

New NSE6_SDW_AD-7.6 Test Forum | NSE6_SDW_AD-7.6 Online Training Materials



If you fail NSE6_SDW_AD-7.6 exam with our NSE6_SDW_AD-7.6 exam dumps, we will full refund the cost that you purchased our NSE6_SDW_AD-7.6 exam dumps. However, our promise of "No help, full refund" doesn't shows our no confidence to our products; oppositely, it expresses our most sincere and responsible attitude to reassure our customers. With our professional NSE6_SDW_AD-7.6 Exam software, you will be at ease about your NSE6_SDW_AD-7.6 exam, and you will be satisfied with our after-sale service after you have purchased our NSE6_SDW_AD-7.6 exam software.

Fortinet NSE6_SDW_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	Rules and routing: This section explains how to design and apply SD-WAN rules to control traffic steering across multiple WAN links. It also includes configuring SD-WAN routing to ensure proper path selection and connectivity between networks.
Topic 2	Advanced IPsec: This section covers the deployment of advanced IPsec configurations within SD-WAN environments. It includes implementing hub-and-spoke IPsec topologies, configuring ADVPN, and supporting multihub, multiregion, and large-scale secure SD-WAN deployments.
Topic 3	SD-WAN setup: This domain covers how to deploy an enterprise SD-WAN environment by designing SD-WAN members and zones and configuring them for efficient traffic management. It also focuses on implementing Performance SLAs to monitor link quality and ensure applications use the best available path.
Topic 4	SD-WAN troubleshooting: This domain explains how to diagnose and resolve issues related to SD-WAN operation. It includes troubleshooting SD-WAN rules, session behavior, routing problems, and ADVPN connectivity to maintain reliable network performance.
Topic 5	Centralized management: This domain focuses on deploying and managing SD-WAN using FortiManager for centralized control. It includes implementing branch configuration deployment and using SD-WAN Manager with overlay orchestration to simplify large-scale network management.

>> NewNSE6_SDW_AD-7.6 Test Forum <<

Fortinet NSE6_SDW_AD-7.6 - Fortinet NSE 6 - SD-WAN 7.6 Enterprise Administrator Marvelous New Test Forum

As one of the most professional dealer of NSE6_SDW_AD-7.6 practice questions, we have connection with all academic institutions in this line with proficient researchers of the knowledge related with the NSE6_SDW_AD-7.6 exam materials to meet your tastes and needs, please feel free to choose. And we have three versions of NSE6_SDW_AD-7.6 training guide: the PDF,

Software and APP online for you. You can choose the one which you like best.

Fortinet NSE 6 - SD-WAN 7.6 Enterprise Administrator Sample Questions (Q13-Q18):

NEW QUESTION # 13

Refer to the exhibits.

SD-WAN overlay template advanced settings

Advanced ▾

Loopback IP Address: 10.200.99.252/255.255.255.0

Overlay Network: 10.200.99.0/255.255.255.0

BGP-AS Number: 65000

BGP on Loopback: ☐

Dynamic BGP: ☒

Route Reflection: ☐

Auto-Discovery VPN: Disable Legacy ADVPN 2.0

Segmentation Over Single Overlay *i*: ☐

Underlay and network advertisement configuration

Secondary HUB

Underlay

#	Private Link <i>i</i>	Override IP <i>i</i>	Action
WAN Underlay 1	port1		☐ x +
WAN Underlay 2	port2		☒ x +

Network Advertisement

Connected Static

#	Interface	Action
Interface 1	port5	x +

The SD-WAN overlay template, advanced settings, and the underlay and network advertisement settings are shown.

These are the configurations for the secondary hub of a dual-hub SD-WAN topology created with the FortiManager SD-WAN overlay orchestrator.

Which two conclusions can you draw from the information shown in the exhibits? (Choose two.)

- A. FortiManager will create an overlay tunnel on the port2 interface.
- B. FortiManager will create an overlay tunnel on the port1 interface.
- C. FortiManager will define port2 as a BGP neighbor.
- D. FortiManager will define port5 as a BGP neighbor.

Answer: A,B

Explanation:

In the SD-WAN overlay orchestrator, the interfaces defined under Underlay (WAN Underlay 1 = port1, WAN Underlay 2 = port2) are used as the physical underlay over which IPsec/overlay tunnels are built. Therefore, FortiManager will create overlay tunnels on port1 and port2.

NEW QUESTION # 14

Refer to the exhibits.

IPsec template for Branch_IPsec_1

Template Groups: IPsec Tunnel | SD-WAN

+ Create New | Edit | Delete

Name: Branch_IPsec_1

Description:

+ Create New | Edit | Delete | More

☐	Name	Type	Outgoing Interface
☐	HUB1-VPN1	Static	\$(ISP1)

IPsec template for Branch_IPsec_2

Template Groups: IPsec Tunnel | SD-WAN

+ Create New | Edit | Delete

Name: Branch_IPsec_2

Description:

+ Create New | Edit | Delete | More

☐	Name	Type	Outgoing Interface
☐	HUB1-VPN2	Static	\$(ISP2)

Error message in FortiManager

Invalid template assignment - conflicting template assignment scope: device branch1_fgt, vdom root, _ipsec template [Branch_IPsec_1] and [Branch_IPsec_2]

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

Answer: D

Explanation:

The FortiManager SD-WAN overlay system allows only one IPsec template to be assigned to each device per overlay operation.

The guide clarifies:

"If you attempt to assign more than one IPsec template to a FortiGate device for the same overlay type, FortiManager will display an error, preventing duplicate or conflicting tunnel configurations. This limitation ensures a one-to-one mapping between device and overlay template per operation, maintaining configuration integrity and preventing routing issues." This prevents complex troubleshooting scenarios and enforces best practices for overlay design.

NEW QUESTION # 15

You are planning a new SD-WAN deployment with the following criteria:

- Two regions
- Most of the traffic is expected to remain within its region
- No requirement for inter-region ADVPN

To remain within the recommended best practices, which routing protocol should you select for the overlays?

- A. IBGP with BGP on loopback within each region and EBGp between the regions.
- B. OSPF for the routing within each region and EBGp between the regions.
- C. IBGP within each region and between the regions.
- D. IBGP with BGP per overlays within each region and IBGP with BGP on loopback between the regions.

Answer: A

Explanation:

Using iBGP with BGP on loopback within each region ensures scalable and stable routing inside the region, while eBGP between regions aligns with best practices to maintain clear boundaries, reduce convergence complexity, and support region separation.

NEW QUESTION # 16

Refer to the exhibit.

```
config system sdwan
  config health_check
    edit "DNS"
      set server "4.2.2.1" "4.2.2.2"
      set detect-mode active
      set protocol ping
      set embed-measured-health enable
      set members 3 4
    config sla
      edit 1
        set link-cost-factor latency
        set latency-threshold 100
      end
    next
  end
end
```

The exhibit shows the health-check configuration on a FortiGate device used as a spoke. You notice that the hub FortiGate doesn't prioritize the traffic as expected.

Which two configuration elements should you check on the hub? (Choose two.)

- A. The performance SLA has the parameter priority-out-sla configured.
- B. This performance SLA uses the same members.
- C. The performance SLA uses the same criteria.
- D. The performance SLA is configured with set embedded-measure accept.

Answer: C,D

Explanation:

The hub must use a performance SLA with the same criteria as the spoke's health check. The spoke's health check is using ping (protocol ping) and measuring latency (link-cost-factor latency). For the hub to use the data sent by the spoke, its performance SLA must be configured to measure the same metrics. If the hub is looking for jitter or packet loss, it will not use the latency data sent by the spoke.

When a spoke sends embedded health data, the hub FortiGate must be configured to receive and use it. This is done by setting set embedded-measure accept within the performance SLA configuration on the hub. This setting explicitly tells the hub to trust and use the performance metrics received from the remote FortiGate (the spoke). Without this setting, the hub will likely ignore the embedded health data and rely on its own health checks, which could lead to incorrect traffic prioritization.

NEW QUESTION # 17

Which two statements correctly describe what happens when traffic matches the implicit SD-WAN rule? (Choose two.)

- Answer: A,D**

• • • • •

NSE6 SDW AD-7.6 Online Training Materials: [https://www.fre dumps.top/NSE6 SDW AD-7.6-real-exam.html](https://www.fre dumps.top/NSE6%20SDW%20AD-7.6-real-exam.html)

- [illegible]