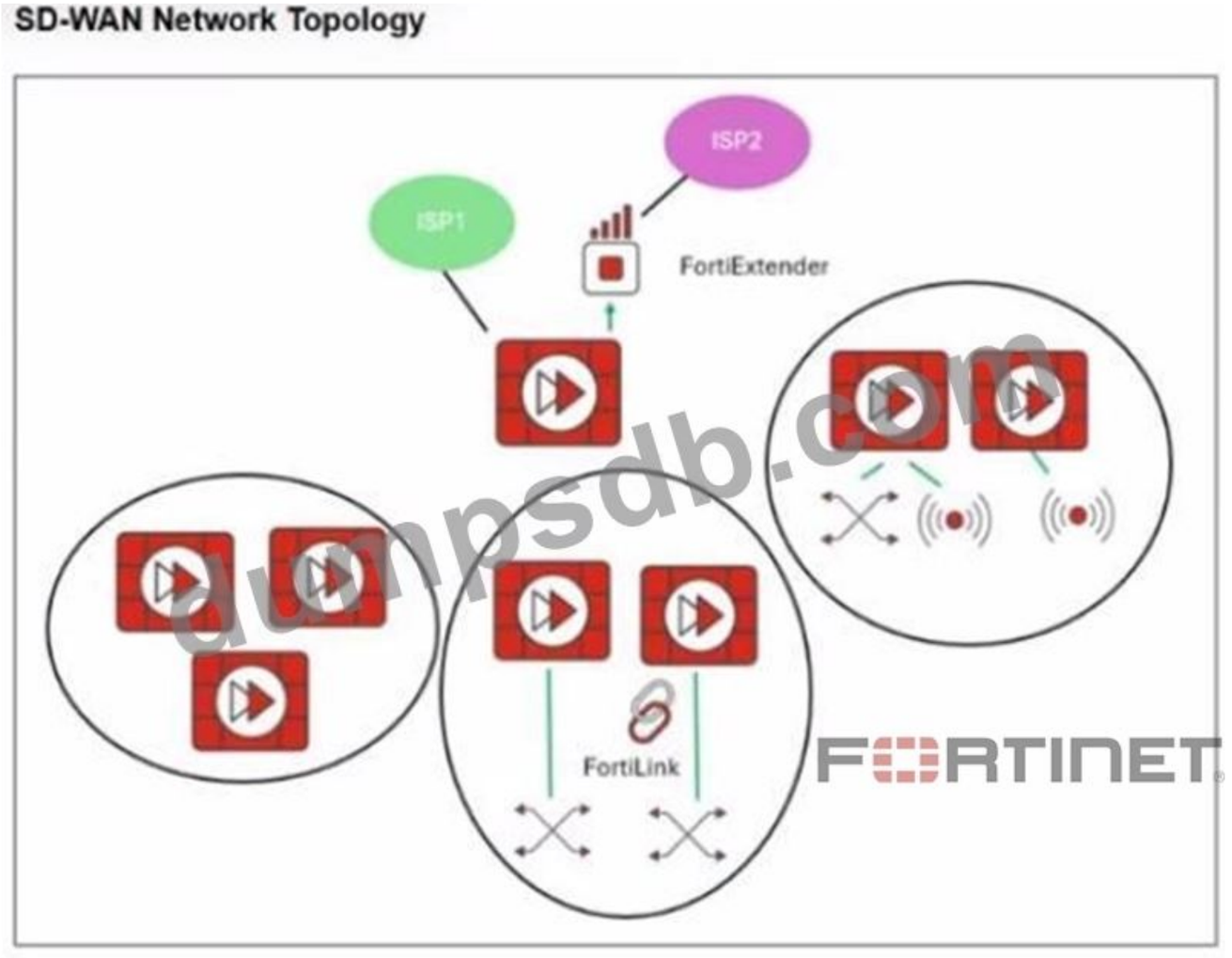
Application	Security Event List	SD-WAN Rule Name	Destination Interface
GoToMeeting	APP 2		port2
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2		port2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



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

NEW QUESTION: 22
Refer to the exhibit. You want to configure SD-WAN on a network as shown in the exhibit. The network contains many FortiGate devices. Some are used as NGFW, and some are installed with extensions such as FortiSwitch, FortiAP or FortiExtender. What should you consider when planning your deployment?



A. You must build multiple SD-WAN topologies. Each topology must contain only one type of extension.
B. You can build an SD-WAN topology that includes all devices. The hubs must be devices without extensions.
C. You must use FortiManager to manage your SD-WAN topology.

D. You can build an SD-WAN topology that includes all devices. The hubs can be FortiGate devices with Forti Extender.

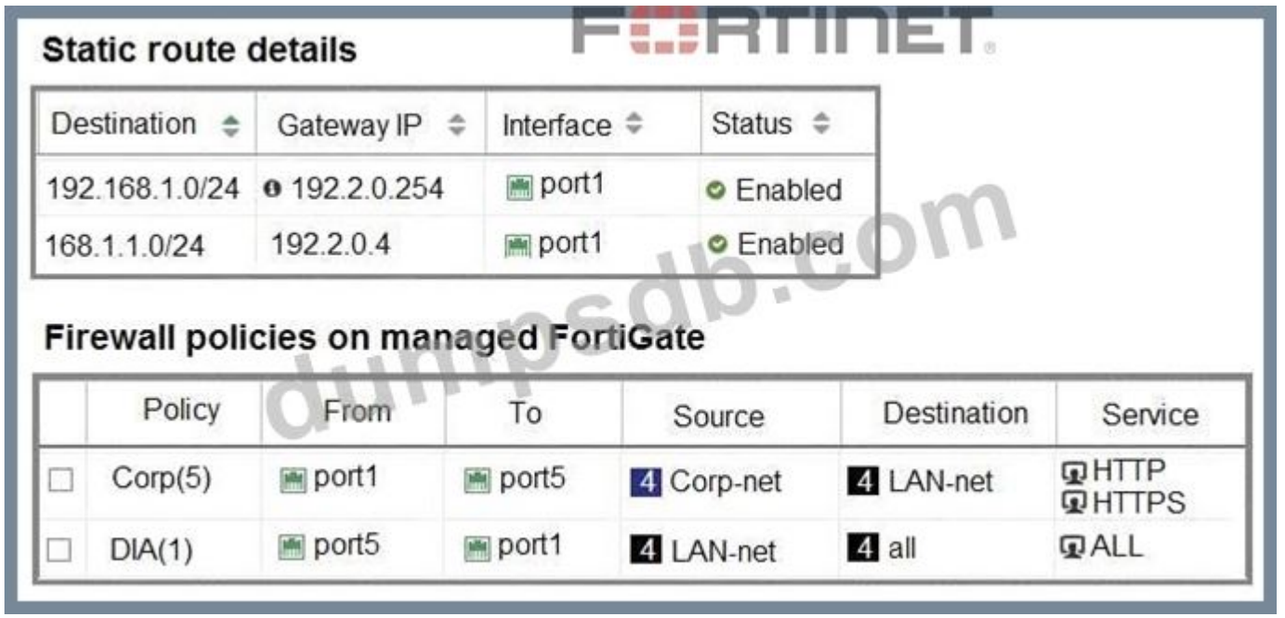
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23

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



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 (LEAVE A REPLY)

In the exhibits, port2 is already assigned to the SD-WAN zone named Test. An interface can only belong to a single SD-WAN zone, so before you can add both port1 and port2 into the new SD-WAN zone Underlay, you must first delete the SD-WAN Zone Test to free port2.

NEW QUESTION: 24

You are tasked with configuring ADVPN 2.0 on an SD-WAN topology already configured for ADVPN. What should you do to implement ADVPN 2.0 in this scenario?

A. Update the IPsec tunnel configurations on the hub.

B. Update the SD-WAN configuration on the branches.

C. Update the IPsec tunnel configuration on the branches.

D. Delete the existing ADVPN configuration and configure ADVPN 2.0.

Answer: (SHOW ANSWER)

To implement ADVPN 2.0 on an existing ADVPN topology, you only need to update the IPsec tunnel configuration on the hub to support the enhanced capabilities. Branch configurations remain unchanged.

NEW QUESTION: 25

Refer to the exhibit, which shows output of the command diagnose sys sdwan health-check status collected on a FortiGate device.

```
# diagnose sys sdwan health-check status

Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393),
bandwidth-up(10235), bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378),
bandwidth-up(10236), bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(131.336), jitter(0.199), mos(4.330),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 T_INET_1): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.226), mos(4.398),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.440), jitter(0.245), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

Which two statements are correct about the health check status on this FortiGate device? (Choose two.)

A. The health-check VPN_PING orders the members according to the measured jitter.

B. There is no SLA criteria configured for the health-check Level3_DNS.

C. The interface T_INET_1 missed one SLA target.

D. The interface T_INET_0 missed three SLA targets.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 26

Refer to the exhibit. 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?

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
```

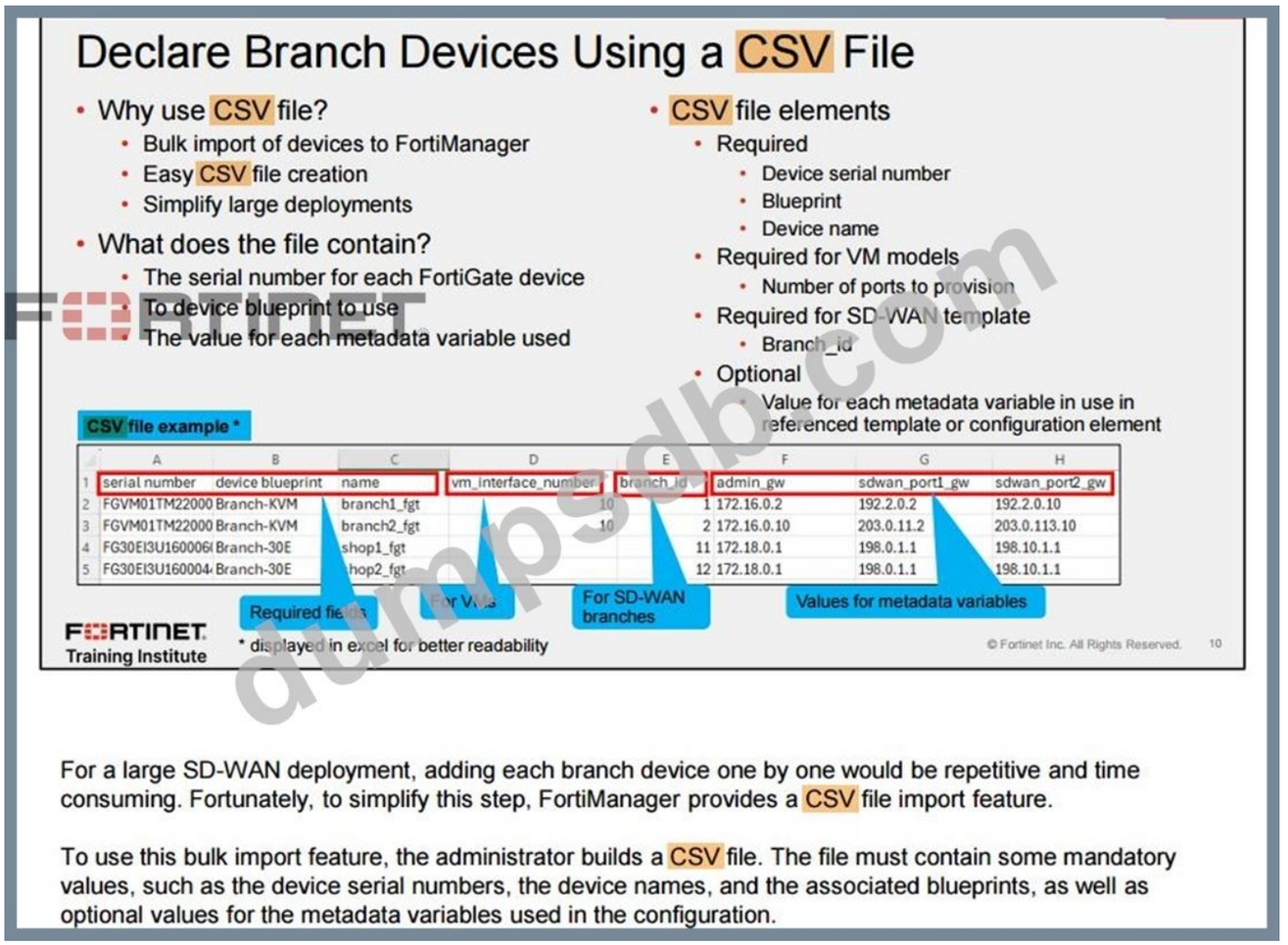
A. SD-WAN service rule 4 and port1 or port2.
B. SD-WAN service rule 4 and interface port2.
C. SD-WAN service rule 3 and interface HUB1-VPN3.
D. SD-WAN service rule 3 and interface HUB1-VPN2.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
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: (SHOW ANSWER)
Fortinet outlines key SD-WAN routing principles:
"Policy routes are always evaluated before SD-WAN rules, meaning if a policy route matches, SD-WAN steering is bypassed. If the best route for a destination is not via an SD-WAN member, SD-WAN rules do not apply, and members are ignored if they lack a valid route. This hierarchy ensures traffic always follows the most deterministic and valid path according to configuration." Understanding these principles is critical for correct SD-WAN and routing integration.

NEW QUESTION: 28
Refer to the exhibit. 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.)

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

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: (SHOW ANSWER)



For a large SD-WAN deployment, adding each branch device one by one would be repetitive and time consuming. Fortunately, to simplify this step, FortiManager provides a CSV file import feature.

To use this bulk import feature, the administrator builds a CSV file. The file must contain some mandatory values, such as the device serial numbers, the device names, and the associated blueprints, as well as optional values for the metadata variables used in the configuration.

NEW QUESTION: 29

Refer to the exhibit. 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.)

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
```


A. There is no service defined for the Facebook application, so FortiGate appliesservice rule 3 and directs the traffic to headquarters.

B. When FortiGate cannot recognize the application of the flow, it load balances the traffic through the tunnels HQ_T1, HQ_T2, HQ_T3.

C. FortiGate steers traffic for social media applications according to the service rule 2 and steers traffic through port2.

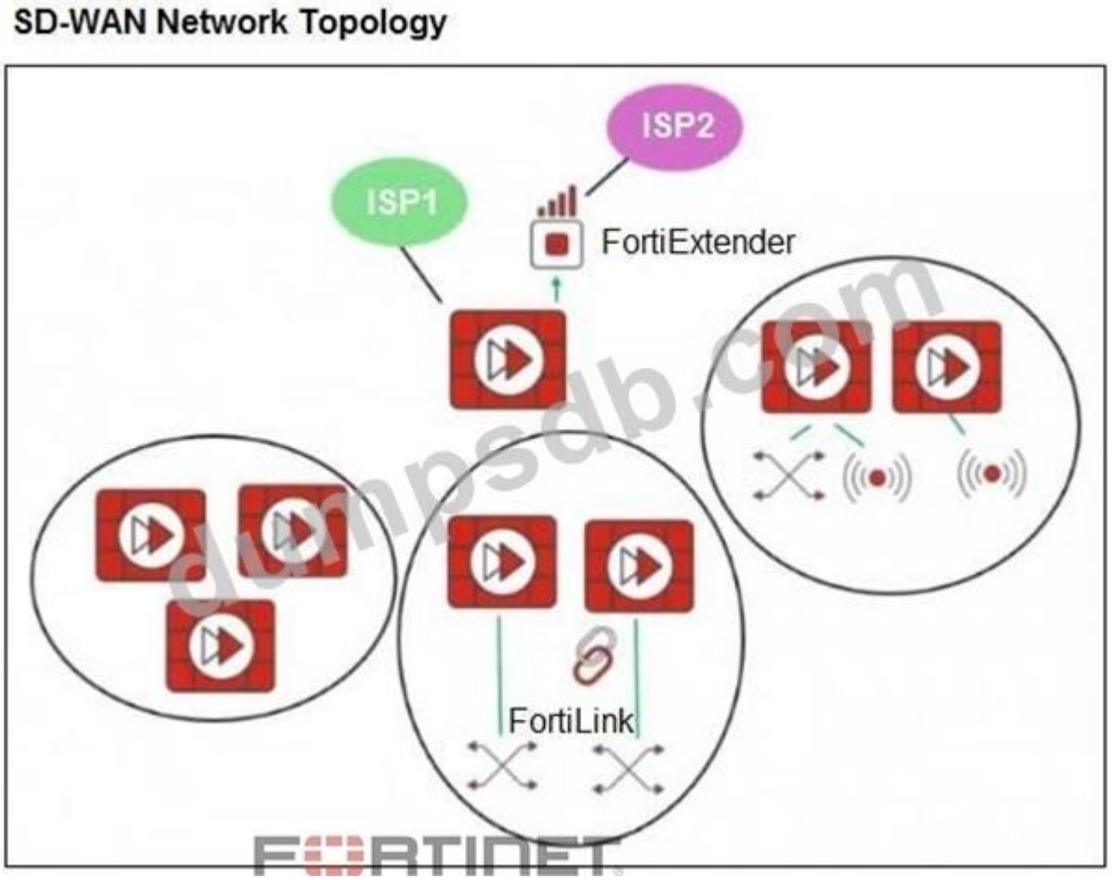
D. When FortiGate cannot recognize the application of the flow, it steers the traffic through the preferred member

of rule 3, HQ_T1.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 30

Refer to the exhibit. You want to configure SD-WAN on a network as shown in the exhibit. The network contains many FortiGate devices. Some are used as NGFW, and some are installed with extensions such as FortiSwitch, FortiAP or FortiExtender. What should you consider when planning your deployment?



A. You can build an SD-WAN topology that includes all devices. The hubs can be FortiGate devices with FortiExtender.

B. You can build an SD-WAN topology that includes all devices. The hubs must be devices without extensions.

C. You must use FortiManager to manage your SD-WAN topology.

D. You must build multiple SD-WAN topologies. Each topology must contain only one type of extension.

Answer: A (LEAVE A REPLY)

FortiGate devices with FortiExtender can act as hubs in an SD-WAN topology. FortiGate supports SD-WAN integration across diverse setups - including those using FortiSwitch, FortiAP, and FortiExtender - as long as the topology and roles are properly defined.

NEW QUESTION: 31

Refer to the exhibits. 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.)

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

```
config system sdwan
     configure 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

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

branch_fgt # get application name status | grep "id: 31077" -B1
app-name: "Youtube"
id: 31077
```

Underlay zone status

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

A. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.

B. Only related TCP traffic is used for performance measurement.

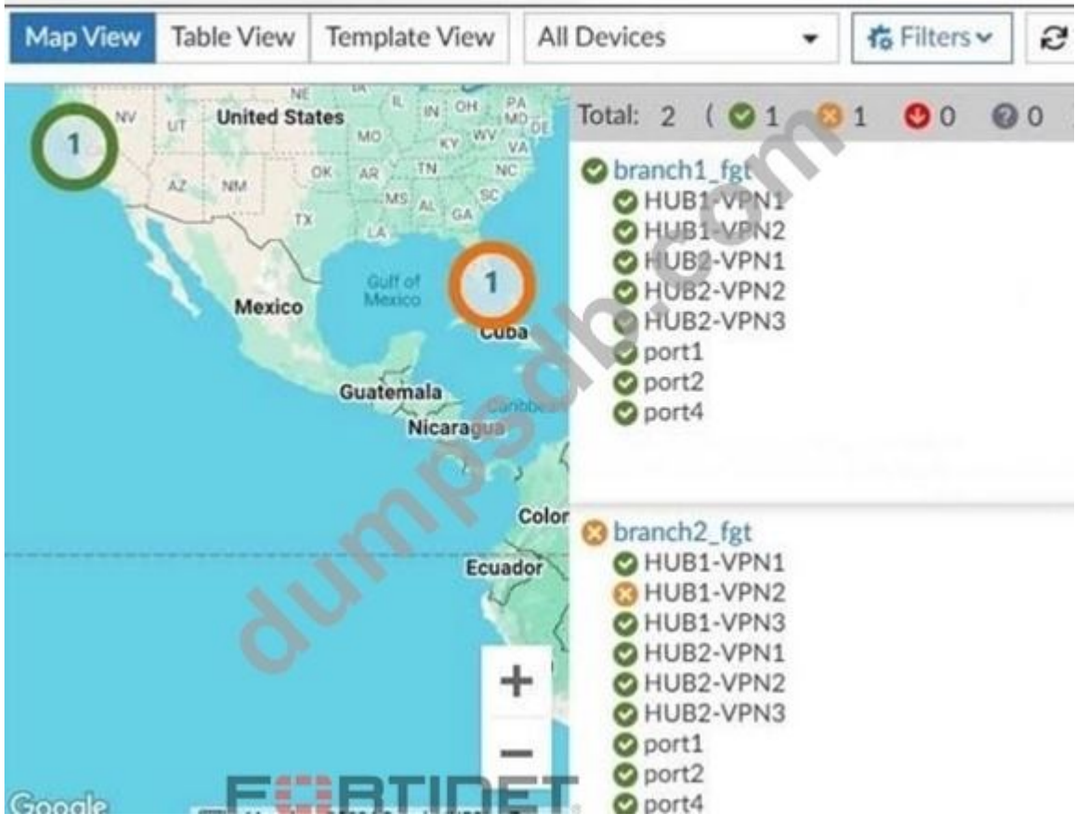
C. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.

D. Encrypted traffic is not used for the performance measurement.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 32
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 members are skipped if they do not have a valid route to the destination.
D. SD-WAN rules are skipped if the best route to the destination is a static route
E. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 33
Refer to the exhibit.An administrator checks the status of an SD-WAN topology using the FortiManager SD-WAN monitor menus. All members are configured with one or two SLAs. Which two conclusions can you draw from the output shown? (Choose two.)

FortiManager SD-WAN monitor



A. The template view should be used to see the hub devices.

B. One member of branch2_fgt is missing the SLAs.

C. branch2_fgt establishes six tunnels to the hubs and they are all up.

D. This SD-WAN topology contains only two branch devices.

Answer: B,D (LEAVE A REPLY)

The monitor shows only two devices (branch1_fgt and branch2_fgt), indicating the topology contains two branch devices.

HUB1-VPN2 under branch2_fgt has an orange X, indicating it's up but not meeting SLA requirements - likely due to missing or failing SLA targets.

NEW QUESTION: 34

Refer to the exhibit that shows event logs on FortiGate. Based on the output shown in the exhibit, what can you say about the tunnels on this device?

Event log on FortiGate

```
6: date=2024-12-18 time=15:15:06 eventtime=1734563705745090691 tz= "-0800" logid=
"0113022925" type= "event" subtype= "sdwan" level= "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" bidandwidthavailable= "20.00Gbps" inbandwidthused=
"0kbps" outbandwidthused= "0bkps" bibandwidthused= "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" action= "tunnel-stats" remip=120.64.1.1 locip=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 tunnelid=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" action= "tunnel-stats" remip=100.64.33.1 locip=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 locip=172.16.0.1 remport=500 locport=500 outintf="port4" srccountry=
"Reserved" cookies= "celc2c62ecc04871/a4d93a059b8df005" user= "172.16.1.1" 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
```


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: (SHOW ANSWER)

The "advpnsc" log field indicates whether a VPN event is based on an ADVPN shortcut. A value of "1" indicates the tunnel is an ADVPN shortcut, and "0" indicates it is not.

In the event logs, the log entry with "vpntunnel="HUB1-VPN1_0"" shows "advpnsc=1", which signifies that HUB1-VPN1_0 is a shortcut tunnel.

https://docs.fortinet.com/document/fortigate/7.2.0/new-features/661245/add-log-field-to-identify- advpn-shortcuts-in-vpn-logs

NEW QUESTION: 35

Refer to the exhibits. 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.)

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
```


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: B,C (LEAVE A REPLY)
The SD-WAN rule (config service edit 1) is configured with set mode priority. This means the rule selects the best interface based on a defined performance metric, as opposed to a simple static priority or SLA. The event log (image_41cfb5.png) shows Metric latency and Message Service prioritized by performance metric will be redirected in sequence order. This indicates that the rule is using latency to determine the preferred member. Given that the log message is about a change, and the most logical reason for a change in a priority mode is that a different member is now the best performer, it implies that the latency on port2 has become lower than that on port1.
The log message Service prioritized by performance metric will be redirected in sequence order confirms that FortiGate is changing the member being used for this service. Because the mode is priority, FortiGate dynamically selects the member that currently meets the best performance criteria, which in this case is latency. The log implies a new member has been selected as the most optimal, and with the default configuration, the members are sorted based on their performance, so the outgoing interface list is effectively updated to prefer the new best- performing member (port2).

NEW QUESTION: 36
You are tasked with configuring ADVPN 2.0 on an SD-WAN topology already configured for ADVPN. What should you do to implement ADVPN 2.0 in this scenario?
A. Update the SD-WAN configuration on the branches.
B. Update the IPsec tunnel configurations on the hub.
C. Update the IPsec tunnel configuration on the branches.
D. Delete the existing ADVPN configuration and configure ADVPN 2.0.
Answer: B (LEAVE A REPLY)
NEW QUESTION: 37

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. Create policy blueprint.

B. Create model devices.

C. Define metadata variables value for each device.

D. Create a ZTP template.

E. Update the DHCP server configuration.

Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 38

Refer to the exhibits.

Ping result

```
root@branch1-client-cli# ping facebook.com
PING facebook.com (157.240.19.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35): icmp_seq=1 ttl=56 time=33.4 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35): icmp_seq=2 ttl=56 time=32.5 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35): icmp_seq=3 ttl=56 time=32.5 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35): icmp_seq=4 ttl=56 time=32.6 ms
```

Diagnose output

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

id=1(0x01) dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=21(HUB1-VPN2)
[illegible]
destination wildcard(1): [illegible]/255.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:44

id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(2): oif=3(port1), oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(2): Salesforce(16920,0) Microsoft.Portal(41469,0)
hit_count=13 rule_last_used=2025-01-06 01:55:12

id=2130903043(0x7f030003) vwl_service=3(Corp) vwl_mbr_seq=4 5 6 7 [illegible] dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(6): oif=20(HUB1-VPN1), oif=21(HUB1-VPN2), oif=22(HUB1-VPN3), oif=23(HUB2-VPN1), oif=24(HUB2-VPN2),
oif=25(HUB2-VPN3)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:47

id=2130903045(0x7f030005) vwl_service=5(Internet) vwl_mbr_seq=3 2 1 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(3): oif=6(port4), oif=4(port2) path_last_used=2025-01-06 02:12:08, oif=3(port1)
source(1): 10.0.1.0-10.0.1.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=27 rule_last_used=2025-01-06 02:12:08
```

Diagnose output

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

Max_App_Ctrl_Size=32768 Num_App_Ctrl_Entry=8

Facebook(15832 23): IP=157.240.19.35 6 443

Addicting.Games(30156 8): IP=172.64.80.1 6 443

Microsoft.Portal(41469 28): IP=184.27.181.201 6 443

LinkedIn(16331 23): IP=13.107.42.14 6 443

MSN.Game(16135 8): IP=13.107.246.35 6 443

Salesforce(16920 29): IP=23.222.17.73 6 443

Salesforce(16920 29): IP=23.222.17.76 6 443

Facebook(15832 23): IP=31.13.80.36 6 443
```


You connect to a device behind a branch FortiGate device and initiate a ping test. The device is part of the LAN subnet and its IP address is 10.0.1.101.

Based on the exhibits, which interface uses branch 1_fgt to steer the test traffic?

A. port4

B. port1

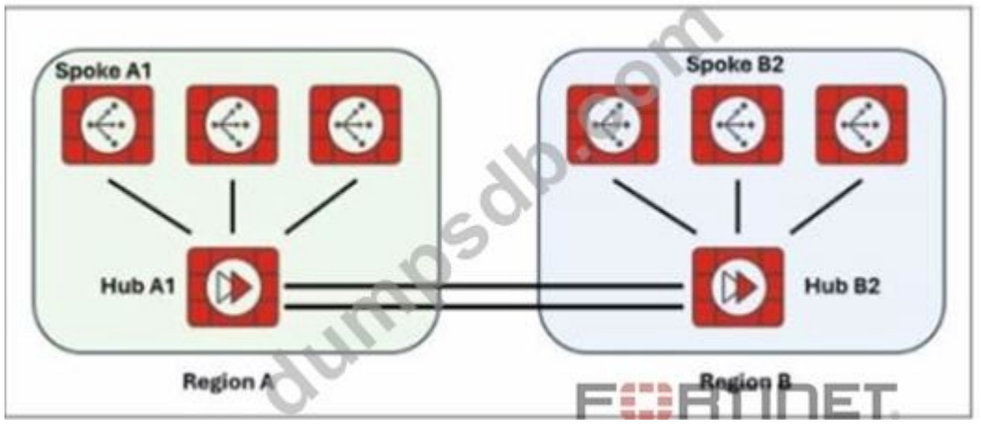
C. HUB1-VPN1

D. port2

Answer: B (LEAVE A REPLY)

NEW QUESTION: 39

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-forwarder must be enabled on the IPsec VPNs to spokes.

C. On hubs, auto-diacovery-sender must be enabled on the IPsec VPNs to spokes

D. On hubs, auto-discovery-receiver must be enabled on the IPsec VPNs to spokes.

Answer: (SHOW ANSWER)

NEW QUESTION: 40

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: (SHOW ANSWER)

The SD-WAN rule (config service edit 1) is configured with set mode priority. This means the rule selects the best interface based on a defined performance metric, as opposed to a simple static priority or SLA. The event log (image_41cfb5.png) shows Metric latency and Message Service prioritized by performance metric will be redirected in sequence order. This indicates that the rule is using latency to determine the preferred member. Given that the log message is about a change, and the most logical reason for a change in a priority mode is that a different member is now the best performer, it implies that the latency on port2 has become lower than that on port1.

The log message Service prioritized by performance metric will be redirected in sequence order confirms that FortiGate is changing the member being used for this service. Because the mode is priority, FortiGate dynamically selects the member that currently meets the best performance criteria, which in this case is latency. The log implies a new member has been selected as the most optimal, and with the default configuration, the members are sorted based on their performance, so the outgoing interface list is effectively updated to prefer the new best-performing member (port2).

NEW QUESTION: 41

Refer to the exhibit. The exhibit shows the health-check configuration on a FortiGate device used as a spoke.
You notice that the hub FortiGate doesn't prioritize the traffic as expected.
Which two configuration elements should you check on the hub? (Choose two.)

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

A. The performance SLA has the parameter priority-out-slaconfigured.

B. This performance SLA uses the same members.

C. The performance SLA uses the same criteria.

D. The performance SLA is configured with set embedded-measure accept.

Answer: C,D (LEAVE A REPLY)

The hub must use a performance SLA with the same criteria as the spoke's health check. The spoke's health check is using ping (protocol ping) and measuring latency (link-cost-factor latency). For the hub to use the data sent by the spoke, its performance SLA must be configured to measure the same metrics. If the hub is looking for jitter or packet loss, it will not use the latency data sent by the spoke.

When a spoke sends embedded health data, the hub FortiGate must be configured to receive and use it. This is done by setting set embedded-measure accept within the performance SLA configuration on the hub. This setting explicitly tells the hub to trust and use the performance metrics received from the remote FortiGate (the spoke). Without this setting, the hub will likely ignore the embedded health data and rely on its own health checks, which could lead to incorrect traffic prioritization.

NEW QUESTION: 42

Refer to the exhibit that shows event logs on FortiGate. Based on the output shown in the exhibit, what can you say about the tunnels on this device?

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" mosvoice="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=1734563086334261977 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="celc2c62ecc04871/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
```

A. The master tunnel HU82-VPN3 cannot accept ADVPN shortcuts.

B. There is one shortcut tunnel built from master tunnel VPN4.
C. The VPN tunnel HUB1-VPN1_0 is a shortcut tunnel.
D. The device steers voice traffic through the VPN tunnel HUB1-VPN3.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
Refer to the exhibit.

BGP configuration

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

     end
     …
end
```


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

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

A. Set additional-pathto send

B. Set additional-pathto forward

C. Enable route-reflector-server

D. Enable route-reflector-client.

E. Set adv-additional-pathto the number of additional paths to advertise.

Answer: A,D,E (LEAVE A REPLY)

The hub must send additional paths to spokes (set additional-path send).

The hub must treat each spoke as a route-reflector client so spoke routes are reflected to other spokes.

The hub must specify how many additional paths to advertise (set adv-additional-path <n>).

NEW QUESTION: 44

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.

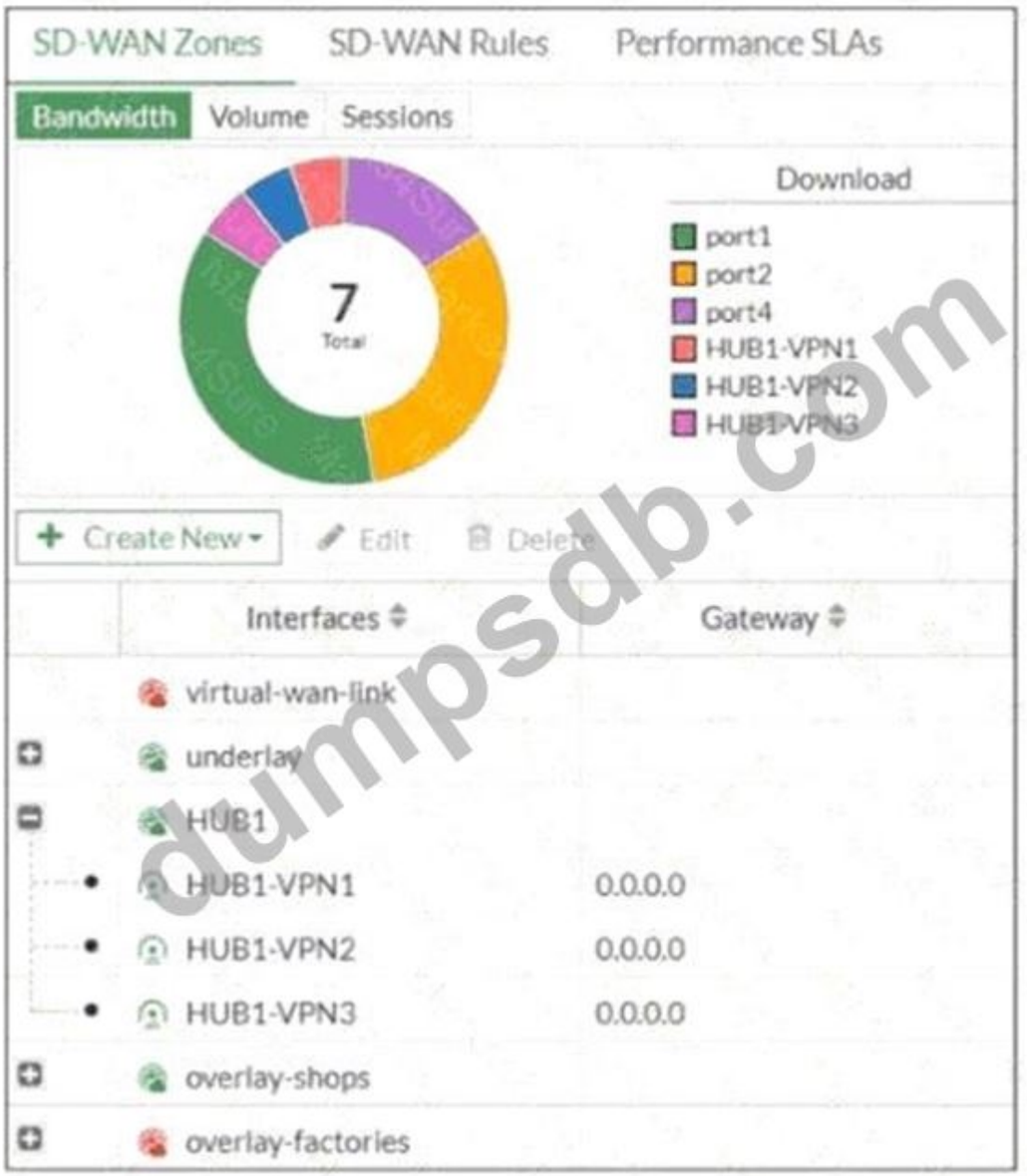
Answer: B (LEAVE A REPLY)

When an SD-WAN member is deleted, FortiGate can also remove static routes that were tied to that interface. If those routes are needed for destinations not covered by SD-WAN rules, traffic to those networks becomes unreachable. This explains why flows not matching SD-WAN rules are interrupted after the member was removed.

NEW QUESTION: 45

Exhibit.

SD-WAN zones



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

A. The underlay zone contains three members.

B. You can delete the virtual-wan-link zones.

C. The overlay-factories zone contains no member.

D. You can move HUB1-VPN3 from the HUB1 zone to the overlay-shops zone.

Answer: C (LEAVE A REPLY)

In the SD-WAN GUI, the absence of members in a zone is visually represented, and the Fortinet guide confirms: "If a zone such as overlay-factories contains no members, it will be displayed as empty in the SD-WAN GUI. This may occur when the zone is reserved for future expansion, or if members have been temporarily removed for maintenance or reconfiguration. Traffic cannot be steered via an empty zone until at least one SD-WAN

member is added." Such visual cues help operators quickly assess configuration status and readiness.

NEW QUESTION: 46
You are planning a large SD-WAN deployment with approximately 1000 spokes and want to allow ADVPN between the spokes. Some remote sites use FortiSASE to connect to the company's SD-WAN hub. Which overlay routing configuration should you use?
A. BGP on loopback with dynamic BGP for ADVPN shortcut routing.
B. BGP on loopback with IPsec phase2 selectors for ADVPN shortcut routing.
C. BGP per overlay with dynamic BGP for ADVPN shortcut routing.
D. BGP per overlay with BGP next-hop convergence for ADVPN shortcut routing.
Answer: (SHOW ANSWER)
For a large-scale SD-WAN deployment (such as 1000 spokes) where ADVPN shortcut routing is required and some remote sites connect via FortiSASE, the recommended overlay routing configuration is BGP running on loopback interfaces, combined with dynamic BGP for ADVPN shortcut routing. This design leverages the scalability and resilience of BGP, allowing dynamic discovery and route exchange necessary for shortcut tunnels between spokes in ADVPN environments. Using loopback interfaces for BGP peering is considered best practice because it decouples routing protocol stability from physical link status, ensuring that if a physical underlay interface fails, the BGP session remains up as long as there's an alternate path. With dynamic BGP, each spoke can efficiently learn the routes to other spokes and dynamically establish shortcuts, which is critical at this scale. This method also integrates smoothly with FortiSASE for remote connectivity to the SD-WAN hub, providing flexibility and centralized management.
References:
[FCSS_SDW_AR-7.4 1-0.docx Q6]
Fortinet SD-WAN Reference Architecture Guide 7.4, "Scalable Routing with BGP on Loopback and ADVPN Shortcuts" Fortinet SD-WAN Concept Guide, "Overlay Routing Designs for Large Deployments"

NEW QUESTION: 47
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 over T2. 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.

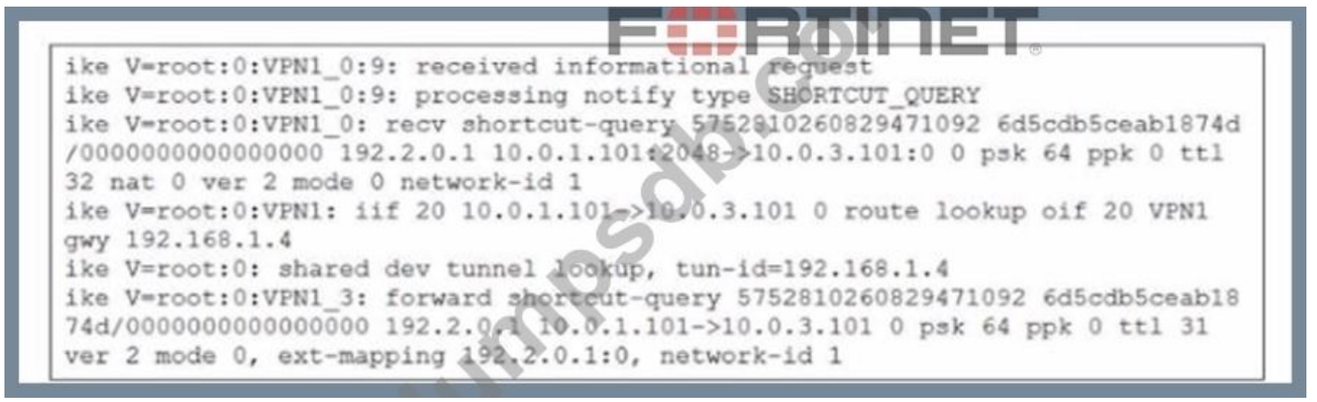
D. FortiGate route lookup for reply traffic only considers routes over the original ingress interface.

Answer: (SHOW ANSWER)

To ensure DC-1 responds via the best-performing SD-WAN member (T1) instead of defaulting to T2, enable auxiliary-sessionunder config system settings, so reply traffic is evaluated against current route policies-not bound to the ingress interface.

NEW QUESTION: 48

Refer to the exhibit.



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 spoke that has received a shortcut query from another spoke and has forwarded the response to its hub.

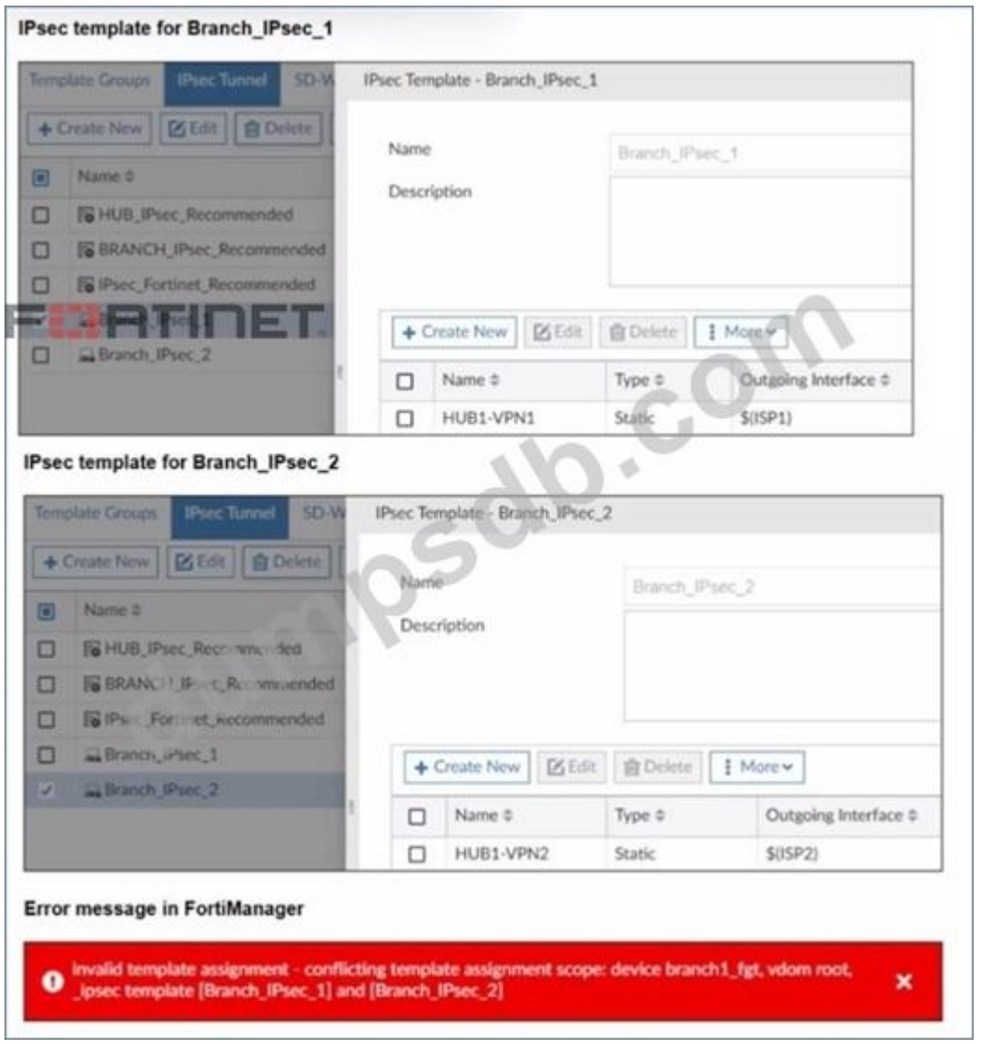
C. This is a spoke. The kernel received a shortcut request and forwards the query to another spoke.

D. This is a hub in a dual-region topology. The remote hub tunnel ID is 10.0.2.101.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 49

Refer to the exhibits.



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

Which statement best describes the cause of the issue?

A. You can assign only one template with a tunnel type of static to each FortiGate device.

B. You can assign only one IPsec template to each FortiGate device.

C. You should review the branch1_fgt configuration for configured tunnels in the rootVDOM.

D. You should use the same outgoing interface of both templates.

Answer: (SHOW ANSWER)

NEW QUESTION: 50

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 data vwl_mbr_seq.

B. You identify sessions steered according to SD-WAN rules with the data sdwan_service_id.

C. You identify sessions steered according to SD-WAN rules with the flag vwl.

D. You cannot identify SD-WAN sessions. You must use the sdwar. session filter.

Answer: (SHOW ANSWER)

NEW QUESTION: 51

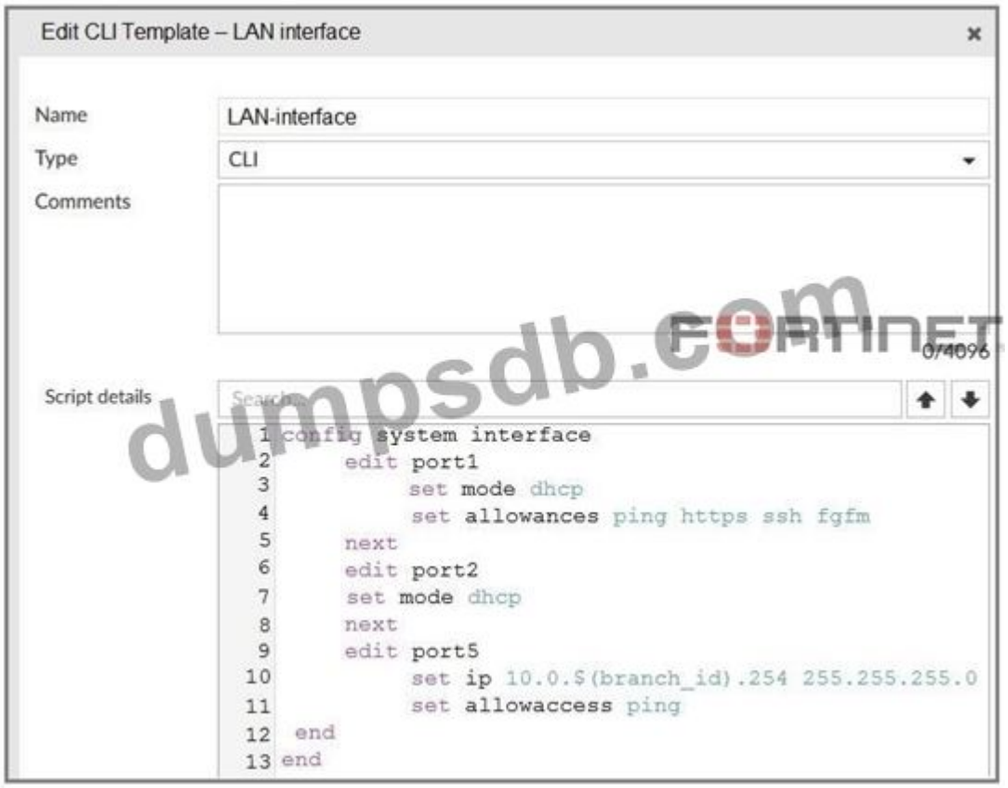
Refer to the exhibits. The administrator configured a device blueprint and CLI scripts as shown in the exhibits, to prepare for onboarding FortiGate devices in the company's stores. Later, a technician prepares a FortiGate 51G with a basic configuration and connects it to the network.

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?

CLI script LAN-interface



A. FortiManager updates the device configuration according to the selected templates. It applies the corp_st template first.

B. FortiManager does not update the port1 configuration because FortiManager does not change the configuration of interfaces with fgfm access.

C. FortiManager updates access rights only for port1. FortiManager cannot update the IP address because it was already set manually.

D. FortiManager updates the configuration of port1, port2, and port5. The three ports might get new IP addresses.

Answer: D (LEAVE A REPLY)

Enforce Device Configuration is enabled and the blueprint applies the provisioning CLI templates.

The LAN-interface script sets port1 and port2 to DHCP and assigns a static IP to port5 (using the branch_id variable). Therefore, when FortiManager pushes the blueprint, it updates the configurations of port1, port2, and port5 - and their IP addresses may change accordingly.

NEW QUESTION: 52

Refer to the exhibit. Which statement best describe the role of the ADVPN device in handling traffic?

```
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 6
d5cdb5ceab18
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, exr-mapping 192.2.0.1:0, network-id 1
```

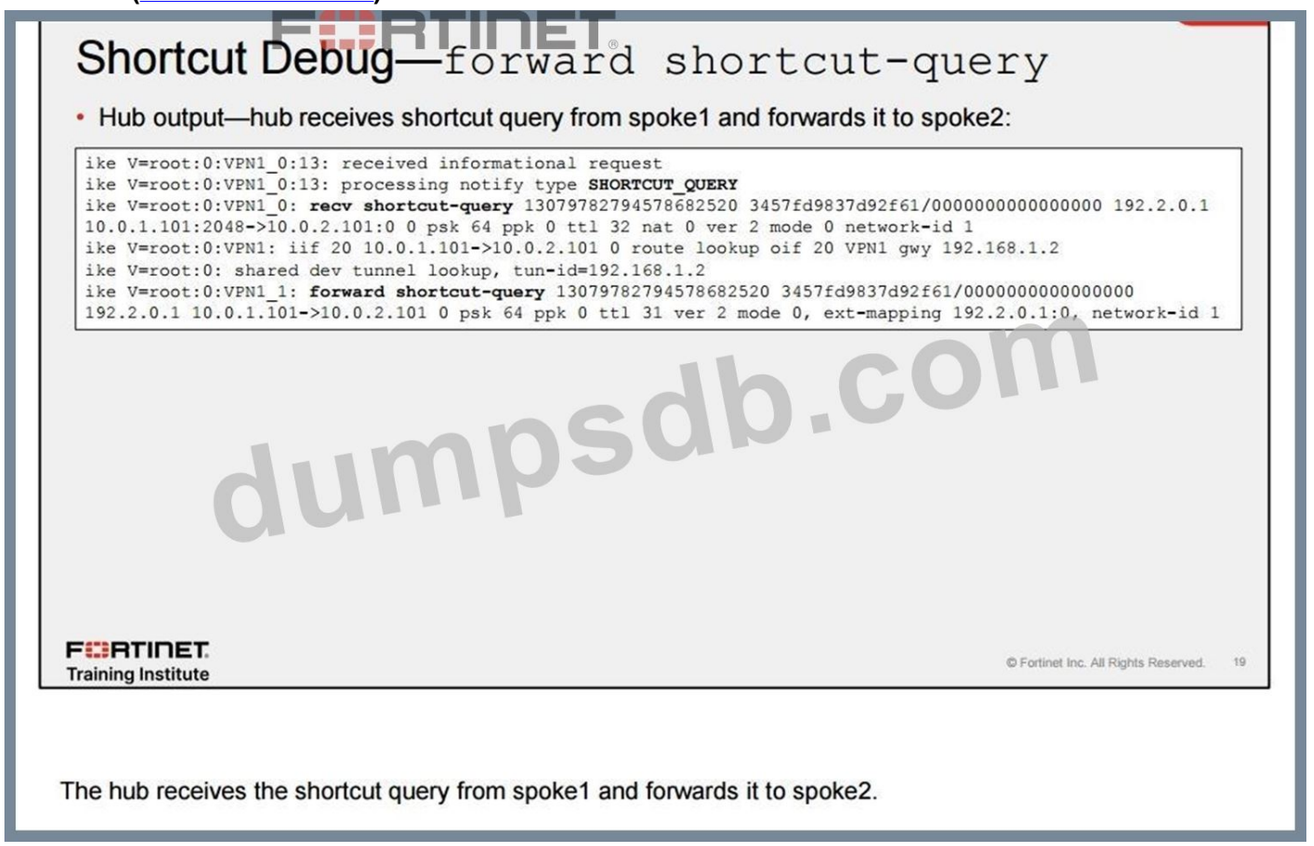
A. This is a hub that has received a query from a spoke and has forwarded it to another spoke.

B. This is a hub in a dual-region topology. The remote hub tunnel ID is 10.0.2.101.

C. This is a spoke that has received a shortcut query from another spoke and has forwarded the response to its hub.

D. This is a spoke. The kernel received a shortcut request and forwards the query to another spoke.

Answer: (SHOW ANSWER)



NEW QUESTION: 53

Refer to the exhibits. You connect to a device behind a branch FortiGate device and initiate a ping test. The device is part of the LAN subnet and its IP address is 10.0.1.101.

Based on the exhibits, which interface uses branch 1_fgt to steer the test traffic?

Diagnose output

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

id=1(0x1) dscp_tag=0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0
port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=21(HUB1-VPN2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 10.1.0.7/255.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:44

id=2130903041 (0x7f030001) vwl_service=1 (Critical-DIA) vwl_mbr_seq=1 2
dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst (0->0) iif=0(any)
path(2): oif=3(port1), oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(2): Salesforce(16920,0) Microsoft.Portal (41469,0)
hit_count=13 rule_last_used=2025-01-06 01:55:12

id=2130903042 (0x7f030002) 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=27 rule_last_used=2025-01-06 01:55:12

id=2130903043 (0x7f030003) vwl_service=3 (Corp) vwl_mbr_seq=4 5 6 7 8 9
dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst (0->0) iif=0(any)
path(6): oif=20(HUB1-VPN1), oif=21(HUB1-VPN2), oif=22(HUB1-VPN3), oif=23
(HUB2-VPN1), oif=24(HUB2-VPN2), oif=25(HUB2-VPN3),
source(1): 10.0.1.0-10.0.1.255
destination (1): 10.0.0.0-10.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:49

id=2130903045 (0x7f030005) vwl_service=5 (Internet) vwl_mbr_seq=3 2
1dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst (0->0) iif=0(any)
path(3): oif=6(port4), oif=4(port2) path_last_used=2025-01-06 02:12:08,
oif=3(port1)
source(1): 10.0.1.0-10.0.1.255
destination (1): 10.0.0.0-10.255.255.255
hit_count=27 rule_last_used=2025-01-06 02:12:08
```

Diagnose output

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

Max_App_Ctrl_Size=32768 Num_App_Ctrl_Entry=8

Facebook(15832 23): IP=157.240.19.35 6 443

Addicting.Games(30156 8): IP=172.64.80.1 6 443

Microsoft.Portal(41469 28): IP=184.27.181 201 6 443

LinkedId(16331 23): IP=13.107.42.14 6 443

MSN.Game(16135 8): IP=13.107.246.35 6 443

Salesforce(16920 29): IP=32,222.17 73 6 443

Salesforce(16920 29): IP=32,222.17 76 6 443

Facebook(15832 23): IP=31.13.80.36 6 443
```


A. port4

B. HUB1-VPN1

C. port1

D. port2

Answer: D (LEAVE A REPLY)

The ping target IP 157.240.19.35 matches an App Control entry for Facebook (ID 15832).
According to the diagnose firewall route list output, this application is handled by vwl_service=2 (Non-Critical-DIA), which routes traffic via oif=4 (port2). Therefore, FortiGate steers the Facebook test traffic through port2.

NEW QUESTION: 54

Refer to the exhibit that shows an SD-WAN zone configuration on the FortiManager GUI.

Based on the exhibit, how will the FortiGate device behave after it receives this configuration?

A. The configuration instructs FortiGate to choose an ADVPN shortcut based on SD-WAN information.

B. The configuration instructs FortiGate to allow ADVPN shortcuts for the tunnels of this SD-WAN zone.

C. The configuration instructs FortiGate to establish shortcuts only when at least two members meet the SLA target.

D. The configuration instructs FortiGate to establish shortcuts only for overlay interfaces that meet the SLA target HUB1_HC.

Answer: C (LEAVE A REPLY)

This is because the setting minimum-sla-meet-members = 2 requires at least two SD-WAN zone members (in this case, HUB2-VPN1, HUB2-VPN2, and HUB2-VPN3) to pass the defined SLA health check (HUB1_HC) before the FortiGate will establish ADVPN shortcuts. If fewer than two members meet the SLA, shortcuts will not be created.

NEW QUESTION: 55

Which three factors about SLA targets and SD-WAN rules should you consider when configuring SD-WAN rules? (Choose three.)

A. Member metrics are measured only if a rule uses the SLA target.

B. SLA targets are used only by SD-WAN rules that are configured with a Lowest Cost (SLA) strategy.

C. SD-WAN rules can use SLA targets to check whether the preferred members meet the SLA requirements.

D. When configuring an SD-WAN rule, you can select multiple SLA targets if they are from the same performance SLA.

E. When configuring an SD-WAN rule, you can select multiple SLA targets from different performance SLAs.

Answer: B,C,E (LEAVE A REPLY)

The use of SLA targets is specific to certain SD-WAN strategies. The "Lowest Cost (SLA)" and "Maximize Bandwidth (SLA)" strategies are explicitly designed to use the configured SLA targets to make routing decisions. The "Best Quality" strategy uses performance metrics but does not necessarily require or reference SLA targets in the same way, while "Manual" does not use metrics at all for path selection.

This is a core function of SD-WAN rules with SLA targets. The purpose of configuring an SLA target with specific

thresholds for latency, jitter, and packet loss is to define what is considered "acceptable" performance for an application. SD-WAN rules then use these targets to check if the members (interfaces) meet these requirements before a flow is steered over them, ensuring that a preferred path still offers a good user experience.
FortiGate allows for a single SD-WAN rule to reference multiple, different performance SLAs. This is crucial for complex deployments where a single SD-WAN rule needs to handle traffic for multiple applications that have distinct performance requirements. For example, a single rule might direct VoIP traffic based on one performance SLA with strict latency/jitter targets, while simultaneously handling general web traffic using another performance SLA with more lenient requirements.

NEW QUESTION: 56
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	203.0.113.2	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	172.16.0.3	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: A,B (LEAVE A REPLY)

NEW QUESTION: 57
Refer to the exhibits.
Configuration for SD-WAN performance SLA, SD-WAN rule configuration, and application ID: 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. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through

the member.
B. Encrypted traffic is not used for the performance measurement.
C. Only related TCP traffic is used for performance measurement.
D. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which two statements correctly describe what happens when traffic matches the implicit SD-WAN rule? (Choose two.)
A. The session information output displays no SD-WAN service id.
B. Traffic is load balanced using the algorithm set for the v4-ecmp-modesetting.
C. The traffic is distributed, regardless of weight, through all available static routes.
D. Traffic does not match any of the entries in the policy route table.
E. FortiGate flags the session with may_dirtyand vwl_default.
Answer: A,D (LEAVE A REPLY)
When traffic matches the implicit SD-WAN rule, no specific SD-WAN service is applied, so the session information output does not show an SD-WAN service ID.
The implicit SD-WAN rule is considered only when no matching entry is found in the policy route table.

NEW QUESTION: 59
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: A (LEAVE A REPLY)
When you enable SD-WAN and add interfaces as SD-WAN members, those interfaces are no longer referenced directly in routing. You must replace routing configuration references (e.g., static routes, policy routes) with the SD-WAN zone. Firewall policies, however, can still point to the SD-WAN zone without requiring replacement of individual member interfaces.

NEW QUESTION: 60
Refer to the exhibits.

SD-WAN zone HUB1 and SD-WAN member configuration

SD-WAN zone HUB2 and SD-WAN member configuration

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: (SHOW ANSWER)

The diagnose output lists SD-WAN members 4(HUB1-VPN1), 5(HUB1-VPN2), 7(HUB2-VPN1), 8(HUB2- VPN2), and 9(HUB2-VPN3). It does not include member 6 (HUB1-VPN3). From the template, HUB1-VPN3 is installed

only on branch2_fgt and branch3_fgt - not on branch1_fgt. Therefore, the output must be from branch1_fgt.

NEW QUESTION: 61
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: (SHOW ANSWER)
FortiGate passively monitors the member if TCP traffic is passing through the member → With Prefer Passive mode, FortiGate inspects existing traffic (like TCP flows) to measure performance metrics without generating its own probes.
FortiGate passively monitors the member if ICMP traffic is passing through the member → Similarly, when ICMP flows exist, FortiGate uses them for SLA checks.

NEW QUESTION: 62
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: (SHOW ANSWER)
A large volume of inter-branch traffic benefits from a local hub to avoid backhauling and reduce latency.
If most traffic is destined for a corporate data center, placing the hub on-premises ensures efficient routing and improved performance.

NEW QUESTION: 63

Refer to the exhibits. 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?

SD-WAN zone configuration on FortiManager

SD-WAN Zones

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

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

7

Policy package configuration

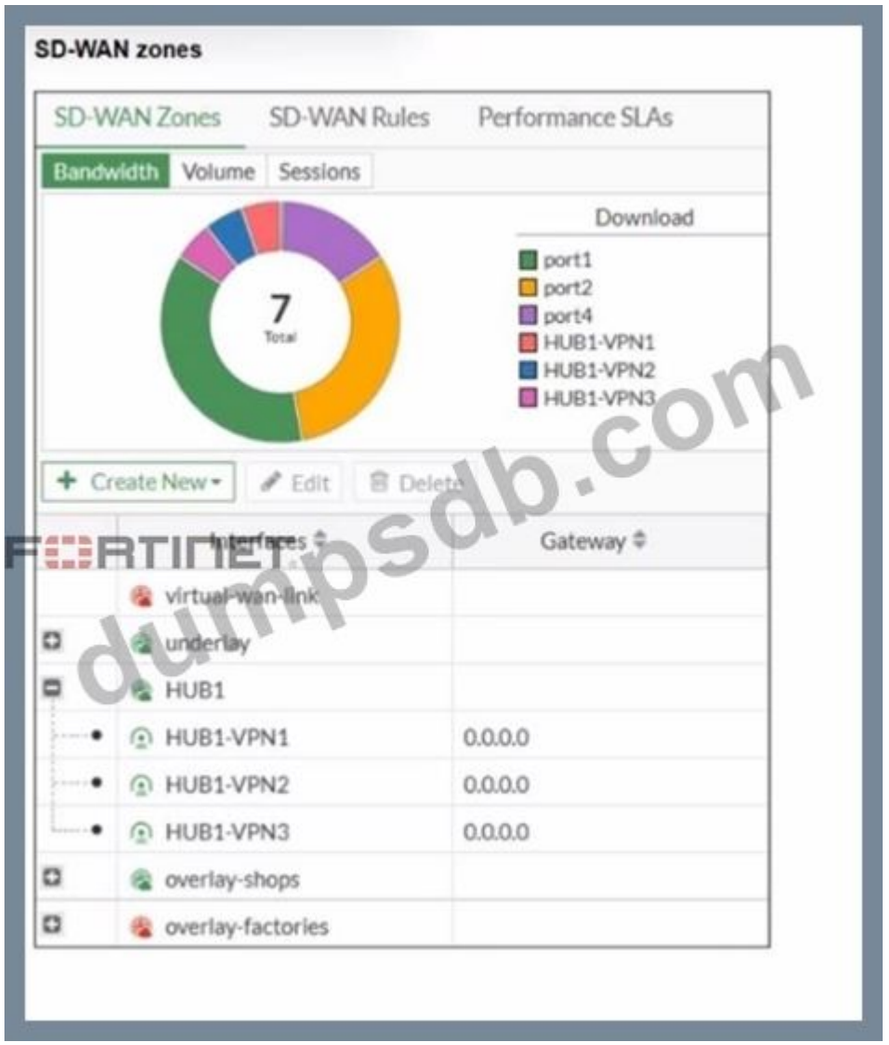
#	Name	From	To	Source	Destination	Install On
Corp-SOT_BBLK(1/1 Total:1)						
2	DIA	LAN	underlay	LAN-net	all	Installation Targets
3	To Hub-Overlay	LAN	HUB1-VPN1	all	all	Installation Targets
Implicit(4/4 Total:1)						
4	Implicit Deny	any	any	all all	all all	

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 (LEAVE A REPLY)
Policy 3 points traffic To = HUB1-VPN1, which is an SD-WAN member interface. In SD-WAN you must reference the SD-WAN zone (the logical interface) in policies, not its member tunnels.
Change the policy's To interface to the zone HUB1, and the install will succeed.

NEW QUESTION: 64
Which statement about SD-WAN zones is true?
A. An SD-WAN zone can contain between 0 and 512 members.
B. An SD-WAN zone can contain only one type of interface.
C. You can configure up to 32 SD-WAN zones per VDOM.

D. You cannot use an SD-WAN zone in static route definitions.
Answer: A (LEAVE A REPLY)

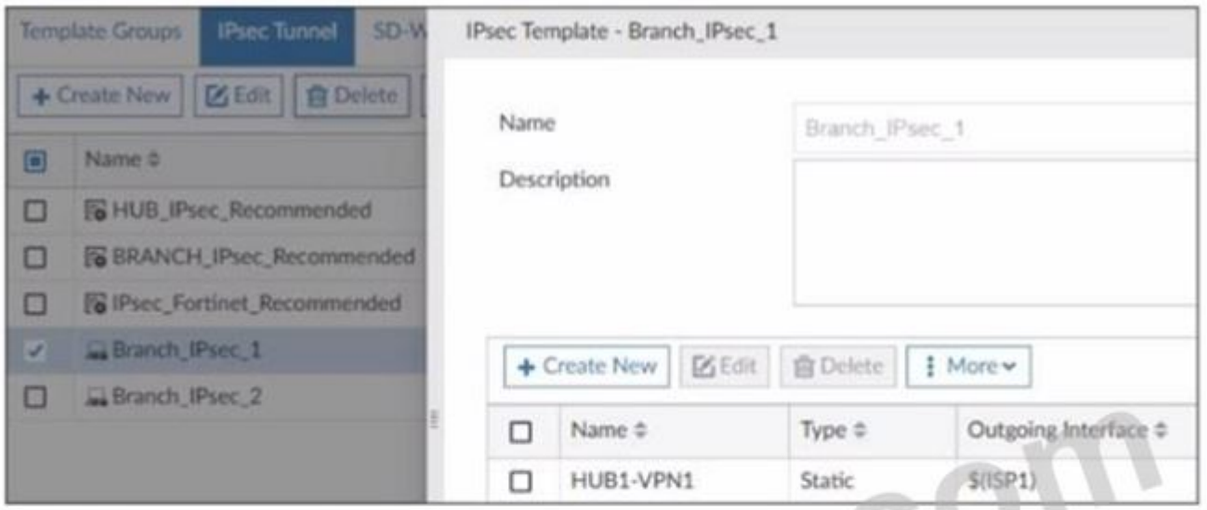
NEW QUESTION: 65
Exhibit.



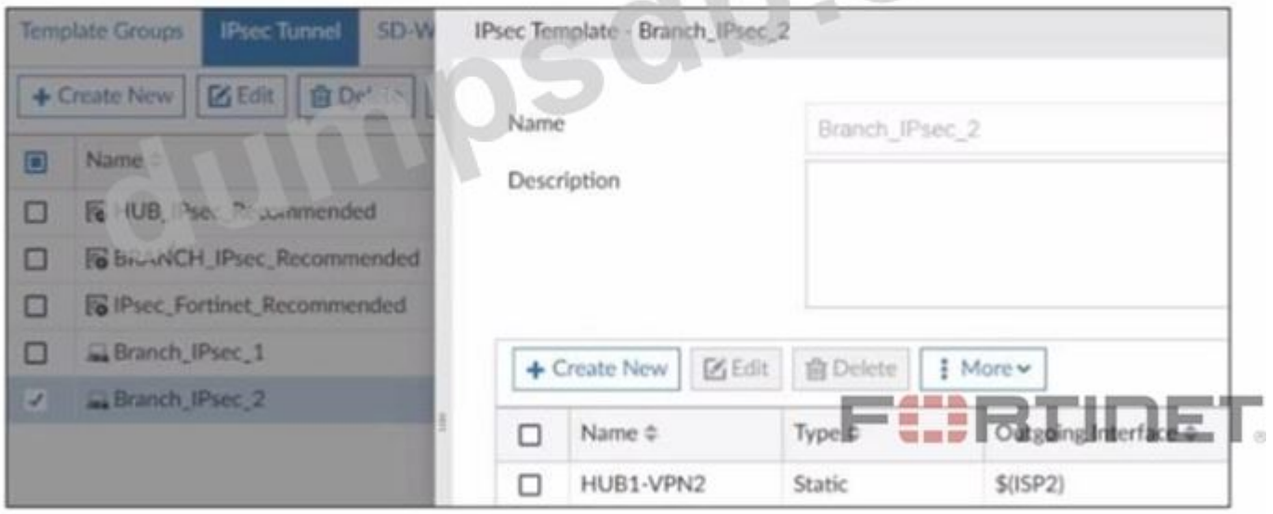
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI. What can you conclude about the zone and member configuration on this device?
A. The underlay zone contains three members.
B. You can delete the virtual-wan-link zones.
C. The overlay-factories zone contains no member.
D. You can move HUB1-VPN3 from the HUB1 zone to the overlay-shops zone.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
Refer to the exhibits. The exhibits show two IPsec templates to define Branch IPsec 1 and Branch_IPsec_2. Each template defines a VPN tunnel. The error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device is also shown. Which statement best describes the cause of the issue?

IPsec template for Branch_IPsec_1



IPsec template for Branch_IPsec_2



Error message in FortiManager

A. You should use the same outgoing interface of both templates.

B. You can assign only one IPsec template to each FortiGate device.

C. You can assign only one template with a tunnel type of static to each FortiGate device.

D. You should review the branch1_fgt configuration for configured tunnels in the rootVDOM.

Answer: (SHOW ANSWER)

NEW QUESTION: 67

Refer to the exhibit that shows event logs on FortiGate.

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 (LEAVE A REPLY)

Event logs (from the exhibit) show how traffic is matched to SD-WAN rules and routed. The log output indicates that voice traffic is being routed through the HUB1-VPN3 tunnel. This matches SD-WAN's application-aware steering, which uses dynamic performance metrics to select the optimal path.

References:

[FCSS_SDW_AR-7.4 1-0.docx Q4]

FortiOS 7.4 SD-WAN Application-Aware Routing Documentation

NEW QUESTION: 68

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

A. You identify sessions steered according to SD-WAN rules with the flag vwl.

B. You cannot identify SD-WAN sessions. You must use the sdwar. session filter.

C. You identify sessions steered according to SD-WAN rules with the data vwl_mbr_seq.

D. You identify sessions steered according to SD-WAN rules with the data sdwan_service_id.

Answer: D (LEAVE A REPLY)

The sdwan_service_id field in the output of diagnose sys session list indicates that the session was selected based on an SD-WAN rule, allowing administrators to trace which SD-WAN service (rule) steered the traffic.

NEW QUESTION: 69

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

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(0), health-check(HUB1_HC)
     Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, packet loss: 2.000%, selected
          2: Seq_num(5 HUB1-VPN2 HUB1), alive, packet loss: 4.000%, selected
          3: Seq_num(6 HUB1-VPN3 HUB1), alive, packet loss: 12.000%, selected
     Src address(1):
          10.0.1.0-10.0.1.255

     Dst address(1):
          10.0.0.0-10.255.255.255

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


A. When HUB1-VPN1 has 4% packet loss

B. When HUB1-VPN1 has 12% packet loss

C. When HUB1-VPN3 has 4% packet loss

D. When all three members have the same packet loss

Answer: B (LEAVE A REPLY)

The SD-WAN rule is in priority mode, and the current priority-members are set as 6 4 5, which means:

- 1st priority: HUB1-VPN3 (seq 6)
- 2nd priority: HUB1-VPN1 (seq 4)
- 3rd priority: HUB1-VPN2 (seq 5)

Currently, HUB1-VPN1 is selected (even though it's not the first in priority) because its packet loss (2%) is better than the higher-priority VPN3 (12%).

FortiGate will prefer a higher-priority member only if its link cost (here, packet loss) is below the link-cost-threshold, which is set to 0.

So, for HUB1-VPN3 to become the new preferred member, all higher-priority members (VPN1 and VPN2) must have equal or higher packet loss than VPN3.

If HUB1-VPN1 increases to 12% packet loss, equal to VPN3, then FortiGate will select VPN3 (priority 6) due to its higher configured priority.

NEW QUESTION: 70

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. FortiGate allows the configuration of applications as the destination of SD-WAN rules only on the CLI.

B. You must enable the feature on the CLI.

C. You must enable the feature first using the GUI menu System > Feature Visibility.

D. You cannot use applications as the destination when FortiGate is used for a DIA setup.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 71

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: A,C (LEAVE A REPLY)

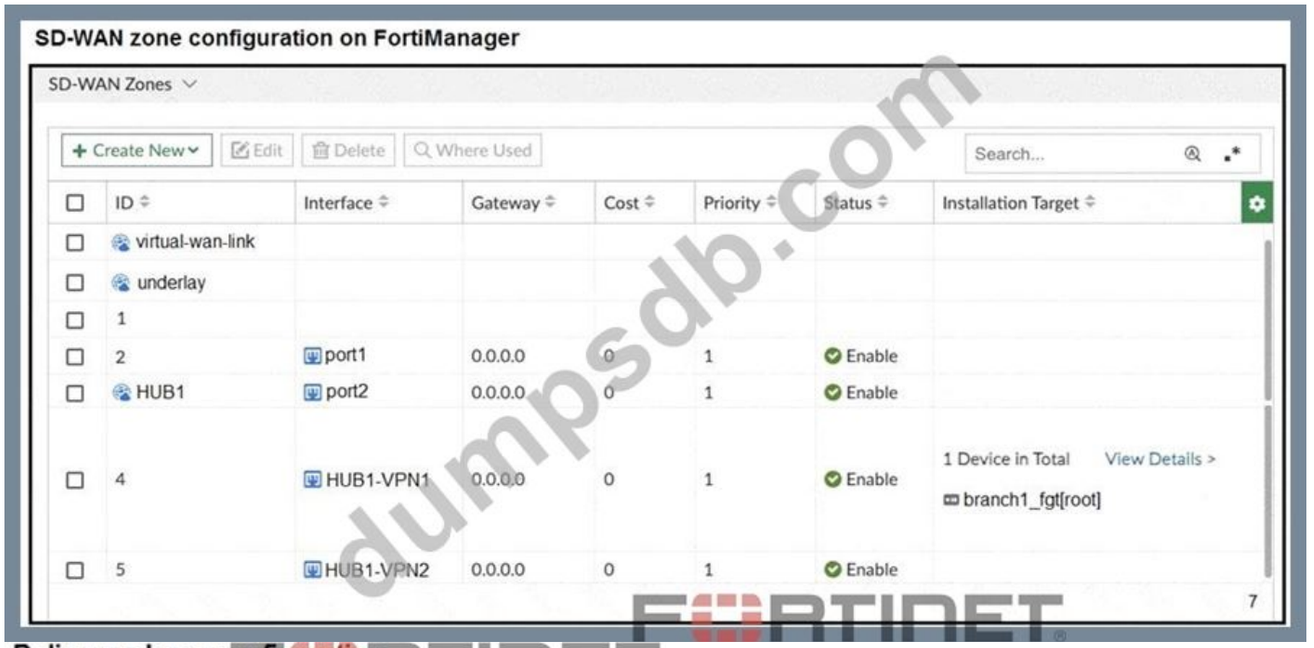
FortiGate passively monitors the member if TCP traffic is passing through the member # With Prefer Passive mode, FortiGate inspects existing traffic (like TCP flows) to measure performance metrics without generating its own probes.

FortiGate passively monitors the member if ICMP traffic is passing through the member # Similarly, when ICMP flows exist, FortiGate uses them for SLA checks.

NEW QUESTION: 72

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 (LEAVE A REPLY)

Policy 3 points traffic To = HUB1-VPN1, which is an SD-WAN member interface. In SD-WAN you must reference the SD-WAN zone (the logical interface) in policies, not its member tunnels. Change the policy's To interface to the zone HUB1, and the install will succeed.

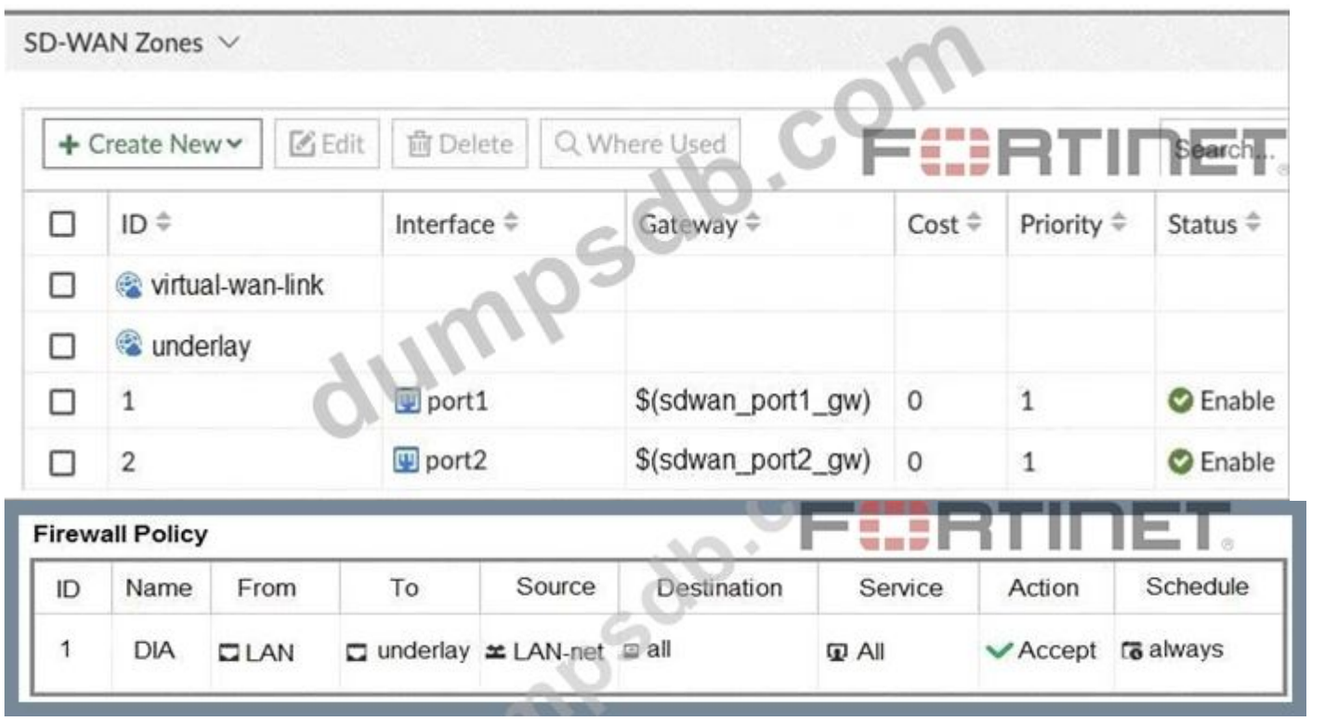
NEW QUESTION: 73

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?

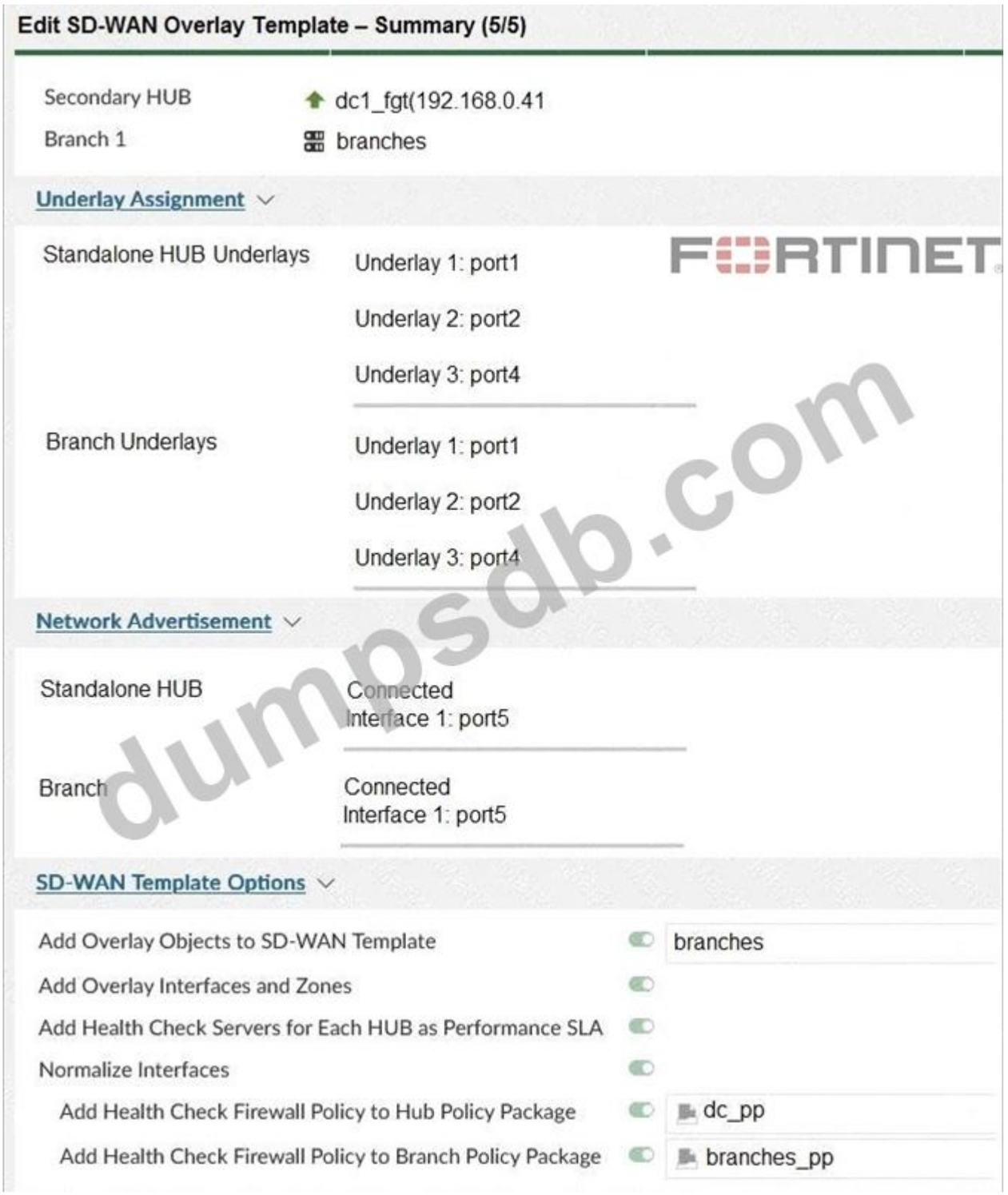
A. Replace references to interfaces used as SD-WAN members in the firewall policies.
B. Replace references to interfaces used as SD-WAN members in the routing configuration.
C. Disable the interface that you want to use as an SD-WAN member.
D. Purchase and install the SD-WAN license, and reboot the FortiGate device.
Answer: B (LEAVE A REPLY)
When you enable SD-WAN and add interfaces as SD-WAN members, those interfaces are no longer referenced directly in routing. You must replace routing configuration references (e.g., static routes, policy routes) with the SD-WAN zone. Firewall policies, however, can still point to the SD-WAN zone without requiring replacement of individual member interfaces.

NEW QUESTION: 74
The FortiGate devices are managed by ForliManager, and are configured for direct internet access (DIA). You confirm that DIA is working as expected for each branch, and check the SD-WAN zone configuration and firewall policies shown in the exhibits.
SD-WAN zones



Firewall Policy

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



Then, you use the SD-WAN overlay template to configure the IPsec overlay tunnels. You create the associated SD-WAN rules to connect existing branches to the company hub device and apply the changes on the branches. After those changes, users complain that they lost internet access. DIA is no longer working.

Based on the exhibit, which statement best describes the possible root cause of this issue?

A. The SD-WAN overlay template defines a zone for each underlay interface and moves the interfaces into those zones.

B. The SD-WAN overlay template didn't configure a firewall policy to allow traffic through the overlay.

C. The SD-WAN overlay template redefines the interface gateway addresses if they are defined with metadata

variables.

D. The SD-WAN overlay template updates the SD-WAN template and the rules.

Answer: A (LEAVE A REPLY)

The SD-WAN overlay template defines a zone for each underlay interface and moves the interfaces into those zones. This statement perfectly describes the likely sequence of events. The template, when applied, re-organizes the interfaces and zones, causing the existing firewall policy that relies on the old zone configuration to fail. This is the most plausible root cause.

NEW QUESTION: 75

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 auxiliary-session under config system settings.

B. FortiGate route lookup for reply traffic only considers routes over the original ingress interface.

C. Enable reply-session under config system sdwan.

D. Enable snat-route-change under config system global.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 76

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

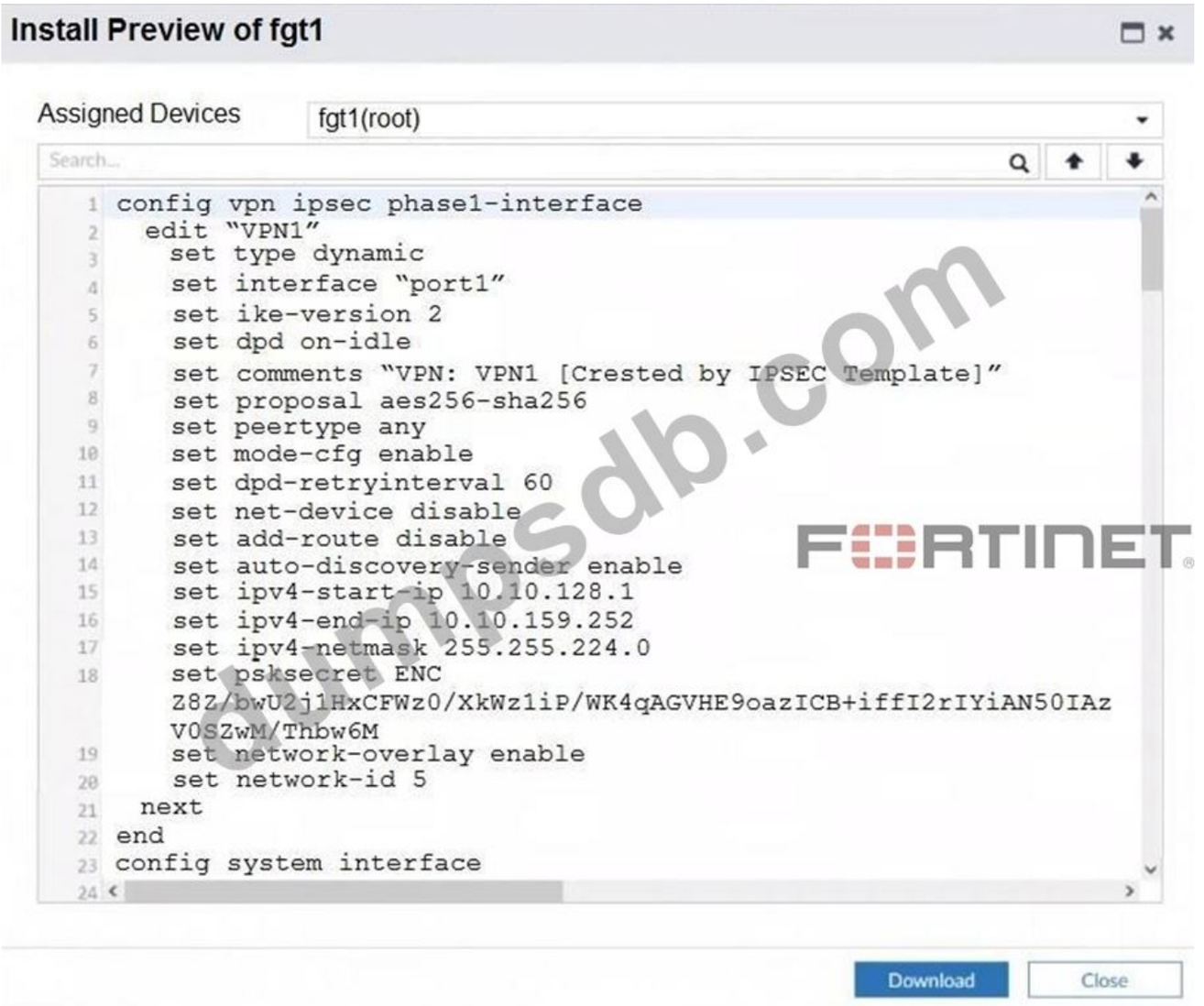
Answer: (SHOW ANSWER)

The rule is in priority mode with HUB1-VPN1 (seq 4) as the first preferred member, HUB1-VPN2 second, and HUB1-VPN3 third. Latency itself does not cause HUB1-VPN3 to become preferred unless a higher- priority member fails SLA. If HUB1-VPN1's latency exceeds the SLA threshold (here simulated by latency reaching 200 ms), FortiGate stops using it and moves down the priority list. That is when HUB1-VPN3 could become the active path.

NEW QUESTION: 77

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 hub. The local subnet range is 10.10.128.0/23.

B. It is a hub device. It can send ADVPN shortcut offers.

C. It is a hub device. It will automatically discover the spoke devices and add them to the SD-WAN topology.

D. It is a spoke device that establishes dynamic IPsec tunnels to the hub It can send ADVPN shortcut requests.

Answer: B (LEAVE A REPLY)

The phase1-interface shows set type dynamic, set peertype any, and set mode-cfg enablewith an address pool (ipv4-start-ip, ipv4-end-ip, ipv4-netmask). Those are dial-up server settings-i.e., a hub handing out virtual IPs to spokes. It also has set auto- discovery-sender enable, allowing the hub to participate in ADVPN shortcut

negotiation (sending offers).