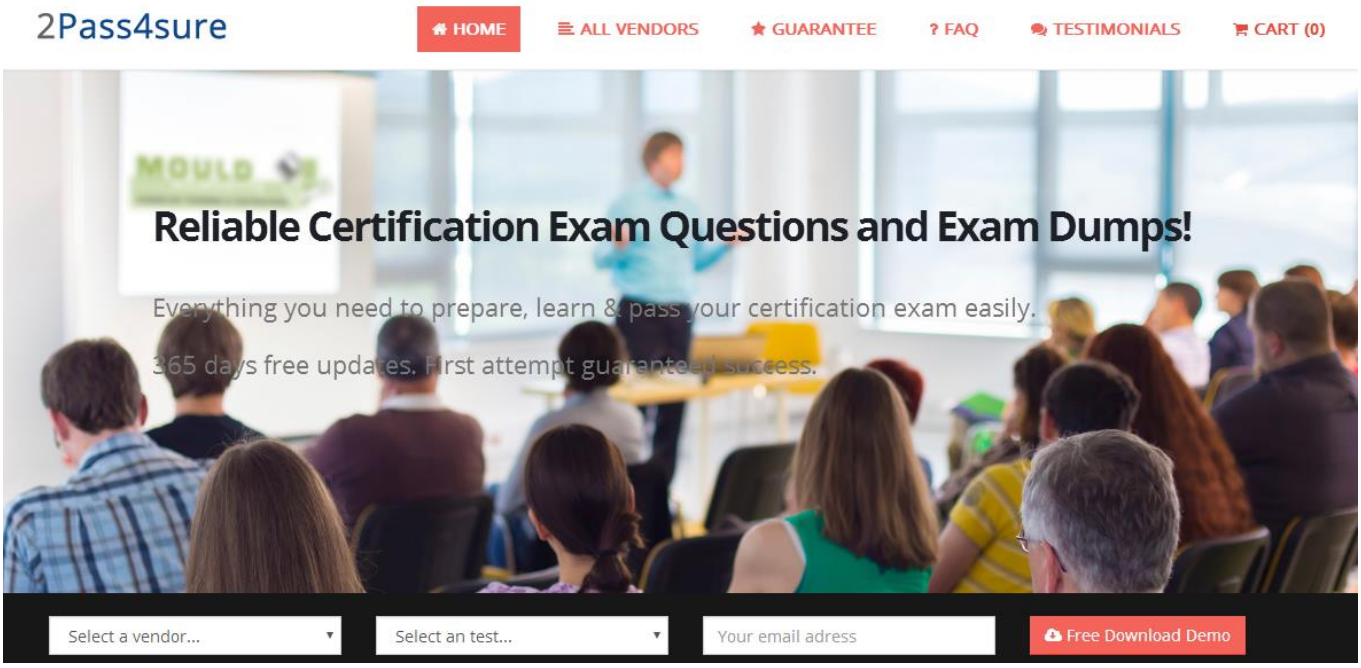
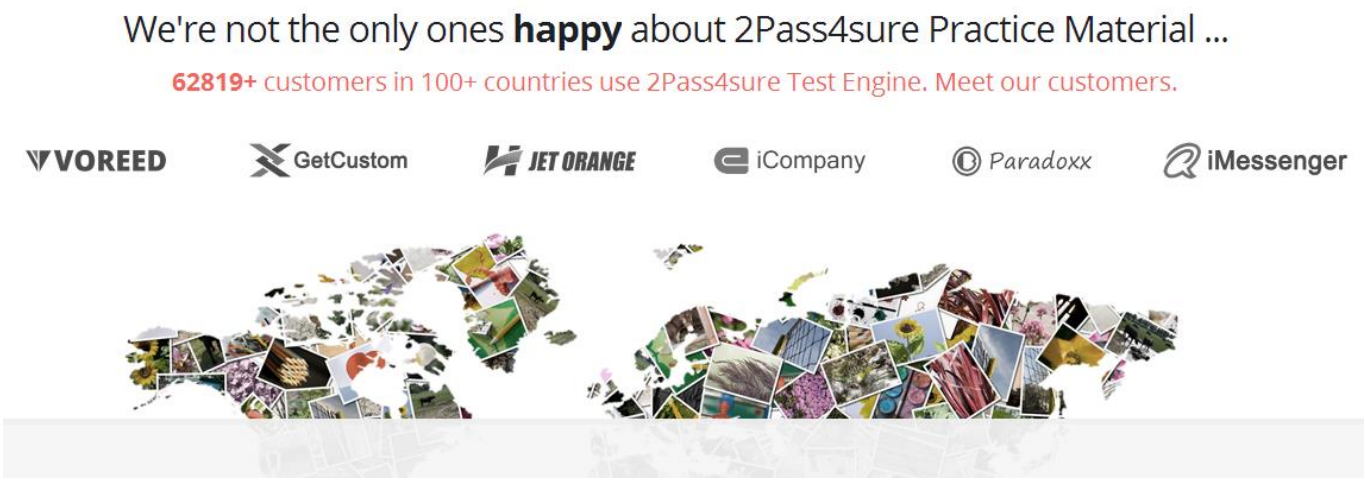
2Pass4sure





http://www.2pass4sure.com/

Reliable Certification Exam Questions and Exam Dumps - 2Pass4sure

Exam : **NSE6_SDW_AD-7.6**

Title : Fortinet NSE 6 - SD-WAN 7.6 Enterprise Administrator

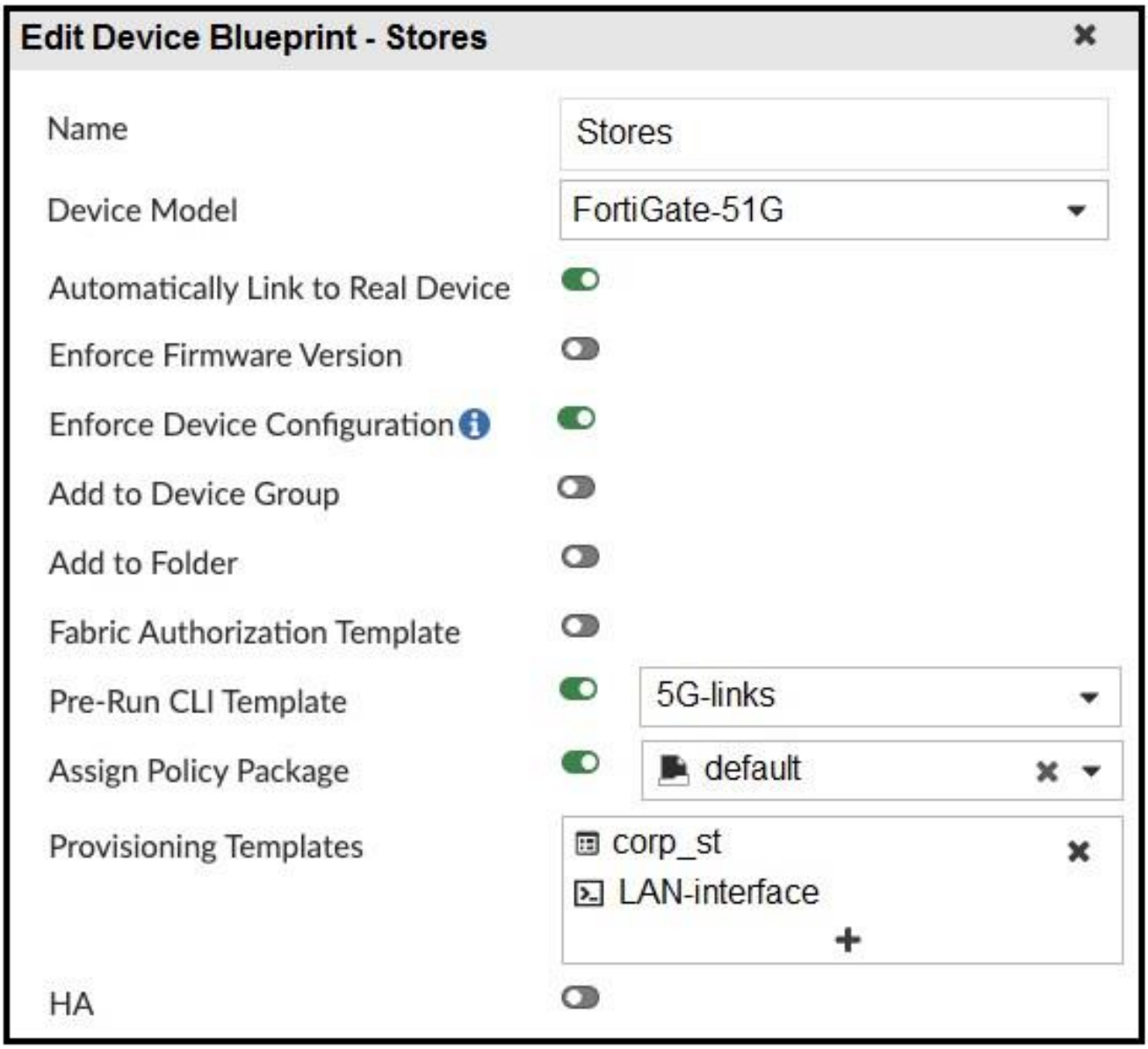
Vendor : Fortinet

Version : DEMO

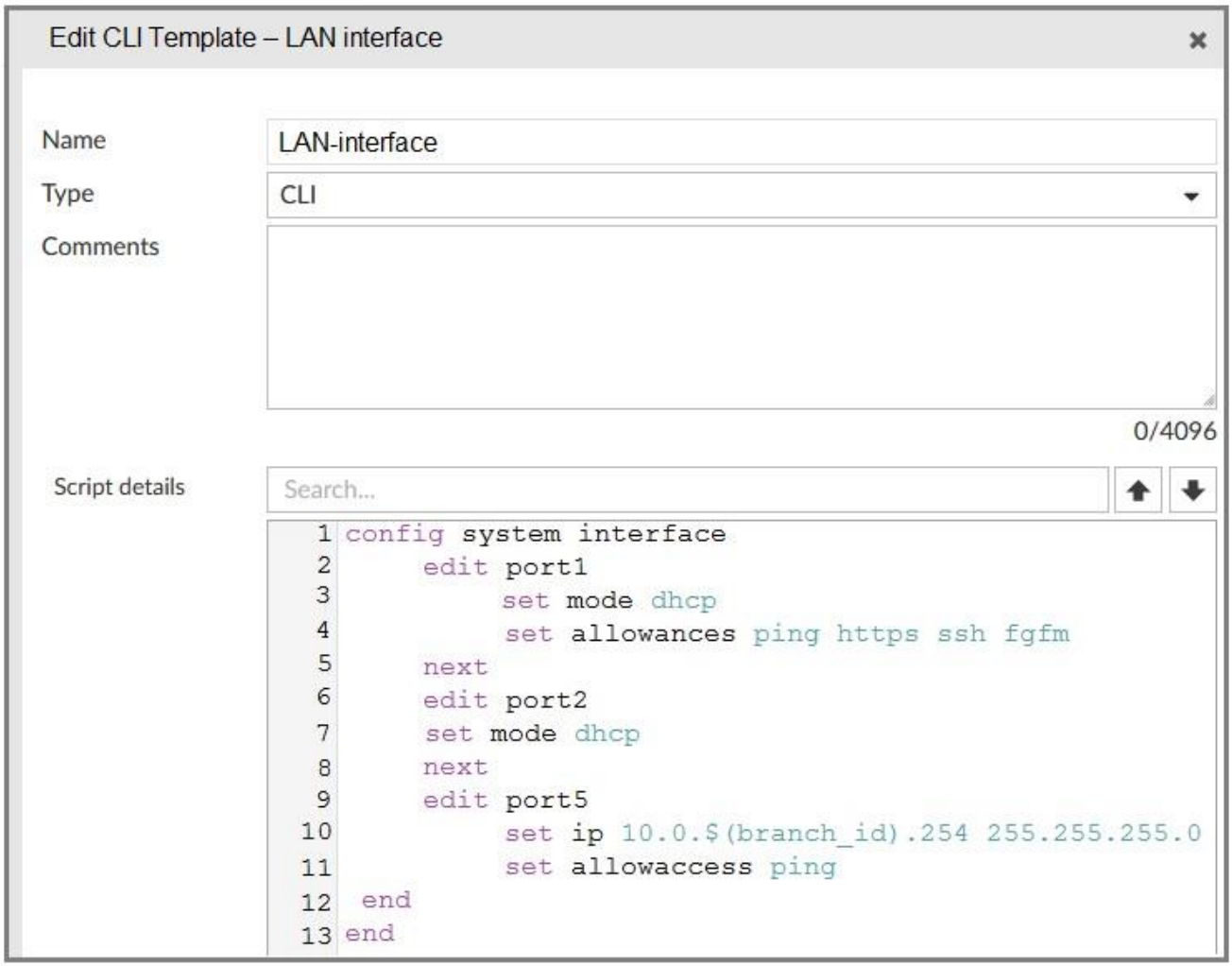
NO.1 As an MSSP administrator, you are asked to configure ADVPN on an existing SD-WAN topology. FortiManager manages the customer devices in a dedicated ADOM. The previous administrator used the SD- WAN overlay topology.
Which two statements apply to this scenario? (Choose two.)
A. You can activate auto-discovery VPN in the SD-WAN overlay template only if it is a single hub topology.
B. When auto-discovery VPN is enabled, FortiManager updates the IPsec and BGP templates in the hub.
C. After you enable auto-discovery VPN in the overlay template, you must select between ADVPN 2.0 and ADVPN 1.0.
D. You can activate auto-discovery VPN in the SD-WAN overlay template for any type of topology, including a primary-primary dual-hub topology.
Answer: B D
Explanation:
When you enable ADVPN (auto-discovery VPN) in the overlay template, FortiManager automatically updates both the IPsec and BGP templates on the hub so that shortcut tunnels can be established dynamically.
ADVPN can be activated in the SD-WAN overlay template for any supported topology, including dual-hub primary-primary, not just single hub.

NO.2 Refer to the exhibits.

Device blueprint



CLI script LAN-interface



The administrator configured a device blueprint and CLI scripts as shown in the exhibits, to prepare for onboarding FortiGate devices in the company's stores. Later, a technician prepares a FortiGate 51G with a basic configuration and connects it to the network. The basic configuration contains the port1 configuration and the minimal configuration required to allow the device to connect to FortiManager.

After the device first connects to FortiManager, FortiManager updates the device configuration.

Based on the exhibits, which actions does FortiManager perform?

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

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

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

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

Answer: D

Explanation:

Enforce Device Configuration is enabled and the blueprint applies the provisioning CLI templates. The LAN- interface script sets port1 and port2 to DHCP and assigns a static IP to port5 (using the branch_id

variable).
Therefore, when FortiManager pushes the blueprint, it updates the configurations of port1, port2, and port5 - and their IP addresses may change accordingly.

NO.3 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 D

NO.4 Refer to the exhibit.

SD-WAN configuration on FortiGate

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

```
branch1_fgt # diag sys sdwan service4

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

  Dst address(1):
        10.0.0.0-10.255.255.255


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

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

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

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

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

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

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

Answer: B

NO.5 Refer to the exhibits.

Ping result

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

Diagnose output

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

id=1(0x01) dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=21(HUB1-VPN2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 10.1.0.7/255.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:44

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

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

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

Diagnose output

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

Max_App_Ctrl_Size=32768 Num_App_Ctrl_Entry=8

Facebook(15832 23): IP=157.240.19.35 6 443

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

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

LinkedIn(16331 23): IP=13.107.42.14 6 443

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

Salesforce(16920 29): IP=23.222.17.73 6 443

Salesforce(16920 29): IP=23.222.17.76 6 443

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

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

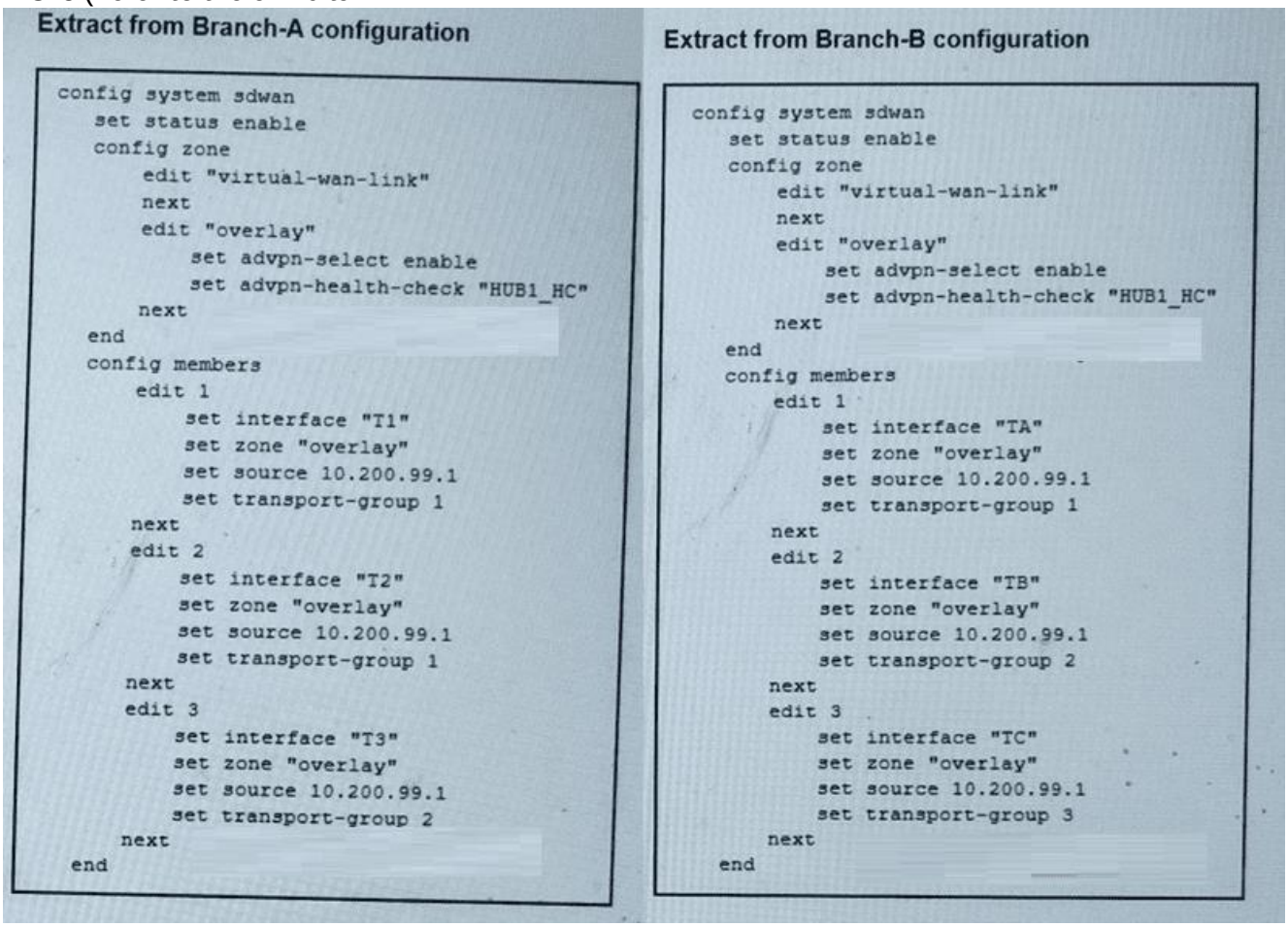
Based on the exhibits, which interface uses branch 1_fgt to steer the test traffic?

A. port4

B. HUB1-VPN1

C. port1
D. port2
Answer: D

NO.6 (Refer to the exhibits.



The SD-WAN zones and members configuration of two branch devices are shown. The two branch devices are part of the same hub-and-spoke topology and connect to the same hub. The devices are configured to allow Auto-Discovery VPN (ADVPN). The configuration on the hub allows the initial communication between the two spokes.
When traffic flows require it, between which interfaces can the devices establish shortcuts? Choose one answer.)
A. Any interface in the overlay zones
B. Interface connected to HUB only
C. Between T3 on Branch-A and TC on Branch-B
D. Between T2 on Branch-A and TA on Branch-B
Answer: D
Explanation:
From the exhibit, both branches have an SD-WAN zone named overlay with set advpn-select enable, and each SD-WAN member in that zone is assigned a transport-group value.
Branch-A members:
* T1 # transport-group 1
* T2 # transport-group 1

* T3 # transport-group 2
Branch-B members:
* TA # transport-group 1
* TB # transport-group 2
* TC # transport-group 3
In FCSS SD-WAN 7.6 ADVPN design, transport-group is used to constrain which underlays are allowed to form ADVPN shortcuts with each other . A spoke can establish an ADVPN shortcut only between interfaces that belong to the same transport-group on both sides. This prevents building shortcuts across dissimilar transports.
Evaluating the options:
* Option D (T2 on Branch-A with transport-group 1 and TA on Branch-B with transport-group 1) is a valid shortcut pairing.
* Option C is not valid because T3 is transport-group 2 while TC is transport-group 3, so they are not permitted to form a shortcut.
* Option A is incorrect because not all overlay-zone interfaces are eligible; eligibility is restricted by transport-group matching.
* Option B is incorrect because ADVPN shortcuts are spoke-to-spoke tunnels (facilitated by the hub), not limited to "interfaces connected to hub only." Therefore, the valid shortcut pairing listed is between T2 on Branch-A and TA on Branch-B , which corresponds to Option D .

NO.7 (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 l
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
Explanation:
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 .

NO.8 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: B

NO.9 You have a FortiGate configuration with three user-defined SD-WAN zones and two members in each of these zones. One SD-WAN member is no longer in use in health-check and SD-WAN rules. You want to delete it.

What happens if you delete the SD-WAN member from the FortiGate GUI?

A. FodiGate accepts the deletion and removes routes as required.

B. FortiGate displays an error message. You must use the CLI to delete an SD-WAN member.

C. FortiGate displays an error message. SD-WAN zones must contain at least two members

D. FortiGate accepts the deletion and places the member in the default SD-WAN zone.

Answer: A

NO.10 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 ea raffic will be routed over HUB1-V ns.

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

Explanation:

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