

Fortinet

Exam Questions FCSS_SDW_AR-7.4

FCSS - SD-WAN 7.4 Architect



NEW QUESTION 1
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: B

NEW QUESTION 2
 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-L... default	

FortiManager error message

Install Wizard - Validate Devices (branches_pp) (3/4)

Task finished with errors.

Installation Preparation **Total: 3/3** Success: 1, Warning: 0, Error: 2 [Show Details](#) **100%**

- Interface Validation
- Policy and Object Validation
- Ready to Install

Device Name	Status	Action
branch1_fgt	Copy Failed	Log
branch2_fgt	Copy Failed	Log

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

NEW QUESTION 3
 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

NEW QUESTION 4

Exhibit.

```
config system sdwan
  set fail-detect enable
  set fail-alert-interfaces "port5"
  config health-check
    edit "Level3_DNS"
      set update-cascade-interface enable
      set members 1 2
    next
    edit "HQ"
      set update-cascade-interface enable
      set members 3
    next
  end
end
```

Which action will FortiGate take if it detects SD-WAN members as dead?

- A. FortiGate bounces port5 after it detects all SD-WAN members as dead.
- B. FortiGate fails over to the secondary device after it detects port5 as dead.
- C. FortiGate sends alert messages through port5 when it detects all SD-WAN members as dead
- D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

Answer: D

NEW QUESTION 5

Refer to the exhibits.

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

```

config system sdwan
  config health-check
    edit "Passive"
      set detect-mode passive
      set members 3 4
    next
  end
end

config system sdwan
  config service
    edit 1
      set name "Facebook-YouTube"
      set src "all"
      set internet-service enable
      set internet-service-app-ctrl 15832 31077
      set health-check "Passive"
      set priority-member 3 4
      set passive-measurement enable
    next
  end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077

```

Firewall policy configuration

```

config firewall policy
  edit 1
    set name "DIA"
    set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
    set srcintf "port5"
    set dstintf "underlay"
    set action accept
    set srcaddr "LAN-net"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set passive-wan-health-measurement enable
    set utm-status enable
    set ssl-ssh-profile "certificate-inspection"
    set application-list "default"
    set logtraffic all
    set auto-asic-offload disable
    set nat enable
  next
end

```

Underlay zone status

```

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

```

The exhibits show the configuration for SD-WAN performance. SD-WAN rule, the application IDs of Facebook and YouTube along with the firewall policy configuration and the underlay zone status.

Which two statements are true about the health and performance of SD-WAN members 3 and 4? (Choose two.)

- A. Only related TCP traffic is used for performance measurement.
- B. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
- C. Encrypted traffic is not used for the performance measurement.
- D. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.

Answer: AB

NEW QUESTION 6

Exhibit.

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

For your ZTP deployment, you review the CSV file shown in exhibit and note that it is missing important information. Which two elements must you change before you can import it into FortiManager? (Choose two.)

- A. You must associate a device blueprint with each device
- B. You must define a name for each device
- C. You must define a value for each device and each metadata variable that defines an IP address.
- D. You must define a value for each device and each user-defined metadata variable.

Answer: AB

NEW QUESTION 7

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. FortiGate accepts the deletion and removes routes as required.
- B. FortiGate displays an error message
- C. You must use the CLI to delete an SD-WAN member.
- D. FortiGate displays an error message
- E. SD-WAN zones must contain at least two members
- F. FortiGate accepts the deletion and places the member in the default SD-WAN zone.

Answer: B

NEW QUESTION 8

Refer to the exhibits.

Global System configuration

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

Interface port2 configuration

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

Routing Table on FortiGate

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

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

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

The administrator increases the member priority on port2 to 20.

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

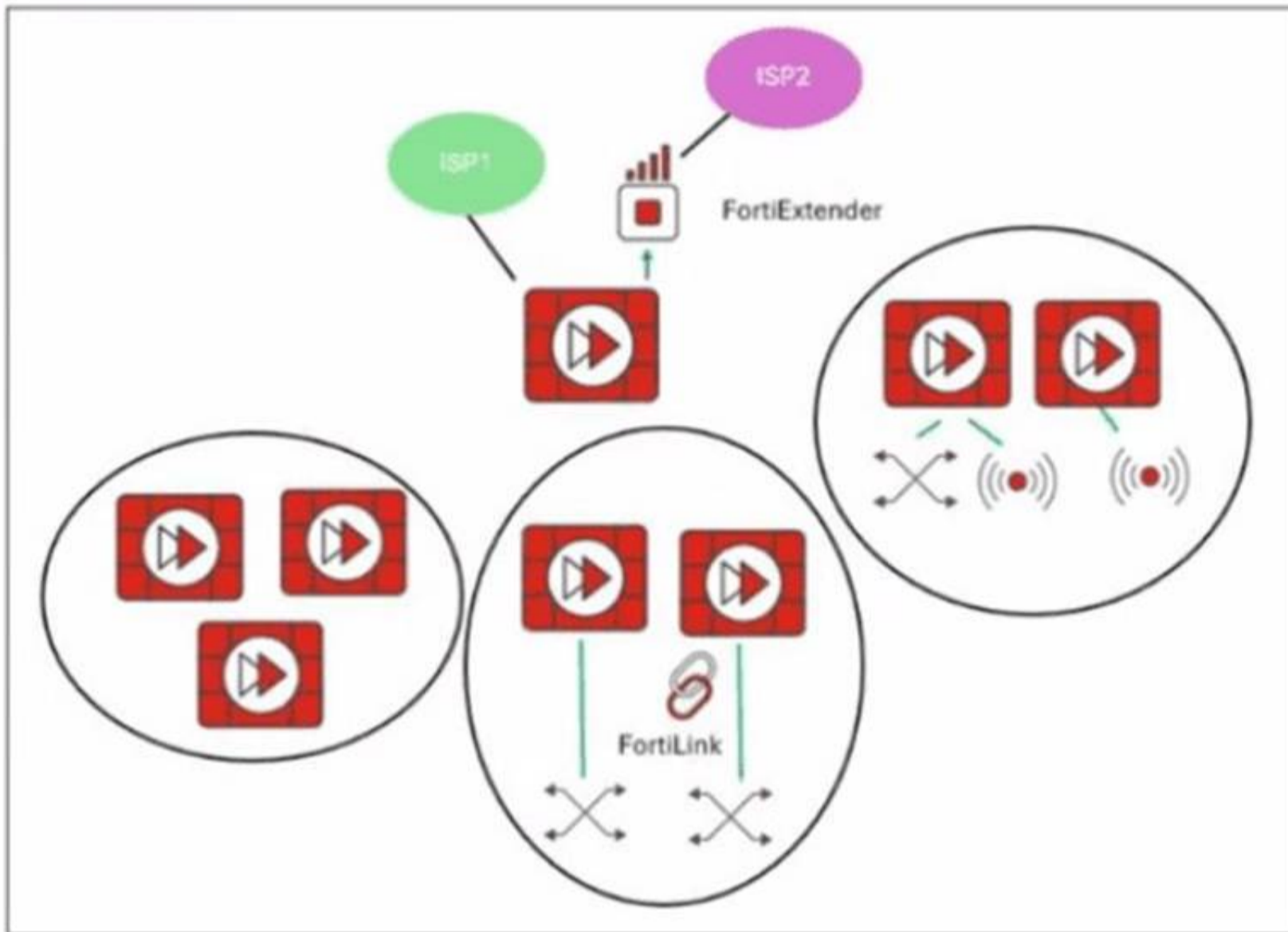
- A. FortiGate continues routing all existing sessions over port2.
- B. FortiGate routes only new sessions over port2.
- C. FortiGate flags the SNAT session as dirty only if the administrator has assigned an IP pool to the firewall policies with NAT.
- D. FortiGate flags the sessions as dirty.
- E. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: DE

NEW QUESTION 9

Refer to the exhibit.

SD-WAN Network Topology



You want to configure SD-WAN on a network as shown in the exhibit.

The network contains many FortiGate devices. Some are used as NGFW, and some are installed with extensions such as FortiSwitch, FortiAP, or Forti Extender. What should you consider when planning your deployment?

- A. You can build an SD-WAN topology that includes all device
- B. The hubs can be FortiGate devices with Forti Extender.
- C. You can build an SD-WAN topology that includes all device
- D. The hubs must be devices without extensions.
- E. You must use FortiManager to manage your SD-WAN topology.
- F. You must build multiple SD-WAN topologie
- G. Each topology must contain only one type of extension.

Answer: B

NEW QUESTION 10

When a customer delegate the installation and management of its SD-WAN infrastructure to an MSSP, the MSSP usually keeps the hub within its infrastructure for ease of management and to share costly resources.

In which two situations will the MSSP install the hub in customer premises? (Choose two.)

- A. The customer requires SIA with centralized breakout.
- B. The administrator expects a large volume of traffic between the branches.
- C. The customer expects a large amount of VoIP traffic.
- D. The majority of the branch traffic is directed to a corporate data center.

Answer: AB

NEW QUESTION 10

An administrator is configuring SD-WAN to load balance their network traffic. Which two things should they consider when setting up SD-WAN? (Choose two.)

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

Answer: AD

NEW QUESTION 11

Refer to the exhibit that shows event logs on FortiGate.

Event log on FortiGate

```
6: date=2024-12-18 time=15:15:06 eventtime=1734563705745090691 tz="-0800" logid="0113022925" type="event" subtype="sdwan" level="information" vd="root" logdesc="SDWAN SLA information" eventtype="SLA" healthcheck="HUB1_HC" slatargetid=1 interface="HUB1-VPN3" status="up" latency="1.001" jitter="0.162" packetloss="0.000" moscodec="g711" mosvalue="4.404" inbandwidthavailable="10.00Gbps" outbandwidthavailable="10.00Gbps" bibandwidthavailable="20.00Gbps" inbandwidthused="0kbps" outbandwidthused="0kbps" 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 locip=192.2.0.1 remport=500 locport=500 outintf="port1" srccountry="Reserved" cookies="50b8a3684ddfd2cb/af3f725d883c5585" user="10.0.64.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=172.168.1.1 vpntunnel="VPN4_0" tunnelip=N/A tunnelid=3050027470 tunneltype="ipsec" duration=2968 sentbyte=245849 rcvbyte=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 locip=192.2.0.1 remport=4500 locport=4500 outintf="port1" srccountry="Reserved" cookies="cff150ded109a548/165f413d17cecc49" user="Branch3" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="HUB1-VPN1_0" tunnelip=192.168.1.4 tunnelid=3050027486 tunneltype="ipsec" duration=1122 sentbyte=92064 rcvbyte=0 nextstat=600 fctuid="N/A" advpnsc=1

9: date=2024-12-18 time=15:04:26 eventtime=1734563066334252138 tz="-0800" logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.1.1 locip=172.16.0.1 remport=500 locport=500 outintf="port4" srccountry="Reserved" cookies="celc2c62ecc04871/a4d93a059b8df005" user="172.16.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=192.168.1.193 vpntunnel="HUB2-VPN3" tunnelip=N/A tunnelid=3050027467 tunneltype="ipsec" duration=2367 sentbyte=195836 rcvbyte=196492 nextstat=600 fctuid="N/A" advpnsc=0
```

Based on the output shown in the exhibit, what can you say about the tunnels on this device?

- A. The master tunnel HUB2-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: B

NEW QUESTION 15

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: BCE

NEW QUESTION 16

Which three characteristics apply to provisioning templates available on FortiManager? (Choose three.)

- A. A template group can include a system template and an SD-WAN template.
- B. Each template group can contain up to three IPsec tunnel templates.
- C. CLI templates are applied in order, from top to bottom
- D. A CLI template group can contain CLI templates of both types.
- E. A CLI template can be of type CLI script or Perl script.

Answer: ACD

NEW QUESTION 21

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCSS_SDW_AR-7.4 Practice Exam Features:

- * FCSS_SDW_AR-7.4 Questions and Answers Updated Frequently
- * FCSS_SDW_AR-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_SDW_AR-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_SDW_AR-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_SDW_AR-7.4 Practice Test Here](#)