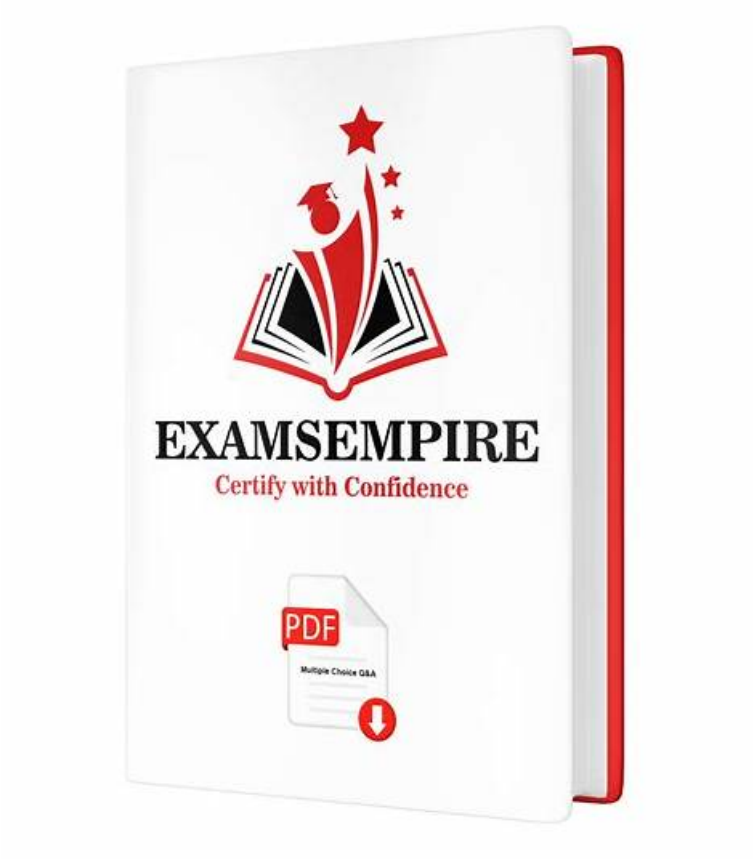
New NSE5_FSW_AD-7.6 Valuable Feedback Free PDF | Pass-Sure NSE5_FSW_AD-7.6 Mock Exams: Fortinet NSE 5 - FortiSwitch 7.6 Administrator



We sincerely suggest you to try these demos of our NSE5_FSW_AD-7.6 study guide and make a well-content choice. Different demos have different functions and each version has its advantages during the process of learning. Our NSE5_FSW_AD-7.6 Preparation exam is suitable for various consumer groups in the world we assure that after having a knowledge of those demos, you can purchase the most suitable NSE5_FSW_AD-7.6 exam materials.

Fortinet NSE5_FSW_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• Monitoring and troubleshooting: This domain covers packet capture methods, FortiLink troubleshooting, and diagnostic tools used to monitor traffic and resolve network issues.

>> NSE5_FSW_AD-7.6 Valuable Feedback <<

Quiz 2026 NSE5_FSW_AD-7.6: Accurate Fortinet NSE 5 - FortiSwitch 7.6 Administrator Valuable Feedback

After using our NSE5_FSW_AD-7.6 learning materials, you will find that things that have been difficult before have become simple. Of course, that's because you are better. Opportunities are for those who are prepared. And our NSE5_FSW_AD-7.6 exam questions are the right tool to help you get prepared. With the most up-to-date knowledge and information of the NSE5_FSW_AD-7.6 Practice Braindumps, you can be capable to deal with all of the conditions in your job. Believe it, good people will be better!

Fortinet NSE 5 - FortiSwitch 7.6 Administrator Sample Questions (Q68-Q73):

NEW QUESTION # 68
Refer to the exhibit.

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)

- A. The device will be assigned to the default management VLAN.
- B. The device will be placed into the VLAN quarantine.
- C. The device will be placed into the VLAN onboarding.
- D. The port will shut down for security reasons.

Answer: B

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.

NEW QUESTION # 69
Which drop policy mode, if assigned to a congested port, will drop incoming packets until there is no congestion on the egress port?

- A. Strict mode
- B. Tail-drop mode
- C. Weighted round robin mode.
- D. Random early detection mode

Answer: B

Explanation:
Tail-drop mode is a congestion management technique used in network devices, including FortiSwitches, to handle congestion on network ports:
* Tail-Drop Mode (A):
* Behavior:When a queue reaches its maximum capacity on a congested port, tail-drop mode simply drops any incoming packets that arrive after the buffer is full. This continues until the congestion is alleviated and there is space in the queue to accommodate new

packets.
* Application:This is a straightforward approach used when the device's buffer allocated to the port becomes full due to sustained high traffic, preventing buffer overflow and maintaining system stability.
References:For more details on congestion management techniques and settings on FortiSwitch, you can refer to the configuration manuals available on:Fortinet Product Documentation

NEW QUESTION # 70
You are configuring FortiSwitch to perform layer 3 inter-VLAN routing while managed by FortiGate over FortiLink. On supported hardware models, FortiSwitch can offload routing decisions for better performance.
1How does FortiSwitch perform routing between VLANs? (Choose one answer)

- A. By disabling routing when managed by FortiGate.
- B. By using a hardware forwarding table (FIB) programmed into ASIC.
- C. By relying entirely on the CPU in software.
- D. By supporting only dynamic routing protocols in hardware.

Answer: B

Explanation:
According to theFortiSwitchOS 7.6 FortiLink Guideand theFortiSwitch 7.6 Study Guide, managed FortiSwitch units support a feature calledInter-VLAN Routing Offload. Traditionally, in a FortiLink deployment, traffic between VLANs is "hair-pinned" back to the FortiGate for routing and security inspection. However, to increase performance and reduce latency, the FortiGate can program the managed FortiSwitch to handle Layer 3 routing of trusted traffic locally.
The technical mechanism behind this performance gain is the use of theForwarding Information Base (FIB) programmed directly into the switch'sASIC (Application-Specific Integrated Circuit). When routing offload is enabled (specifically using the set switch-controller-offload enable command on the VLAN interface), the FortiGate pushes the necessary routing table and gateway information to the switch hardware.
This allows the FortiSwitch to perform packet lookups and forwarding decisions at wire speed within the silicon, bypassing the general-purpose CPU and the FortiLink control plane for that specific traffic flow.
The documentation notes that this feature requires anAdvanced Features Licenseon the tier-1 FortiSwitch and is typically applied to the switch closest to the FortiGate.2While dynamic routing (Option B) is supported on FortiSwitch, it is not theonlything offloaded; static routes and inter-VLAN gateway traffic are the primary use cases for this offload mechanism. Therefore, the correct architectural description is that the switch utilizes its hardware-based FIB to accelerate inter-VLAN communication.

NEW QUESTION # 71
You are deploying a new FortiSwitch device in a branch office and you want it to be automatically detected and managed by FortiGate. Which FortiSwitch feature enables automatic detection during deployment?
(Choose one answer)

- A. FortiLink heartbeat
- B. Zero-touch deployment
- C. Link Layer Discovery Protocol (LLDP)
- D. Auto-discovery

Answer: C

Explanation:
According to theFortiOS 7.6 Study Guideand theFortiSwitch 7.6 FortiLink Guide, the automatic discovery and subsequent management of a FortiSwitch by a FortiGate controller is primarily facilitated by theLink Layer Discovery Protocol (LLDP). LLDP is an industry-standard, layer-2 protocol that allows network devices to advertise their identities and capabilities to neighbors on the same physical link.
When a factory-default FortiSwitch is connected to a FortiGate port (specifically one configured as a FortiLink interface), the switch automatically sends outLLDP advertisements. These advertisements include specificOrganizationally Specific TLVs (Type-Length-Values)that identify the device as a FortiSwitch and provide its management MAC address and current state. The FortiGate "listens" for these LLDP frames; once it receives a frame from a compatible FortiSwitch, it automatically lists the switch in theManaged FortiSwitchinventory as a "discovered" device awaiting authorization.
WhileZero-touch deployment (Option A)describes the overall goal of deploying a switch without manual CLI configuration, it is the underlyingLLDPprotocol that provides the technical mechanism for the initial detection. Once the switch is discovered via LLDP and authorized, the FortiGate uses a DHCP server on the FortiLink interface to assign an IP address to the switch and establishes a

secureCAPWAP(Control and Provisioning of Wireless Access Points) tunnel for management. TheFortiLink heartbeat (Option D)is a secondary mechanism usedafterthe connection is established to monitor the health and status of the link, rather than for the initial detection of the device.

NEW QUESTION # 72
Refer to the exhibit.

The security port policy is configured as shown in the exhibit. Which behavior occurs if a device connected to the port that does not support 802.1X? (Choose one answer)

- A. The device is blocked from accessing the network.
- B. The device is placed into the onboarding VLAN.
- C. The device is assigned to the default management VLAN.
- D. The device is placed into the quarantine VLAN.

Answer: B

Explanation:
According to theFortiSwitchOS 7.6 Administration Guideand theFortiSwitch 7.6 Study Guide, the interaction between a managed switch and a connected endpoint depends on whether the endpoint can participate in the 802.1X authentication process. When a security policy is applied to a port, the switch sends EAP (Extensible Authentication Protocol) requests to the device to initiate the login.
The FortiSwitch handles two primary failure scenarios differently:
* Non-supplicant (No 802.1X Support):If a device, such as a legacy PC or a basic printer, does not have an 802.1X supplicant, it will not respond to the switch's EAP requests. In this case, the switch waits for the duration specified in theGuest authentication delayfield (30 seconds in the exhibit). Once this timer expires without a response, the switch places the device into theGuest VLAN. As shown in the exhibit, the Guest VLAN is explicitly set to"onboarding.fortilink (onboarding)".
* Authentication Failure:If a devicedoessupport 802.1X but the user provides incorrect credentials, the RADIUS server returns an Access-Reject message. In this scenario, the device is moved to the Authentication fail VLAN, which the exhibit identifies as"quarantine.fortilink (quarantine)".
Note:BecauseMAC authentication bypass (MAB)is disabled in the exhibit, the switch will not attempt to authenticate the device's MAC address against the RADIUS server before defaulting to the Guest VLAN.
Therefore, for any device lacking an 802.1X supplicant, the result is placement into theonboardingVLAN.

NEW QUESTION # 73
.....

- Pass Guaranteed 2026 Fortinet High Hit-Rate NSE5_FSW_AD-7.6: Fortinet NSE 5 - FortiSwitch 7.6 Administrator Valuable Feedback □ Download ➠ NSE5_FSW_AD-7.6 □ for free by simply entering □ www.pdfvce.com □ website □NSE5_FSW_AD-7.6 Excellect Pass Rate
- Precise NSE5_FSW_AD-7.6 Valuable Feedback Spend Your Little Time and Energy to Pass NSE5_FSW_AD-7.6: Fortinet NSE 5 - FortiSwitch 7.6 Administrator exam ♣ Search for □ NSE5_FSW_AD-7.6 □ on □ www.vce4dumps.com □ immediately to obtain a free download □NSE5_FSW_AD-7.6 Actual Tests
- NSE5_FSW_AD-7.6 Valid Exam Cram □ New NSE5_FSW_AD-7.6 Practice Questions □ NSE5_FSW_AD-7.6 Valid Exam Cram □ 【 www.pdfvce.com 】 is best website to obtain 《 NSE5_FSW_AD-7.6 》 for free download □ □Exam NSE5_FSW_AD-7.6 Tips
- NSE5_FSW_AD-7.6 Learning Materials - NSE5_FSW_AD-7.6 Exam Simulation - NSE5_FSW_AD-7.6 Test Dumps □ □ Immediately open □ www.prepawayexam.com □ and search for ✔ NSE5_FSW_AD-7.6 □✔□ to obtain a free download □NSE5_FSW_AD-7.6 Certified
- NSE5_FSW_AD-7.6 Actual Tests □ Latest NSE5_FSW_AD-7.6 Dumps Ebook □ Practice NSE5_FSW_AD-7.6 Exam □ The page for free download of □ NSE5_FSW_AD-7.6 □ on （ www.pdfvce.com ） will open immediately □ □New NSE5_FSW_AD-7.6 Exam Simulator
- NSE5_FSW_AD-7.6 Test Dumps Free □ NSE5_FSW_AD-7.6 Actual Tests □ NSE5_FSW_AD-7.6 Actual Tests □ □ Search for 【 NSE5_FSW_AD-7.6 】 and easily obtain a free download on □ www.troytecdumps.com □ □Exam NSE5_FSW_AD-7.6 Fee
- 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, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, witpacourses.com, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes