Fortinet.NSE6_SDW_AD-7.6.v2026-05-02.q33

Exam Code:	NSE6_SDW_AD-7.6
Exam Name:	Fortinet NSE 6 - SD-WAN 7.6 Enterprise Administrator
Certification Provider:	Fortinet
Free Question Number:	33
Version:	v2026-05-02
# of views:	163
# of Questions views:	330
https://www.dumpsdb.com/dumps/Fortinet/NSE6_SDW_AD-7.6/Fortinet.NSE6_SDW_AD-7.6.v2026-05-02.q33	

NEW QUESTION: 1

Event log on FortiGate

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

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

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

9: date=2024-12-18 time=15:04:26 eventtime=1734563066334252138 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.1.1 loci
p=172.16.0.1 remport=500 locport=500 outintf="port4" srccountry="Reserved" cookies="ce1c2c62ecc04871/a4d93a059b8df005" user="1
72.16.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=192.168.1.193 vpntunnel="HUB2-VPN3" tunnelip=N/
A tunnelid=3050027467 tunneltype="ipsec" duration=2367 sentbyte=195826 rcvdbyte=196492 nextstat=600 fctuid="N/A" advpnsc=0
```


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: 2

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

SD-WAN rule configuration

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

Proute list

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

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

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

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

Sniffer trace

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

Routing table

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

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

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

A. Only HUB1-VPN1

B. Either HUB1-VPN1 or HUB1-VPN2

C. Only HUB1-VPN2

D. Either HUB1-VPN1, HUB1-VPN2, or HUB1-VPN3

Answer: B (LEAVE A REPLY)

From the SD-WAN rule configuration (service ID 3, name "Corp"), the rule is configured as:

* set mode sla

* set load-balance enable

* set hash-mode source-ip-based

* set priority-members 3 4 5

* Two SLAs are referenced under config sla

In the diagnose firewall proute list output for service=3 (Corp), FortiGate shows the actual members considered for this rule and their SLA pass status:

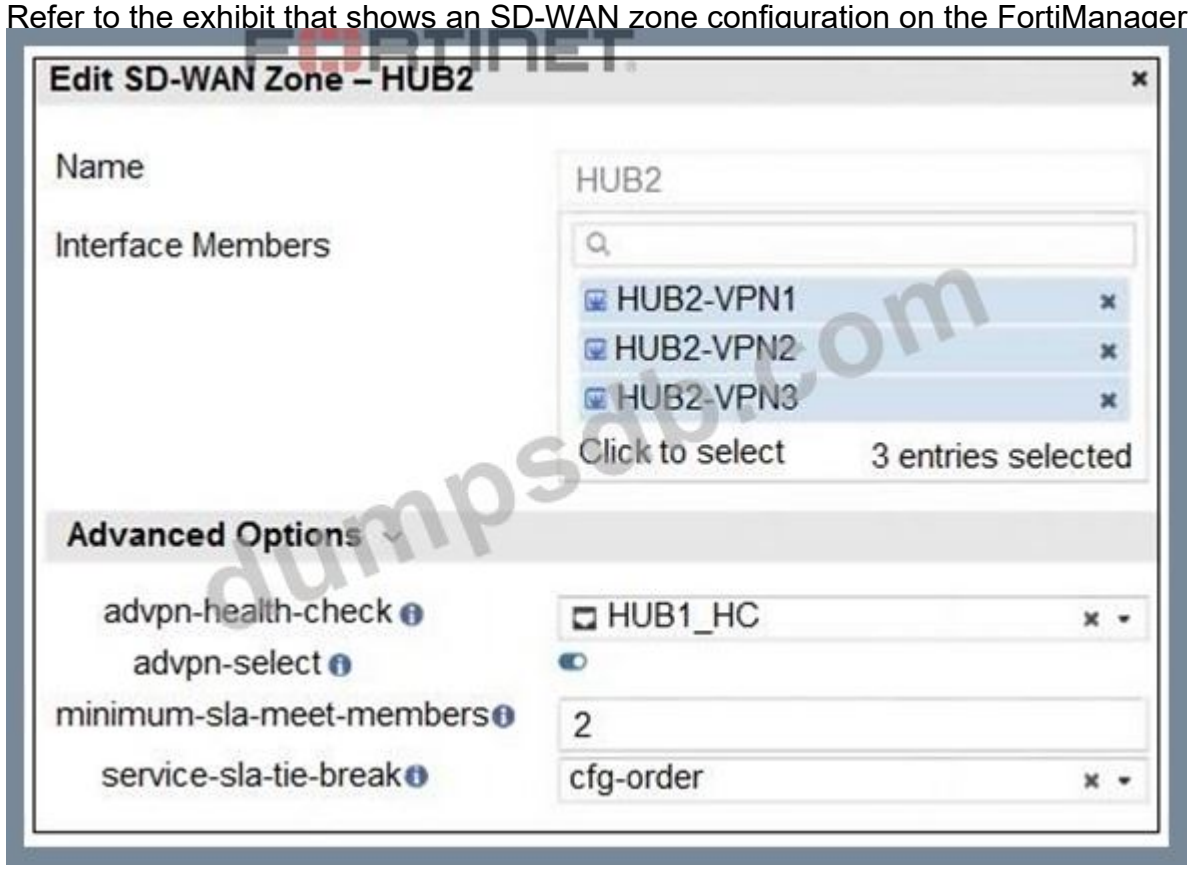
* oif=19 (HUB1-VPN1) num_pass=2

* oif=20 (HUB1-VPN2) num_pass=2

* oif=21 (HUB1-VPN3) num_pass=1

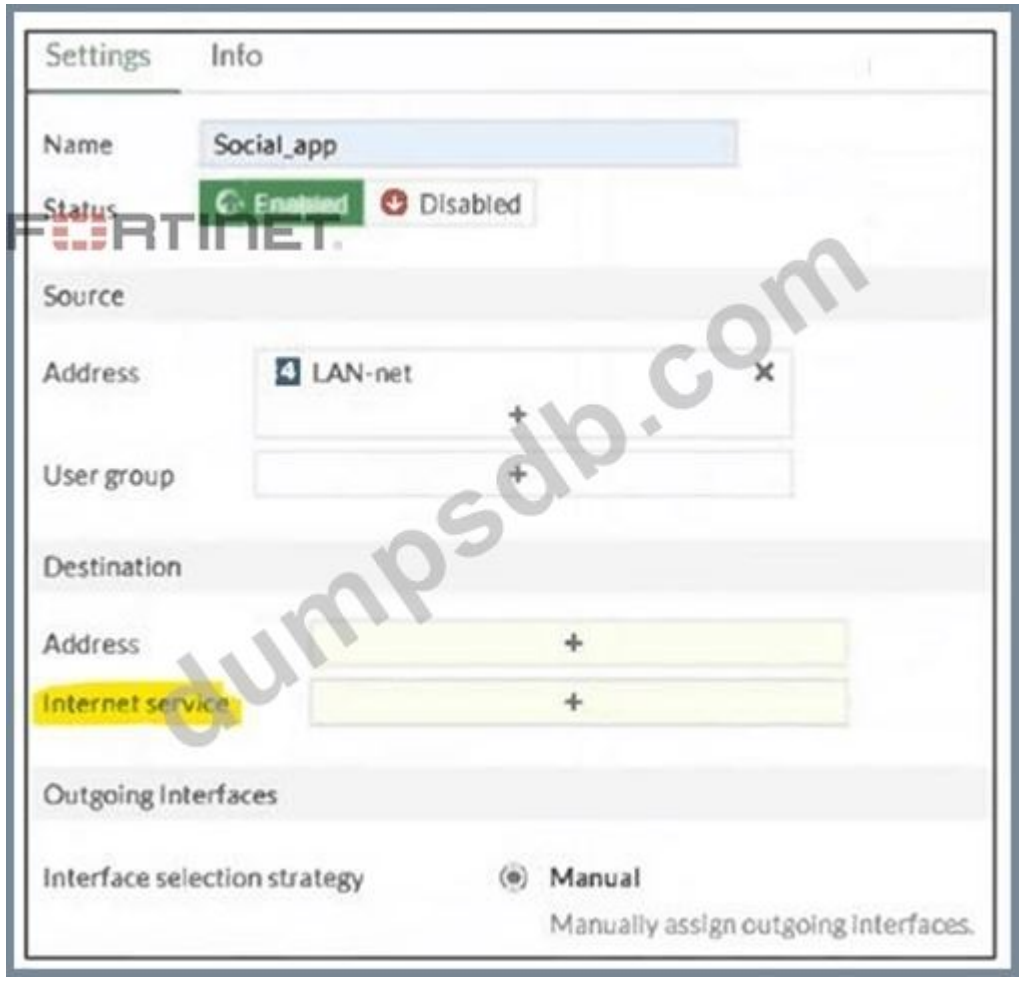
Because the rule is SLA-based, FortiGate selects only members that meet the SLA requirements for the rule.
The output indicates that HUB1-VPN1 and HUB1-VPN2 pass both SLA checks (num_pass=2), while HUB1-VPN3 passes only one (num_pass=1) and therefore is not selected as an eligible forwarding interface for this rule.
Since load-balance is enabled and the rule uses hash-mode source-ip-based, FortiGate will consistently choose an eligible member based on the source IP hash. For traffic sourced from 10.0.1.101, the session can be steered through either HUB1-VPN1 or HUB1-VPN2 (whichever the hash selects), but not HUB1-VPN3.
Therefore, the correct answer is B.

NEW QUESTION: 3
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: 4
(Refer to the exhibit.



You configure SD-WAN on a standalone FortiGate device.

You want to create an SD-WAN rule that steers traffic related to Facebook and LinkedIn through the less costly internet link.

What must you do to set Facebook and LinkedIn applications as destinations from the GUI? Choose one answer.)

A. Enable the visibility of the applications field as destinations of the SD-WAN rule.

B. In the Internet service field, select Facebook and LinkedIn.

C. You cannot configure applications as destinations of an SD-WAN rule on a standalone FortiGate device.

D. Install a license to allow applications as destinations of SD-WAN rules.

Answer: (SHOW ANSWER)

In FortiOS 7.6, SD-WAN rules can steer traffic based on Internet Services, which represent predefined application and service signatures maintained by FortiGuard. Common applications such as Facebook and LinkedIn are included in the Internet Service database.

According to the FCSS SD-WAN 7.6 curriculum, when configuring an SD-WAN rule from the GUI on a standalone FortiGate device, applications are selected as destinations using the Internet service field, not by enabling a separate application destination field. The exhibit highlights the Internet service option under the Destination section, which is the correct method to match traffic for specific applications.

Option A is incorrect because there is no GUI option to enable application visibility as destinations for SD- WAN rules. Application matching is already abstracted through Internet Services.

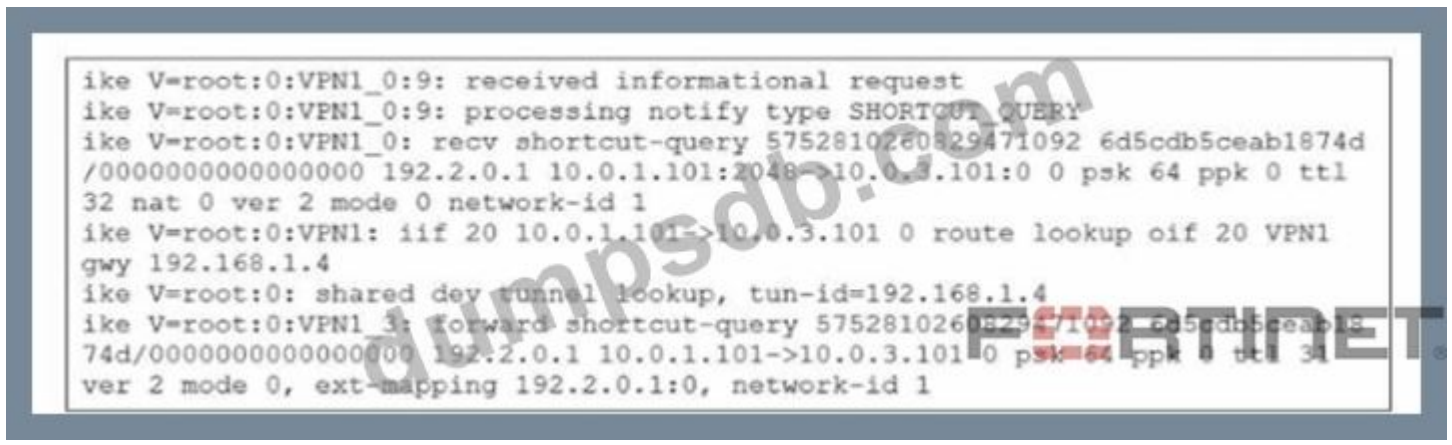
Option C is incorrect because standalone FortiGate devices fully support application-based steering using Internet Services in SD-WAN rules.

Option D is incorrect because no additional license is required to use Internet Services in SD-WAN rules.

This functionality is included in FortiOS and relies on the built-in FortiGuard Internet Service database.

Therefore, to steer Facebook and LinkedIn traffic through a specific WAN link, you must select Facebook and LinkedIn in the Internet service field, which corresponds to option B.

NEW QUESTION: 5
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 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)
Within ADVPN topologies, shortcut requests and responses traverse spokes and hubs. Fortinet documentation states:
"When a spoke receives a shortcut query from another spoke, it may forward the response to its hub for validation or to facilitate dynamic shortcut tunnel setup. This mechanism allows direct spoke-to-spoke communication for optimized routing and performance, reducing latency and offloading the hub after initial control-plane mediation." This is a core benefit of ADVPN's dynamic shortcut feature.

NEW QUESTION: 6
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: (SHOW ANSWER)
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.
References:
[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: 7
(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: (SHOW ANSWER)
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: 8
Refer to the exhibit.

```
        set auto-discovery-sender enable
        set ipv4-start-ip 10.10.128.1
        set ipv4-end-ip 10.10.159.252
        set ipv4-netmask 255.255.224.0
        set psksecret ENC Z8Zpc/bwU2j1HxCFWzO/XkWz1iP/WK4qAGVHE9oazICB+iffI2rIYiAN50IAzV0SZwM/Thbw6M
        set network-overlay enable
        set network-id 5
    next
end
config system interface
```

Download Close

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: (SHOW ANSWER)
The FortiManager SD-WAN overlay template preview, as described in the document, indicates:
"When the device is acting as a hub, the configuration enables the sending of ADVPN shortcut offers to spokes. This means the hub can facilitate on-demand dynamic shortcut tunnel creation between spokes, improving performance for branch-to-branch communication by bypassing the hub for inter-branch traffic after initial discovery." Such a role is critical in scalable ADVPN topologies, enabling hub devices to optimize overlays dynamically.

NEW QUESTION: 9
You want FortiGate to use SD-WAN rules to steer local-out traffic.
Which two constraints should you consider? (Choose two.)
A. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.
B. By default, local-out traffic does not use SD-WAN.
C. You can steer local-out traffic only with SD-WAN rules that use the manual strategy.
D. You must configure each local-out feature individually to use SD-WAN.
Answer: B,D (LEAVE A REPLY)
By default, local-out traffic does not use SD-WAN # FortiGate normally sends local-out traffic (e.g., DNS, NTP, FortiGuard updates) directly through its interfaces without applying SD-WAN rules.
You must configure each local-out feature individually to use SD-WAN # To steer local-out traffic via SD- WAN, you must explicitly configure the desired local-out features (e.g., DNS, FortiGuard, CAPWAP) to use SD-WAN rules.

NEW QUESTION: 10
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)
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.

References:
[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: 11
Refer to the exhibit.

```
ike V=root:0:HUB1-VPN1:0: received informational request
ike V=root:0:HUB1-VPN1:0: processing notify type SHORTCUT_QUERY
ike V=root:0:HUB1-VPN1: recv shortcut-query 16573251835242579210
cff150ded109a548/0000000000000000 192.2.0.1 10.0.1.101:2048->
10.0.3.101:0 0 psk 64 ppk 0 ttl 31 nat 0 ver 2 mode 0 network-id 1
ike V=root:0:HUB1-VPN1: iif 20 10.0.1.101->10.0.3.101 0 route lookup
oif 7 port5 gwy 0.0.0.0
ike V=root:0:HUB1-VPN1: shortcut-query received from 192.2.0.1:500,
local-nat=yes, peer-nat=no
ike V=root:0:HUB1-VPN1: NAT hole punching for peer at 192.2.0.1:4500
```

Which statement best describe the role of the ADVPN device in handling traffic?
A. This is a spoke that has received a direct shortcut query from a remote spoke.
B. This is a hub, and two spokes, 192.2.0.1 and 10.0.3.101, establish a shortcut.
C. This is a hub that has received a shortcut query from a spoke and has forwarded it to another spoke.
D. This is a spoke that has received a shortcut query from a remote hub.
Answer: B (LEAVE A REPLY)
The log shows messages on HUB1-VPN1 where the device processes a SHORTCUT_QUERY and performs NAT hole punching (peer at 192.2.0.1:4500). This indicates that the device is acting as a hub, helping two spokes (192.2.0.1 and 10.0.3.101) establish a direct ADVPN shortcut tunnel between each other, instead of routing their traffic through the hub.

NEW QUESTION: 12
(In the context of SD-WAN, the terms underlay and overlay are commonly used to categorize links.
Which two statements about underlay and overlay links are correct? Choose two answers.)
A. A VLAN is a type of overlay link.
B. Overlay links provide routing flexibility.
C. FortiLink interface is considered an underlay link.
D. Wireless connections can be used to build overlay links.
E. Only wired connections can be used as underlay links.
Answer: B,D (LEAVE A REPLY)
In Fortinet SD-WAN architecture, underlay and overlay have distinct meanings:
* Underlay links are the physical or logical transport networks that provide basic IP connectivity (for example, broadband, MPLS, LTE/5G).
* Overlay links are virtual tunnels (such as IPsec VPNs) built on top of the underlay, providing abstraction, routing control, and segmentation.
Option B is correct.
Overlay links (for example, IPsec tunnels used in SD-WAN and ADVPN) decouple routing from the physical transport. This allows dynamic path selection, segmentation, and flexible routing policies independent of the underlay. Providing routing flexibility is a core purpose of overlays in SD-WAN.
Option D is correct.

Wireless connections such as LTE or 5G can be used as underlay transports, and overlay tunnels can be built over them. Fortinet SD-WAN fully supports building IPsec overlays on wireless underlays, making wireless links valid for overlay construction.
Why the other options are incorrect:
* Option A is incorrect because a VLAN is a Layer 2 segmentation mechanism, not an SD-WAN overlay link.
* Option C is incorrect because FortiLink is used for internal management and switch/AP connectivity, not as a WAN underlay for SD-WAN.
* Option E is incorrect because underlay links can be wired or wireless; they are not limited to wired connections.
Therefore, the two correct statements are B and D.

NEW QUESTION: 13
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: (SHOW ANSWER)
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.
References:
[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: 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
        ...
    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: (SHOW ANSWER)

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.

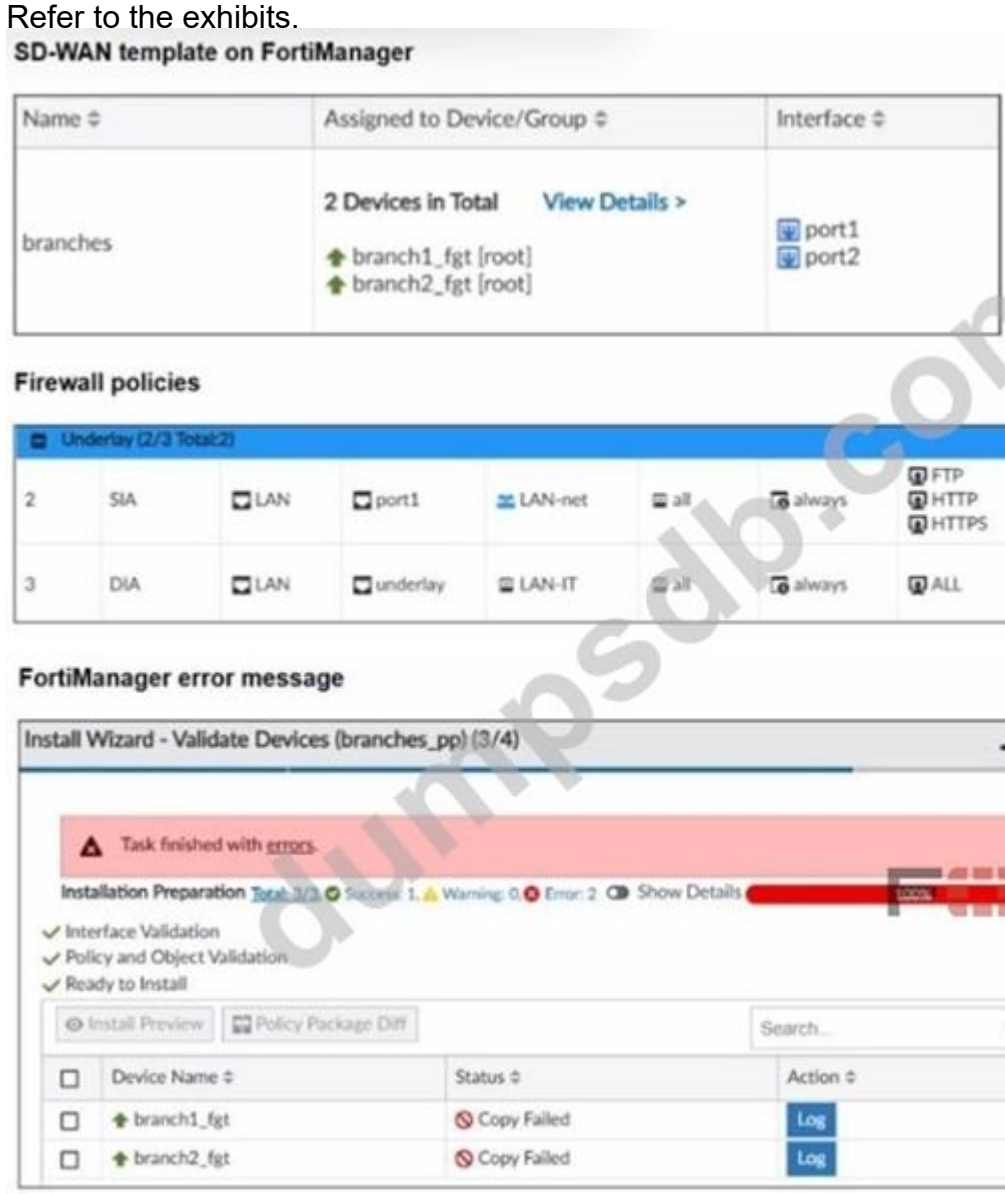
References:

[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

Refer to the exhibits.



You use FortiManager to manage the branch devices and configure the SD-WAN template. You have configured direct internet access (DIA) for the IT department users. Now. you must configure secure internet access (SIA) for all local LAN users and have set the firewall policies as shown in the

second exhibit.
Then, when you use the install wizard to install the configuration and the policy package on the branch devices, FortiManager reports an error as shown in the third exhibit.
Which statement describes why FortiManager could not install the configuration on the branches?
A. You must direct SIA traffic to a VPN tunnel.
B. You cannot install firewall policies that reference an SD-WAN zone.
C. You cannot install firewall policies that reference an SD-WAN member.
D. You cannot install SIA and DIA rules on the same device.
Answer: C (LEAVE A REPLY)
FortiManager enforces a strict distinction:
"Firewall policies must reference SD-WAN zones, not individual SD-WAN members, when used in conjunction with SD-WAN templates. Attempting to install a policy that references a specific member (interface) will result in a deployment error, as member-level targeting is not supported in SD-WAN policy abstraction. This enforces centralized policy consistency and proper SD-WAN operation." Ensuring policies target zones allows FortiGate to dynamically select the optimal member.

NEW QUESTION: 16
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. FortiGate flags the session with may_dirty and vwl_def ault.
C. Traffic does not match any of the entries in the policy route table.
D. The traffic is distributed, regardless of weight, through all available static routes.
E. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.
Answer: (SHOW ANSWER)

NEW QUESTION: 17

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.

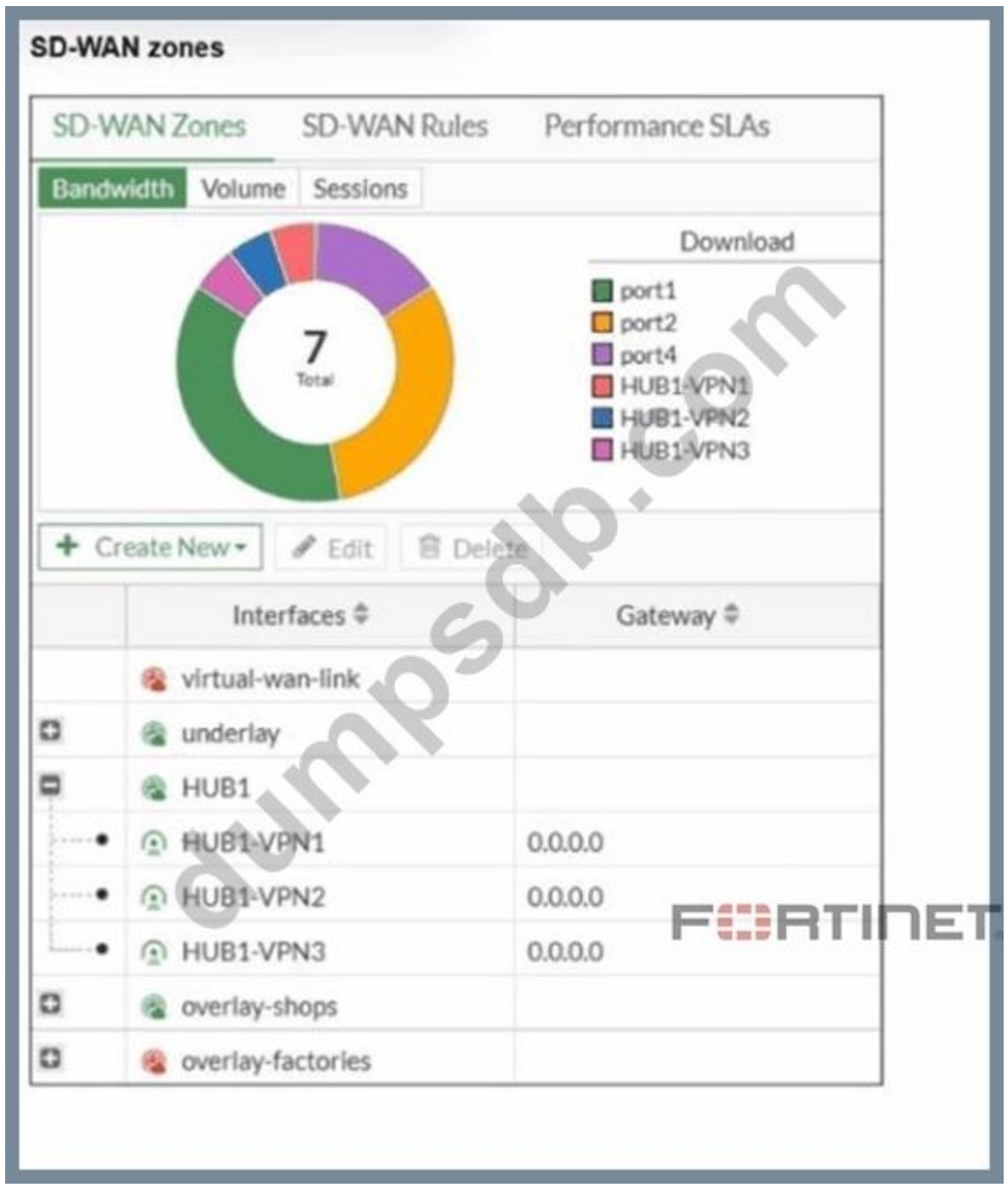
Option B is incorrect because, although members are listed under different interfaces, the output does not indicate SD-WAN zones. Zones are shown only in configuration output, not in this diagnostic command.

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.

NEW QUESTION: 18
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: 19
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: 20
You are planning a new SD-WAN deployment with the following criteria:
- Two regions
- Most of the traffic is expected to remain within its region
- No requirement for inter-region ADVPN
To remain within the recommended best practices, which routing protocol should you select for the overlays?
A. OSPF for the routing within each region and EBGP between the regions.
B. IBGP with BGP on loopback within each region and EBGP between the regions.
C. IBGP with BGP per overlays within each region and IBGP with BGP on loopback between the regions.
D. IBGP within each region and between the regions.
Answer: B (LEAVE A REPLY)
For SD-WAN deployments that span multiple regions-where most traffic is intra-region and there is no requirement for inter-region ADVPN-the best practice is to use IBGP with BGP on loopback interfaces for routing within each region and EBGP between the regions. This approach ensures robust and scalable routing, isolates regional routing domains, and enables policy control at region boundaries. BGP on loopback is preferred for its reliability and flexibility, as it enables peering that is not tied to specific physical interfaces.
EBGP between regions allows each region to maintain independent routing policies and summarization, optimizing performance and manageability. By separating IBGP (intra-region) and EBGP (inter-region), you create a modular architecture that scales easily and simplifies fault isolation and troubleshooting.
References:
[FCSS_SDW_AR-7.4 1-0.docx Q10]
Fortinet SD-WAN Reference Architecture Guide 7.4, "Regional Routing Best Practices" FortiOS 7.4 SD-WAN Overlay Design Guidelines

NEW QUESTION: 21
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: 22
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: (SHOW ANSWER)
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: 23
(Refer to the exhibit.

```
ike V=root:0:HUB1-VPN1:0: received informational request
ike V=root:0:HUB1-VPN1:0: processing notify type SHORTCUT_QUERY
ike V=root:0:HUB1-VPN1: recv shortcut-query 16573251835242579210
cff150ded109a548/0000000000000000 192.2.0.1 10.0.1.101:2048->
10.0.3.101:0 0 psk 64 ppk 0 ttl 31 nat 0 ver 2 mode 0 network-id 1
ike V=root:0:HUB1-VPN1: iif 20 10.0.1.101->10.0.3.101 0 route lookup
oif 7 port5 gwy 0.0.0.0
ike V=root:0:HUB1-VPN1: shortcut-query received from 192.2.0.1:500,
local-nat=yes, peer-nat=no
ike V=root:0:HUB1-VPN1: NAT hole punching for peer at 192.2.0.1:4500
```

Which statement correctly describes the role of the ADVPN device in handling traffic? Choose one answer.)
A. This device is a spoke that has received a direct shortcut query from a remote spoke.
B. This device is a hub, and two spokes, 192.2.0.1 and 10.0.3.101, established a shortcut.
C. This device is a hub that has received a shortcut query from a spoke and has forwarded it to another spoke.
D. This device is a spoke that has received a shortcut query from a remote hub.
Answer: C (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: 24
Refer to the exhibit, which shows the SD-WAN rule status and configuration.

SD-WAN rule status and configuration

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority:2
      Gen(43), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
      link-cost-factor(packet loss), link-cost-threshold(10), heath-check(HUB1_HC)
     Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, latency: 96.349, selected
          2: Seq_num(5 HUB1-VPN2 HUB1), alive, latency: 141.278, selected
          3: Seq_num(6 HUB1-VPN3 HUB1), alive, latency: 190.984, selected
     Src address(1):
          10.0.1.0-10.0.1.255

     Dst address(1):
          10.0.0.0-10.255.255.255

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


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

A. When HUB1-VPN3 has a lower latency than HUB1-VPN1 and HUB1-VPN2

B. When HUB1-VPN3 has a latency of 80 ms

C. When HUB1-VPN3 has a latency of 90 ms

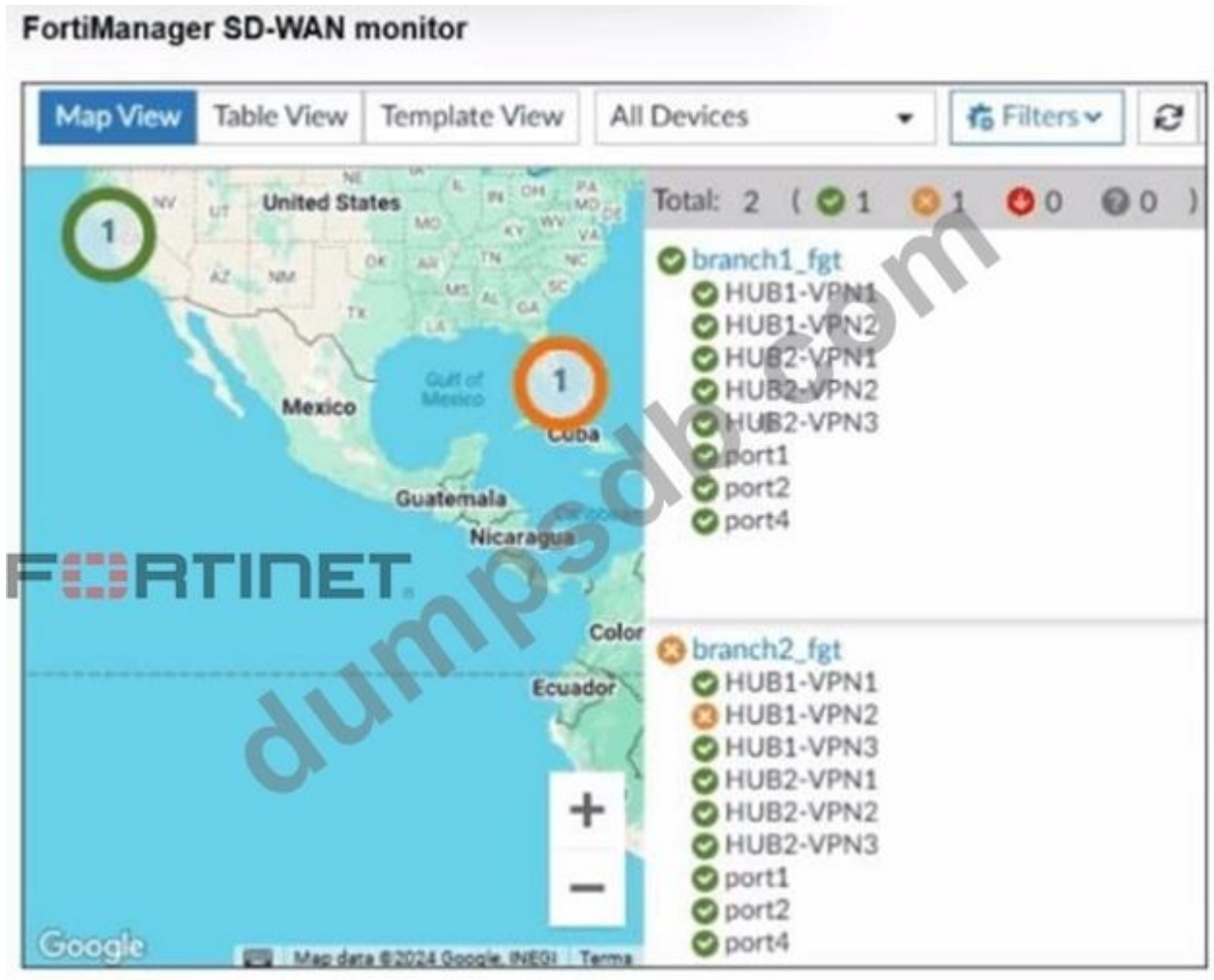
D. When HUB1-VPN1 has a latency of 200 ms

Answer: D (LEAVE A REPLY)

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: 25

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.

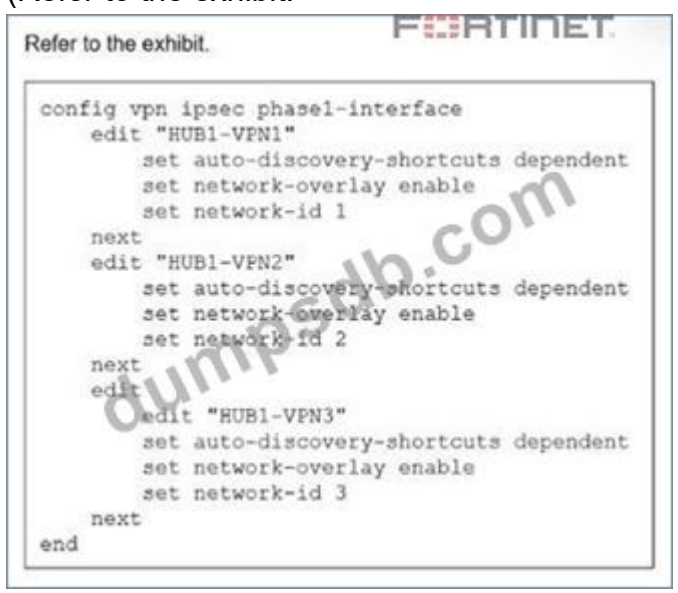
Answer: B,D (LEAVE A REPLY)

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.
References:
[FCSS_SDW_AR-7.4 1-0.docx Q18]
FortiManager SD-WAN Monitoring Guide, "Branch Device Health and SLA Status Visualization"

NEW QUESTION: 26
(Refer to the exhibit.



You update the spokes configuration of an existing auto-discovery VPN (ADVPN) topology by adding the parameters shown in the exhibit.
Which is a valid objective of those settings? Choose one answer.)
A. Enable the tunnels as overlay links.
B. Convert the configuration from ADVPN to ADVPN 2.0.
C. Prevent cross-overlay shortcuts.
D. Prevent multiple shortcuts from being established over the same overlay.
Answer: C (LEAVE A REPLY)
The exhibit shows the following IPsec phase1-interface configuration applied on spoke tunnels:
* set auto-discovery-shortcuts dependent
* set network-overlay enable
* set network-id <value>
In the FCSS SD-WAN 7.6 ADVPN architecture, the network-overlay and network-id parameters are used to logically group IPsec tunnels into separate overlays. When network-overlay is enabled, FortiGate treats the tunnel as part of an overlay network rather than a simple transport tunnel.
The network-id parameter is critical in multi-overlay ADVPN designs. Fortinet documentation specifies that ADVPN shortcuts are only allowed between tunnels that share the same network-id. This mechanism explicitly prevents cross-overlay shortcuts, ensuring that shortcuts are formed only within the same logical overlay and not across different overlays that may serve different purposes (for example, different hubs, regions, or transport groups).
The use of auto-discovery-shortcuts dependent further enforces correct shortcut behavior by ensuring that shortcut tunnels depend on the state of the parent overlay tunnel, but it does not by itself prevent multiple shortcuts or convert ADVPN versions.
Why the other options are incorrect:
* Option A is incorrect because simply enabling network-overlay does not exist to "enable overlay links" in general; its purpose is to define overlay membership and control shortcut behavior.

* Option B is incorrect because there is no concept of "ADVPN 2.0" conversion using these parameters in FortiOS 7.6.
* Option D is incorrect because preventing multiple shortcuts over the same overlay is not controlled by network-id; multiple shortcuts within the same overlay are allowed when required.
Therefore, the valid objective of these settings is to prevent cross-overlay shortcuts, which corresponds to Option C.

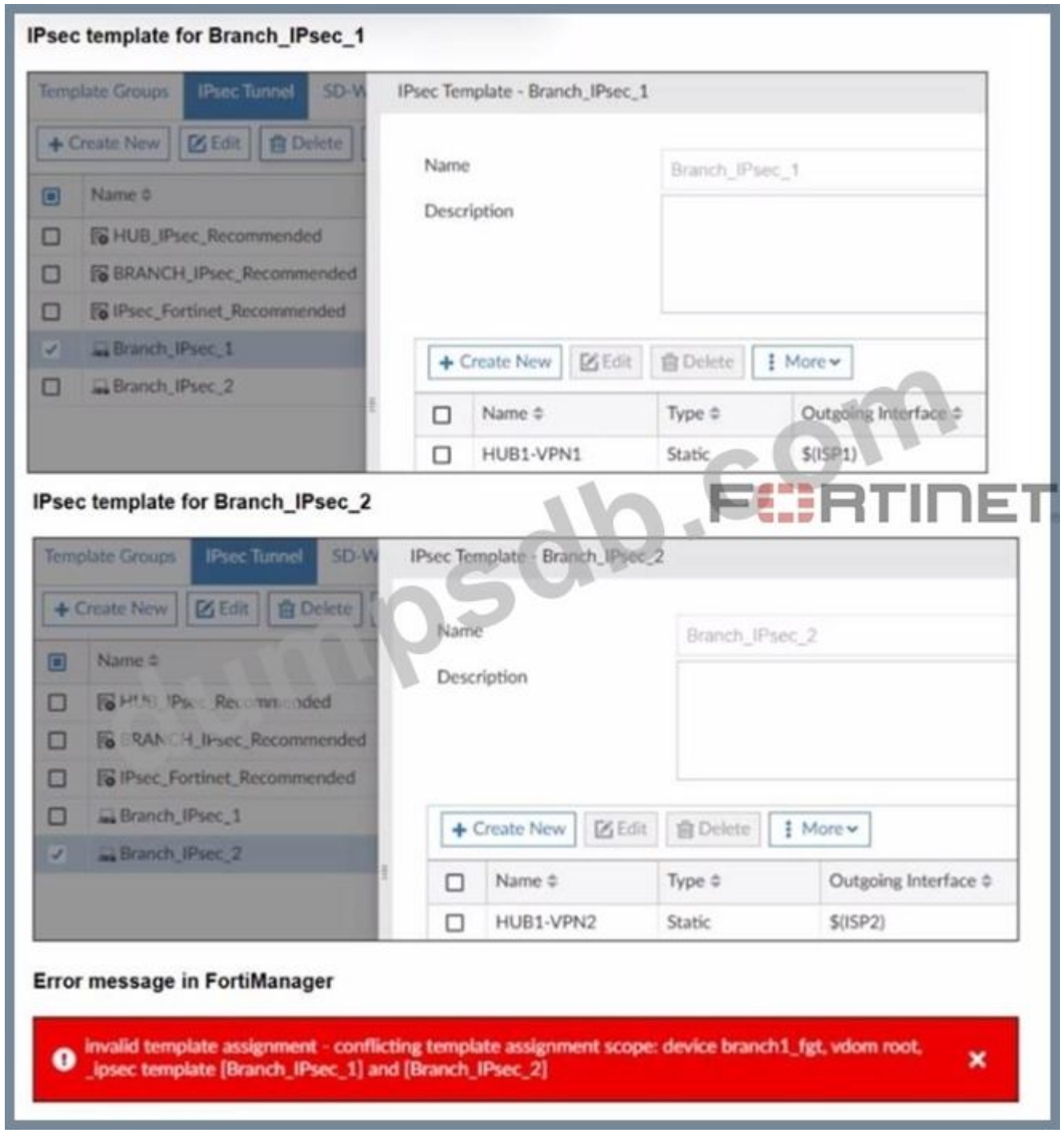
NEW QUESTION: 27
Refer to the exhibit.

```
# diagnose sys session list
session info: proto=6 prote_state=11 duration=180 expire=3424 timeout=3600
refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may dirty ndr f00 app_valid route preserve
statistic (bytes/packets/allow_err): org=3369/19/1 reply=3881/19/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=192.2.0.2/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:58630->128.66.0.1:22(192.2.0.100:58630)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.100:58360(10.0.1.101:58360)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:58630(0.0.0.0:0)
pos/ (before, after) 0/(0,0), 0/(0,0)
misc=0 policy id=1 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=00000c0c tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service id=4
rpdb_link_id=ff000004 ngfwid=n/a
npu_stave=0x001108
no_offoad_reason: redir-to-ips denied-by-nturbo
```

The administrator configured the SD-WAN rule ID 4 with two members (port1 and port2) and strategy lowest cost (SLA).
What are the two characteristics of the session shown in the exhibit? (Choose two.)
A. FortiGate steered this flow according to an SD-WAN rule 4.
B. FortiGate will never re-evaluate this session.
C. FortiGate steered this flow according to the application detected and the outgoing interface is port3.
D. FortiGate will re-evaluate this session if the outgoing interface goes down.
Answer: 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: 28

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: 29
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: A (LEAVE A REPLY)
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: 30
Refer to the exhibits.

SD-WAN zone configuration on FortiManager

SD-WAN Zones

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

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

7

Policy package configuration

#	Name	From	To	Source	Destination	Install On
	Corp-SOT_BBLK(1/1 Total:1)					
2	DIA	LAN	underlay	LAN-net	all	Installation Targets
3	To Hub-Overlay	LAN	HUB1-VPN1	all	all	Installation Targets
	Implicit(4/4 Total:1)					
4	Implicit Deny	any	any	all 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: 31

You manage an SD-WAN topology. You will soon deploy 50 new branches.
Which three tasks can you do in advance to simplify this deployment? (Choose three.)
A. Update the DHCP server configuration.
B. Create model devices.
C. Create a ZTP template.
D. Define metadata variables value for each device.
E. Create policy blueprint.
Answer: B,C,E (LEAVE A REPLY)
When planning to deploy a large number of branches (e.g., 50), Fortinet recommends several preparatory steps to simplify and automate the rollout. Creating model devices allows you to predefine configurations and settings that can be cloned or adapted for each branch, saving time and minimizing manual errors. Preparing a Zero Touch Provisioning (ZTP) template enables automatic onboarding and provisioning of new FortiGates as soon as they come online, reducing manual intervention. Lastly, creating a policy blueprint allows for standardized policy deployment across all branches, ensuring consistent security and SD-WAN rule enforcement. This holistic approach streamlines the deployment process, allows for rapid scaling, and ensures that all devices are configured according to corporate policy from day one.
References:
[FCSS_SDW_AR-7.4 1-0.docx Q8]
Fortinet SD-WAN 7.4 Reference Architecture, "ZTP and Model Device Strategies for Scalable Rollouts" FortiManager Admin Guide, "Policy Blueprints and Automation for Branch Deployment"

NEW QUESTION: 32
Refer to the exhibit.

Diagnose output

```
spoke_A # 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=17 port=src(0->65535):dst(0->65535)
iif=0(any)
path(1): oif=0(any) gwy=10.0.1.253
destination(1): 10.22.0.0-10.22.0.255
source wildcard(1): 0.0.0.0/255.255.255.0
hit_count=5 rule_last_used=2024-12-19 07:53:31

id=2130968577(0x7f040001) vwl_service=1(Critical-DIA) vwl_mbr_seq=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(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): Microsoft.Portal(41469,0) Storage.Backup(0,22)
hit_count=8597 rule_last_used=2024-12-19 07:31:00

id=2130968578(0x7f040002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xfc 0xfc flags=0x0 tos=
0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(2): Operational.Technology(0,26) Social.Media(0,23)
hit_count=36589 rule_last_used=2024-12-19 07:31:00

id=2130968580(0x7f040004) vwl_service=4 (Critical-Web-Server) vwl_mbr_seq=3 dscp_tag=0xfc flags=0x0 tos=
0x00
tos_mask=0x00 protocol=0 port=src(0->0) iif=0(any)
path(1): oif=6(port4)
source(1): 10.0.1.0-10.0.1.255
destination(1): 128.66.0.1-128.66.0.1
hit_count=12587 rule_last_used=2024-12-19 07:31:00

id=2130968579(0x7f040003) vwl_service=3 (VOIP) vwl_mbr_seq=1 dscp_tag=0xfc flags=0x0 tos=0x00 tos_mask=0x00
protocol=17 port=src(1->65535):dst(1->65535) iif=0(any)
path(1): oif=3(port1) path_last_used=2024-12-19 08:09:00
source(1): 10.0.1.0-10.0.1.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=13 rule_last_used=2024-12-19 08:09:00
```

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

A. One SD-WAN rule is defined with application categories as the destination.

B. UDP traffic destined to the subnet 10.22.0.0/24 matches a manual SD-WAN rule.

C. One SD-WAN rule allows traffic load balancing.

D. UDP traffic destined to the subnet 10.22.0.0/24 matches a policy route.

Answer: A,D (LEAVE A REPLY)

One SD-WAN rule is defined with application categories as the destination # The diagnose output shows application control matches such as Microsoft.Portal, Operational.Technology, and Social.Media, confirming that SD-WAN rules are using application categories as destinations.
UDP traffic destined to the subnet 10.22.0.0/24 matches a policy route # The first entry (id=1) shows protocol=17 (UDP) with destination 10.22.0.0/24,

confirming this traffic is handled by a policy route instead of an SD-WAN rule.

NEW QUESTION: 33
Within the context of SD-WAN, what does SIA correspond to?
A. Remote Breakout
B. Secure Internet Authorization
C. Software Internet Access
D. Local Breakout
Answer: (SHOW ANSWER)