Fortinet.FCSS_SDW_AR-7.6.v2026-02-20.q45

Exam Code:	FCSS_SDW_AR-7.6
Exam Name:	FCSS - SD-WAN 7.6 Architect
Certification Provider:	Fortinet
Free Question Number:	45
Version:	v2026-02-20
# of views:	119
# of Questions views:	450
https://www.freepdfdumps.com/Fortinet.FCSS_SDW_AR-7.6.v2026-02-20.q45.html	

NEW QUESTION: 1

Refer to the exhibit.

FortiGate policy route

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

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

id=2131427329(0x7f0b0001) vwl_service=1(Critical-DIA), vwl_mbr_seq=2 1 dscp_tag=0xfc 0xfc flags=
0x0 tos=0x0
tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(2): oif=4(port2), oif=3(port1)
source(1) : 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(2): Salesforce(16920,0) SMTP_Signed.Email(28991,0)
hit_count=732 rule_last_used=2024-12-12 12:30:16

id=2131427329(0x7f070003) vwl_service=3(Corp), vwl_mbr_seq=4 5 6 dscp_tag=0xfc 0xfc flags=0x0
tos=0x0 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(3): oif=20(HUB1-VPN1), oif=21(HUB1-VPN2), oif=22(HUB1-VPN3)
source(1) : 10.0.1.0-10.0.1.255
destination (1): 10.0.0.0-10.255.255.255
hit_count=0 rule_last_used=2024-12-12 02:29:25

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

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

A. FortiGate steers the traffic from the LAN device 10.0.1.133 to the company SMTP mail server 10.66 0.125 through port3.
B. ForliGate steers the traffic from the LAN device 10.0.1.133 to the company SMTP mail server 10.66.0.125 through port2.
C. FortiGate steers the traffic from the LAN device 10.0.1.133 to the company SMTP mail server 10.66.0.125 through the SD-WAN member ID 4.
D. FortiGate steers the traffic from the LAN device 10.0.1.133 to the SMTP mail server 10.66.0.125 through the SD-WAN member ID 1 or 2.
Answer: D (LEAVE A REPLY)
The policy-route output shows the matching SD-WAN service for destination 10.66.0.0/24 is vwl_service=4 (LAN-to-Corp2) with vwl_mbr_seq=1 2 and paths oif=3(port1) and oif=4(port2). Therefore, traffic from 10.0.1.133 to 10.66.0.125 is steered via SD-WAN member ID 1 or 2.

NEW QUESTION: 2
(In which order does FortiGate consider the following elements during the route lookup process? Choose one answer.)
A. SD-WAN rules, ISDB routes, policy routes, BGP routes
B. Policy routes, SD-WAN rules, Internet Service Database (ISDB) routes, BGP routes
C. SD-WAN rules, policy routes, static routes, ISDB routes
D. Policy routes, ISDB routes, SD-WAN rules, static routes
Answer: D (LEAVE A REPLY)
In FortiOS (including FortiOS 7.6), FortiGate follows a strict and well-defined route lookup order when determining how to forward traffic. This order is critical for understanding SD-WAN behavior and is explicitly referenced in the FCSS SD-WAN curriculum.
The correct lookup sequence is:
Policy routes (Policy-Based Routing)
Policy routes are evaluated first. If traffic matches a policy route, FortiGate immediately forwards the traffic according to that policy and bypasses all other routing mechanisms.
Internet Service Database (ISDB) routes
If no policy route matches, FortiGate checks ISDB routes. These routes match traffic based on Internet Services rather than destination IP prefixes.
SD-WAN rules
If neither a policy route nor an ISDB route matches, FortiGate evaluates SD-WAN rules to determine the outgoing interface based on the configured SD-WAN strategy.
Routing table (connected, static, and dynamic routes such as BGP)
If no SD-WAN rule matches, FortiGate performs a normal routing table lookup.
FIB (Forwarding Information Base)
The FIB is used to forward the packet based on the selected route.
Drop
If no valid route exists, the packet is dropped.

Among the options provided, only Option D correctly reflects the beginning of this sequence by placing policy routes first, followed by ISDB routes, then SD-WAN rules, and finally static routes (representing the routing table).
Therefore, the correct answer is D.

NEW QUESTION: 3
(Which two features must you configure before FortiGate can steer traffic according to SD-WAN rules? Choose two answers.)
A. Security profiles
B. Underlay links
C. Overlay links
D. Traffic shaping
E. Firewall policies
Answer: B,E (LEAVE A REPLY)
For FortiGate to steer traffic using SD-WAN rules, two foundational elements must be in place: available WAN paths (underlay links) and firewall policies that allow traffic to reach the SD-WAN interface.
Underlay links (Option B) are mandatory because SD-WAN operates by selecting among multiple WAN transports (for example, broadband, MPLS, LTE, or IPsec tunnels). These links are configured as SD-WAN members and form the physical or logical paths over which traffic can be steered. Without underlay links, SD-WAN has no paths to evaluate or select.
Firewall policies (Option E) are also mandatory because FortiGate only processes and forwards traffic that is explicitly permitted by a firewall policy. When SD-WAN is enabled, firewall policies must reference the SD-WAN interface or SD-WAN zone as the outgoing interface. If no such policy exists, traffic will not be forwarded and SD-WAN rules will never be evaluated.
Why the other options are incorrect:
Security profiles (Option A) are optional and relate to inspection, not SD-WAN steering.
Overlay links (Option C) are used in specific designs such as ADVPN or hub-and-spoke overlays, but SD-WAN can steer traffic without overlays (for example, DIA-only designs).
Traffic shaping (Option D) is not required for SD-WAN decision-making; it is an optional optimization feature.
Therefore, the two required features that must be configured before FortiGate can steer traffic according to SD-WAN rules are underlay links and firewall policies, which correspond to B and E.

NEW QUESTION: 4
Refer to the exhibit.

BGP configuration

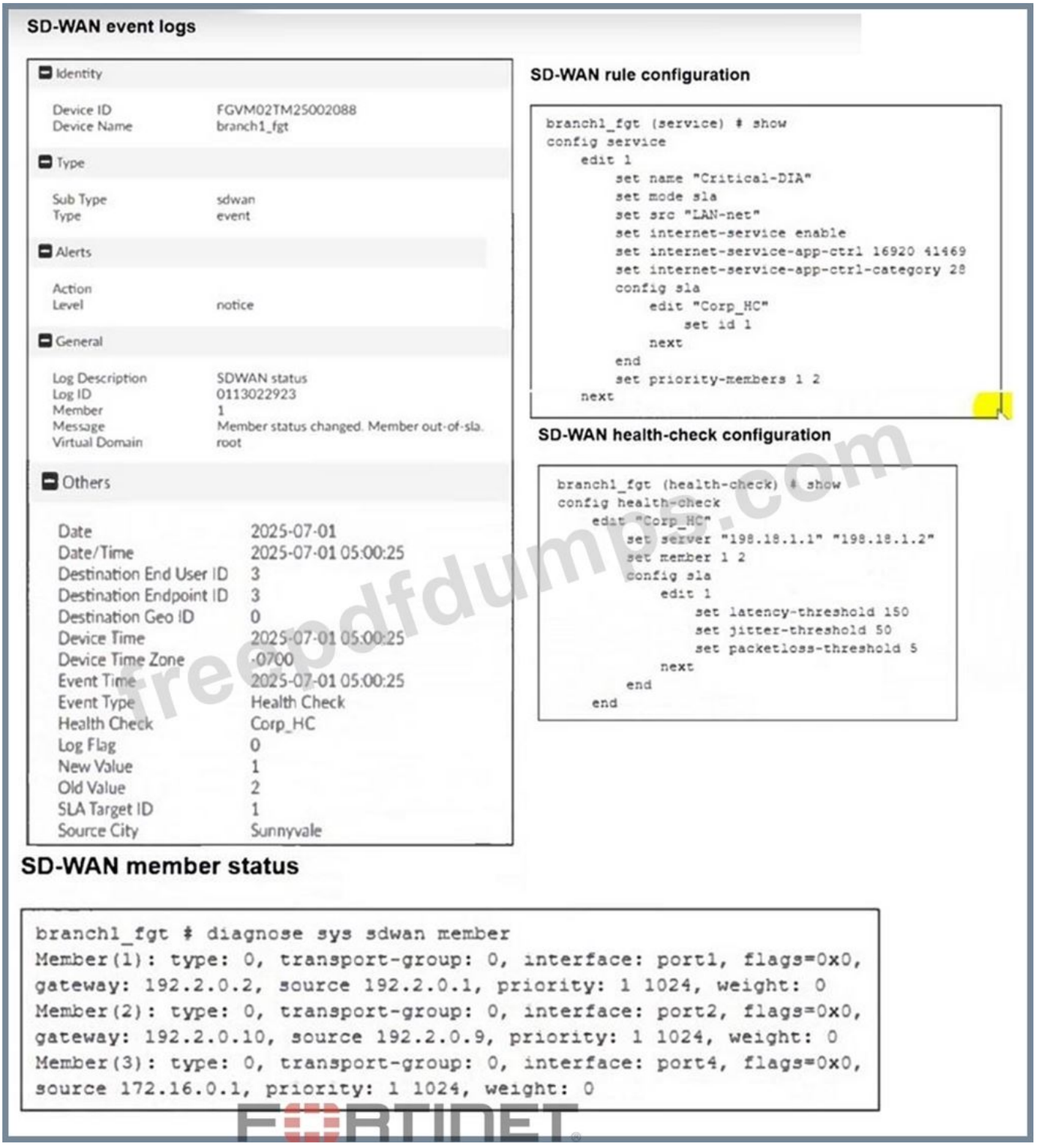
```
config router bgp
     set as 65000
     set router-id 10.200.99.253
     set ibgp-multipath enable
     set additional-path enable
     set additional-path-select 3
     config neighbor-group
          edit "VPN1"
               set soft-reconfiguration enable
               set remote-as 65000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

     end
     …
end
```


The exhibit shows the BGP configuration on the hub in a hub-and-spoke topology. The administrator wants BGP to advertise prefixes from spokes to other spokes over the IPsec overlays, including additional paths. However, when looking at the spoke routing table, the administrator does not see the prefixes from other spokes and the additional paths Which three settings must the administrator configure inside each BGP neighbor group so spokes can learn the prefixes of other spokes and their additional paths? (Choose three.)

A. Set additional-path to send
B. Set additional-path to forward
C. Enable route-reflector-server
D. Enable route-reflector-client.
E. Set adv-additional-path to the number of additional paths to advertise.
Answer: (SHOW ANSWER)
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: 5
(Refer to the exhibits.



Two SD-WAN event logs, the member status, the SD-WAN rule configuration, and the health-check configuration for a FortiGate device are shown.

Immediately after the log messages are displayed, how will the FortiGate steer the traffic based on the information shown in the exhibits? Choose one answer.)

A. FortiGate skips SD-WAN rule ID 1.

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

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

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

Answer: (SHOW ANSWER)

From the SD-WAN rule configuration (service edit 1, "Critical-DIA"), the rule uses mode sla and specifies:
set priority-members 1 2
This means, for traffic matching SD-WAN rule ID 1, FortiGate prefers member 1 first, then member 2, but only if the selected member meets the SLA requirements.
From the SD-WAN event log, the message explicitly states:
Member status changed. Member out-of-sla.
The log includes Member: 1
This indicates SD-WAN member 1 is now out of SLA immediately after the log is generated.
From the SD-WAN member status output:
Member(1) corresponds to interface port1
Member(2) corresponds to interface port2
Because member 1 (port1) is out of SLA, FortiGate cannot use it for an SLA-based rule at that moment. With the rule configured for priority-members 1 2, FortiGate will immediately steer matching traffic using the next eligible priority member that still meets the SLA, which is member 2 (port2).
Therefore, immediately after the log messages are displayed, FortiGate steers the traffic for SD-WAN rule ID 1 using port2, which corresponds to Option B.
Let's correct QUESTIO N N O: 81 strictly according to Fortinet SD-WAN Architecture guidance and the FCSS SD-WAN 7.6 design principles.
Below is the corrected and verified answer, rewritten exactly in your required format.

NEW QUESTION: 6
Refer to the exhibit.

Diagnose output

```
fgt_A # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


fgt_A # diagnose sys sdwan member | grep HUB1
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xd  may_child, gateway: 100.64.1.1,
peer: 192.168.1.29, source 192.168.1.1, priority: 15 1024, weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xd  may_child, gateway: 100.64.1.9,
peer: 192.168.1.61, source 192.168.1.33, priority: 10 1024, weight: 0
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xd  may_child, gateway: 172.16.1.5,
peer: 192.168.1.93, source 192.168.1.65, priority: 1 1024, weight: 0


fgt_A # get router info routing-table all | grep HUB1
S       10.0.0.0/8 [10/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 04:11:41, [1/0]
                    [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 04:11:41, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 04:11:42, [1/0]
                    [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 04:11:42, [1/0]
                    [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 04:11:42, [1/0]
```


An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1_fgt generates traffic to the 10.0.0.0/8 network.

The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over HUB1-VPN1. However, the traffic is routed over HUB1-VPN3.

Based on the output shown in the exhibit, which two reasons, individually or together, could explain the observed behavior? (Choose two.)

A. HUB1-VPN3 has a lower route priority value (higher priority) than HUB1-VPN1.

B. HUB1-VPN1 does not have a valid route to the destination

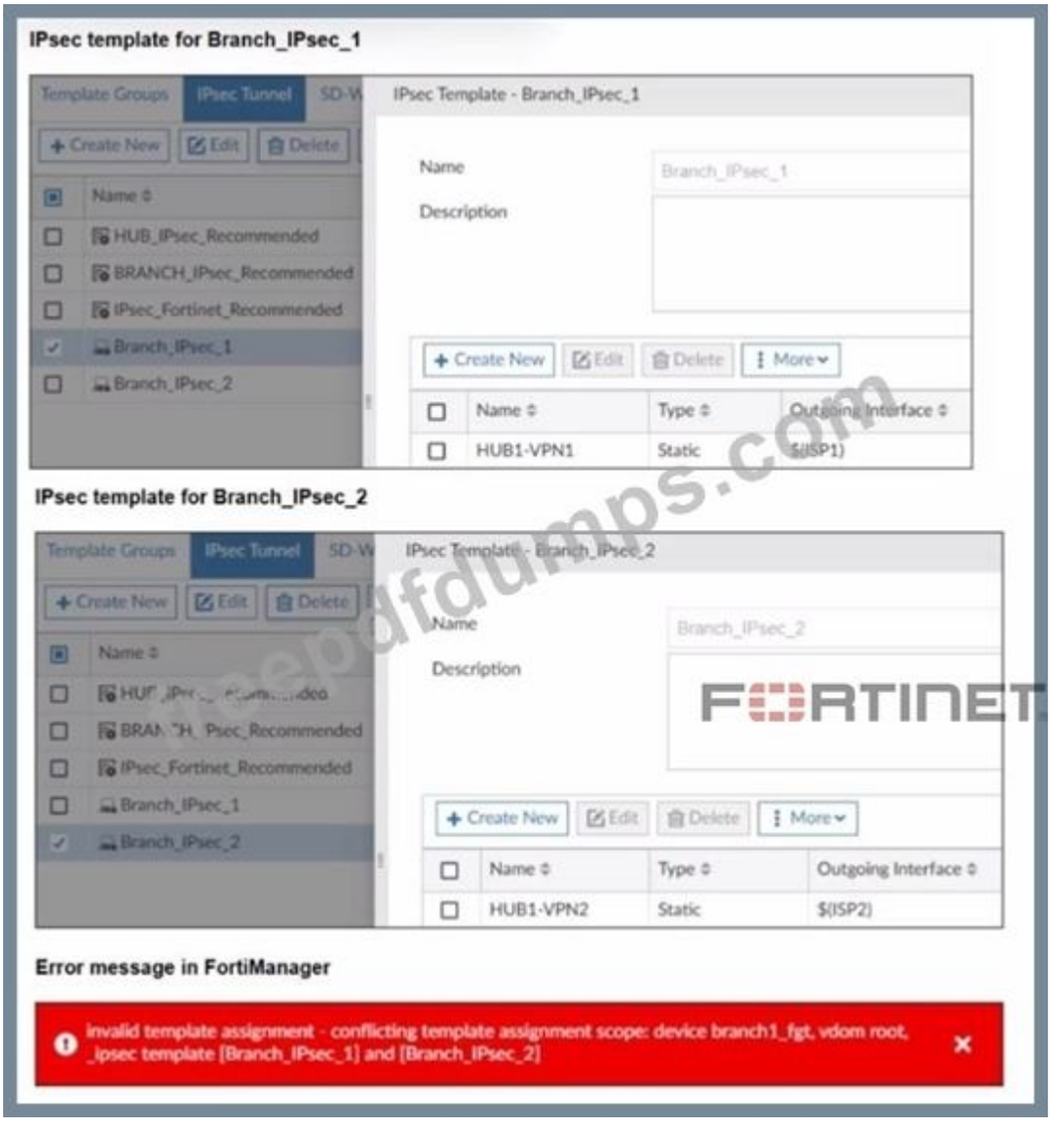
C. HUB1-VPN3 has a higher member configuration priority than HUB1-VPN1.

D. The traffic matches a regular policy route configured with HUB1-VPN3 as the outgoing device

Answer: (SHOW ANSWER)

NEW QUESTION: 7

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.

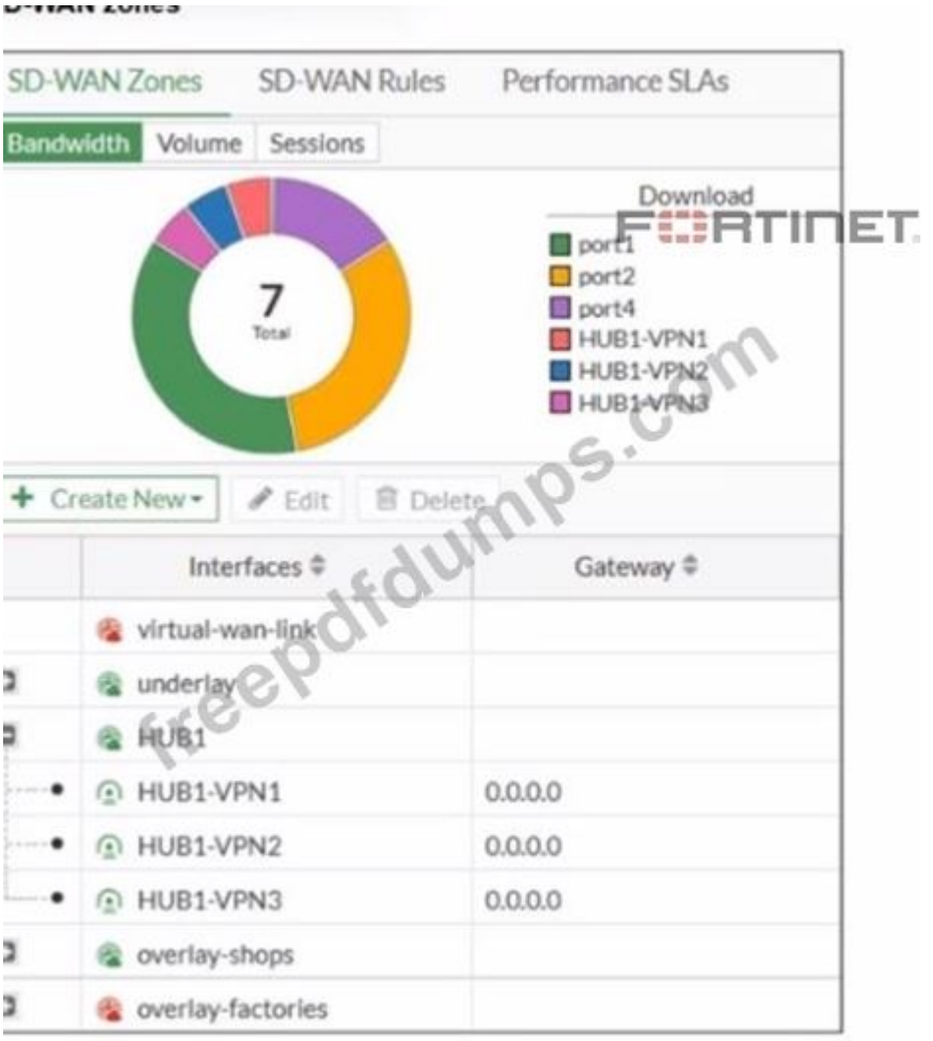
D. You should use the same outgoing interface of both templates.

Answer: B (LEAVE A REPLY)

The FortiManager SD-WAN overlay system allows only one IPsec template to be assigned to each device per overlay operation. The guide clarifies:

"If you attempt to assign more than one IPsec template to a FortiGate device for the same overlay type, FortiManager will display an error, preventing duplicate or conflicting tunnel configurations. This limitation ensures a one-to-one mapping between device and overlay template per operation, maintaining configuration integrity and preventing routing issues." This prevents complex troubleshooting scenarios and enforces best practices for overlay design.

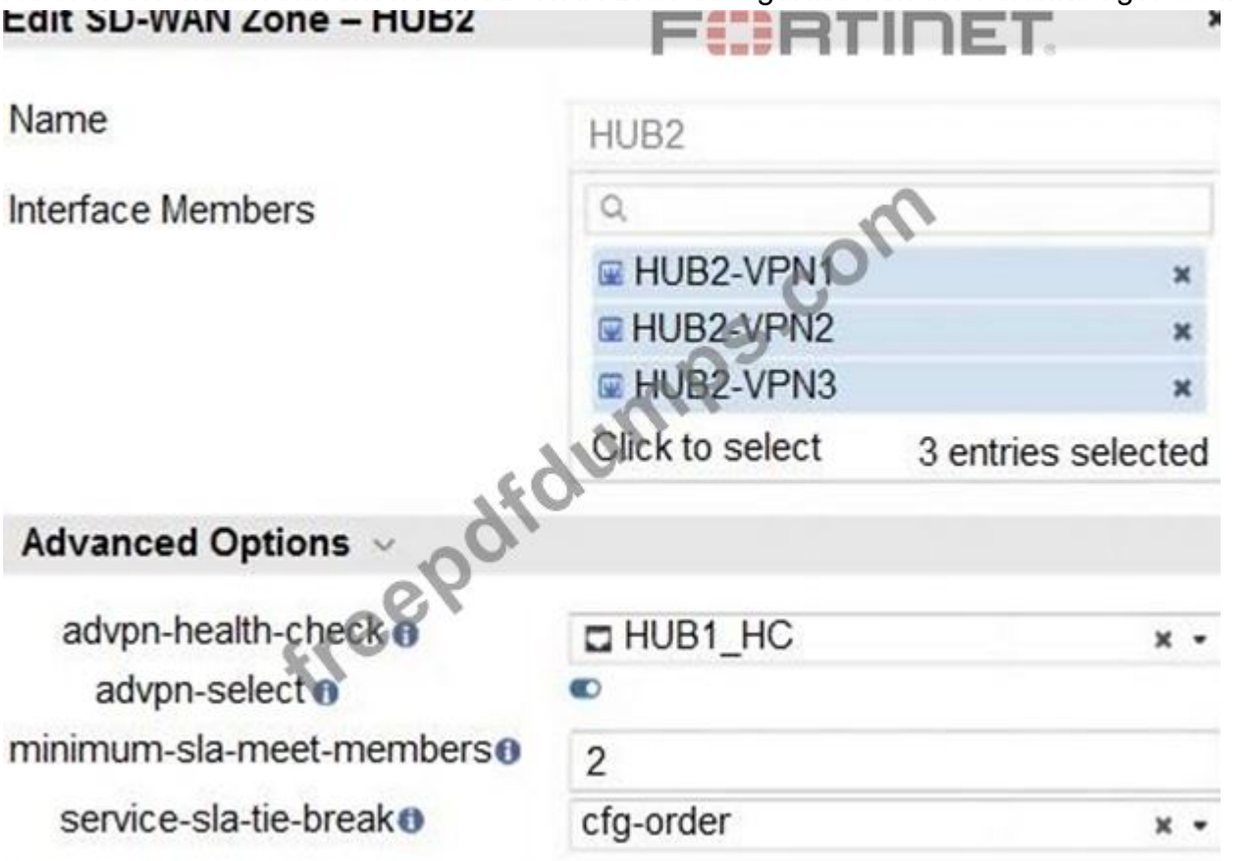
NEW QUESTION: 8
Exhibit.



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: (SHOW ANSWER)
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: 9

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: (SHOW ANSWER)

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: 10

Refer to the exhibit.

Diagnose output

```
fgt_1 # diagnose  sys sdwan service4

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


Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


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


Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


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

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

The exhibit shows output of the command diagnose sys adwan aervice4 collected on a FortiGate device.
The administrator wants to know through which interface FortiGate will steer traffic from local users on subnet 10.0.1.0/255.255.255.192 and with a destination of the social media application Facebook.
Based on the exhibits, which two statements are correct? (Choose two.)
A. When FortiGate cannot recognize the application of the flow, it steers the traffic through the preferred member of rule 3, HQ_T1.
B. There is no service defined for the Facebook application, so FortiGate appliesservice rule 3 and directs the traffic to headquarters.
C. FortiGate steers traffic for social media applications according to the service rule 2 and steers traffic through port2.
D. When FortiGate cannot recognize the application of the flow, it load balances the traffic through the tunnels HQ_T1. HQ_T2. HQ_T3.
Answer: C,D (LEAVE A REPLY)
Application-based SD-WAN rules enable intelligent traffic steering. The guide specifies:
"If a flow is identified as belonging to a defined application category (such as social media), FortiGate will match it to the corresponding service rule (rule 2) and route it through the specified interface, such as port2. However, if the application is not recognized during the session setup, the system defaults to load balancing the traffic using the available tunnels according to the policy for unclassified traffic, ensuring continuous connectivity while waiting for application classification." This guarantees both performance and resilience.

NEW QUESTION: 11
Refer to the exhibit.

The administrator configured the SD-WAN rule ID 4 with two members (port1 and port2) and strategy lowest cost (SLA).

What are the two characteristics of the session shown in the exhibit? (Choose two.)

A. FortiGate steered this flow according to an SD-WAN rule 4.

B. FortiGate will never re-evaluate this session.

C. FortiGate steered this flow according to the application detected and the outgoing interface is port3.

D. FortiGate will re-evaluate this session if the outgoing interface goes down.

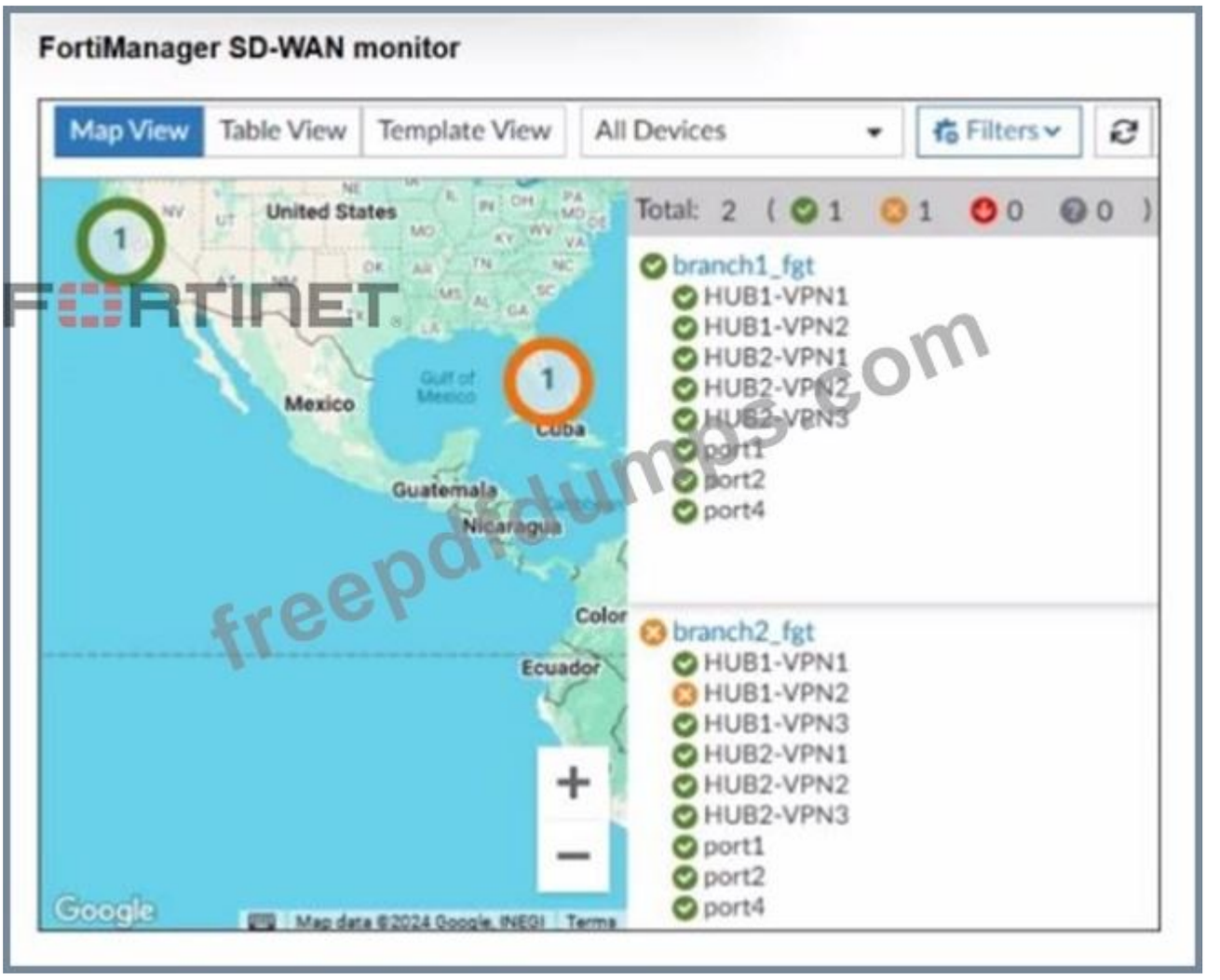
Answer: A,D (LEAVE A REPLY)

The line sdwan_mbr_seq=1 sdwan_service_id=4 indicates that this session is part of an SD-WAN rule. sdwan_service_id=4 confirms that the session is being handled by SD-WAN rule ID 4. This directly links the flow to the SD-WAN configuration.

The line no_offload_reason: redir-to-ips denied-by-nturbo shows that the session is not offloaded to the NPU (Network Processing Unit) and is being processed by the main CPU. A session that is not offloaded can be re-evaluated. If the outgoing interface (the one currently being used) goes down, the FortiGate will re-evaluate the session against the SD-WAN rules to find a new active member to steer the traffic through. This is a fundamental behavior of SD-WAN, which ensures network resilience.

NEW QUESTION: 12

Refer to the exhibit.



An administrator checks the status of an SD-WAN topology using the FortiManager SD-WAN monitor menus. All members are configured with one or two SLAs.

Which two conclusions can you draw from the output shown? (Choose two.)

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

B. One member of branch2_fgt is missing the SLAs.

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

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

Answer: (SHOW ANSWER)

From the SD-WAN monitor in FortiManager:

"The SD-WAN monitor provides a summary view of the branch devices and their members. In the scenario shown, it is clear that branch2_fgt is missing SLA configuration for one member, as evidenced by the lack of performance metrics. The monitor also shows only two branches in the current topology, allowing quick assessment of branch health and configuration completeness."

This kind of visibility is vital for proactive monitoring and rapid troubleshooting in SD-WAN environments.

Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q18]

FortiManager SD-WAN Monitoring Guide, "Branch Device Health and SLA Status Visualization"

NEW QUESTION: 13
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 VPN monitor map view to get a map view of the branches, hub, and tunnel status, including the SLA pass or missed status.
C. 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.
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: (SHOW ANSWER)
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: 14
Exhibit.

```
config vpn ipsec phase1-interface
    edit "VPN1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set exchange-interface-ip enable
        set mode-cfg disable
        set proposal aes256-sha256
    next
    end
end
```


The administrator configured the IPsec tunnel VPN1 on a FortiGate device with the parameters shown in exhibit.
Based on the configuration, which three conclusions can you draw about the characteristics and requirements of the VPN tunnel? (Choose three.)
A. The tunnel interface IP address on the spoke side is provided by the hub.
B. The remote end can be a third-party IPsec device.

C. The administrator must manually assign the tunnel interface IP address on the hub side
D. The remote end must support IKEv2.
E. This configuration allows user-defined overlay IP addresses.
Answer: B,C,E (LEAVE A REPLY)
This configuration demonstrates a typical IPsec setup for SD-WAN overlays where the hub side requires a manually defined tunnel IP address, and the spoke can be flexibly configured, including interoperability with third-party IPsec devices. As described in the Fortinet SD-WAN Architect Guide: "For some overlays, the tunnel interface IP is configured statically on the hub side, which allows more control over overlay subnetting and facilitates the use of user-defined overlay IP addresses. This approach is also a requirement for compatibility with non-FortiGate endpoints, such as third-party IPsec devices that may not support dynamic address assignment via IKE or proprietary mechanisms." This enables hybrid SD-WAN environments and advanced designs involving external partners or cloud services. Overlay IP flexibility is critical for route control and segmentation.
Reference:
[FCSS_SDW_AR-7.4 1-0.docx Q11]
FortiOS 7.4 SD-WAN Reference Architecture, "Overlay IP Address Management" SD-WAN 7.4 Concept Guide, Section: "Interoperability with Third-Party Devices"

NEW QUESTION: 15
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: 16
Refer to the exhibit that shows a diagnose output on FortiGate.

```
pke_fgt # diagnose sys sdwan advpn-session
Session head(jfk-0-HUB1:1)
(1) Service ID(3), last access(4136110), remote health check info(3)
Selected path: local(HUB1-VPN1, port1) gw: 192.2.0.1 remote IP: 203.0.113.1
(192.168.1.2)
Remote information:
1: latency: 1.833133 jitter: 0.482600 pktloss: 0.000000 mos: 4.403007 sla: 0x1
cost: 0 remote gw: HUB1-VPN1 transport_group: 1 bandwidth up: 10239 down: 10239
bidirection: 2048 ipv4: 203.0.113.1(192.168.1.2) ipv6
::1bc2(20e6:7e0c:fe7f:0:1c:256d:487:1bc2)
2: latency: 1.725933 jitter: 0.469833 pktloss: 0.000000 mos: 4.403073 sla: 0x1
cost: 0 remote gw: HUB1-VPN2 transport_group: 1 bandwidth up: 10239 down: 10239
bidirection: 2048 ipv4: 203.0.113.9(192.168.1.66) ipv6
6465:7228:3229:2c20:6c6f:6361:6c20:636f(7374:2830:292c:2073:6563:7465:6400)
3: latency: 1.240333 jitter: 0.269700 pktloss: 0.000000 mos: 4.403513 sla: 0x1
cost: 0 remote gw: HUB1-VPN3 transport_group: 0 bandwidth up: 9999999 down:
9999999 bidirection: 19999998 ipv4: 172.16.0.9(192.168.1.130)
```


Based on the output shown in the exhibit, what can you say about the device role and how it handles health checks?

A. The device is a spoke. It receives health-check measures for the tunnels of another spoke.

B. The device is a hub. It receives embedded health-check measures for each tunnel from the spoke.

C. The device is a spoke. It provides embedded health-check measures for each tunnel to the hub.

D. The device is a hub. It receives health-check measures for the tunnels of a spoke.

Answer: C (LEAVE A REPLY)

The diagnose output shows multiple ADVPN tunnels (HUB1-VPN1, HUB1-VPN2, HUB1-VPN3) with detailed latency, jitter, and packet loss values being reported for each. In ADVPN, the spoke performs embedded health checks and provides the hub with the performance metrics for each tunnel. Therefore, the device in the exhibit is a spoke, and it is sending health-check measurements for each tunnel to the hub.

NEW QUESTION: 17

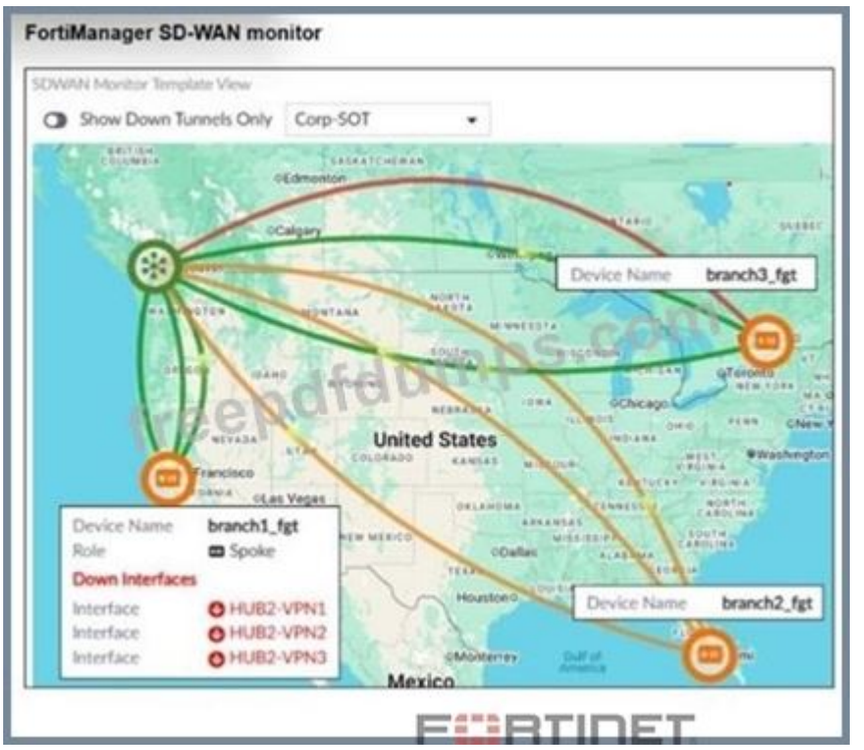
(You configure the overlay tunnels for an SD-WAN hub-and-spoke topology defined with IPsec tunnels, BGP on loopback, and dynamic BGP.

Which are two recommended IPsec settings for this topology? Choose two answers.)

A. On the spoke, configure the parameter localid.
B. On the hub, set the parameter mode-cfg to enable.
C. On the hub, set the tunnel type to static.
D. On the spoke, set the parameter net-device to enable.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
The administrator uses the FortiManager SD-WAN overlay template to prepare an SD-WAN deployment. Using information provided through the SD-WAN overlay template wizard, FortiManager creates templates ready to install on the spoke and hub devices.
What are the three templates created by the SD-WAN overlay template for a spoke device? (Choose three.)
A. Static route template
B. Rules template
C. CLI template
D. BGP template
E. IPsec tunnel template
Answer: B,D,E (LEAVE A REPLY)
Rules template → Defines the SD-WAN rules for traffic steering.
BGP template → Configures dynamic routing for overlay tunnels.
IPsec tunnel template → Builds the IPsec VPN tunnels from the spoke to the hubs.

NEW QUESTION: 19
(You are using the FortiManager SD-WAN monitor menus to check the status of an SD-WAN topology. When you place the mouse next to branch1_fgt, you receive the output shown in the exhibit.



Which two conclusions can you draw from the output shown in the exhibit? Choose two answers.)

A. branch1_fgt is configured with six SD-WAN overlay tunnels and three are down.

B. The template Corp-SOT defines a dual-hub topology.

C. branch3_fgt is configured with three SD-WAN overlay tunnels and one is down.

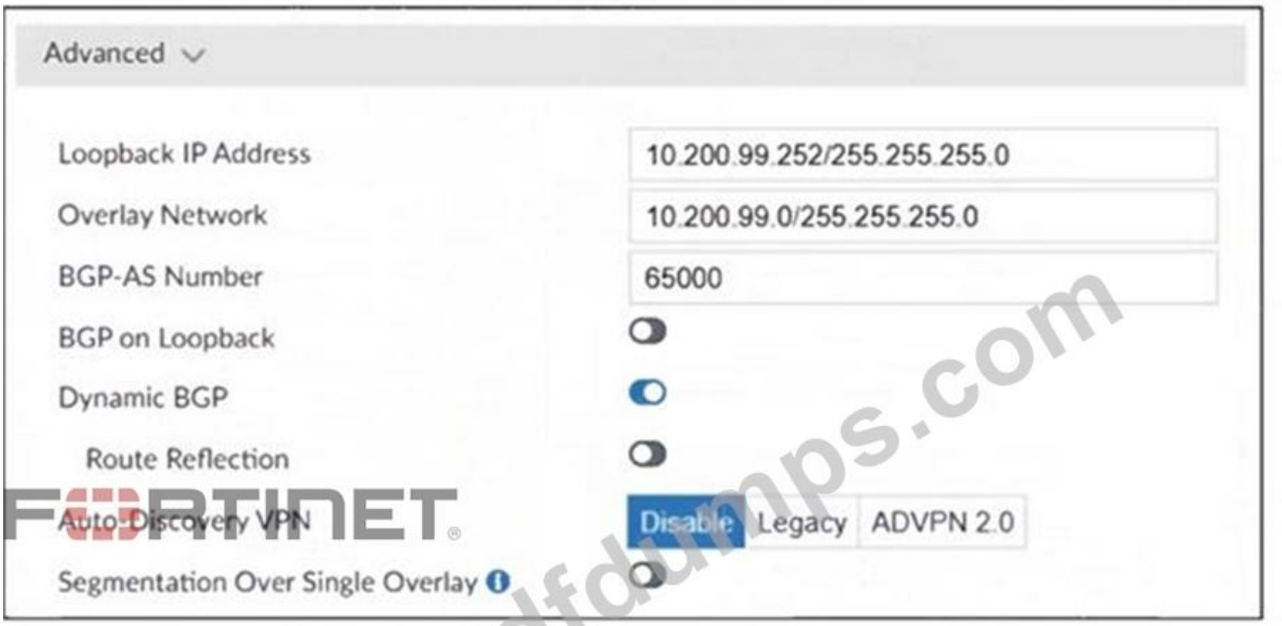
D. Three spokes have tunnels that are out of SLA.

Answer: (SHOW ANSWER)

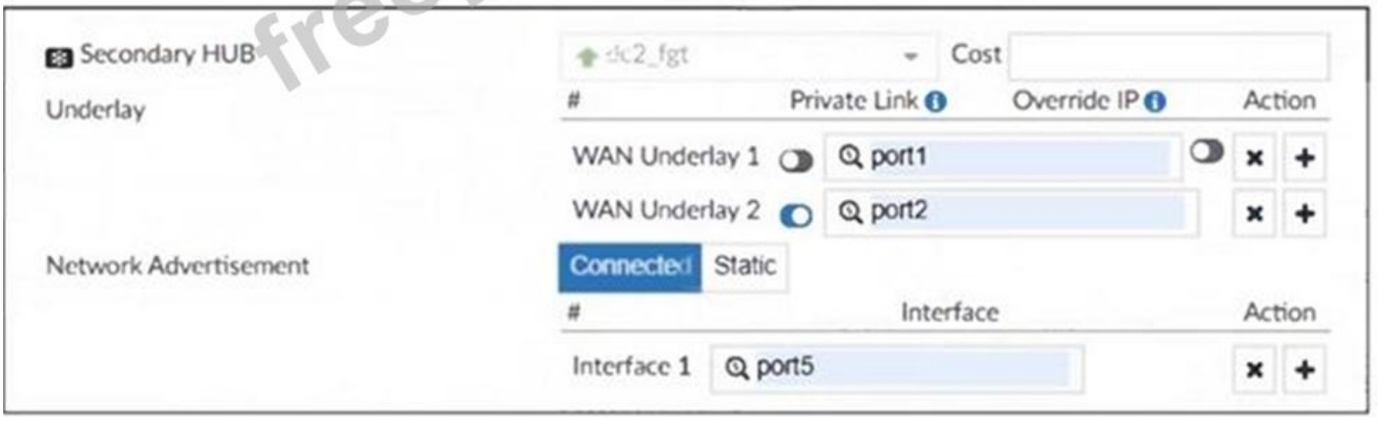
NEW QUESTION: 20

(Refer to the exhibits.

SD-WAN overlay template advanced settings



Underlay and network advertisement configuration



The SD-WAN overlay template advanced settings and the underlay and network advertisement settings are shown. These are the configurations for the secondary hub of a dual-hub SD-WAN topology created with the FortiManager SD-WAN overlay orchestrator.

Which two conclusions can you draw from the information shown in the exhibits? Choose two answers.)

A. FortiManager will define port2 as a BGP neighbor.

B. FortiManager will create an overlay tunnel on the port2 interface.

C. FortiManager will create an overlay tunnel on the port1 interface.

D. FortiManager will define port5 as a BGP neighbor.

Answer: B,C (LEAVE A REPLY)

From the Underlay and network advertisement configuration exhibit for the Secondary HUB:

Under Underlay, the template explicitly lists:

WAN Underlay 1 = port1

WAN Underlay 2 = port2

In FortiManager SD-WAN Overlay Orchestrator, underlay interfaces selected for a hub are the transports used to build the overlay IPsec tunnels (one overlay per underlay, per peer as defined by the template). Because both port1 and port2 are configured as underlays, FortiManager will build overlay tunnels over both underlay links. That supports:
Option C (overlay tunnel on port1)
Option B (overlay tunnel on port2)
For the BGP neighbor options:
The Network Advertisement section shows Interface 1 = port5, which indicates a LAN/internal interface whose connected or static networks may be advertised into the overlay routing domain. This does not make port5 a BGP neighbor interface; it is the interface whose routes are being advertised.
The template indicates Dynamic BGP is enabled. In Overlay Orchestrator designs, BGP neighbor relationships are formed across the overlay tunnel interfaces / overlay endpoints, not directly on the raw underlay interfaces (port1/port2) and not on the advertised LAN interface (port5).
Therefore, options A and D are not valid conclusions from what is shown.
So, the two correct conclusions are B and C.

NEW QUESTION: 21
The FortiGate devices are managed by ForliManager, and are configured for direct internet access (DIA). You confirm that DIA is working as expected for each branch, and check the SD-WAN zone configuration and firewall policies shown in the exhibits.

SD-WAN Zones

SD-WAN Zones

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

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

Firewall Policy

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

Then, you use the SD-WAN overlay template to configure the IPsec overlay tunnels. You create the associated SD-WAN rules to connect existing branches to the company hub device and apply the changes on the branches.

After those changes, users complain that they lost internet access. DIA is no longer working.

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

A. The SD-WAN overlay template defines a zone for each underlay interface and moves the interfaces into those zones.
B. The SD-WAN overlay template didn't configure a firewall policy to allow traffic through the overlay.
C. The SD-WAN overlay template redefines the interface gateway addresses if they are defined with metadata variables.
D. The SD-WAN overlay template updates the SD-WAN template and the rules.
Answer: A (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: 22
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: 23

The SD-WAN overlay template helps to prepare SD-WAN deployments. To complete the tasks performed by the SD-WAN overlay template, the administrator must perform some post-run tasks. What are two mandatory post-run tasks that must be performed? (Choose two.)

A. Configure routing through the overlay tunnels created by the SD-WAN overlay template.

B. Create policy packages and assign them to the branch devices.

C. Assign a hub id metadata variable to each hub device.

D. Configure SD-WAN rules

E. Assign an sdwan_id metadata variable to each device (branch and hub)

Answer: B,D (LEAVE A REPLY)

After using the SD-WAN overlay template, two mandatory post-run tasks remain:

"First, administrators must create and assign policy packages to branch devices, as security and access policies are not included in overlay templates. Second, SD-WAN rules must be configured so that traffic can be matched and steered appropriately through the established overlays. Neglecting either task results in ungoverned traffic or inefficient routing, undermining the benefits of SD-WAN." Templates automate topology, but policy and rule definition are critical for operational effectiveness.

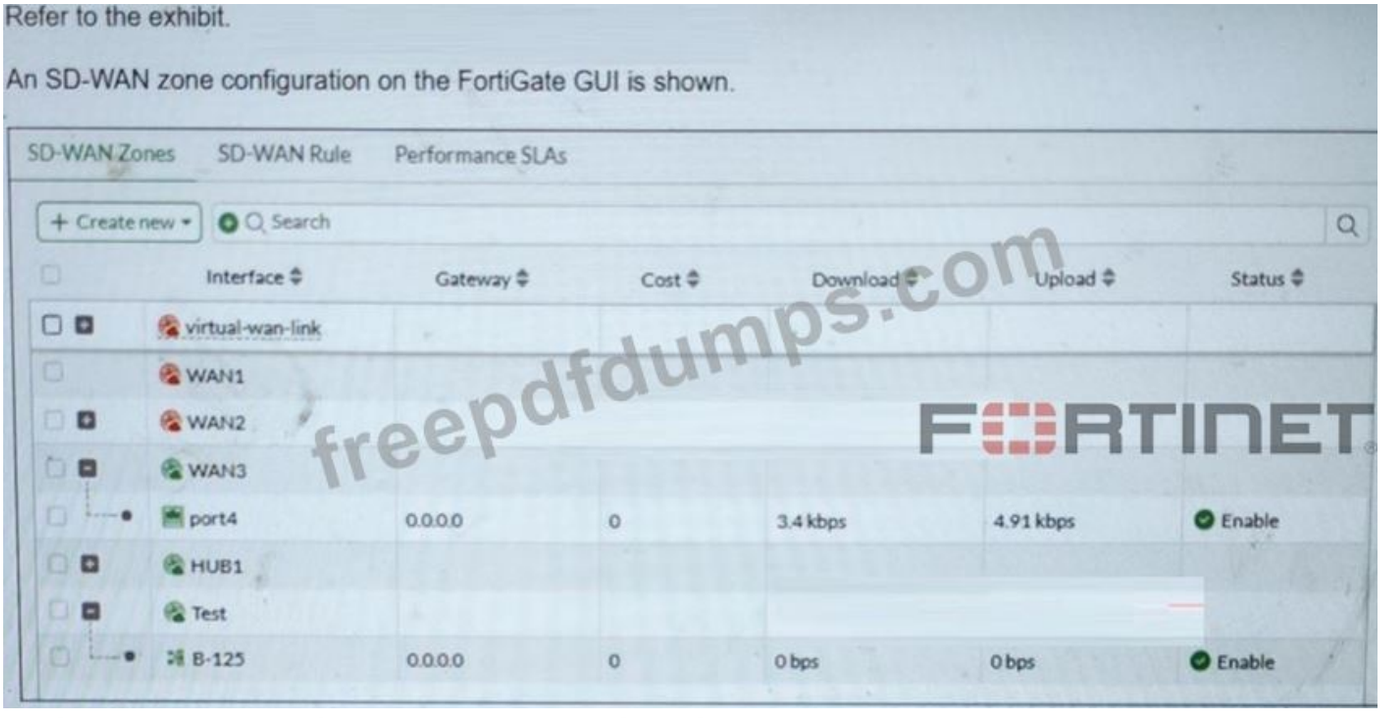
Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q25]

Fortinet SD-WAN Reference Architecture 7.4, "Post-Deployment Tasks for SD-WAN Overlay Templates"

NEW QUESTION: 24

Refer to the exhibit.



An SD-WAN zone configuration on the FortiGate GUI is shown.

What can you conclude about the zone and member configuration on this device? Choose one answer.)

A. You can delete the virtual-wan-link zone.
B. The WAN2 zone contains no member.
C. You can delete the WAN1 zone.
D. You can add the member B-125 to the WAN3 zone and keep it as a member of the Test zone.
Answer: B (LEAVE A REPLY)
From the SD-WAN Zones view in the FortiGate GUI:
virtual-wan-link is the default SD-WAN zone. This zone is system-defined and cannot be deleted, which makes option A incorrect.
The WAN2 zone is displayed without any expandable members beneath it, indicating that no SD-WAN members are currently assigned to the WAN2 zone. This directly supports option B.
A zone can be deleted only if it has no members and is not system-defined, but the exhibit does not indicate that WAN1 is eligible for deletion. Therefore, option C cannot be concluded from the information shown.
In FortiOS SD-WAN, an SD-WAN member can belong to only one SD-WAN zone at a time. A member such as B-125 cannot be assigned to both the WAN3 zone and the Test zone simultaneously, which makes option D incorrect.

NEW QUESTION: 25
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 3dwan_service_id.
Answer: D (LEAVE A REPLY)
When using the diagnose sys session list command, SD-WAN-specific session steering is indicated by the presence of the sdwan_service_id field in the session data. This identifier ties the session directly to a specific SD-WAN rule or service. As noted in the Fortinet documentation: "Sessions that are handled according to SD-WAN rules will include a service ID tag (sdwan_service_id) in their session listing. This allows administrators to correlate live sessions with SD-WAN policy matches for troubleshooting and visibility." This is a crucial diagnostic tool, as it distinguishes between traffic managed by traditional routing and that explicitly controlled by SD-WAN steering logic, aiding in operational insight and troubleshooting.
Reference:
[FCSS_SDW_AR-7.4 1-0.docx Q15]
FortiOS 7.4 CLI Reference, "diagnose sys session list: SD-WAN Service ID Tagging" SD-WAN 7.4 Concept Guide, Section: "Session Identification for SD-WAN Traffic"

NEW QUESTION: 26
As an IT manager for a healthcare company, you want to delegate the installation and management of your SD-WAN deployment to a managed security service provider (MSSP). Each

site must maintain direct internet access and ensure that it is secure. You expected significant traffic flow between the sites and want to delegate as much of the network administration and management as possible to the MSSP.
Which two MSSP deployment blueprints best address the customer's requirements? (Choose two.)
A. Use a shared hub at the MSSP premises with a dedicated VDOM for the new customer, and install the spokes at the customer premises.
B. Use a shared hub at the MSSP premises and a dedicated hub at the customer premises and install the spokes at the customer premises.
C. Install a dedicated hub at the MSSP premises for the new customer, and install the spokes at the customer premises.
D. Install the hub and spokes at the customer premises and enable the MSSP to manage the SD-WAN deployment using FortiManager with a dedicated ADOM.
Answer: A,C (LEAVE A REPLY)
Hosting the hub at the MSSP centralizes installation, security, and ongoing management while each site (spoke) keeps local DIA. This can be done multi-tenant with a shared hub using a dedicated VDOM or with a fully dedicated hub per customer for stricter isolation and control, both meeting the requirement to delegate administration to the MSSP and support high inter-site traffic.

NEW QUESTION: 27
Refer to the exhibit.

An administrator configures SD-WAN rules for a DIA setup using the FortiGate GUI. The page to configure the source and destination part of the rule looks as shown in the exhibit. The GUI page shows no option to configure an application as the destination of the SD-WAN rule Why?
A. You must enable the feature on the CLI.
B. FortiGate allows the configuration of applications as the destination of SD-WAN rules only 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: (SHOW ANSWER)

NEW QUESTION: 28

Refer to the exhibit.

SD-WAN configuration on FortiGate

```
branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [10/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 1d03h58m, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 1d03h58m, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 1d03h58m, [1/0]
C       10.200.99.1/32 is directly connected, Branch-Lo
B       10.2.0.0/16 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 00:03:01, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 00:00:51, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 00:00:51, [1/0]
B       10.2.5.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 00:00:01, [1/0]
...


branch1_fgt # diag sys sdwan service4

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: fib
 Shortcut priority: 2
  Gen(3), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    3: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


Service(4): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(2 port2 underlay), alive, sla(0x3), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(1 port1 underlay), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.2.0.0-10.2.255.255
```


Which SD-WAN rule and interface uses FortiGate to steer the traffic from the LAN subnet 10.0.1.0/24 to the corporate server 10.2.5.254?

A. SD-WAN service rule 3 and interface HUB1-VPN2.

B. SD-WAN service rule 3 and interface HUB1-VPN3.

C. SD-WAN service rule 4 and port1 or port2.

D. SD-WAN service rule 4 and interface port2.

Answer: (SHOW ANSWER)

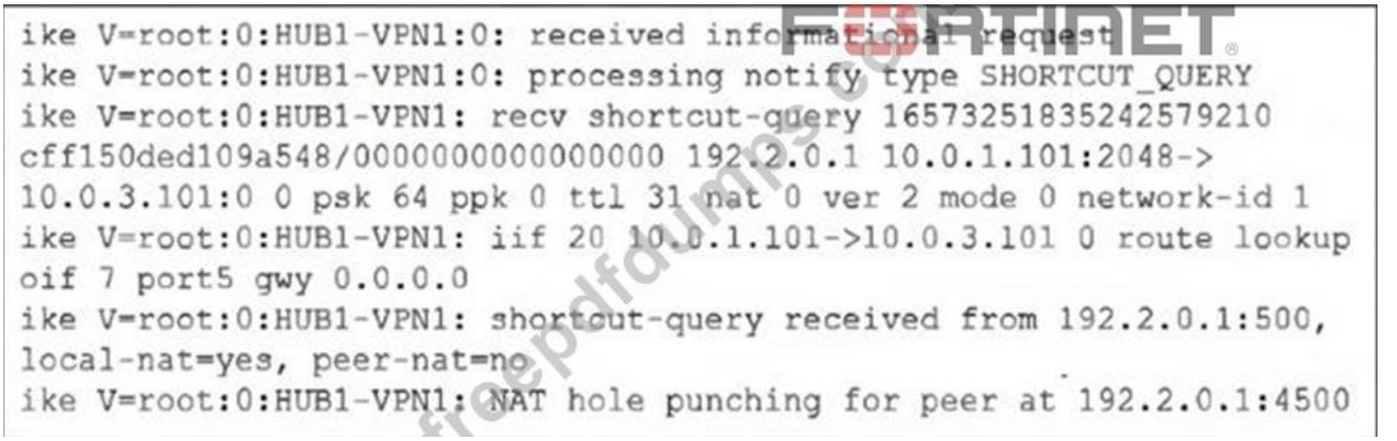
Traffic steering in Fortinet SD-WAN is based on defined rules and the corresponding outgoing interfaces. The exhibit (not shown here) would indicate that the traffic from the LAN subnet 10.0.1.0/24 to the server 10.2.5.254 is matched by SD-WAN rule 3 and sent out via the HUB1-VPN3 interface.
Reference:
[FCSS_SDW_AR-7.4 1-0.docx Q2]
FortiOS 7.4 SD-WAN Concept Guide - Rule Matching

NEW QUESTION: 29
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: B,D,E (LEAVE A REPLY)
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: 30
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.

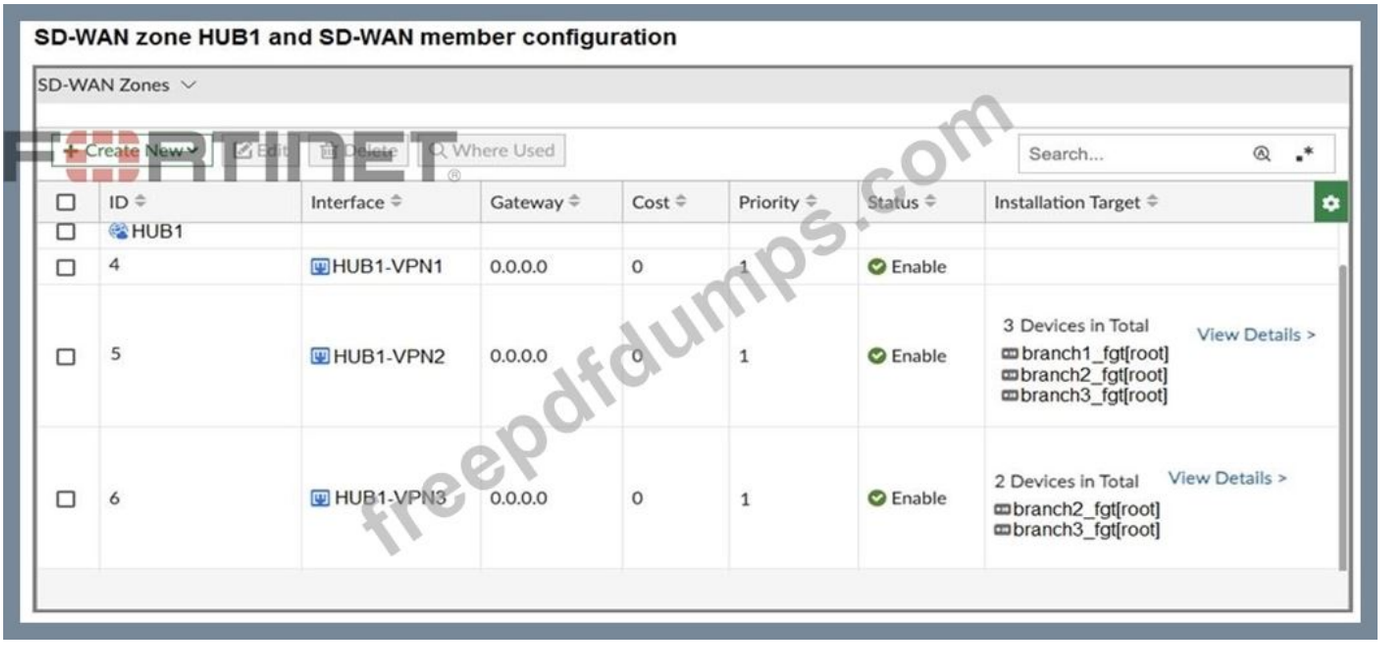
NEW QUESTION: 31
Refer to the exhibit.



Which statement correctly describes the role of the ADVPN device in handling traffic? Choose one answer.)
A. This device is a spoke that has received a direct shortcut query from a remote spoke.
B. This device is a hub, and two spokes, 192.2.0.1 and 10.0.3.101, established a shortcut.
C. This device is a hub that has received a shortcut query from a spoke and has forwarded it to another spoke.
D. This device is a spoke that has received a shortcut query from a remote hub.
Answer: C (LEAVE A REPLY)
The log messages shown in the exhibit include the following key indicators:
processing notify type SHORTCUT_QUERY
shortcut-query received from 192.2.0.1
local-nat=yes, peer-nat=no
NAT hole punching for peer at 192.2.0.1:4500
In the FCSS SD-WAN 7.6 ADVPN workflow, shortcut queries are always initiated by spokes, not hubs. A spoke sends a shortcut query to its hub when it detects traffic destined for another spoke. The hub's role is to receive this shortcut query and forward the discovery information toward the destination spoke, enabling the two spokes to build a direct shortcut tunnel.

The device name in the log (HUB1-VPN1) and the presence of NAT hole punching coordination clearly indicate that this device is acting as a hub, not a spoke. Hubs do not form shortcuts themselves; instead, they facilitate shortcut establishment between spokes by relaying discovery and negotiation information.
Option A is incorrect because a spoke does not receive shortcut queries from other spokes directly.
Option B is incorrect because the log does not indicate that the shortcut has already been established; it shows the query and coordination phase, not completion.
Option D is incorrect because hubs do not initiate shortcut queries toward spokes.
Therefore, the correct description is that this device is a hub that has received a shortcut query from a spoke and has forwarded it to another spoke, which corresponds to option C.

NEW QUESTION: 32
Refer to the exhibits.



SD-WAN zone HUB2 and SD-WAN member configuration

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

Output of command `diagnose sys sdwan member`

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

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

Which statement best describes what the diagnose output shows?

A. The diagnose output shows that HUB1-VPN1 and all HUBx-VPNy members are dead.

B. The diagnose output does not correspond to a device configured with the SD-WAN template shown in the exhibit.

C. The diagnose output was collected on the device branch2_fgt.

D. The diagnose output was collected on the device branch1_fgt

Answer: (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: 33

Your FortiGate is in production. To optimize WAN link use and improve redundancy, you enable and configure SD-WAN.

What must you do as part of this configuration update process?

A. Replace references to interfaces used as SD-WAN members in the routing configuration.

B. Purchase and install the SD-WAN license, and reboot the FortiGate device.

C. Replace references to interfaces used as SD-WAN members in the firewall policies.

D. Disable the interface that you want to use as an SD-WAN member.

Answer: C (LEAVE A REPLY)

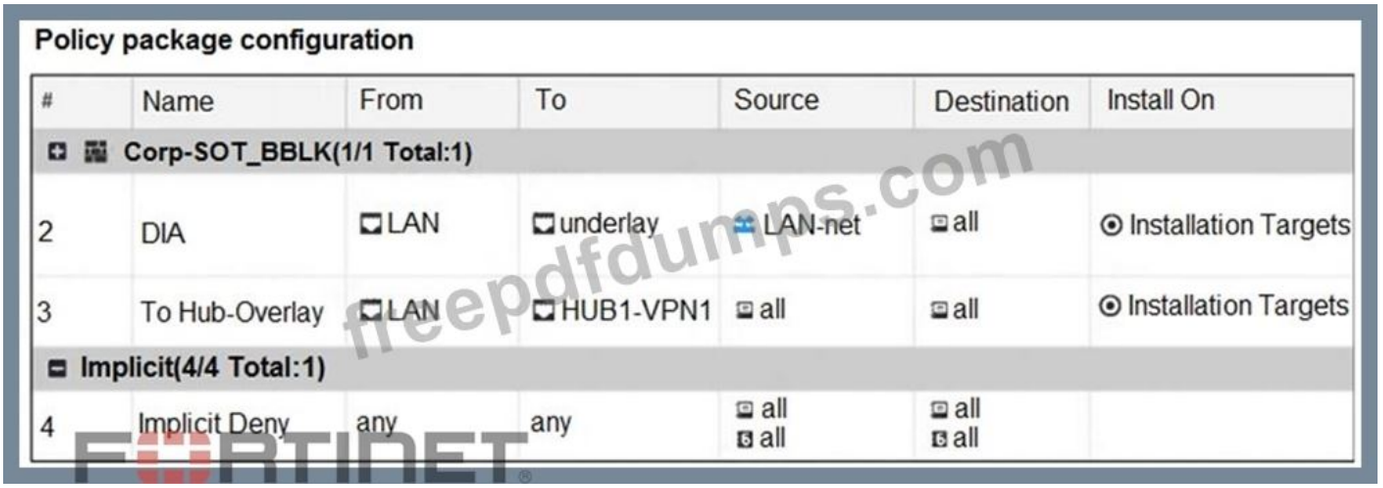
In FortiOS 7.6, when SD-WAN is enabled, physical and logical WAN interfaces are added as SD-WAN members and are abstracted behind the SD-WAN interface (virtual-wan-link or SD-WAN zone). Traffic forwarding decisions are then made by SD-WAN rules instead of individual interfaces.
As documented in the FCSS SD-WAN 7.6 curriculum and Fortinet SD-WAN architecture guides, firewall policies must reference the SD-WAN interface or SD-WAN zone, not the individual WAN interfaces that are members of SD-WAN. Therefore, during the configuration update process, existing firewall policies that reference physical WAN interfaces must be updated to reference the SD-WAN interface.
Option A is incorrect because routing configuration does not require replacing interface references when SD-WAN is enabled. Static and dynamic routes typically point to the SD-WAN interface automatically, and SD-WAN rules handle path selection.
Option B is incorrect because SD-WAN is a built-in FortiOS feature. It does not require a separate license and does not require a reboot when enabled.
Option D is incorrect because interfaces must remain enabled to function as SD-WAN members. Disabling an interface would prevent SD-WAN from using it for traffic forwarding.
Therefore, the required action during the SD-WAN configuration update process is to replace references to interfaces used as SD-WAN members in the firewall policies, which corresponds to option C.

NEW QUESTION: 34
(You are configuring SD-WAN to load balance network traffic and you want to take into account the link quality.
Which two facts should you consider? Choose two answers.)
A. When applicable, FortiGate load balances the traffic through all members that meet the SLA target.
B. You can select the best quality strategy and allow SD-WAN load balancing.
C. You can select the lowest cost service level agreement (SLA) strategy and allow SD-WAN load balancing.
D. The best quality strategy supports only the round-robin hash mode.
Answer: A,C (LEAVE A REPLY)
When SD-WAN load balancing is required with link quality awareness, FortiOS relies on SLA-based strategies. These strategies evaluate link performance using performance SLAs (latency, jitter, packet loss, MOS) and then make forwarding decisions accordingly.
Option A is correct.
In FortiOS 7.6, when an SLA-based SD-WAN rule has load balancing enabled, FortiGate distributes traffic only across the members that meet the SLA targets. Any member that is out of SLA is excluded from load balancing. This behavior ensures that traffic is not forwarded over degraded links while still allowing load distribution across healthy paths.
Option C is correct.

The lowest cost (SLA) strategy is an SLA-based strategy that considers link quality while also allowing SD-WAN load balancing. When multiple members meet the SLA requirements and have equal cost, FortiGate can load balance traffic across them using the configured hash mode. This makes the lowest cost SLA strategy suitable when both link quality and load balancing are required.
Why the other options are incorrect:
Option B is incorrect because the best quality strategy is designed to select the single best-performing link based on SLA metrics. It does not support SD-WAN load balancing across multiple links.
Option D is incorrect because the best quality strategy does not support load balancing at all, so the statement about round-robin hash mode is invalid.
Therefore, the two correct facts to consider are A and C.

NEW QUESTION: 35
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 majority of the branch traffic is directed to a corporate data center.
B. The customer requires SIA with centralized breakout.
C. The administrator expects a large volume of traffic between the branches.
D. The customer expects a large amount of VoIP traffic.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 36
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: 37

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: (SHOW ANSWER)

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: 38
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-mode setting.
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_dirty and vwl_def ault.
Answer: A,D (LEAVE A REPLY)
The implicit SD-WAN rule serves as the final catch-all. Per Fortinet:
"Sessions matching the implicit SD-WAN rule do not have an SD-WAN service id, as they are not associated with any specific user-defined SD-WAN rule. Additionally, this occurs only when traffic fails to match any entry in the policy route table. This default handling guarantees connectivity while minimizing the risk of blackholed traffic." Administrators can observe this in diagnostic outputs for troubleshooting.

NEW QUESTION: 39
Refer to the exhibits.

Global System configuration

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

Interface port2 configuration

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

Routing Table on FortiGate

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

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


The exhibits show the source NAT (SNAT) global setting. port2 interface settings, and the routing table on FortiGate.

The administrator increases the member priority on port2 to 20.

Upon configuration changes and the receipt of new packets, which two actions does FortiGate perform on existing sessions established over port2? (Choose two.)

A. FortiGate continues routing all existing sessions over port2.

B. FortiGate routes only new sessions over port2.

C. FortiGate flags the SNAT session as dirty only if the administrator has assigned an IP pool to the firewall policies with NAT.

D. FortiGate flags the sessions as dirty.

E. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: D,E (LEAVE A REPLY)

When the member priority of a port is increased (e.g., port2 to 20), FortiGate evaluates existing sessions and applies "dirty" flags where applicable. The SD-WAN session management mechanism is described in detail: "Upon a change in SD-WAN member priority, all existing sessions using that member are marked as dirty. For SNAT sessions, the gateway information is updated to ensure future packets are routed through the newly preferred member, in this case,

port1. This automatic re-evaluation allows SD-WAN to dynamically respond to topology or priority changes, maintaining optimal routing." This is fundamental to seamless failover and session persistence in Fortinet SD-WAN, ensuring active flows are redirected based on updated priorities or health status.
Reference:
[FCSS_SDW_AR-7.4 1-0.docx Q13]
FortiOS 7.4 SD-WAN Concept Guide, "Session Management During Path Change" FortiGate CLI Reference: diagnose sys session list

NEW QUESTION: 40
(As an IT manager, you want to delegate the installation and management of your SD-WAN deployment to a managed security service provider (MSSP). Each site must maintain direct internet access and be secure. You expect significant traffic flow between the sites and want to delegate as much of the network administration and management as possible to the MSSP.
Which two MSSP deployment blueprints address your requirements? Choose two answers.)
A. Install a dedicated hub on the MSSP premises for the customer, and install the spokes on the customer premises.
B. Use a shared hub on the MSSP premises with a dedicated VDOM for the customer, and install the spokes on the customer premises.
C. Install the hub and spokes on the customer premises, and enable the MSSP to manage the SD-WAN deployment using FortiManager with a dedicated ADOM.
D. Use a shared hub on the MSSP premises and a dedicated hub on the customer premises, and install the spokes on the customer premises.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
(Refer to the exhibit.

```
pke_fgt # diagnose sys sdwan advpn-session
Session head(jfk-0-HUB1:1)
(1) Service ID(3), last access(4136110), remote health check info(3)
Selected path: local(HUB1-VPN1, port1) gw: 192.2.0.1  remote IP: 203.0.113.1(192.168.1.2)
Remote information:
1: latency: 1.833133 jitter: 0.482600 pktloss: 0.000000 mos: 4.403007 sla: 0x1 cost: 0 remote gw: HUB1-VPN1
transport_group: 1 bandwidth up: 10239 down: 10239 bidirection: 20478 ipv4: 203.0.113.1(192.168.1.2) ipv6
::1bc2(20e6:7e0c:fe7f:0:1c:256d:487:1bc2)
2: latency: 1.725933 jitter: 0.469833 pktloss: 0.000000 mos: 4.403073 sla: 0x1 cost: 0 remote gw: HUB1-VPN2
transport_group: 1 bandwidth up: 10239 down: 10239 bidirection: 20478 ipv4: 203.0.113.9(192.168.1.66) ipv6
6465:7228:3229:2c20:6c6f:6361:6c20:636f(7374:2830:292c:2073:656c:6563:7465:6400)
3: latency: 1.240333 jitter: 0.269700 pktloss: 0.000000 mos: 4.403513 sla: 0x1 cost: 0 remote gw: HUB1-VPN3
transport_group: 0 bandwidth up: 9999999 down: 9999999 bidirection: 19999998 ipv4: 172.16.0.9(192.168.1.130)
ipv6 ::(::)
```


Based on the output shown in the exhibit, what can you conclude about the device role and how it handles health checks? Choose one answer.)
A. The device is a hub and it receives embedded health-check measures for each tunnel from the spoke.
B. The device is a hub and it receives health-check measures for the tunnels of a spoke.

C. The device is a spoke and it provides embedded health-check measures for each tunnel to the hub.
D. The device is a spoke and it receives health-check measures for the tunnels of another spoke.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
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: A,B,E (LEAVE A REPLY)
Before FortiGate can steer traffic according to SD-WAN rules, certain configuration elements must be present. The guide states:
"SD-WAN is not a standalone feature and interacts with several fundamental FortiGate configurations. Specifically, you must: (1) Define the interfaces (physical, VLAN, or IPsec) that will act as SD-WAN members, (2) Create firewall policies to allow traffic to be steered by SD-WAN, and (3) Set up routing so that traffic has valid routes via SD-WAN members. Without these, SD-WAN rules will not be able to match or steer any traffic." Security profiles and traffic shaping are not mandatory for basic SD-WAN steering but can be layered on for enhanced security and QoS once foundational elements are present.
Reference:
[FCSS_SDW_AR-7.4 1-0.docx Q16]
FortiOS 7.4 SD-WAN Concept Guide, "Prerequisite Configuration Elements for SD-WAN Steering

NEW QUESTION: 43
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. When applicable. FortiGate load balances the traffic through all members that meet the SLA target.
B. Only the manual and best-quality strategies allow SD-WAN load balancing.
C. You can select the outbandwidth hash mode with all strategies that allow load balancing.
D. SD-WAN load balancing is possible only using the best quality and lowest cost (SLA) strategies.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 44

Refer to the exhibit.

FortiGate router policy and diagnose output

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

branch1_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla
use-shortcut
     Tie break: cfg
     Shortcut priority: 2
          Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst
(1->65535), Mode(priority),
          link-cost-factor(latency), link-cost-threshold(10),
health-check(Corp_HC)
          Members(2):
               1: Seq_num(2 port2 underlay), alive, latency:
0.769, selected
               2: Seq_num(1 port1 underlay), alive, latency:
71.022, selected
          Application Control(3): Microsoft.Portal(41469,0)
Salesforce(16920,0) Collaboration (0,28)
          Src address(1):
               10.0.1.0-10.0.1.255

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

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


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

A. FortiGate drops the traffic flow.
B. FortiGate routes the traffic flow according to the forwarding information base (FIB).
C. FortiGate load balances the traffic flow through port7 and port8.
D. FortiGate steers the traffic flow through port7.
Answer: C (LEAVE A REPLY)
The router policy explicitly denies traffic with source 10.0.1.128/25 (which includes 10.0.1.130) and destination 128.66.0.0/24 (which includes 128.66.0.125). Even though SD-WAN service 4 shows members (port1 and port2) alive and available for this traffic, the router policy is evaluated first and blocks it. Therefore, FortiGate drops the traffic flow.

NEW QUESTION: 45
(Refer to the exhibit.

```
London_1 # diagnose sys sdwan service4 3

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

What can you conclude from the output shown? Choose one answer.)
A. It is a spoke device. SD-WAN rule 3 is configured with nine members.
B. It is a spoke device. The members of SD-WAN rule 3 are grouped into two zones.
C. It is a hub device. It allowed the establishment of three auto-discovery VPN (ADVPN) shortcuts.
D. It is a spoke device. SD-WAN rule 4 allows three shortcut tunnels.
Answer: A (LEAVE A REPLY)
The command shown in the exhibit is:
diagnose sys sdwan service 4 3

This command displays the runtime state of SD-WAN rule ID 3 on the device. The output explicitly shows:
Service(3) which confirms the SD-WAN rule being evaluated is rule number 3 Members(9) which indicates that nine SD-WAN members are associated with this rule The listed members include multiple IPsec tunnel interfaces such as HUB1-VPN1, HUB1-VPN2, HUB1-VPN3, HUB2-VPN1, HUB2-VPN2, and HUB2-VPN3, which is characteristic of a spoke device connecting to multiple hubs in a hub-and-spoke ADVPN topology, as defined in the FCSS SD-WAN 7.6 architecture.
Option B is incorrect because, although members are listed under different interfaces, the output does not indicate SD-WAN zones. Zones are shown only in configuration output, not in this diagnostic command.
Option C is incorrect because this is not a hub device. The presence of multiple hub tunnels as SD-WAN members indicates a spoke role. Additionally, the output does not confirm the number of established ADVPN shortcuts.
Option D is incorrect because the output clearly references SD-WAN rule 3, not rule 4, and it does not state that exactly three shortcut tunnels are allowed.
Therefore, the correct conclusion is that this is a spoke device and SD-WAN rule 3 is configured with nine members, which matches option A.