Passcert

Higher Quality, better service!



Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **FCSS_SDW_AR-7.6**

Title : FCSS - SD-WAN 7.6 Architect

Version : DEMO

1.Refer to the exhibits.

SD-WAN service configuration

```
branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set load-balance enable
        set mode sla
        set dst "Corp-net"
        set src "LAN-net"
        config sla
            edit "HUB1_HC"
                set id 1
            next
            edit "HUB1_HTTP"
                set id 1
            next
        end
        set priority-members 3 4 5
    next
end
```

Proute list

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

id=2131034113(0x7f050001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xfc 0xfc flags=0x0
tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(2): oif=3(port1), oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(2): Salesforce(16920,0) Microsoft.Portal(41469,0)
hit_count=0 rule_last_used=2025-06-19 03:14:42

id=2131034114(0x7f050002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xfc 0xfc flags=0x0
tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
application control(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
hit_count=0 rule_last_used=2025-06-19 03:14:42

id=2131034115(0x7f050003) vwl_service=3(Corp) vwl_mbr_seq=5 4 3 dscp_tag=0xfc 0xfc flags=0x10
load-balance hash-mode=round-robin tos=0x00 tos_mask=0x00 protocol=0 port=src(0->0):dst(0->0) iif=0(any)
path(3): oif=21(HUB1-VPN3) num_pass=0, oif=20(HUB1-VPN2) num_pass=0, oif=19(HUB1-VPN1) num_pass=0
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=660 rule_last_used=2025-06-19 04:33:21
```

Sniffer trace

```
branch1_fgt # diagnose sniffer packet any "host 10.0.1.101 and icmp" 4 0 1
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.1.101 and icmp]
2025-06-19 04:34:49.626332 port5 in 10.0.1.101 -> 10.0.2.101: icmp: echo
2025-06-19 04:34:49.626391 HUB1-VPN3 out 10.0.1.101 -> 10.0.2.101: icmp: echo
request
2025-06-19 04:34:49.883401 HUB1-VPN3 in 10.0.2.101 -> 10.0.1.101: icmp: echo
2025-06-19 04:34:49.883430 port5 out 10.0.2.101 -> 10.0.1.101: icmp: echo
```

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
       * - candidate default

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

You collected the output shown in the exhibits and want to know which interface HTTP traffic will flow through from the user device 10.0.1.101 to the corporate web server 10.0.0.126. All SD-WAN links are stable.

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

A. Only HUB1-VPN3

B. Only HUB1-VPN2

C. Either HUB1-VPN2 or HUB1-VPN3

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

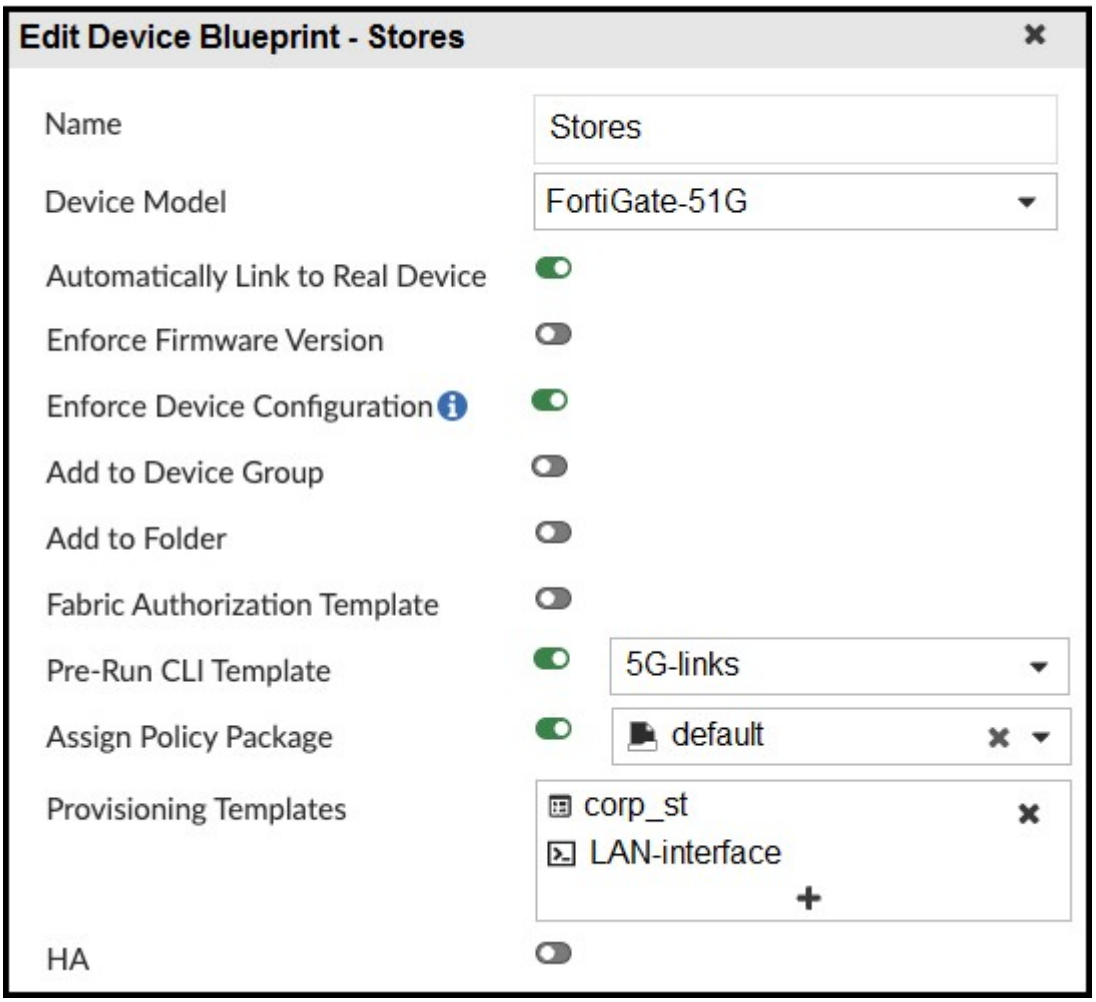
Answer: D

Explanation:

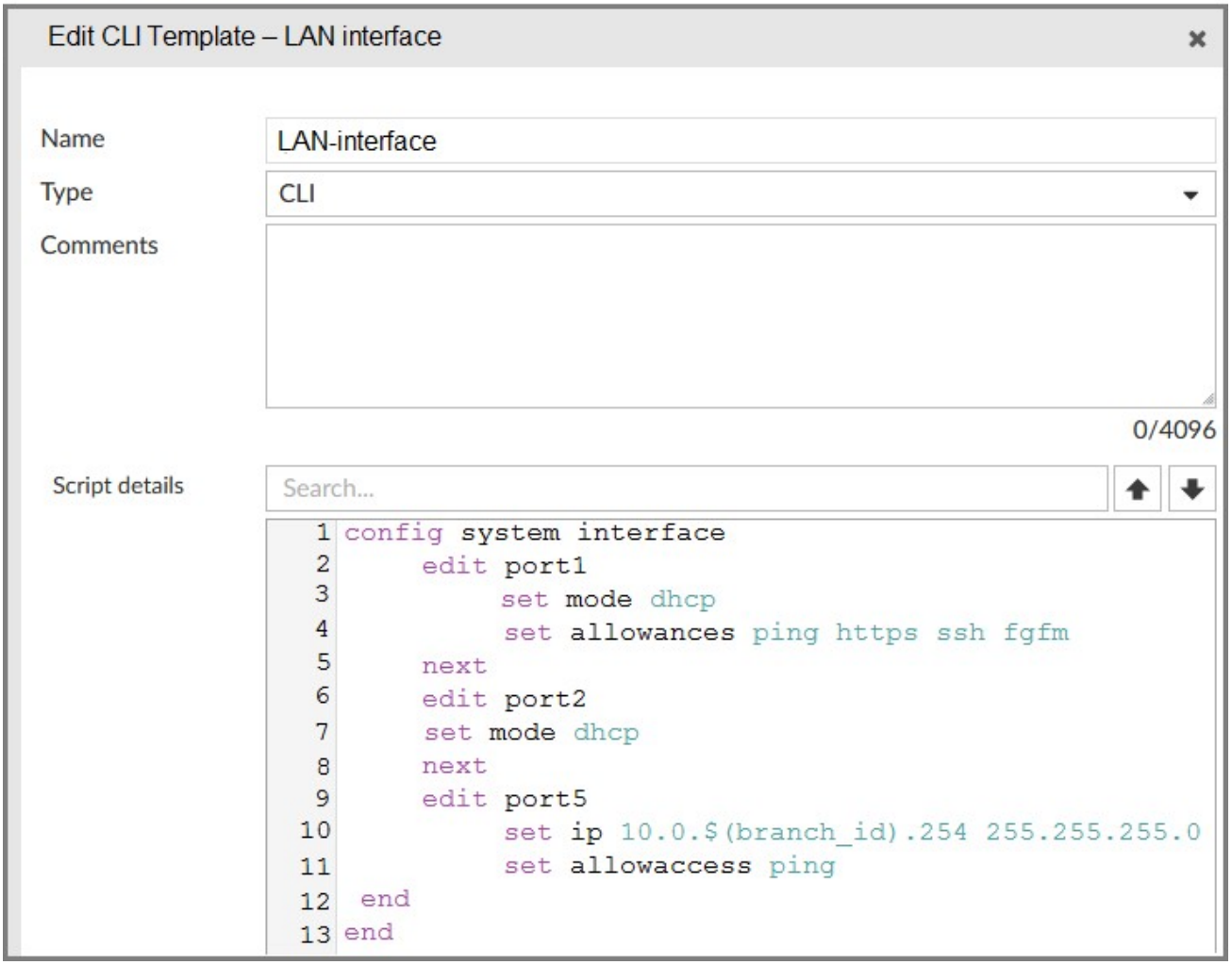
From the SD-WAN service configuration, rule edit 3 (name "Corp") is configured with:
set mode sla set load-balance enable set dst "Corp-net"
set src "LAN-net"
SLA checks referenced under config sla
Traffic from 10.0.1.101 to 10.0.0.126 matches this rule because the destination is within the corporate network range (shown in the policy-route/proute output as destination 10.0.0.0–10.255.255.255 for the Corp service).
In the diagnose firewall proute list output for vwl_service=3 (Corp), FortiGate shows which SD-WAN members are eligible based on SLA pass results:
oif=21 (HUB1-VPN3) num_pass=2 oif=20 (HUB1-VPN2) num_pass=0 oif=19 (HUB1-VPN1) num_pass=0
This indicates that, for the SLA-based rule, only HUB1-VPN3 is meeting the SLA requirements (it is the only member with num_pass=2). The other members have num_pass=0, so they are not eligible for forwarding under this SLA rule even though links are up.
The sniffer trace further corroborates the forwarding decision by showing the traffic egressing through HUB1-VPN3.
Therefore, FortiGate will steer the HTTP traffic through only HUB1-VPN3, which corresponds to Option A.

2.Refer to the exhibits.

Device blueprint



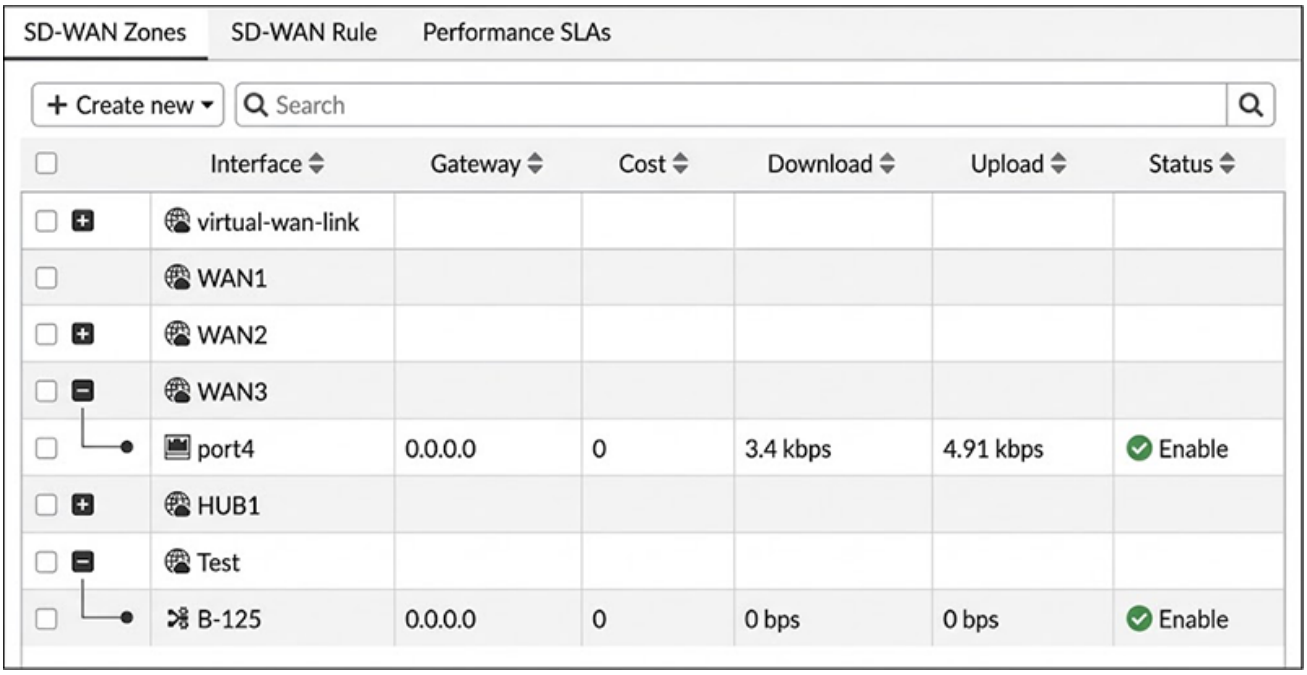
CLI script LAN-interface



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.

3.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

Explanation:

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.

4.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
Explanation:
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.

5.Refer to the exhibits.

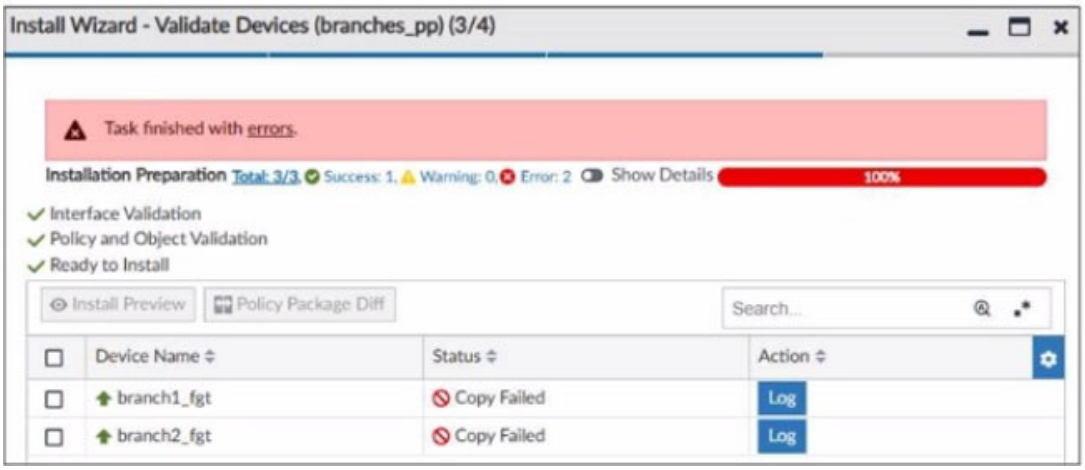
SD-WAN template on FortiManager

Name	Assigned to Device/Group	Interface
branches	2 Devices in Total View Details > branch1_fgt [root] branch2_fgt [root]	port1 port2

Firewall policies

Underlay (2/3 Total:2)									
2	SIA	LAN	port1	LAN-net	all	always	FTP HTTP HTTPS	Accept	no-inspection default
3	DIA	LAN	underlay	LAN-IT	all	always	ALL	Accept	default certificate-i... default

FortiManager error message



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

Explanation:

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.