prep BOLT

Prepare Smart for Success Free Fortinet NSE6_SDW_AD-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 6 - SD-WAN 7.6 Enterprise Administrator exam PDF questions now. Get authentic NSE6_SDW_AD-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE6_SDW_AD-7.6 exam pdf questions and answers.

Thank you for Downloading NSE6_SDW_AD-7.6 exam PDF Demo

https://prepbolt.com/NSE6_SDW_AD-7.6.html

QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Question 1

Question Type: MultipleChoice

Refer to the exhibits.

To prepare to onboard FortiGate devices to your company's stores, you configure the device blueprint and CLI scripts shown in the exhibit. Then, a technician prepares a FortiGate 90G 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 initially connects to FortiManager, FortiManager updates the device configuration.

Based on what is shown in the exhibits, which statement about the actions taken by FortiManager is true?

Options:

A- FortiManager updates the configuration of port1, port2, and port5. The three ports might get new IP addresses

B- FortiManager updates access rights only for port1. FortiManager cannot update the IP address because it was already set manually

C- FortiManager updates the device configuration according to the selected templates and it applies the corp_st template first

D- FortiManager does not update the port1 configuration because FortiManager does not change the configuration of interfaces with FortiGate-FortiManager communication protocol (FGFM) access

Answer:

A

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of SD-WAN 7.6 Enterprise Administrator documents:

When a FortiGate device is onboarded using a Device Blueprint in FortiManager, the system automates the provisioning process by applying the linked templates and scripts as soon as the device is authorized and connects. In this scenario, the Device Blueprint includes a CLI Template named 'LAN-interface' and Provisioning Templates (corp_st and LAN-interface).

According to Fortinet documentation regarding Zero-Touch Provisioning (ZTP) and Blueprint workflows, FortiManager processes the CLI script configuration as part of the initial onboarding sync. The provided CLI script explicitly contains instructions for port1, port2, and port5. Specifically, it sets port1 and port2 to mode dhcp. Even though port1 already has a manual IP address ($15.1.0.154$) used for the initial FGFM connection, the FortiManager will push the configuration defined in the template.

When FortiManager pushes a configuration change to the interface used for the FGFM tunnel (port1), it does so by updating the configuration database. Since the template specifies set mode dhcp for port1 and port2, and a specific IP range for port5 using a metadata variable (10.0.$(branch_id).254), all three ports will be updated. Consequently, they may receive new IP addresses based on DHCP assignments or variable substitution. FortiManager is capable of updating the management interface as long as the new configuration does not permanently sever the FGFM connection.

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

An SD-WAN zone configuration on the FortiGate GUI is shown.

What can you conclude about the zone and member configuration on this device? Choose one answer.)

Options:

A- You can delete the virtual-wan-link zone.
B- The WAN2 zone contains no member.
C- You can delete the WAN1 zone.
D- You can add the member B-125 to the WAN3 zone and keep it as a member of the Test zone.

Answer:

B

Explanation:

From the SD-WAN Zones view in the FortiGate GUI:

virtual-wan-link is the default SD-WAN zone. This zone is system-defined and cannot be deleted, which makes option A incorrect.

The WAN2 zone is displayed without any expandable members beneath it, indicating that no SD-WAN members are currently assigned to the WAN2 zone. This directly supports option B.

A zone can be deleted only if it has no members and is not system-defined, but the exhibit does not indicate that WAN1 is eligible for deletion. Therefore, option C cannot be concluded from the information shown.

In FortiOS SD-WAN, an SD-WAN member can belong to only one SD-WAN zone at a time. A member such as B-125 cannot be assigned to both the WAN3 zone and the Test zone simultaneously, which makes option D incorrect.

Question 3

Question Type: MultipleChoice

(In which order does FortiGate consider the following elements during the route lookup process? Choose one answer.)

Options:

A- SD-WAN rules, ISDB routes, policy routes, BGP routes

B- Policy routes, SD-WAN rules, Internet Service Database (ISDB) routes, BGP routes

C- SD-WAN rules, policy routes, static routes, ISDB routes

D- Policy routes, ISDB routes, SD-WAN rules, static routes

Answer:

D

Explanation:

In FortiOS (including FortiOS 7.6), FortiGate follows a strict and well-defined route lookup order when determining how to forward traffic. This order is critical for understanding SD-WAN behavior and is explicitly referenced in the FCSS SD-WAN curriculum.

The correct lookup sequence is:

Policy routes (Policy-Based Routing)

Policy routes are evaluated first. If traffic matches a policy route, FortiGate immediately forwards the traffic according to that policy and bypasses all other routing mechanisms.

Internet Service Database (ISDB) routes

If no policy route matches, FortiGate checks ISDB routes. These routes match traffic based on Internet Services rather than destination IP prefixes.

SD-WAN rules

If neither a policy route nor an ISDB route matches, FortiGate evaluates SD-WAN rules to determine the outgoing interface based on the configured SD-WAN strategy.

Routing table (connected, static, and dynamic routes such as BGP)

If no SD-WAN rule matches, FortiGate performs a normal routing table lookup.

FIB (Forwarding Information Base)

The FIB is used to forward the packet based on the selected route.

Drop

If no valid route exists, the packet is dropped.

Among the options provided, only Option D correctly reflects the beginning of this sequence by placing policy routes first, followed by ISDB routes, then SD-WAN rules, and finally static routes (representing the routing table).

Therefore, the correct answer is D.

Question 4

Question Type: MultipleChoice

(In the context of SD-WAN, the terms underlay and overlay are commonly used to categorize links.

Which two statements about underlay and overlay links are correct? Choose two answers.)

Options:

A- A VLAN is a type of overlay link.
B- Overlay links provide routing flexibility.
C- FortiLink interface is considered an underlay link.
D- Wireless connections can be used to build overlay links.
E- Only wired connections can be used as underlay links.

Answer:

B, D

Explanation:

In Fortinet SD-WAN architecture, underlay and overlay have distinct meanings:

Underlay links are the physical or logical transport networks that provide basic IP connectivity (for example, broadband, MPLS, LTE/5G).

Overlay links are virtual tunnels (such as IPsec VPNs) built on top of the underlay, providing abstraction, routing control, and segmentation.

Option B is correct.

Overlay links (for example, IPsec tunnels used in SD-WAN and ADVPN) decouple routing from the physical transport. This allows dynamic path selection, segmentation, and flexible routing policies independent of the underlay. Providing routing flexibility is a core purpose of overlays in SD-WAN.

Option D is correct.

Wireless connections such as LTE or 5G can be used as underlay transports, and overlay tunnels can be built over them. Fortinet SD-WAN fully supports building IPsec overlays on wireless underlays, making wireless links valid for overlay construction.

Why the other options are incorrect:

Option A is incorrect because a VLAN is a Layer 2 segmentation mechanism, not an SD-WAN overlay link.

Option C is incorrect because FortiLink is used for internal management and switch/AP connectivity, not as a WAN underlay for SD-WAN.

Option E is incorrect because underlay links can be wired or wireless; they are not limited to wired connections.

Therefore, the two correct statements are B and D.

Question 5

Question Type: MultipleChoice

(You are configuring SD-WAN to load balance network traffic and you want to take into account the link quality.

Which two facts should you consider? Choose two answers.)

Options:

A- When applicable, FortiGate load balances the traffic through all members that meet the SLA target.
B- You can select the best quality strategy and allow SD-WAN load balancing.

C- You can select the lowest cost service level agreement (SLA) strategy and allow SD-WAN load balancing.
D- The best quality strategy supports only the round-robin hash mode.

Answer:

A, C

Explanation:

When SD-WAN load balancing is required with link quality awareness, FortiOS relies on SLA-based strategies. These strategies evaluate link performance using performance SLAs (latency, jitter, packet loss, MOS) and then make forwarding decisions accordingly.

Option A is correct.

In FortiOS 7.6, when an SLA-based SD-WAN rule has load balancing enabled, FortiGate distributes traffic only across the members that meet the SLA targets. Any member that is out of SLA is excluded from load balancing. This behavior ensures that traffic is not forwarded over degraded links while still allowing load distribution across healthy paths.

Option C is correct.

The lowest cost (SLA) strategy is an SLA-based strategy that considers link quality while also allowing SD-WAN load balancing. When multiple members meet the SLA requirements and have equal cost, FortiGate can load balance traffic across them using the configured hash mode. This makes the lowest cost SLA strategy suitable when both link quality and load balancing are required.

Why the other options are incorrect:

Option B is incorrect because the best quality strategy is designed to select the single best-performing link based on SLA metrics. It does not support SD-WAN load balancing across multiple links.

Option D is incorrect because the best quality strategy does not support load balancing at all, so the statement about round-robin hash mode is invalid.

Therefore, the two correct facts to consider are A and C.

Question 6

Question Type: MultipleChoice

(You plan a large SD-WAN deployment for a global company. You want to divide the network architecture into five geographical regions and install two hubs in each region for increased redundancy. You expect a significant amount of traffic within each region and limited traffic flow between spokes in different regions. You plan to connect the small branch sites to only the closest hub in their regions and the large branch sites to the two hubs in the regions.

Which statement about your plan is true? Choose one answer.)

Options:

A- It is possible. You should use eBGP as the routing protocol between the regions.
B- It is not possible. FortiOS 7.6 supports multihub topologies with up to four hubs.
C- It is possible. You should use FortiManager and the overlay orchestrator multihub topology to simplify the deployment.
D- It is not possible. In a region, all spokes must have either single-hub or dual-hub connectivity.

Answer:

A

Explanation:

The described design is a multi-region SD-WAN architecture, where:

Each region has its own dual-hub ADVPN domain

Most traffic is intra-region

Inter-region traffic is limited and controlled

Spokes can be single-hub or dual-hub, depending on size and redundancy requirements

According to Fortinet's SD-WAN Architecture for Enterprise guidance, when deploying multiple ADVPN regions, eBGP is the recommended routing protocol between regions. Each region operates as an independent routing domain (typically iBGP within the region), while eBGP is used to exchange routes between regional hubs. This approach:

Prevents excessive route reflection and scaling issues

Provides clear administrative boundaries between regions

Improves stability and scalability in large global deployments

Matches the exact traffic pattern described (high intra-region, low inter-region traffic)

This is explicitly documented in Fortinet guidance for ''Using eBGP between regions with intra-region ADVPN'', which confirms that the architecture described in the question is valid and recommended when eBGP is used between regions.

Why the other options are incorrect:

Option B is incorrect because FortiOS does not impose a hard ''four-hub'' architectural limit in the described regional model. Each region has its own hubs, not a single flat multihub domain.

Option C is incomplete. While FortiManager Overlay Orchestrator can help operationally, it is not the key architectural requirement that makes this design valid. The question asks what makes the plan correct from a design standpoint, not a tooling standpoint.

Option D is incorrect because FortiOS fully supports mixed spoke connectivity within the same region (some spokes single-hub, others dual-hub), which is a common enterprise SD-WAN design.

Therefore, the correct and documented conclusion is that the plan is possible and eBGP should be used as the routing protocol between regions, which corresponds to Answer A.

Thank You for trying NSE6_SDW_AD-7.6 PDF Demo

To try our NSE6_SDW_AD-7.6 practice exam software visit link below

https://prepbolt.com/NSE6_SDW_AD-7.6.html

Start Your NSE6_SDW_AD-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE6_SDW_AD-7.6 preparation with actual exam questions.