Prepare Smart for Success Free Fortinet NSE5_FSW_AD-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 5 - FortiSwitch 7.6 Administrator exam PDF questions now. Get authentic NSE5_FSW_AD-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE5_FSW_AD-7.6 exam pdf questions and answers.

Thank you for Downloading NSE5_FSW_AD-7.6 exam PDF Demo

https://prepbolt.com/NSE5_FSW_AD-7.6.html

QUESTIONS & ANSWERS

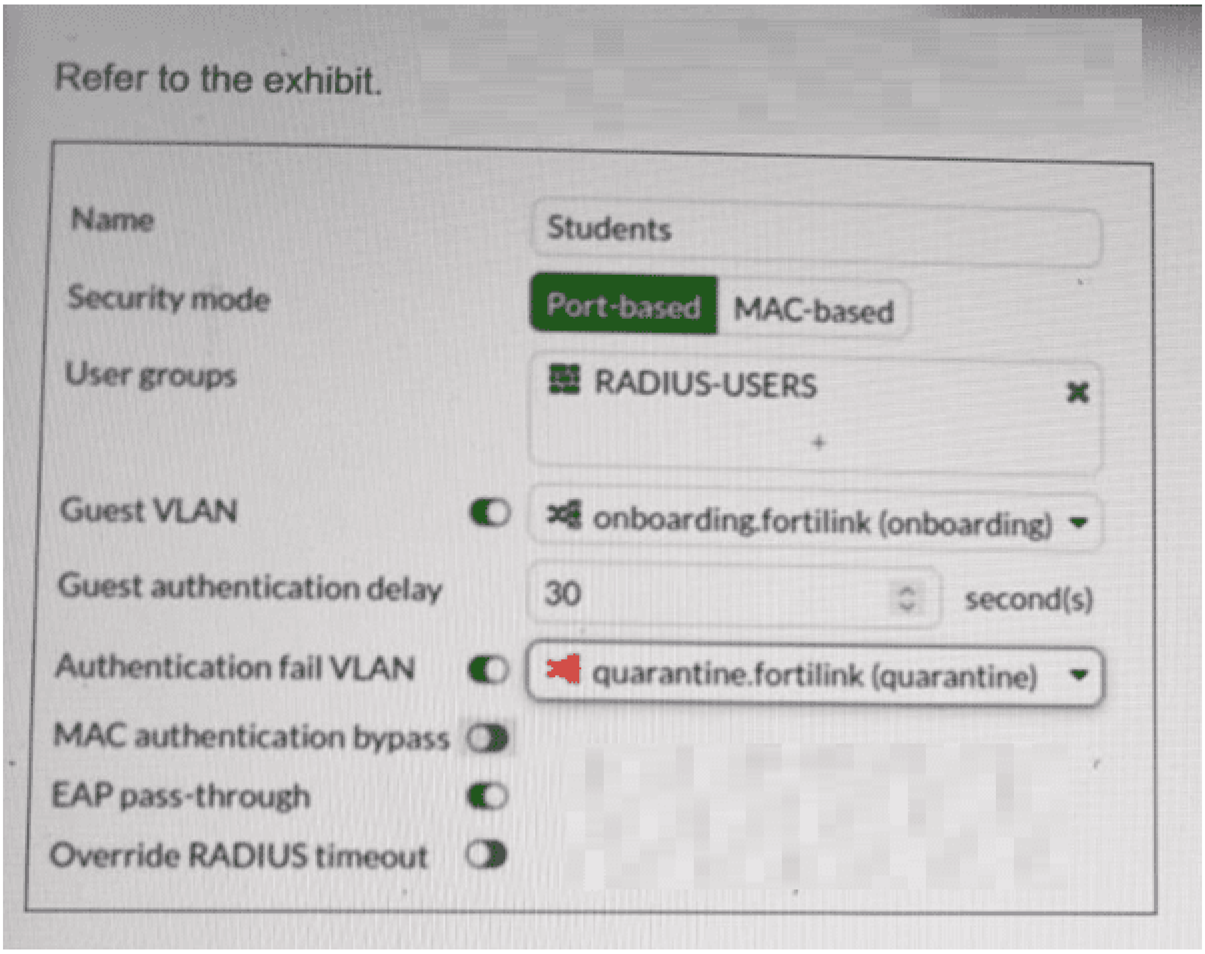
DEMO VERSION

(LIMITED CONTENT)

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit.

Name: Students

Security mode: [✓ Port-based] MAC-based

User groups: RADIUS-USERS

Guest VLAN: ● onboarding.fortilink (onboarding)

Guest authentication delay: 30 second(s)

Authentication fail VLAN: ● quarantine.fortilink (quarantine)

MAC authentication bypass: ○

EAP pass-through: ●

Override RADIUS timeout: ○

FortiSwitch 802.1X port security configuration is shown. A user connects their laptop to the port and attempts to authenticate using 802.1X, but enters the wrong credentials multiple times. What will the result to the device be? (Choose one answer)

Options:

A- The device will be placed into the VLAN quarantine.

B- The port will shut down for security reasons.

C- The device will be placed into the VLAN onboarding.

D- The device will be assigned to the default management VLAN.

Answer:

A

Explanation:

According to theFortiSwitchOS 7.6 Administration Guideand theFortiSwitch 7.6 Study Guide, 802.1X port security allows administrators to define specific actions based on the outcome of an authentication attempt. The configuration exhibit shows a security policy named 'Students' with two specialized VLAN assignments enabled: aGuest VLANand anAuthentication fail VLAN.

In FortiSwitchOS 7.6, these two settings serve distinct purposes based on the client's behavior:

Guest VLAN (Option C):This is used when a connected device doesnothave an 802.1X supplicant (software) or does not respond to EAP (Extensible Authentication Protocol) requests within the specified 'Guest authentication delay'. In this scenario, the device is moved to the 'onboarding' VLAN to allow for basic network access or software downloads.

Authentication fail VLAN (Option A):This is triggered specifically when a devicedoesattempt to authenticate via 802.1X but the authentication server (RADIUS) returns anAccess-Rejectmessage, typically due toincorrect credentials.

As stated in the scenario, the userattemptsto authenticate but enters thewrong credentials. According to the policy shown in the exhibit, theAuthentication fail VLANis enabled and set to'quarantine.fortilink (quarantine)'. Therefore, the FortiSwitch will logically move the port's traffic into the quarantine VLAN, isolating the user from the production network due to the failed login attempt. Option B is incorrect as there is no 'shutdown' action configured, and Option D refers to a default state that is overridden by the explicit failure policy.

Question 2

Question Type: MultipleChoice

What can an administrator do to maintain the existing standalone FortlSwltch configuration while changing the management mode to FortLink?

Options:

A- Use a migration tool based on python script to convert the configuration
B- Enable the Forti-link setting on FortiSwitch before the authorization process
C- FortiGate will automatically save the existing FortiSwitch configuration during the Forti-link management process.
D- Register FortiSwitch to For1ISwitch Cloud to save a copy before managing by Forti-Gate.

Answer:

A

Explanation:

'The tool is a Python script that converts the supported settings in a FortiSwitch standalone configuration file to the equivalent FortiOS settings for a managed switch.'Reference: FortiSwitch 7.6 Study Guide, page 349

Question 3

Question Type: MultipleChoice

(Full question statement start from here)

When you change FortiSwitch management mode fromstandalonetomanaged, what happens to the existing standalone configuration? (Choose one answer)

Options:

A- FortiSwitch registers to FortiSwitch Cloud to save a copy before managing with FortiGate.
B- FortiSwitch merges the existing standalone configuration with the default FortiLink configuration.
C- FortiSwitch saves the standalone configuration and changes to the default FortiLink configuration.
D- FortiGate automatically saves the existing FortiSwitch configuration during the FortiLink management process.

Answer:

C

Explanation:

When a FortiSwitch is converted fromstandalone (local) management modetoFortiGate-managed mode using FortiLink, FortiSwitchOS follows a well-defined and protective transition process. According to the FortiSwitchOS 7.6 Administrator Guide, the switchdoes not mergeits existing standalone configuration with FortiLink-managed settings, nor does FortiGate import or preserve the active configuration for reuse.

Instead, when the management mode change occurs, the FortiSwitchsaves the current standalone configuration internallyand thenresets its operational configuration to the default FortiLink configuration. This default configuration is required so the switch can correctly establish FortiLink control-plane communication with the FortiGate, including CAPWAP-based management, VLAN 4094 usage, and dynamic policy provisioning.

Once the FortiSwitch is under FortiGate management,all configuration is controlled centrally by the FortiGate, including VLANs, port policies, security features, and firmware management. The previously saved standalone configuration is retained only as a backup reference on the switch and isnot actively usedunless the switch is later reverted back to standalone mode.

This behavior ensures configuration consistency, prevents conflicts between local and centralized policies, and aligns the switch with the FortiGate-centricSecurity Fabric architecture. It also avoids unpredictable results that could occur if legacy standalone settings were merged with FortiLink-managed profiles.

The other options are incorrect because FortiSwitch does not register with FortiSwitch Cloud automatically, does not merge configurations, and FortiGate does not back up the standalone configuration during onboarding.

Therefore, the correct and fully documented answer isC. FortiSwitch saves the standalone configuration and changes to the default FortiLink configuration.

Question 4

Question Type: MultipleChoice

You need to deploy routing on a standalone FortiSwitch and want to maximize routing performance. Which type of routing is best for this deployment? (Choose one answer)

Options:

A- Hardware-based routing because it relies on ASIC for faster performance1
B- Software-based routing because it bypasses the CPU to increase routing speed
C- Hardware-based routing because the routing is performed directly by the kernel
D- Software-based routing because it is preferred for high-speed backbone networks

Answer:

A

Explanation:

According to theFortiSwitchOS 7.6 Administration Guideand theFortiSwitch 7.6.1 Administration Guide---Standalone Mode, FortiSwitch units support two primary methods for processing Layer 3 traffic: software-based routing and hardware-based routing. To maximize performance, the documentation specifies thatHardware-based routing (Option A)is the superior choice for high-speed environments.

The primary technical reason for this performance advantage is the use ofApplication-Specific Integrated Circuits (ASICs). In hardware-based routing, the routing table and forwarding information are programmed directly into the switch's specialized hardware silicon. This allows the FortiSwitch to perform packet lookups and forwarding decisions at 'wire speed,' which refers to the full throughput capacity of the physical ports. By offloading these tasks to the ASIC, the switch minimizes latency and prevents the performance bottlenecks associated with general-purpose CPU processing.

In contrast,software-based routing(Options B and D) requires the main system CPU and kernel to process every packet, which is significantly slower and can lead to high CPU utilization during heavy traffic loads. Option C is factually incorrect because hardware-based routing specifically avoids the kernel's software path to increase speed. Therefore, for a deployment focused on maximizing routing performance, especially in a backbone or high-density branch environment, utilizing the ASIC-driven hardware forwarding path is the recommended approach in FortiSwitchOS 7.6.

Question 5

Question Type: MultipleChoice

Which LLDP-MED Type-Length-Values does FortiSwitch collect from endpoints to track network devices and determine their characteristics?

Options:

A- Network policy
B- Power management
C- Location
D- Inventory management

Answer:

D

Explanation:

While FortiSwitch can collect all the listed LLDP-MED TLVs (Network Policy, Power Management, Location, and Inventory Management), the primary focus for tracking and identifying network devices is on theInventory ManagementTLV.

This TLV carries critical details such as:

Manufacturer

Model

Hardware/Firmware versions

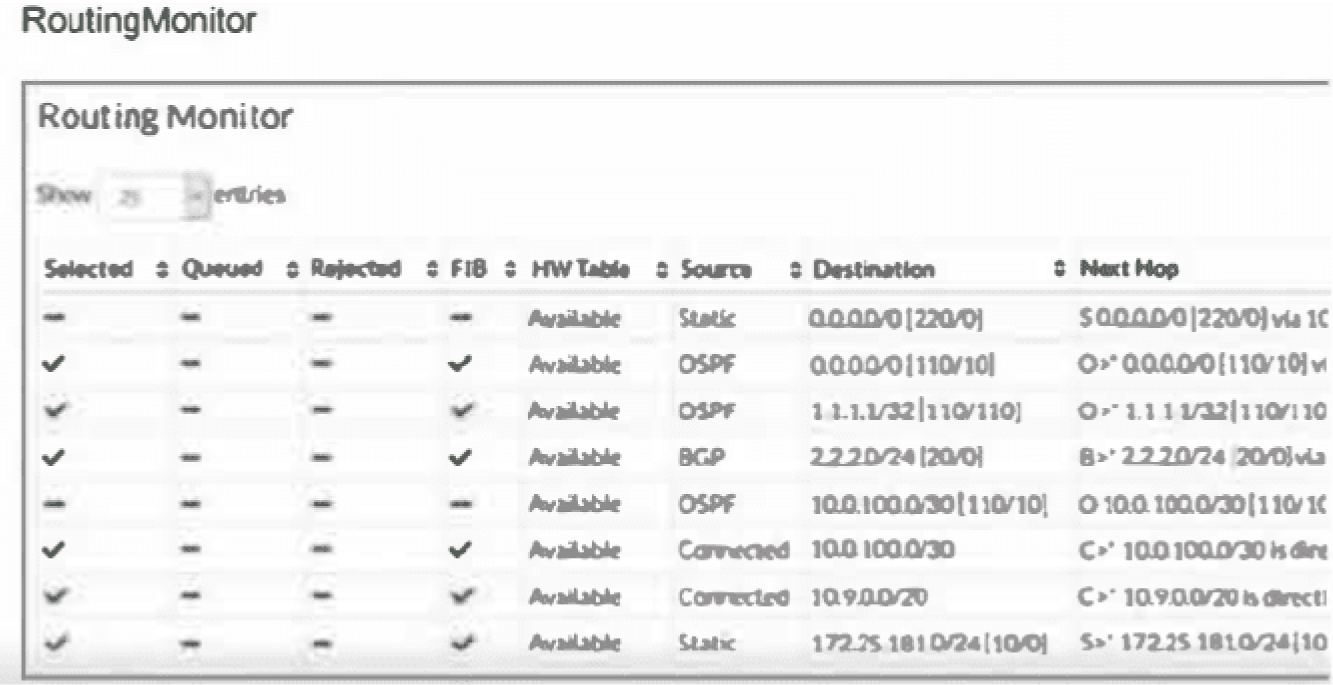
Serial/Asset numbers

This information provides a granular understanding of the devices on your network.

Question 6

Question Type: MultipleChoice

Exhibit.



RoutingMonitor

Routing Monitor

Show 25 entries

Selected	Queued	Rejected	FIB	HW Table	Source	Destination	Next Hop
–	–	–	–	Available	Static	0.0.0.0/0 [220/0]	S 0.0.0.0/0 [220/0] via 1
✓	–	–	✓	Available	OSPF	0.0.0.0/0 [110/10]	O>* 0.0.0.0/0 [110/10] v
✓	–	–	✓	Available	OSPF	1.1.1.1/32 [110/110]	O>* 1.1.1.1/32 [110/110
✓	–	–	✓	Available	BGP	2.2.2.0/24 [20/0]	B>* 2.2.2.0/24 [20/0] via
–	–	–	–	Available	OSPF	10.0.100.0/30 [110/10]	O 10.0.100.0/30 [110/1
✓	–	–	✓	Available	Connected	10.0.100.0/30	C>* 10.0.100.0/30 is dire
✓	–	–	✓	Available	Connected	10.9.0.0/20	C>* 10.9.0.0/20 is direct
✓	–	–	✓	Available	Static	172.25.181.0/24 [10/0]	S>* 172.25.181.0/24 [10

Two routes are not installed in the forwarding information base (FIB) as shown in the exnibit. Which two statements about these two route entries are true? (Choose two.)

Options:

A- These two routes have a higher administrative distance value available to the destination networks.

B- These two routes will become primary, if the best routes are removed.

C- These two routes will be used as load-balancing routes.

D- These two routes are available in the hardware routing table.

Answer:

A, B

Explanation:

From the exhibit and the details given about the routes not installed in the FIB:

These two routes have a higher administrative distance value available to the destination networks (Option A): Administrative distance is a measure used by routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. A higher administrative distance means that the route is considered less trustworthy, thus not selected for the FIB unless the more preferred routes fail.

These two routes will become primary, if the best routes are removed (Option B): In routing, if the currently installed routes (which are considered the best due to reasons like lower administrative distance) are removed or become unavailable, the next best routes based on administrative distance will be used. This behavior ensures redundancy and maintains network connectivity in diverse scenarios.

This approach is aligned with standard routing protocol behavior as documented in networking protocols and Fortinet's routing mechanisms which prioritize routes based on administrative distance and other metrics to maintain efficient and reliable network routing.

Question 7

Question Type: MultipleChoice

Which statement best describes a benefit of using MAC, IP address, or protocol-based VLAN assignments on FortiSwitch? (Choose one answer)

Options:

A- It disables 802.1X authentication while preserving user access control.1

B- It requires devices to authenticate through a RADIUS server before VLAN tagging.

C- It assigns ports to VLANs regardless of device type or traffic.

D- It offers dynamic segmentation benefits similar to 802.1X authentication.2

Answer:

D

Explanation:

According to theFortiSwitchOS 7.6 Administration Guideand theFortiSwitch 7.6 Study Guide, MAC-based, IP-based, and protocol-based VLAN assignments are methods ofdynamic VLAN assignment. These features allow the switch to categorize incoming traffic and assign it to a specific VLAN based on the packet's attributes rather than just the physical port it is connected to.3

The primary benefit of these methods is that theyoffer dynamic segmentation benefits similar to 802.1X authentication (Option D). In a modern network, devices with different security requirements (such as IoT devices, printers, and workstations) often connect to the same physical switch ports. 802.1X is the 'gold standard' for dynamic segmentation but requires a supplicant on the client device.4For devices that do not support 802.1X, MAC or protocol-based assignments provide a similar result: they ensure the device is automatically placed into its designated secure segment (VLAN) the moment it is identified by the switch.

MAC-based:Assigns a VLAN based on the source MAC address.

IP-based:Assigns a VLAN based on the source IP address or subnet.

Protocol-based:Assigns a VLAN based on the Ethernet type (e.g., IPv4, IPv6, or AppleTalk).

Option A is incorrect because these features complement rather than 'disable' 802.1X. Option B is incorrect because these specific assignment types can be configured locally on the switch without a RADIUS server. Option C is the opposite of how these features work, as they explicitly look at the device type or traffic to make an assignment.