

Fortinet

NSE6_SDW_AD-7.6

Fortinet NSE 6 - SD-WAN 7.6 Enterprise Administrator

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



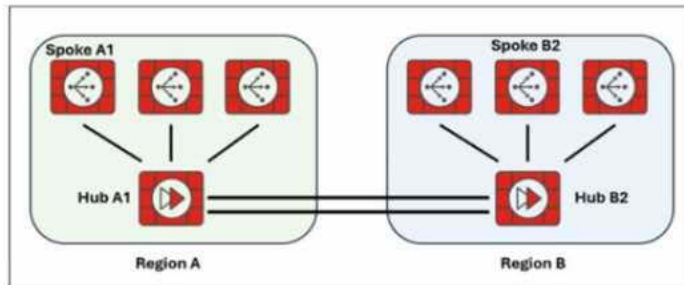
<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/nse6-sdw-ad-7-6>

Latest Version: 6.0

Question: 1

Exhibit.



Two hub-and-spoke groups are connected through redundant site-to-site IPsec VPNs between Hub 1 and Hub 2

Which two configuration settings are required for the spoke A1 to establish an ADVPN shortcut with the spoke B2? (Choose two.)

- A. On hubs, auto-discovery-forwarder must be enabled on the IPsec VPNs to hubs.
- B. On hubs, auto-discovery-receiver must be enabled on the IPsec VPNs to spokes.
- C. On hubs, auto-discovery-forwarder must be enabled on the IPsec VPNs to spokes.
- D. On hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes

Answer: A, D

Explanation:

To allow spokes in different hub-and-spoke groups to establish ADVPN shortcuts, the hubs must be configured to forward and send ADVPN shortcut offers. The key required settings on the hub are auto-discovery-forwarder (for VPNs to hubs) and auto-discovery-sender (for VPNs to spokes). This ensures the hub can facilitate and advertise ADVPN shortcut offers between spokes.

Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q1]

Fortinet SD-WAN 7.4 ADVPN Guide (Auto-discovery settings for hub-and-spoke topologies)

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: D

Explanation:

Traffic steering in Fortinet SD-WAN is based on defined rules and the corresponding outgoing interfaces. The exhibit (not shown here) would indicate that the traffic from the LAN subnet 10.0.1.0/24 to the server 10.2.5.254 is matched by SD-WAN rule 3 and sent out via the HUB1-VPN3

interface.

Reference:

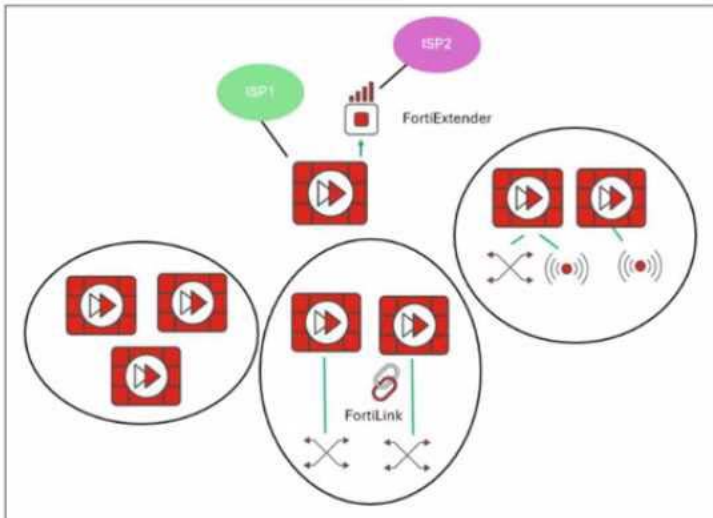
[FCSS_SDW_AR-7.4 1-0.docx Q2]

FortiOS 7.4 SD-WAN Concept Guide – Rule Matching

Question: 3

Refer to the exhibit.

SD-WAN Network Topology



Refer to the exhibit.

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

Answer: B

Explanation:

In Fortinet SD-WAN, hubs should not have extensions like FortiSwitch, FortiAP, or FortiExtender installed, as these can affect hub functionality and scalability. While all device types can be included in the topology, the hubs must be "clean" FortiGate devices without such extensions to ensure proper ADVPN and overlay management.

Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q3]

Fortinet SD-WAN Reference Architecture Guide 7.4 – Hub requirements

Question: 4

Refer to the exhibit.

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="cffi150ded109a548/165f413d17cecc49" 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
```

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 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: C

Explanation:

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 SDWAN's application-aware steering, which uses dynamic performance metrics to select the optimal path.

Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q4]

FortiOS 7.4 SD-WAN Application-Aware Routing Documentation

Question: 5

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: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>