Precise NSE5_FSW_AD-7.6 Exam Questions offer you high-efficient Study Materials - Dumpkiller

P.S. Free & New NSE5_FSW_AD-7.6 dumps are available on Google Drive shared by Dumpkiller: https://drive.google.com/open?id=1p9mN8uKOpprcQo7ovpPQ_Rt00O5FQHiq

If you want the NSE5_FSW_AD-7.6 certification to change your life and make it better, what are you waiting for? You should act quickly and make use of spare time of study or work to obtain a NSE5_FSW_AD-7.6 certification and master one more skill. With the help of our NSE5_FSW_AD-7.6 Exam Materials, you will find all of these desires are not dreams anymore. With the high pass rate as 98% to 100%, our NSE5_FSW_AD-7.6 learning questions can help you get your certification with ease.

Fortinet NSE5_FSW_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Layer 2 control and security: This section focuses on Layer 2 security features such as port security, filtering, antispoofing, ACLs, security profiles, and VLAN security mechanisms to protect switched networks.
Topic 2	• Deployment and management: This domain includes provisioning and deploying FortiSwitch in supported topologies, including multi-tenancy environments. It emphasizes proper setup, scalability, and centralized management.
Topic 3	• FortiSwitch concepts: This domain covers core FortiSwitch features including VLAN configuration, QoS, LLDP-MED, stacking, switching and routing, STP for loop prevention, and port and transceiver configuration. It focuses on essential switching operations and network integration.
Topic 4	• Monitoring and troubleshooting: This domain covers packet capture methods, FortiLink troubleshooting, and diagnostic tools used to monitor traffic and resolve network issues.

>> Study NSE5_FSW_AD-7.6 Center <<

Reliable NSE5_FSW_AD-7.6 Exam Question, New NSE5_FSW_AD-7.6 Exam Price

As a worldwide leader in offering the best NSE5_FSW_AD-7.6 test torrent, we are committed to providing comprehensive service to the majority of consumers and strive for constructing an integrated service. What's more, we have achieved breakthroughs in NSE5_FSW_AD-7.6 certification training application as well as interactive sharing and after-sales service. A good deal of researches has been made to figure out how to help different kinds of candidates to get Fortinet NSE 5 - FortiSwitch 7.6 Administrator certification. We revise and update the Fortinet NSE 5 - FortiSwitch 7.6 Administrator guide torrent according to the changes of the syllabus and the latest developments in theory and practice. We base the NSE5_FSW_AD-7.6 Certification Training on the test of recent years and the industry trends through rigorous analysis.

Fortinet NSE 5 - FortiSwitch 7.6 Administrator Sample Questions (Q20-Q25):

NEW QUESTION # 20
Which statement about 802.1X security profiles using MAC-based authentication mode is true?

- A. FortiSwitch can grant each device a different access level based on the credentials provided
- B. FortiSwitch performs faster when using this security mode on the ports.
- C. FortiSwitch must communicate with the RADIUS server to authenticate devices
- D. FortiSwitch allows connectivity to all hosts connected to a port, if one host is authenticated.

Answer: A

Explanation:
Pag 232, FortiSwitch_7.2_Study_Guide-Online "However, if you want to authenticate each device behind a port, and optionally, grant each device a different access level based on the credentials provided, then MAC- based is required." According to theFortiSwitchOS 7.6 Administration Guideand theFortiLink Guide (FortiOS 7.6), FortiSwitch supports two primary modes for 802.1X authentication:port-basedandMAC-based.
In802.1X port-based authentication, once a single supplicant (user or device) successfully authenticates, the physical port is transitioned to an "authorized" state, allowing all traffic from any device connected to that port (e.g., through a hub or unmanaged switch) to pass through. This is summarized by Option D, which is incorrect for MAC-based mode.
In contrast,802.1X MAC-based authentication(Option B) treats each device's MAC address as a distinct session. The switch maintains a table of authenticated MAC addresses for each port and applies security policies to each one individually. This granular approach allows the FortiSwitch to grantdifferent access levelsto different devices on the same physical port. For example, a laptop might be assigned to a corporate VLAN with a specific Dynamic Access Control List (DACL), while an IP phone on the same port is assigned to a Voice VLAN.
Furthermore, FortiSwitchOS 7.6 documentation specifies that MAC-based mode can support up to20 devices per port. Each device must provide its own credentials (or be validated via MAC Authentication Bypass), enabling the switch to enforce specific security attributes-such as VLAN IDs, QoS marking, and ingress ACLs-tailored to each uniquely identified device. While the switch typically communicates with aRADIUS server(Option C) for these credentials, MAC-based mode's primary functional advantage is this individual session management and authorization flexibility.

NEW QUESTION # 21
You are deploying a multitier FortiSwitch topology with redundant links between access and aggregation switches. The team is considering Multiple Spanning Tree Protocol (MSTP) to manage spanning tree across multiple VLANs. Which two Rapid STP (RSTP) features would be useful in this deployment to ensure fast convergence and predictable port roles? (Choose two answers)

- A. The rules for determining port roles
- B. The process for selecting the root bridge
- C. Recalculating paths after a topology change
- D. Automatic VLAN assignment

Answer: A,B

Explanation:
According to theFortiSwitchOS 7.6 Administration Guideand theFortiSwitch 7.6 Study Guide, Multiple Spanning Tree Protocol (MSTP) is built directly upon the foundations ofRapid Spanning Tree Protocol (RSTP), inheriting its mechanisms for fast convergence and fault recovery.12 In a multitier deployment (Access, Aggregation, and Core)3, theprocess for selecting the root bridge (Option A)is a fundamental RSTP feature that MSTP utilizes to create a stable and predictable logical topolog4y. By configuring the Bridge ID (priority and MAC address), administrators can manually ensure that the aggregation or core switches act as the Root Bridge for specific MST instances. This placement is critical for ensuring that traffic follows the most efficient physical paths and that high-bandwidth aggregation links are utilized effectively rather than blocked by suboptimal root selection.
Furthermore, therules for determining port roles (Option D)are essential for achieving the "Rapid" part of the protocol. RSTP/MSTP defines specific port roles such asRoot,Designated,Alternate, andBackup. Unlike legacy STP, which relies on slow listening and learning timers, RSTP uses the Alternate and Backup roles to identify secondary paths that are already in a "blocking" state but ready to transition to "forwarding" immediately through a proposal/agreement handshake if a primary link fails. This mechanism allows for sub- second convergence times in redundant multitier environments. While Option B (recalculating paths) occurs, it is the role-based synchronization process that characterizes the modern protocol's speed, making A and D the most relevant "useful features" for predictability and speed in this context.

NEW QUESTION # 22
Exhibit.
You need to manage three FortiSwitch devices using a FortiGate device. Two of the FortiSwitch devices initiated a reboot after the authorization process. However, the FortiSwitch device with the configuration shown in the exhibit. did not reboot All three devices completed FortiLink manage-ment authorization successfully.
Why did the FortiSwitch device shown in the exhibit not reboot to complete the authorization pro-cess?
The management mode was set to use FortiLink mode.

- A. Switch auto-discovery is enabled.
- B. The FortiSwitch device is scheduled to reboot as part the authorization process
- C. The management mode was set to use FortiLink mode.
- D. The system time is not in-sync and is using a non-default value

Answer: C

Explanation:
Regarding the scenario where a FortiSwitch did not reboot after the authorization process while the other devices did, the most likely cause, given the configuration settings in the exhibit, is:
* The management mode was set to use FortiLink mode (Option B): If the FortiSwitch was already configured to use FortiLink for its management mode, it may not require a reboot to complete the authorization process as its management interface settings are already aligned with FortiLink requirements. This is unlike switches that might be transitioning from a standalone or another management mode, which would typically require a reboot to apply new management settings fully.
References:
FortiLink mode specifically tailors FortiSwitch to be managed via a FortiGate device, integrating its operation into the wider security fabric without needing a reboot if it is already set to this mode before authorization.
This contrasts with other management modes where transitioning to FortiLink could necessitate a system restart to initialize the new configuration.

NEW QUESTION # 23
Which LLDP-MED Type-Length-Values does FortiSwitch collect from endpoints to track network devices and determine their characteristics?

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

Answer: B

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.

NEW QUESTION # 24
Which QoS mechanism maps packets with specific class of service (COS) or Differentiated Services Code Point (DSCP) markings to an egress queue? (Choose one answer)

- A. Classification for ingress traffic
- B. Shaping for egress traffic
- C. Queuing for egress traffic
- D. Policing for ingress traffic

Answer: C

Explanation:
According to theFortiSwitchOS 7.6 Administration Guideand theFortiSwitch 7.6 Study Guide, Quality of Service (QoS) on a FortiSwitch involves several distinct stages to manage traffic priority and bandwidth. The specific process of taking identified packets and placing them into a specific priority buffer for transmission is known asQueuing.1 On FortiSwitch, when a frame enters an ingress port, it is first classified based on its incomingCoS(Layer 2) or DSCP(Layer 3) markings.2However, it is theQueuing for egress traffic (Option B)mechanism that dictates which of the eight available hardware queues the frame will reside in before it is sent out of the destination port. The switch uses a mapping table (such as a CoS-to-queue or DSCP-to-queue map) to ensure that high-priority traffic, like voice or video, is placed in a higher-priority queue to minimize latency and jitter.
Regarding the other options:Classification (Option A)is the initial identification of the packet's priority but does not perform the physical mapping to a buffer.Policing (Option C)is an ingress mechanism used to drop or remark traffic that exceeds a defined rate.Shaping (Option D)is an egress mechanism that smooths out traffic bursts by delaying packets but is separate from the initial queue assignment. Therefore, the act of mapping specific markings to an egress queue is a fundamental function of the queuing mechanism.

NEW QUESTION # 25
.....

myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, telegra.ph, jacobscott67888.blogspot.com, Disposable vapes

2026 Latest Dumpkiller NSE5_FSW_AD-7.6 PDF Dumps and NSE5_FSW_AD-7.6 Exam Engine Free Share: https://drive.google.com/open?id=1p9mN8uKOpprcQo7ovpPQ_Rt00O5FQHiq