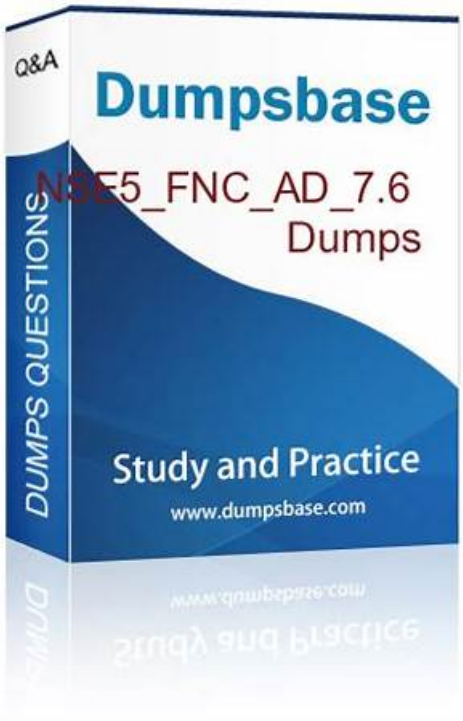
Fortinet NSE5_FSW_AD-7.6 Real Dumps & Related NSE5_FSW_AD-7.6 Exams



P.S. Free & New NSE5_FSW_AD-7.6 dumps are available on Google Drive shared by TestPassed: https://drive.google.com/open?id=1PjgCczHRz-7h4REl7GgKU3V2vMZoyt2J

For the recognition of skills and knowledge, more career opportunities, professional development, and higher salary potential, the Fortinet NSE5_FSW_AD-7.6 certification exam is the proven way to achieve these tasks quickly. Overall, we can say that with the Fortinet NSE 5 - FortiSwitch 7.6 Administrator (NSE5_FSW_AD-7.6) exam you can gain a competitive edge in your job search and advance your career in the tech industry.

We are not satisfied with that we have helped more candidates pass NSE5_FSW_AD-7.6 exam, because we know that the IT industry competition is intense, we must constantly improve our dumps so that we cannot be eliminated. So our technical teams continue to renew the NSE5_FSW_AD-7.6 Study Materials in time, in order to let the examinee using our products to keep up with the NSE5_FSW_AD-7.6 exam reform tightly.

>> Fortinet NSE5_FSW_AD-7.6 Real Dumps <<

Pass Guaranteed Quiz Fortinet - Fantastic NSE5_FSW_AD-7.6 Real Dumps

Our NSE5_FSW_AD-7.6 exam braindump is revised and updated according to the change of the syllabus and the latest development situation in the theory and the practice. The NSE5_FSW_AD-7.6 exam torrent is compiled elaborately by the experienced professionals and of high quality. The contents of NSE5_FSW_AD-7.6 guide questions are easy to master and simplify the important information. It conveys more important information with less answers and questions, thus the learning is easy and efficient. The language is easy to be understood makes any learners have no obstacles to study and pass the NSE5_FSW_AD-7.6 Exam.

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	• 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 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.

Fortinet NSE 5 - FortiSwitch 7.6 Administrator Sample Questions (Q72-Q77):

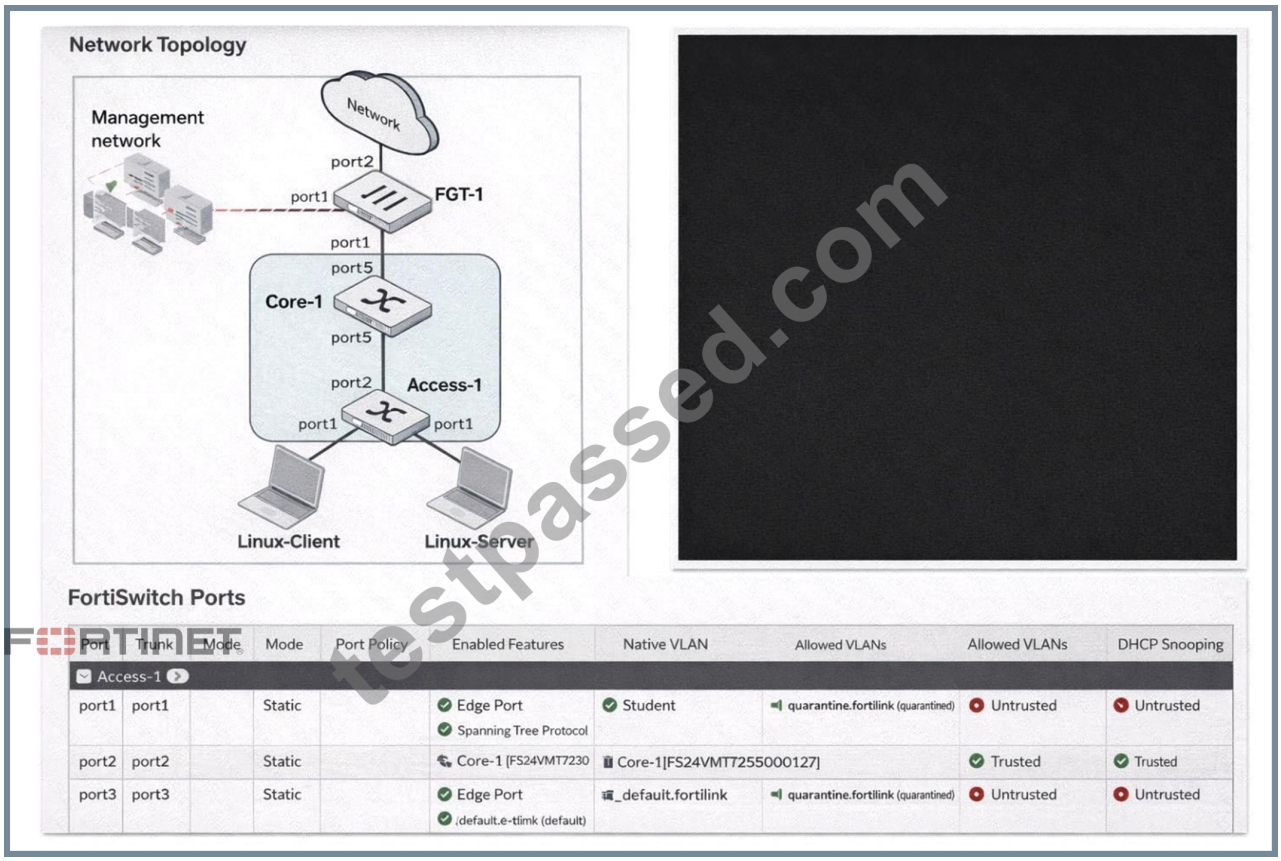
NEW QUESTION # 72
Which interfaces on FortiSwitch send out FortiLink discovery frames by default in order to detect a FortiGate with an enabled FortiLink interface?

- A. All ports have auto-discovery enabled by default.
- B. No ports are enabled by default for auto-discovery. This must be configured under config switch interface.
- C. The ports with auto-discovery enabled by default are dependent upon the FortiSwitch model.
- D. The last four switch ports on FortiSwitch have auto-discovery enabled by default.

Answer: A

Explanation:
* Fortinet FortiLink Protocol:The FortiLink protocol is Fortinet's proprietary mechanism for managing FortiSwitch units from a FortiGate firewall. It simplifies configuration and security policy enforcement across the connected network devices.
* Auto-Discovery:FortiLink's auto-discovery feature means that by default, all ports on a FortiSwitch will actively send out discovery frames. This allows them to locate a FortiGate device that has a FortiLink interface enabled, streamlining the device management process.
* No Configuration Needed:You don't have to manually configure individual ports for FortiLink discovery on FortiSwitch devices.
References
* FortiSwitchOS FortiLink Guide (FortiSwitch Devices Managed by FortiOS 7.2):Refer to pages 13 and 14 for details on zero-touch management and FortiLink configuration. [https://fortinetweb.s3.
amazonaws.com/docs.fortinet.com/v2/attachments/27f63c72-b083-11ec-9fd1-fa163e15d75b
/FortiSwitchOS-7.2.0-FortiLink_Guide%E2%80%94FortiSwitch_Devices_Managed_by_FortiOS_7.2.
pdf]

NEW QUESTION # 73
(Full question statement start from here)
Refer to the exhibits.



You enable Dynamic Host Configuration Protocol (DHCP) snooping on the VLAN,Student. The Linux- Client VM sends DHCP requests, and tcpdump confirms the broadcasts. However, the Linux-Server VM, acting as a DHCP server, receives no DHCP traffic. What is the most likely cause of this intra-VLAN traffic being blocked? (Choose one answer)

- A. The Student VLAN must be configured as an allowed VLAN on port1.
- B. The DHCP requests are being sent on the wrong VLAN.
- C. Port1 is configured as an untrusted port.
- D. Port4 is not configured as a trusted port.

Answer: C

Explanation:
In FortiSwitchOS 7.6,DHCP snoopingis a Layer 2 security feature that validates DHCP traffic and protects the LAN from rogue DHCP servers. The feature enforces atrust modelon switch ports: ports connected toward legitimate DHCP server infrastructure must be markedtrusted, while edge/access ports facing clients are typicallyuntrusted. When DHCP snooping is enabled on a VLAN (in this case,Student), FortiSwitch inspects DHCP messages and applies filtering rules based on port trust status.
From the exhibit, bothport1(connected to the Linux-Server DHCP server) andport4(connected to the Linux- Client) showDHCP Snooping: Untrusted. In this configuration, the switch treats the DHCP server-facing port as untrusted and, by design, willblock DHCP server-originated messages(such as DHCPOFFER
/DHCPACK) arriving on that interface. This prevents the DHCP handshake from completing and effectively stops DHCP from functioning across that VLAN segment. Operationally, this is commonly observed as "no DHCP traffic" at the server/application layer because the exchange cannot progress normally when the server side is not trusted.
Option C is incorrect because the client-facing port is expected to be untrusted. Options A and D do not align with the exhibit: the ports are already placed in the Student VLAN as native VLAN, so the primary issue is the DHCP snooping trust role.
Therefore, the most likely cause is thatport1 is configured as an untrusted port(it must be trusted for a DHCP server), makingBthe correct answer.

NEW QUESTION # 74
Which statement about the IGMP snooping querier when enabled on a VLAN is true?

- A. The setting can only be enabled using the FortiSwitch CLI.
- B. Active multicast receiver entries are aging on each IGMP query sent on the VLAN
- C. All other indirectly connected switches will be unable to get IGMP multicast traffic.

- D. IGMP reports on the VLAN are forwarded to all switch ports.

Answer: B

Explanation:
Active multicast receiver entries are aging on each IGMP query sent on the VLAN (A): When IGMP snooping querier is enabled on a VLAN, it functions to manage multicast traffic within the VLAN by keeping track of multicast group memberships. The IGMP querier sends queries to determine which ports require the multicast traffic. The multicast receiver entries, which are entries that indicate which devices have requested the multicast data, age or time out based on these IGMP queries. Each query refreshes active connections but ages out entries that no longer respond, helping to ensure that multicast traffic is only sent to ports with active receivers.

NEW QUESTION # 75
Which statement about 802.1X security profiles using MAC-based authentication mode is true?

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

Answer: C

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 # 76
(Full question statement start from here)
You are planning to deploy FortiSwitch devices on your network. Your goal is to simplify management and ensure integration with the Security Fabric. Which deployment approach should you choose? (Choose one answer)

- A. Manage FortiSwitch on FortiGate using FortiLink.
- B. Use the FortiSwitch-Manager device for centralized management.
- C. Manage FortiSwitch from FortiManager for large-scale enterprise deployments.
- D. Use FortiEdge Cloud for centralized management with advanced analytics.

Answer: A

Explanation:
Fortinet's recommended approach for simplified management and full Security Fabric integration is to manage FortiSwitch devices directly from a FortiGate using FortiLink. According to the FortiOS 7.6 and FortiSwitchOS 7.6 documentation, FortiLink enables FortiGate to act as the centralized controller for all connected FortiSwitch units, providing seamless integration between switching, routing, and security services.
When FortiSwitch is managed through FortiGate with FortiLink, the switches become native members of the Security Fabric. This

allows FortiGate to centrally define VLANs, enforce Layer 2 and Layer 3 security policies, control inter-VLAN routing, apply NAC and quarantine actions, and provide end-to-end visibility across users, devices, and applications. Inter-VLAN traffic is routed and inspected by FortiGate, ensuring consistent policy enforcement and logging.
FortiLink management significantly reduces operational complexity by eliminating the need for separate switch management platforms. Configuration, firmware upgrades, monitoring, troubleshooting, and topology visualization are all performed from the FortiGate GUI or CLI. This tightly integrated model is specifically designed for branch, campus, and mid-sized enterprise deployments that prioritize simplicity, security consistency, and operational efficiency.
The other options do not meet the stated objective. FortiSwitch-Manager is not a current management solution, FortiManager is intended for large-scale multi-device orchestration rather than direct Security Fabric integration, and FortiEdge Cloud focuses on cloud-based management without native FortiGate security enforcement.
Therefore, to simplify management and ensure full Security Fabric integration, the correct and fully verified choice is D. Manage FortiSwitch on FortiGate using FortiLink.

NEW QUESTION # 77
.....

Now we can say that Fortinet NSE 5 - FortiSwitch 7.6 Administrator (NSE5_FSW_AD-7.6) exam questions are real and top-notch NSE5_FSW_AD-7.6 exam questions that you can expect in the upcoming Fortinet NSE 5 - FortiSwitch 7.6 Administrator (NSE5_FSW_AD-7.6) exam. In this way, you can easily pass the NSE5_FSW_AD-7.6 exam with good scores. The countless NSE5_FSW_AD-7.6 Exam candidates have passed their dream Fortinet NSE5_FSW_AD-7.6 certification exam and they all got help from real, valid, and updated NSE5_FSW_AD-7.6 practice questions, You can also trust on TestPassed and start preparation with confidence.

estellelwls572796.blog4youth.com, www.stes.tyc.edu.tw, elainertir166107.ourcodeblog.com, www.stes.tyc.edu.tw, jemimaosvu956862.blogofchange.com, amaanpwgl381269.bloggip.com, katrinajnqr951948.buyoutblog.com, mypresspage.com, Disposable vapes

What's more, part of that TestPassed NSE5_FSW_AD-7.6 dumps now are free: https://drive.google.com/open?id=1PjgCczHRz-7h4REl7GgKU3V2vMZoyt2J