検証するNSE5_FSW_AD-7.6資格取得講座試験-試験の準備方法-ハイパスレートのNSE5_FSW_AD-7.6テスト対策書

無料でクラウドストレージから最新のShikenPASS NSE5_FSW_AD-7.6 PDFダンプをダウンロードする：https://drive.google.com/open?id=1qW9-154s25aXouPoaVKxvOKNZroBRmav

NSE5_FSW_AD-7.6試験に出席するための勉強は、メソッドに注意を払います。良い方法は、多くの場合、半分の労力で結果をもたらすことができます。したがって、私たちは試験の時間であり、また受験スキルを知っている必要があります。 NSE5_FSW_AD-7.6クイズガイドは過去数年間の要約に基づいており、回答には特定のルールがあり、主観的または客観的な質問のいずれかが見つかります。共通する類似の対応モジュールで見つけることができます。このため、NSE5_FSW_AD-7.6試験のダンプでは、NSE5_FSW_AD-7.6試験に合格するのに役立つ資格試験のいくつかのタイプの質問をまとめています。

Fortinet NSE5_FSW_AD-7.6 認定試験の出題範囲：

トピック	出題範囲
トピック 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.
トピック 2	• Monitoring and troubleshooting: This domain covers packet capture methods, FortiLink troubleshooting, and diagnostic tools used to monitor traffic and resolve network issues.
トピック 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.

トピック４	• 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.

>> NSE5_FSW_AD-7.6資格取得講座 <<

信頼できるNSE5_FSW_AD-7.6資格取得講座 | 素晴らしい合格率のNSE5_FSW_AD-7.6: Fortinet NSE 5 - FortiSwitch 7.6 Administrator | 権威のあるNSE5_FSW_AD-7.6テスト対策書

我々社のFortinet NSE5_FSW_AD-7.6認定試験問題集の合格率は高いのでほとんどの受験生はNSE5_FSW_AD-7.6認定試験に合格するのを保証します。もしあなたはFortinet NSE5_FSW_AD-7.6試験問題集に十分な注意を払って、NSE5_FSW_AD-7.6試験の解答を覚えていれば、NSE5_FSW_AD-7.6認定試験の成功は明らかになりました。Fortinet NSE5_FSW_AD-7.6模擬問題集で実際の質問と正確の解答に疑問があれば、無料の練習問題集サンプルをダウンロードし、チェックしてください。

Fortinet NSE 5 - FortiSwitch 7.6 Administrator 認定 NSE5_FSW_AD-7.6 試験問題 (Q80-Q85):

質問 # 80
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. The FortiSwitch device is scheduled to reboot as part the authorization process
- B. Switch auto-discovery is enabled.
- 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

正解：C

解説：
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.

質問 # 81
Which drop policy mode, if assigned to a congested port, will drop incoming packets until there is no congestion on the egress port?

- A. Random early detection mode

- B. Weighted round robin mode.
- C. Tail-drop mode
- D. Strict mode

正解：C

解説：
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

質問 # 82
Refer to the exhibit.
Core-1 and Access-1 are managed and authorized by FortiGate-1. which uses port4 as the FortiLink interface.
After FortiGate authorizes and manages Core-2. Port1 status becomes STP discarding.
Why is port1 in the discarding state?

- A. Access-1 is the root bridge and can only have one root port.
- B. Core-2 has the lowest bridge priority.
- C. port1 on Core-2 is discarding only management traffic.
- D. Core-1 and Core-2 do not have MCLAG configuration.

正解：D

解説：
The STP (Spanning Tree Protocol) discarding state on port1 of Core-2, after Core-1 and Access-1 are managed and authorized by FortiGate-1, is likely due to the lack of an MCLAG (Multi-Chassis Link Aggregation Group) configuration between Core-1 and Core-2. In typical network configurations involving STP and MCLAG, the absence of MCLAG can lead to STP blocking one of the redundant paths to prevent loops, which is a critical function of STP. Port1 on Core-2 being in a discarding state suggests that it has been identified as providing a redundant path that could potentially create a network loop, hence STP has placed this port in a blocking (discarding) state to maintain a loop-free topology.
References:
For a deeper understanding of STP operations and MCLAG configurations in FortiGate managed environments, consult the Fortinet knowledge base:Fortinet Knowledge Base.

質問 # 83
Refer to the exhibits. An IP phone is connected to port1 of FortiSwitch Access-1. The IP phone tags its traffic with VLAN ID 20.
On FortiGate, VLAN IP_Phone (VLAN ID 20) has been configured, and port1 of Access-
1 is set with VLAN 20 as the native VLAN. However, the IP phone cannot reach the network. The exhibit shows the partial VLAN configuration and the port1 configuration on Access-1.
Which configuration change must you make on FortiSwitch to allow ingress and egress traffic for the IP phone? (Choose one answer)

- A. On VLAN IP_Phone, enable vlanforward
- B. On port1, add VLAN 20 to the allowed_vlans list
- C. On port1, disable the edge_port
- D. On VLAN IP_Phone, enable l2forward

正解：B

解説：
According to theFortiSwitchOS 7.6 Administration GuideandFortiOS 7.6 FortiLink Guide, the processing of Ethernet frames on a

managed FortiSwitch port depends on whether the frame is tagged or untagged upon arrival (ingress) and how the port's VLAN membership is defined.
In the provided exhibit,port1is configured with set vlan "IP_Phone" (VLAN 20) as itsnative VLAN. By definition, the native VLAN handles untagged traffic; any untagged frame arriving at the port is assigned to VLAN 20, and any egress traffic from VLAN 20 is sent out of the port without a tag. However, the scenario specifically states that theIP phone tags its traffic with VLAN ID 20.
When a FortiSwitch receives atagged frame, it checks the VLAN ID against theallowed-vlanslist configured on that port. Although VLAN 20 is the native VLAN, the exhibit shows that the port has been explicitly configured with set allowed-vlans "quarantine". This creates a restrictive filter that permits only tagged frames belonging to the "quarantine" VLAN to enter or exit the port. Because VLAN 20 (IP_Phone) is not present in the allowed-vlans list, the switch drops the tagged frames from the IP phone during ingress processing.
To resolve this, the administrator must modify theFortiSwitch port configurationby adding VLAN 20 to the allowed_vlans list (e.g., set allowed-vlans "quarantine" "IP_Phone" or set allowed-vlans-all enable). This ensures that the switch recognizes and permits tagged traffic for VLAN 20 on that physical interface. Option B is incorrect because l2forward is a Layer 3 interface setting on the FortiGate and does not address the physical port's ingress filtering logic on the switch. Disabling the edge_port (Option D) relates to Spanning Tree Protocol (STP) convergence and would not impact VLAN tag filtering.

質問 # 84
An administrator needs to deploy managed FortiSwitch devices in a remote location where multiple VLANs must be utilized to segment devices. No Layer 3 switch or router is present. The the only WAN connectivity is the router provided by the ISP connected to the public internet.
Which two items will the administrator need to use? (Choose two.)

- A. FortiSwitch and FortiGate devices configured with IPsec interfaces.
- B. FortiSwitch devices configured with NAT disabled.
- C. FortiSwitch devices that have the required internal hardware for this configuration.
- D. FortiSwitch and FortiGate devices configured with VXLAN interfaces.
- E. A FortiSwitch interface connected to the ISP router configured with fortilink-13-mode enabled.

正解：B、E

解説：
To deploy FortiSwitch in a remote location with multiple VLANs and no Layer 3 switch or router, you would need specific configurations:
* VXLAN Interfaces (B):
* Purpose:VXLAN (Virtual Extensible LAN) allows network segmentation without a Layer 3 device, extending VLAN capabilities across dispersed geographical locations over the WAN.
* Implementation:Configuring VXLAN on both FortiSwitch and FortiGate can encapsulate Layer 2 traffic over a Layer 3 network, making it ideal for scenarios lacking dedicated routing hardware.
* Appropriate Hardware (D):
* Requirement:Not all FortiSwitch models might support advanced features like VXLAN; hence, ensuring that the hardware can support such configurations is crucial.
References:For specific information on VXLAN configuration and hardware requirements, refer to the technical documentation provided by Fortinet:Fortinet Product Documentation

質問 # 85
.....

NSE5_FSW_AD-7.6基礎訓練 □ ➤ NSE5_FSW_AD-7.6 □の試験問題は（ www.goshiken.com ）で無料配信中NSE5_FSW_AD-7.6合格記

- NSE5_FSW_AD-7.6復習時間 □ NSE5_FSW_AD-7.6学習範囲 □ NSE5_FSW_AD-7.6模擬解説集 □ 「 www.japancert.com 」を開いて⇛ NSE5_FSW_AD-7.6 ⇚を検索し、試験資料を無料でダウンロードしてくださいNSE5_FSW_AD-7.6練習問題
- 真実的なNSE5_FSW_AD-7.6資格取得講座 - 合格スムーズNSE5_FSW_AD-7.6テスト対策書 | 高品質なNSE5_FSW_AD-7.6基礎訓練 Fortinet NSE 5 - FortiSwitch 7.6 Administrator □ サイト➽ www.goshiken.com □で ➥ NSE5_FSW_AD-7.6 □問題集をダウンロードNSE5_FSW_AD-7.6日本語認定対策
- NSE5_FSW_AD-7.6合格対策 □ NSE5_FSW_AD-7.6合格受験記 □ NSE5_FSW_AD-7.6復習資料 □ 今すぐ▶ www.it-passports.com ◀を開き、✔ NSE5_FSW_AD-7.6 □✔□を検索して無料でダウンロードしてくださいNSE5_FSW_AD-7.6的中合格問題集
- NSE5_FSW_AD-7.6試験解説 □ NSE5_FSW_AD-7.6ウェブトレーニング □ NSE5_FSW_AD-7.6日本語版 □ □ www.goshiken.com □には無料の ➡ NSE5_FSW_AD-7.6 □□□問題集がありますNSE5_FSW_AD-7.6的中合格問題集
- 完璧-素晴らしいNSE5_FSW_AD-7.6資格取得講座試験-試験の準備方法NSE5_FSW_AD-7.6テスト対策書 □ □ □ www.xhs1991.com □で《 NSE5_FSW_AD-7.6 》を検索し、無料でダウンロードしてください NSE5_FSW_AD-7.6学習範囲
- NSE5_FSW_AD-7.6日本語版 □ NSE5_FSW_AD-7.6合格記 □ NSE5_FSW_AD-7.6日本語認定対策 □ [www.goshiken.com]を開いて▹ NSE5_FSW_AD-7.6 ◃を検索し、試験資料を無料でダウンロードしてください NSE5_FSW_AD-7.6復習時間
- NSE5_FSW_AD-7.6的中合格問題集 □ NSE5_FSW_AD-7.6試験解説 □ NSE5_FSW_AD-7.6模擬解説集 □ ☀ www.goshiken.com □☀□で □ NSE5_FSW_AD-7.6 □を検索して、無料で簡単にダウンロードできます NSE5_FSW_AD-7.6日本語
- Fortinet 認定資格試験対策書 NSE5_FSW_AD-7.6 要な知識をカバー □ 今すぐ □ www.goshiken.com □を開き、⇛ NSE5_FSW_AD-7.6 ⇚を検索して無料でダウンロードしてくださいNSE5_FSW_AD-7.6合格記
- NSE5_FSW_AD-7.6模擬解説集 □ NSE5_FSW_AD-7.6最新対策問題 □ NSE5_FSW_AD-7.6専門知識 □ 最新“NSE5_FSW_AD-7.6 ”問題集ファイルは“www.mogiexam.com ”にて検索NSE5_FSW_AD-7.6模擬解説集
- matteotsub630368.bloginder.com, sites2000.com, ronaldllbn955659.blogchaat.com, dillanllux063709.blogspothub.com, ianytyr446922.idblogmaker.com, myatphw254584.wikisona.com, montyeoal742194.homewikia.com, webookmarks.com, lexieofzu257186.webbuzzfeed.com, orlandoijuz462171.mysticwiki.com, Disposable vapes

ちなみに、ShikenPASS NSE5_FSW_AD-7.6の一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=1qW9-154s25aXouPoaVKxvOKNZroBRmav