

Exam Questions NSE7_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2

https://www.2passeasy.com/dumps/NSE7_SDW-7.2/



NEW QUESTION 1

Refer to the exhibits.

Exhibit A

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

Exhibit B -

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
Members(2):
  1: Seq_num(5 T_MPLS_0), alive, sla(0x3), gid(0), cfg_order(2), cost(0), selected
  2: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  3: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), 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

branch1_fgt # get router info routing-table all | grep T_
S      10.0.0.0/8 [1/0] via T_INET_0_0 tunnel 100.64.1.1
        [1/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.201.1.254/32 [15/0] via T_INET_0_0 tunnel 100.64.1.1
S      10.202.1.254/32 [15/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.203.1.254/32 [15/0] via T_MPLS_0 tunnel 172.16.1.5

branch1_fgt # diagnose sys sdwan member | grep T_
Member(3): interface: T_INET_0_0, flags=0x4, gateway: 100.64.1.1, peer: 10.201.1.254,
priority: 0 1024, weight: 0
Member(4): interface: T_INET_1_0, flags=0x4, gateway: 100.64.1.9, peer: 10.202.1.254,
priority: 0 1024, weight: 0
Member(5): interface: T_MPLS_0, flags=0x4, gateway: 172.16.1.5, peer: 10.203.1.254,
priority: 0 1024, weight: 0
```

Exhibit A shows the configuration for an SD-WAN rule and exhibit B shows the respective rule status, the routing table, and the member status.

The administrator wants to understand the expected behavior for traffic matching the SD- WAN rule.

Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

- A. The traffic will be load balanced across all three overlays.
- B. The traffic will be routed over T_INET_0_0.
- C. The traffic will be routed over T_MPLS_0.
- D. The traffic will be routed over T_INET_1_0.

Answer: C

NEW QUESTION 2

What is a benefit of using application steering in SD-WAN?

- A. The traffic always skips the regular policy routes.
- B. You steer traffic based on the detected application.
- C. You do not need to enable SSL inspection.
- D. You do not need to configure firewall policies that accept the SD-WAN traffic.

Answer: B

NEW QUESTION 3

Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.

```
config vpn ipsec phase1-interface
edit "T_INET_0_0"
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
set comments "[created by FMG VPN Manager]"
set idle-timeout enable
set idle-timeoutinterval 5
set auto-discovery-receiver enable
set remote-gw 100.64.1.1
set psksecret ENC
6D5rVsaKlMeAyVYt1z95BS24Psew76lwY023hnFVviwb6deItSc5ltCa+iNYhujT8gycfD4+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUFaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
LReOFShoH0lSPFKz5IYCVa==
next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD- WAN?

- A. You must set ike-version to 1.
- B. You must enable net-device.
- C. You must enable auto-discovery-sender.
- D. You must disable idle-timeout.

Answer: B

NEW QUESTION 4

Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(2):
  1: Seq_num(1 port1), alive, selected
  2: Seq_num(2 port2), alive, selected
Internet Service(3): GoToMeeting(4294836966,0,0,0 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0 41468) Salesforce(4294837976,0,0,0 16920)
Src address(1):
  10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(1):
  1: Seq_num(2 port2), alive, selected
Internet Service(2): Facebook(4294836806,0,0,0 15832) Twitter(4294838278,0,0,0 16001)
Src address(1):
  10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list

Facebook(15832 4294836806): 157.240.229.35 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.205.106.86 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.212.249.144 6 443 Tue Mar  8 12:24:39 2022
Salesforce(16920 4294837976): 23.212.249.11 6 443 Tue Mar  8 12:24:04 2022

branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1
         [1/0] via 192.2.0.10, port2
...
```

Exhibit B

Destination IP	Service	Application	Security Event Lst	SD-WAN Rule Name	Destination Interface
23.212.248.208	HTTPS	GoToMeeting	asn:2	Critical-DIA	port2
23.205.106.86	HTTPS	GoToMeeting	asn:2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	asn:2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	asn:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	asn:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	asn:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	asn:2	Critical-DIA	port2
23.205.106.86	HTTPS	GoToMeeting	asn:2	Critical-DIA	port2

Security	APP Count	0
Level	Level	notice
General	Log ID	0000000013
	Session ID	769
	Trans Display	enat
	Virtual Domain	nat
Source	Country	Reserved
	Device ID	FDVH017H42000077
	Device Name	branch1_fgt
	IP	10.0.1.101
	Interface	port1
	Interface Role	outbound
	NAT IP	192.2.0.9
	NAT Port	55042
	Port	55042
	Source	10.0.1.101
	UEBA Endpoint ID	1025
	UEBA User ID	3
Destination	Country	United States
	End User ID	3
	Endpoint ID	155
	Host Name	www.gotomeeting.com
	IP	23.212.248.208
	Interface	port2

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in exhibit A. After generating GoToMeeting test traffic, the administrator examined the respective traffic log on FortiAnalyzer, which is shown in exhibit B. The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1. Which two reasons explain why the traffic matched the implicit SD-WAN rule? (Choose two.)

- A. FortiGate did not refresh the routing information on the session after the application was detected.
- B. Port1 and port2 do not have a valid route to the destination.
- C. Full SSL inspection is not enabled on the matching firewall policy.
- D. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

Answer: BC

Explanation:

Study guide 7.2 Page 191

NEW QUESTION 5

Exhibit.

```
# diagnose sys sdwan health-check status

Health Check(Level3 DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393),
bandwidth-up(10235), bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378),
bandwidth-up(10236), bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(131.336), jitter(0.199), mos(4.330),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 T_INET_1): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.226), mos(4.398),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.440), jitter(0.245), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

The exhibit shows the output of the command `diagnose sys sdwan health-check status` collected on a FortiGate device. Which two statements are correct about the health check status on this FortiGate device? (Choose two.)

- A. The health-check VPN_PING orders the members according to the lowest jitter.
- B. The interface T_INET_1 missed one SLA target.
- C. There is no SLA criteria configured for the health-check Level3_DNS.
- D. The interface T_INET_0 missed three SLA targets.

Answer: AC

Explanation:

According to the FortiGate / FortiOS 6.4.2 Administration Guide, the health check status command displays the status of the health check probes for each SD-WAN member interface. The output includes the following information:

? state: the current state of the interface, either alive or dead

? packet-loss: the percentage of packets lost during the health check

? latency: the average round-trip time in milliseconds

? jitter: the variation in latency

? mos: the mean opinion score, a measure of voice quality

? bandwidth: the available bandwidth in kilobits per second for each direction (up, down, bi)

? sla map: a bitmap that indicates which SLA criteria are met or failed Based on the exhibit, the following statements are correct:

? The health-check VPN_PING orders the members according to the lowest jitter. This means that the interface with the lowest jitter value is listed first, followed by the next lowest, and so on1. In the exhibit, the order is T_MPLS, T_INET_1, and T_INET_0.

? There is no SLA criteria configured for the health-check Level3_DNS. This means that the health check does not use any SLA parameters to determine the state of the interface2. In the exhibit, the sla map value is 0x0 for both port1 and port2, indicating that no SLA criteria are applied.

NEW QUESTION 6

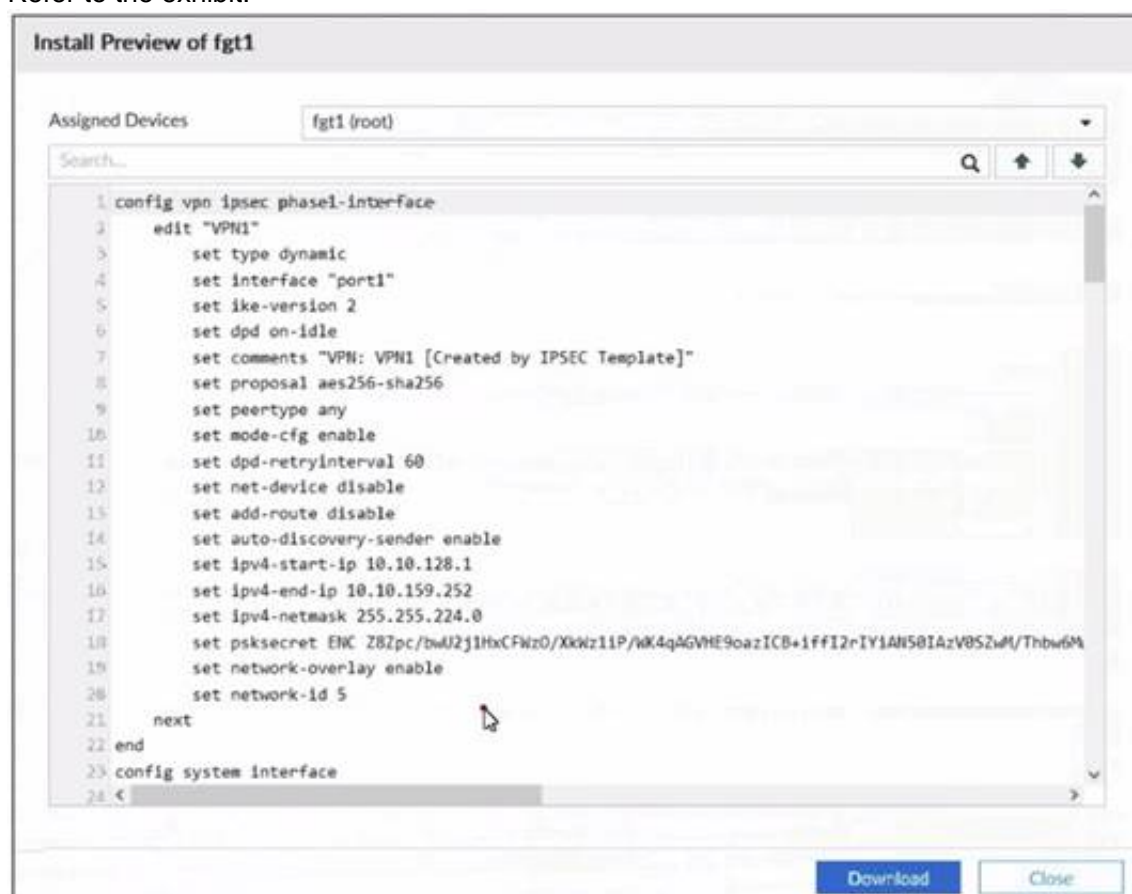
What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

- A. FEC supports hardware offloading.
- B. FEC improves reliability of noisy links.
- C. FEC transmits parity packets that can be used to reconstruct packet loss.
- D. FEC can leverage multiple IPsec tunnels for parity packets transmission.

Answer: BC

NEW QUESTION 7

Refer to the exhibit.



An administrator used the SD-WAN overlay template to prepare an IPsec configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the installation preview for one FortiGate device. In the exhibit, which statement best describes the configuration applied to the FortiGate device?

- A. It is a hub device

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

Answer: C

Explanation:

According to the SD-WAN 7.2 Study Guide, the SD-WAN overlay template simplifies the configuration of IPsec tunnels in a hub-and-spoke topology. The template defines the following parameters:

- ? type: dynamic for spokes, static for hubs
 - ? interface: the WAN interface to use for the IPsec tunnel
 - ? network-overlay: enable for spokes, disable for hubs
 - ? network-id: a unique identifier for each spoke
 - ? auto-discovery-sender: enable for hubs, disable for spokes
 - ? auto-discovery-receiver: enable for spokes, disable for hubs
- Based on the exhibit, the FortiGate device has the following configuration:
- ? type: dynamic
 - ? interface: port1
 - ? network-overlay: enable
 - ? network-id: 5
 - ? auto-discovery-sender: disable
 - ? auto-discovery-receiver: enable

Therefore, the FortiGate device is a spoke that establishes dynamic IPsec tunnels to the hub. It also has the network-overlay and auto-discovery-receiver options enabled, which means it can send ADVPN shortcut requests to other spokes when it receives a shortcut offer from the hub

NEW QUESTION 8

Which statement about SD-WAN zones is true?

- A. An SD-WAN zone can contain only one type of interface.
- B. An SD-WAN zone can contain between 0 and 512 members.
- C. You cannot use an SD-WAN zone in static route definitions.
- D. You can configure up to 32 SD-WAN zones per VDOM.

Answer: D

Explanation:

SD-WAN zones are a group of interfaces that share the same SD-WAN settings, such as health check, SLA, and load balancing. Some characteristics of SD-WAN zones are:

- ? An SD-WAN zone can contain different types of interfaces, such as physical, VLAN, aggregate, and tunnel interfaces1.
- ? An SD-WAN zone can contain up to 512 members1.
- ? You can use an SD-WAN zone in static route definitions, as long as the destination interface is also an SD-WAN zone1.
- ? You can configure up to 32 SD-WAN zones per VDOM1.

NEW QUESTION 9

Which diagnostic command can you use to show the member utilization statistics measured by performance SLAs for the last 10 minutes?

- A. diagnose sys sdwan sla-log
- B. diagnose ays sdwan health-check
- C. diagnose sys sdwan intf-sla-log
- D. diagnose sys sdwan log

Answer: A

NEW QUESTION 10

Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

```
# diagnose firewall shaper traffic-shaper list name VoIP_Shaper
name VoIP_Shaper
maximum-bandwidth 6250 KB/sec
guaranteed-bandwidth 2500 KB/sec
current-bandwidth 93 KB/sec
priority 2
overhead 0
tos ff
packets dropped 0
bytes dropped 0
```

- A. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.
- B. The measured bandwidth is less than 100 KBps.
- C. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.
- D. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

Answer: BC

NEW QUESTION 10

What are two benefits of using the Internet service database (ISDB) in an SD-WAN rule? (Choose two.)

- A. The ISDB is dynamically updated and reduces administrative overhead.
- B. The ISDB requires application control to maintain signatures and perform load balancing.
- C. The ISDB applies rules to traffic from specific sources, based on application type.
- D. The ISDB contains the IP addresses and port ranges of well-known internet services.

Answer: AD

NEW QUESTION 12

In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

- A. It provides the benefits of a full-mesh topology in a hub-and-spoke network.
- B. It provides direct connectivity between spokes by creating shortcuts.
- C. It enables spokes to bypass the hub during shortcut negotiation.
- D. It enables spokes to establish shortcuts to third-party gateways.

Answer: AB

NEW QUESTION 17

Refer to the exhibits. Exhibit A -

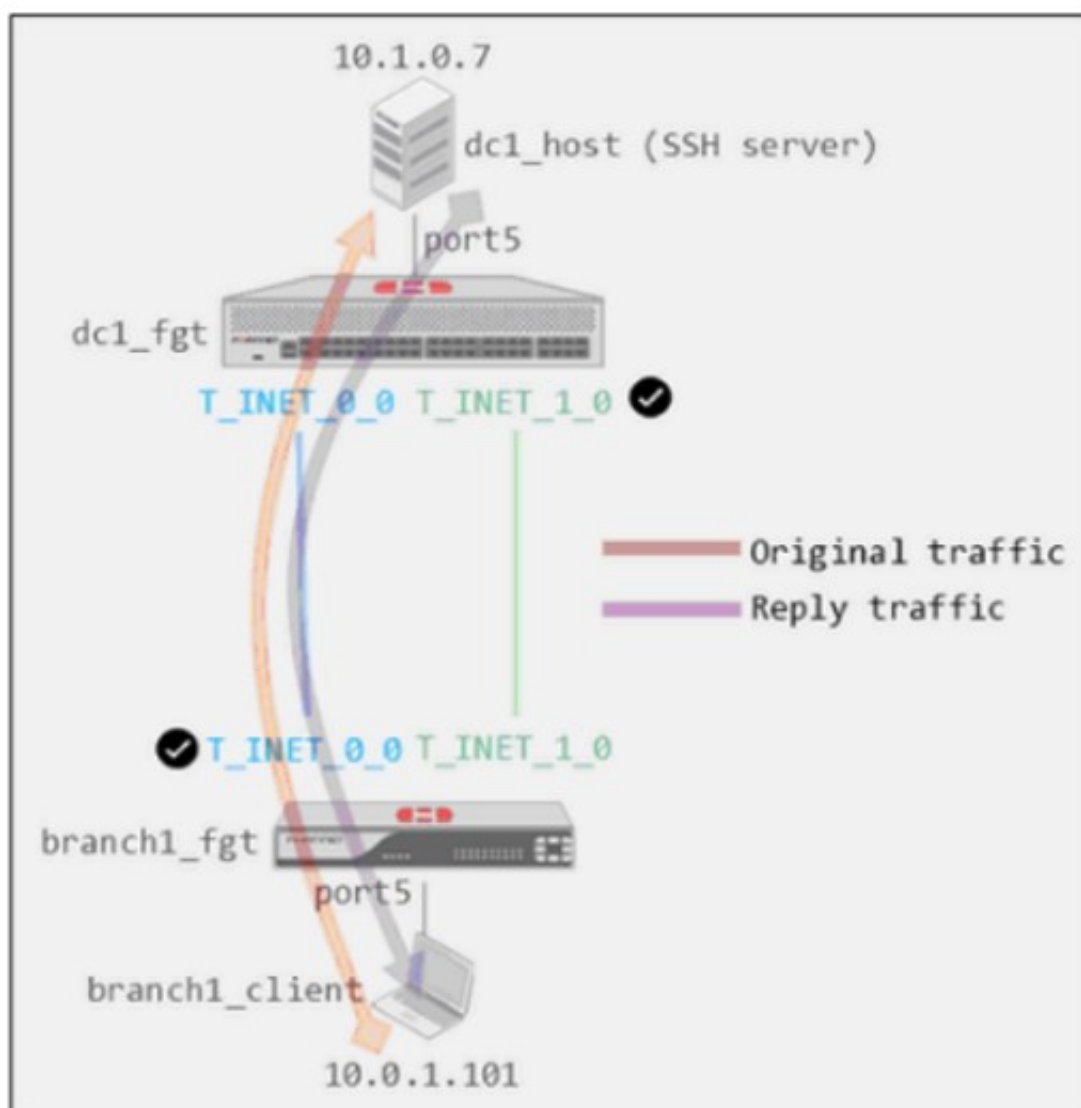


Exhibit B -

```
dc1_fgt # show system global
config system global
    set admin-https-redirect disable
    set admintimeout 480
    set alias "FortiGate-VM64"
    set hostname "dc1_fgt"
    set timezone 04
end

dc1_fgt # show system settings
config system settings
    set tcp-session-without-syn enable
    set allow-subnet-overlap enable
    set gui-allow-unnamed-policy enable
    set gui-multiple-interface-policy enable
end
```

Exhibit A shows a site-to-site topology between two FortiGate devices: branch1_fgt and dc1_fgt. Exhibit B shows the system global and system settings configuration on dc1_fgt.

When branch1_client establishes a connection to dc1_host, the administrator observes that, on dc1_fgt, the reply traffic is routed over T_INET_0_0, even though T_INET_1_0 is the preferred member in the matching SD-WAN rule.

Based on the information shown in the exhibits, what configuration change must be made on dc1_fgt so dc1_fgt routes the reply traffic over T_INET_1_0?

- A. Enable auxiliary-session under config system settings.
- B. Disable tp-session-without-syn under config system settings.

- C. Enable snat-route-change under config system global.
- D. Disable allow-subnet-overlap under config system settings.

Answer: A

NEW QUESTION 20

Which two statements describe how IPsec phase 1 main mode is different from aggressive mode when performing IKE negotiation? (Choose two.)

- A. A peer ID is included in the first packet from the initiator, along with suggested security policies.
- B. XAuth is enabled as an additional level of authentication, which requires a username and password.
- C. Three packets are exchanged between an initiator and a responder instead of six packets.
- D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Answer: AC

NEW QUESTION 25

What is the route-tag setting in an SD-WAN rule used for?

- A. To indicate the routes for health check probes.
- B. To indicate the destination of a rule based on learned BGP prefixes.
- C. To indicate the routes that can be used for routing SD-WAN traffic.
- D. To indicate the members that can be used to route SD-WAN traffic.

Answer: B

NEW QUESTION 26

The administrator uses the FortiManager SD-WAN overlay template to prepare an SD-WAN deployment. With information provided through the SD-WAN overlay template wizard, FortiManager creates templates ready to install on spoke and hub devices.

Select three templates created by the SD-WAN overlay template for a spoke device. (Choose three.)

- A. System template
- B. BGP template
- C. IPsec tunnel template
- D. CLI template
- E. Overlay template

Answer: ACE

Explanation:

In a FortiManager SD-WAN overlay template configuration for a spoke device, the system template (A) is created to provide basic device settings. The IPsec tunnel template (C) is generated to establish secure tunnels between the spoke and the hub devices. Lastly, the overlay template (E) is configured to specify the overlay network settings, which often include the SD-WAN rules and performance SLAs.

NEW QUESTION 30

Which type statements about the SD-WAN members are true? (Choose two.)

- A. You can manually define the SD-WAN members sequence number.
- B. Interfaces of type virtual wire pair can be used as SD-WAN members.
- C. Interfaces of type VLAN can be used as SD-WAN members.
- D. An SD-WAN member can belong to two or more SD-WAN zones.

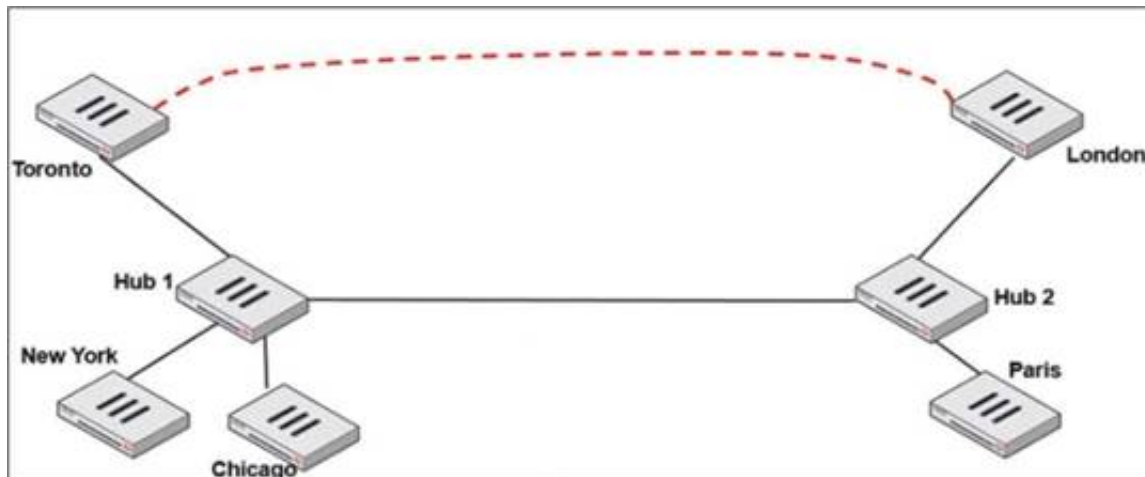
Answer: AC

Explanation:

SD-WAN members can be manually ordered by changing their sequence number (A), which allows administrators to prioritize the interfaces according to the routing requirements. Also, VLAN interfaces can be used as SD-WAN members (C), providing flexibility in network design and the use of existing VLAN infrastructure within the SD-WAN setup.

NEW QUESTION 35

Refer to the exhibit.



Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2.

Which two configuration settings are required for Toronto and London spokes to establish an ADVPN shortcut? (Choose two.)

- A. On the hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.

- B. On the spokes, auto-discovery-receiver must be enabled on the IPsec VPN to the hub.
- C. auto-discovery-forwarder must be enabled on all IPsec VPNs.
- D. On the hubs, net-device must be enabled on all IPsec VPNs.

Answer: AB

NEW QUESTION 37

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_SDW-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_SDW-7.2 Product From:

https://www.2passeasy.com/dumps/NSE7_SDW-7.2/

Money Back Guarantee

NSE7_SDW-7.2 Practice Exam Features:

- * NSE7_SDW-7.2 Questions and Answers Updated Frequently
- * NSE7_SDW-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_SDW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year