



Fortinet

Exam Questions FCSS_SDW_AR-7.4

FCSS - SD-WAN 7.4 Architect

NEW QUESTION 1

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: BCE

NEW QUESTION 2

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 3

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

NEW QUESTION 4

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 5

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.)

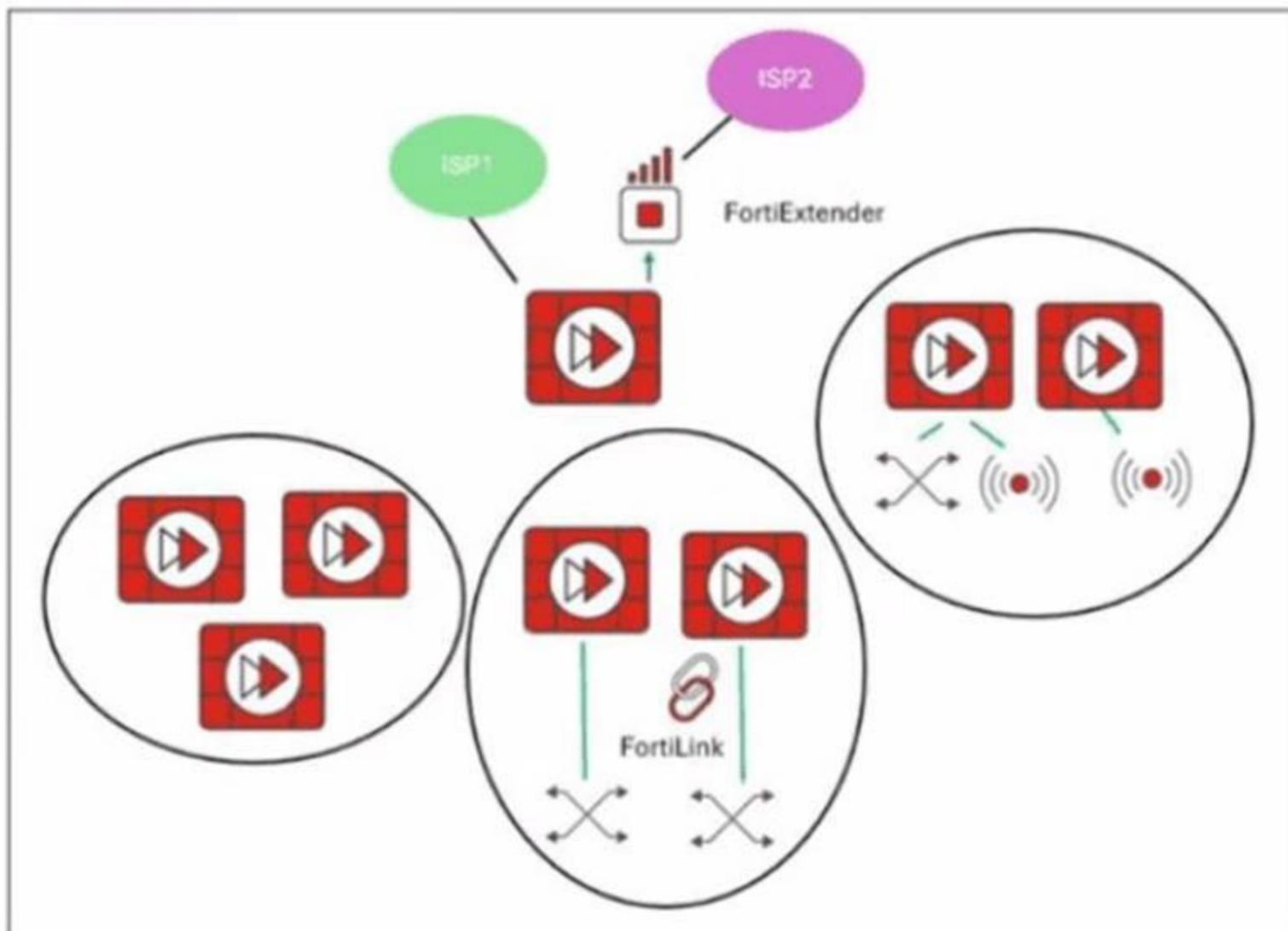
- A. FortiGate continues routing all existing sessions over port2.
- B. FortiGate routes only new sessions over port2.
- C. FortiGate flags the SNAT session as dirty only if the administrator has assigned an IP pool to the firewall policies with NAT.
- D. FortiGate flags the sessions as dirty.
- E. FortiGate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

Answer: DE

NEW QUESTION 6

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 7

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 8

Refer to the exhibits.

IPsec template for Branch_IPsec_1

The screenshot shows the FortiManager interface for configuring an IPsec template. On the left, under 'Template Groups', the 'IPsec Tunnel' group is active, and 'Branch_IPsec_1' is selected. The main area shows the configuration for 'IPsec Template - Branch_IPsec_1'. The 'Name' field is 'Branch_IPsec_1' and the 'Description' field is empty. Below the configuration fields, there is a table of associated VPNs:

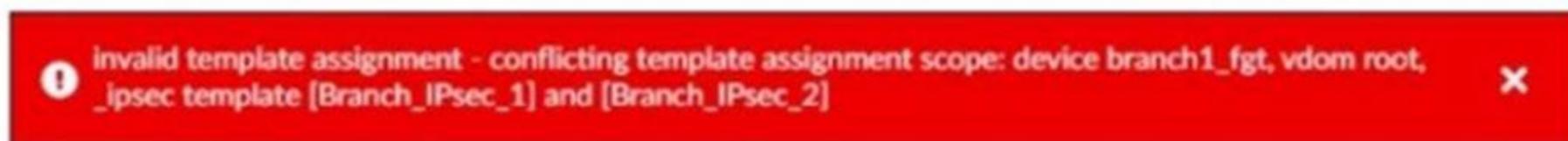
<input type="checkbox"/>	Name ↕	Type ↕	Outgoing Interface ↕
<input type="checkbox"/>	HUB1-VPN1	Static	\$(ISP1)

IPsec template for Branch_IPsec_2

The screenshot shows the FortiManager interface for configuring an IPsec template. On the left, 'Branch_IPsec_2' is selected. The main area shows the configuration for 'IPsec Template - Branch_IPsec_2'. The 'Name' field is 'Branch_IPsec_2' and the 'Description' field is empty. Below the configuration fields, there is a table of associated VPNs:

<input type="checkbox"/>	Name ↕	Type ↕	Outgoing Interface ↕
<input type="checkbox"/>	HUB1-VPN2	Static	\$(ISP2)

Error message in FortiManager



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?

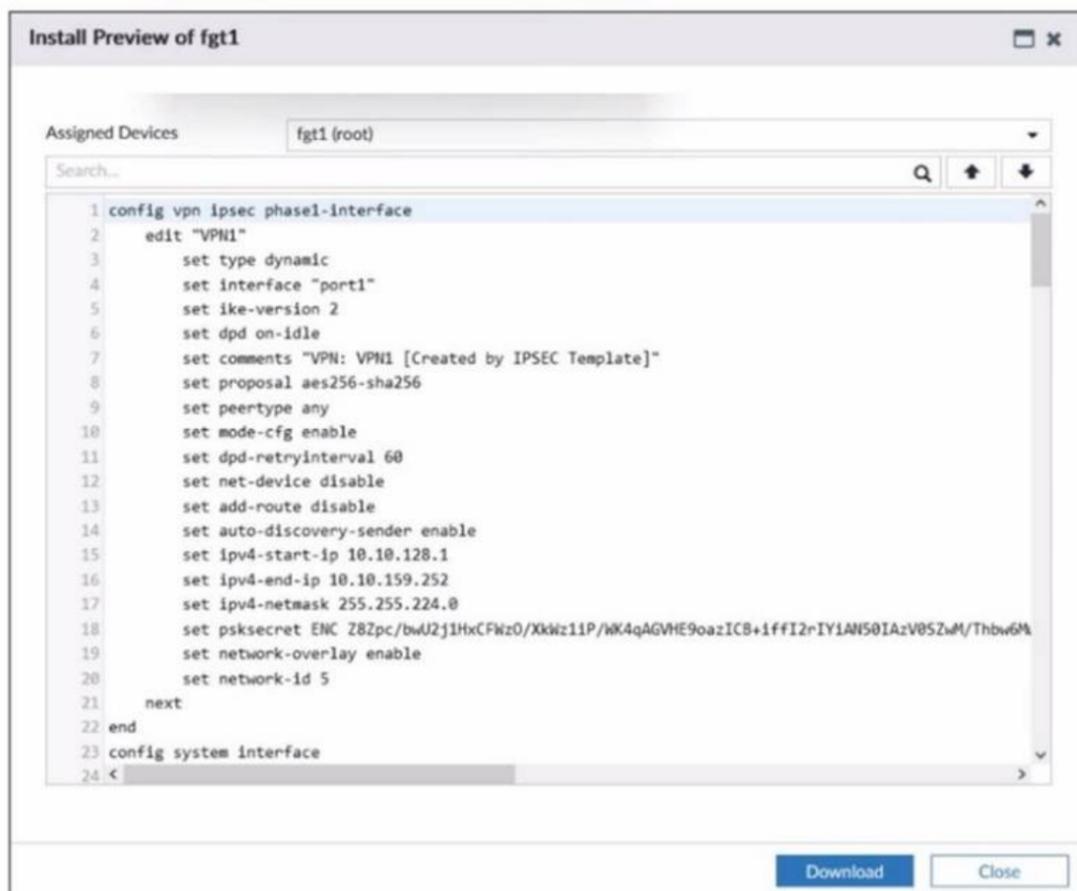
- A. You can assign only one template with a tunnel type of static to each FortiGate device.
- B. You can assign only one IPsec template to each FortiGate device.
- C. You should review the branch1_fgt configuration for configured tunnels in the rootVDM.
- D. You should use the same outgoing interface of both templates.

Answer: B

NEW QUESTION 9

Refer to the exhibit.

SD-WAN overlay template



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 hu
- B. The local subnet range is 10.10.128.0/23.
- C. It is a hub devic
- D. It can send ADVPN shortcut offers.
- E. It is a hub devic
- F. It will automatically discover the spoke devices and add them to the SD-WAN topology.
- G. It is a spoke device that establishes dynamic IPsec tunnels to the hub It can send ADVPN shortcut requests.

Answer: B

NEW QUESTION 10

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="10.64.1.1" 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="cfl150ded109a548/165f413d17cecc49" 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
```

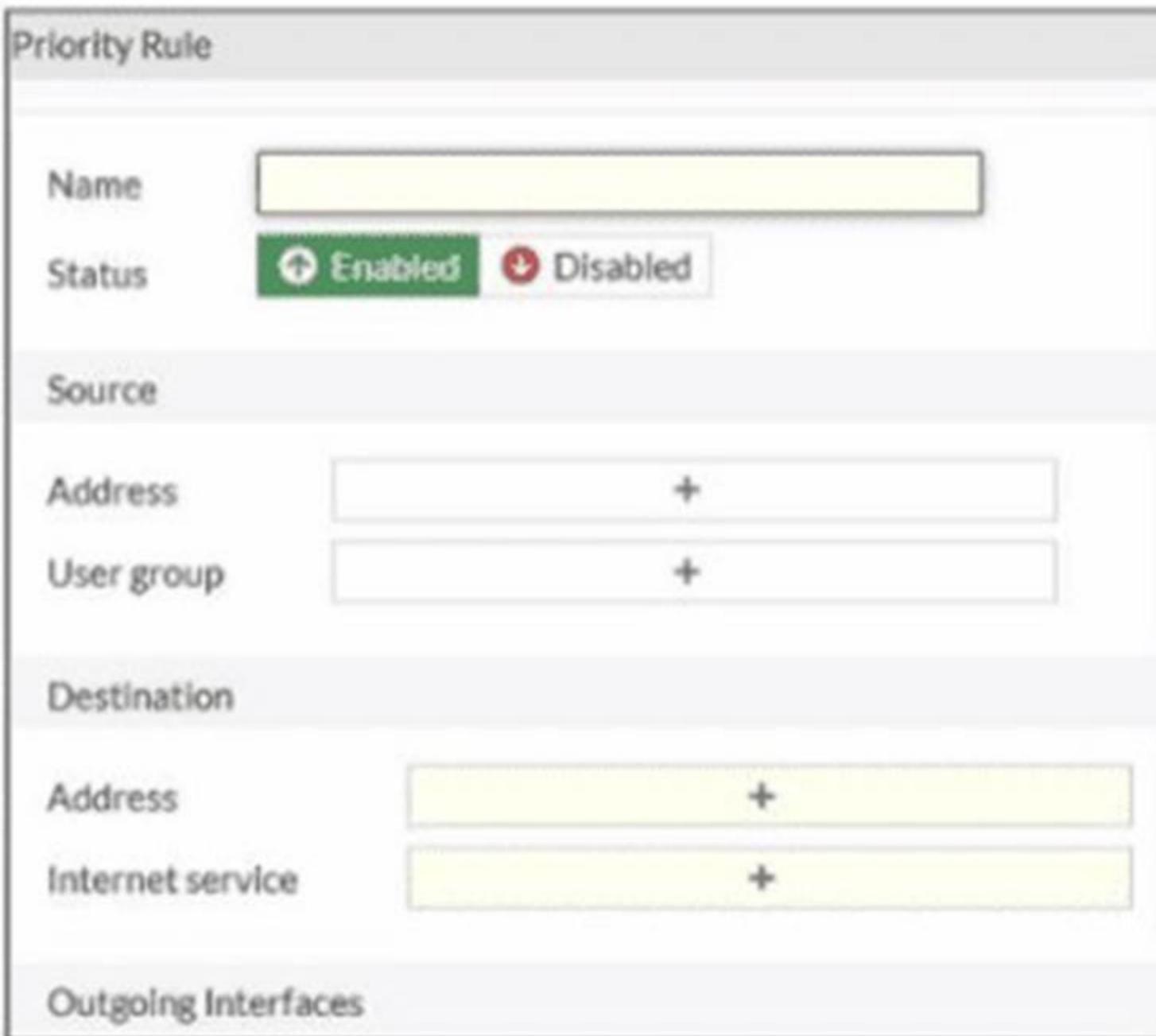
Based on the output shown in the exhibit, what can you say about the tunnels on this device?

- 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 10

Refer to the exhibit.



An administrator configures SD-WAN rules for a DIA setup using the FortiGate GUI. The page to configure the source and destination part of the rule looks as shown in the exhibit. The GUI page shows no option to configure an application as the destination of the SD-WAN rule Why?

- A. You cannot use applications as the destination when FortiGate is used for a DIA setup.
- B. FortiGate allows the configuration of applications as the destination of SD-WAN rules only on the CLI.

- C. You must enable the feature on the CLI.
- D. You must enable the feature first using the GUI menu System > Feature Visibility.

Answer: A

NEW QUESTION 15

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 16

.....

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](#)