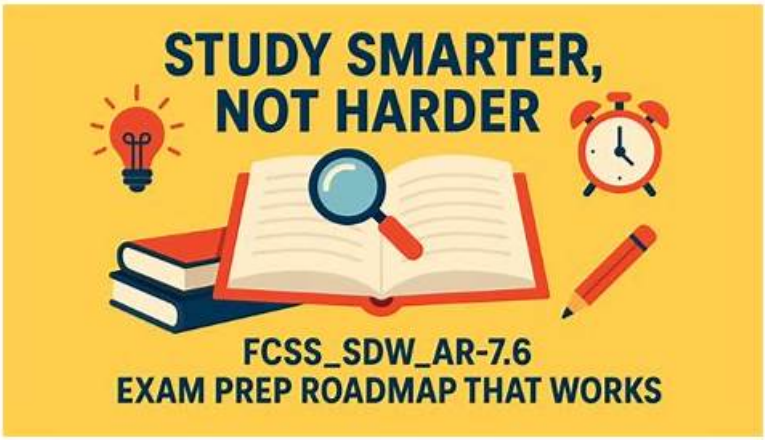
Latest FCSS_SDW_AR-7.6 Exam Book - Latest FCSS_SDW_AR-7.6 Exam Guide



As a responsible company, we don't ignore customers after the deal, but will keep an eye on your exam situation. Although we can assure you the passing rate of our FCSS_SDW_AR-7.6 training guide nearly 100 %, we can also offer you a full refund if you still have concerns. So you have nothing to worry about, only to study with our FCSS_SDW_AR-7.6 Exam Questions with full attention. And as we have been in this career for over ten years, our FCSS_SDW_AR-7.6 learning materials have became famous as a pass guarantee.

Fortinet FCSS_SDW_AR-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Centralized Management: This domain addresses FortiManager-based SD-WAN deployment, branch configuration implementation, and overlay orchestration using SD-WAN Manager.
Topic 2	• Rules and Routing: This section focuses on configuring SD-WAN rules for traffic steering and routing policies for path selection and failover.
Topic 3	• SD-WAN Basic Setup: This domain covers initial SD-WAN configuration, member and zone setup, and Performance SLA creation for link monitoring.
Topic 4	• Advanced IPsec: This section covers hub-and-spoke topologies, ADVPN configuration, and scalable multihub and multiregion IPsec deployments.
Topic 5	• SD-WAN Troubleshooting: This domain focuses on diagnosing SD-WAN rule behavior, routing issues, and ADVPN tunnel problems.

>> Latest FCSS_SDW_AR-7.6 Exam Book <<

Latest FCSS_SDW_AR-7.6 Exam Guide | FCSS_SDW_AR-7.6 Valid Exam Voucher

Nowadays, online learning is very popular among students. Most candidates have chosen our FCSS_SDW_AR-7.6 learning engine to help them pass the exam. Our company has accumulated many experiences after ten years' development. We never stop researching and developing the new version of the FCSS_SDW_AR-7.6 practice materials. With our FCSS_SDW_AR-7.6 study questions, you can easily get your expected certification as well as a brighter future.

Fortinet FCSS - SD-WAN 7.6 Architect Sample Questions (Q87-Q92):

NEW QUESTION # 87
Refer to the exhibit.
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 uses the same criteria.
- B. The performance SLA has the parameter priority-out-sla configured.
- C. This performance SLA uses the same members.
- D. The performance SLA is configured with set embedded-measure accept.

Answer: A,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 # 88
(Refer to the exhibits.
The SD-WAN zones and members configuration of two branch devices are shown. The two branch devices are part of the same hub-and-spoke topology and connect to the same hub. The devices are configured to allow Auto-Discovery VPN (ADVPN). The configuration on the hub allows the initial communication between the two spokes.
When traffic flows require it, between which interfaces can the devices establish shortcuts? Choose one answer.)

- A. Interface connected to HUB only
- B. Between T2 on Branch-A and TA on Branch-B
- C. Any interface in the overlay zones
- D. Between T3 on Branch-A and TC on Branch-B

Answer: B

Explanation:
From the exhibit, both branches have an SD-WAN zone named overlay with set advpn-select enable, and each SD-WAN member in that zone is assigned a transport-group value.
Branch-A members:
T1 → transport-group 1
T2 → transport-group 1
T3 → transport-group 2
Branch-B members:
TA → transport-group 1
TB → transport-group 2
TC → transport-group 3
In FCSS SD-WAN 7.6 ADVPN design, transport-group is used to constrain which underlays are allowed to form ADVPN shortcuts with each other. A spoke can establish an ADVPN shortcut only between interfaces that belong to the same transport-group on both sides. This prevents building shortcuts across dissimilar transports.
Evaluating the options:
Option D (T2 on Branch-A with transport-group 1 and TA on Branch-B with transport-group 1) is a valid shortcut pairing.
Option C is not valid because T3 is transport-group 2 while TC is transport-group 3, so they are not permitted to form a shortcut.
Option A is incorrect because not all overlay-zone interfaces are eligible; eligibility is restricted by transport-group matching.
Option B is incorrect because ADVPN shortcuts are spoke-to-spoke tunnels (facilitated by the hub), not limited to "interfaces connected to hub only." Therefore, the valid shortcut pairing listed is between T2 on Branch-A and TA on Branch-B, which corresponds to Option D.

NEW QUESTION # 89
Refer to the exhibits. The administrator configured a device blueprint and CLI scripts as shown in the exhibits, to prepare for onboarding FortiGate devices in the company's stores. Later, a technician prepares a FortiGate 51G with a basic configuration and connects it to the network.
The basic configuration contains the port1 configuration and the minimal configuration required to allow the device to connect to FortiManager.
After the device first connects to FortiManager, FortiManager updates the device configuration.
Based on the exhibits, which actions does FortiManager perform?

- A. FortiManager updates access rights only for port1. FortiManager cannot update the IP address because it was already set manually.
- B. FortiManager updates the configuration of port1, port2, and port5. The three ports might get new IP addresses.
- C. FortiManager does not update the port1 configuration because FortiManager does not change the configuration of interfaces with fgfm access.
- D. FortiManager updates the device configuration according to the selected templates. It applies the corp_st template first.

Answer: B

Explanation:
Enforce Device Configuration is enabled and the blueprint applies the provisioning CLI templates.
The LAN-interface script sets port1 and port2 to DHCP and assigns a static IP to port5 (using the branch_id variable). Therefore, when FortiManager pushes the blueprint, it updates the configurations of port1, port2, and port5 - and their IP addresses may change accordingly.

NEW QUESTION # 90
(Refer to the exhibit. The administrator configured two SD-WAN rules to load balance the traffic.
Which interfaces does FortiGate use to steer the traffic from 10.0.1.124 to 10.0.0.254? Choose one answer.)

- A. HUB2-VPN2
- B. port1 or port2
- C. HUB1-VPN2 or HUB2-VPN2
- D. Any interface in the HUB1 or HUB2 zones

Answer: C

Explanation:
The exhibit shows the runtime details of two SD-WAN services (rules):
Service(2)
Mode(manual hash-mode=inbandwidth)
Members(2): port2 (WAN2), port1 (WAN1)
Application matching: Facebook, LinkedIn, Game
Source: 10.0.1.0-10.0.1.255
This rule is clearly intended for internet/DIA application steering and does not show a corporate destination range.
Service(3)
Mode(sla hash-mode=round-robin)
Members(6): HUB1-VPN1/2/3 and HUB2-VPN1/2/3
Source: 10.0.1.0-10.0.1.255
Destination: 10.0.0.0-10.255.255.255
Traffic from 10.0.1.124 to 10.0.0.254 matches Service(3) because the destination IP 10.0.0.254 falls within the destination range 10.0.0.0-10.255.255.255.
Within Service(3), the member list shows SLA results per interface:
HUB1-VPN2 has sla(0x1) and num of pass(1)
HUB2-VPN2 has sla(0x2) and num of pass(1)
The remaining members (HUB1-VPN1, HUB2-VPN1, HUB1-VPN3, HUB2-VPN3) show sla(0x0) and num of pass(0) This indicates that, for Service(3), only HUB1-VPN2 and HUB2-VPN2 are currently meeting the SLA requirements (passing), and because the rule uses hash-mode=round-robin, FortiGate load-balances sessions across the passing members.
Therefore, FortiGate will steer the traffic using HUB1-VPN2 or HUB2-VPN2, which corresponds to Option B.

NEW QUESTION # 91
Refer to the exhibit. Which action will FortiGate take if it detects SD-WAN members as dead?

- A. FortiGate sends alert messages through poft5 when it detects all SD-WAN members as dead.
- B. FoftiGate bounces port5 after it detects all SD-WAN members as dead.
- C. FortiGate fails over to the secondary device after it detects port5 as dead.
- D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

Answer: D

Explanation:

NEW QUESTION # 92
......

Of course, when we review a qualifying exam, we can't be closed-door. We should pay attention to the new policies and information related to the test FCSS_SDW_AR-7.6 certification. For the convenience of the users, the FCSS_SDW_AR-7.6 test materials will be updated on the homepage and timely update the information related to the qualification examination. As a result, the FCSS_SDW_AR-7.6 Test Prep can help users to spend the least time, know the test information directly, let users save time and used their time in learning the new hot spot concerning about the knowledge content.

myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, dl.instructure.com, Disposable vapes