KillTest

質量更高　服務更好

學習資料

http://www.killtest.net

一年免費更新服務

Exam : **NSE5_FSW_AD-7.6**

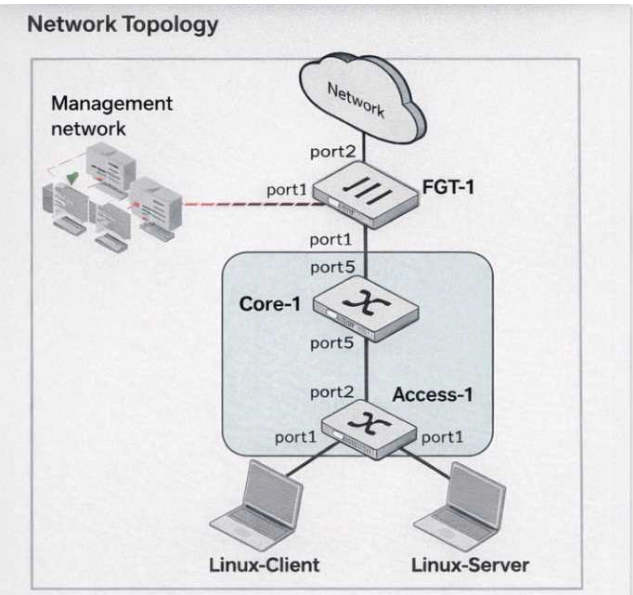
Title : Fortinet NSE 5 - FortiSwitch 7.6 Administrator

Version : DEMO

1.Which two statements about DHCP snooping enabled on a FortiSwitch VLAN are true? (Choose two.)
A. Enabling DHCP snooping on a FortiSwitch VLAN ensures requests and replies are seen by all DHCP servers.
B. switch-controller-dhcp-snooping-verify-mac verifies the destination MAC address to protect against DHCP exhaustion attacks.
C. By default, all FortiSwitch ports are set to forward client DHCP requests to untrusted ports.
D. Settings related to DHCP option 82 are only configurable through the CLI
Answer: B, D
Explanation:
Switch-controller-dhcp-snooping-verify-mac verifies the destination MAC address to protect against DHCP exhaustion attacks (B): This feature of DHCP snooping helps prevent DHCP exhaustion attacks by ensuring that the destination MAC addresses in DHCP packets match the MAC addresses learned by the switch. This check helps prevent attackers from overwhelming the DHCP server with requests from spoofed MAC addresses.
Settings related to DHCP option 82 are only configurable through the CLI (D): DHCP Option 82 is used for "agent information, " and it's typically used in network environments where additional information between DHCP clients and servers is necessary for policy and billing purposes. Configuration of these settings in FortiSwitch is only available through the Command Line Interface (CLI), not the Graphical User Interface (GUI**).**

2.Which statement about the quarantine VLAN on FortiSwitch is true?
A. Quarantine VLAN has no DHCP server
B. Users who fail 802.1X authentication can be placed on the quarantine VLAN.
C. It is only used for quarantined devices if global setting is set to quarantine by VLAN.
D. FortiSwitch can block devices without configuring quarantine VLAN to be part of the allowed VLANs.
Answer: B
Explanation:
The correct statement about the quarantine VLAN on FortiSwitch is:
B. Users who fail 802.1X authentication can be placed on the quarantine VLAN. This feature allows network administrators to isolate devices that do not meet the network’s security criteria as determined through 802.1X authentication. Placing these devices in a quarantine VLAN restricts their network access, thereby protecting the network from potential security threats posed by unauthorized or compromised devices.
Option A is incorrect as the presence of a DHCP server in a quarantine VLAN depends on specific network configurations.
Option C is incorrect without more context regarding global settings, and option D misstates the functionality of quarantine VLANs, as their primary use is to restrict, not block, devices without additional VLAN configuration changes.

3.Refer to the exhibits.



FortiSwitch Ports

Port	Trunk	Mode	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	Allowed VLANs	DHCP Snooping
Access-1									
port1	port1		Static		Edge Port Spanning Tree Protocol	Student	quarantine.fortilink (quarantined)	Untrusted	Untrusted
port2	port2		Static		Core-1 [FS24VMT7230	Core-1[FS24VMT7255000127]		Trusted	Trusted
port3	port3		Static		Edge Port default.e-tlimk (default)	_default.fortilink	quarantine.fortilink (quarantined)	Untrusted	Untrusted

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 DHCP requests are being sent on the wrong VLAN.

B. Port1 is configured as an untrusted port.

C. Port4 is not configured as a trusted port.

D. The Student VLAN must be configured as an allowed VLAN on port1.

Answer: B

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) show DHCP 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.

4.Which is a requirement to enable SNMP v2c on a managed FortiSwitch?
A. Create an SNMP user to use for authentication and encryption.
B. Specify an SNMP host to send traps to.
C. Enable an SNMP v3 to handle traps messages with SNMP hosts.
D. Configure SNMP agent and communities.
Answer: D
Explanation:
To enable SNMP v2c on a managed FortiSwitch, the essential requirement involves configuring the SNMP agent and community strings:
Configure SNMP Agent and Communities (D):
SNMP Agent: Activating the SNMP agent on FortiSwitch allows it to respond to SNMP requests.
Community Strings: SNMP v2c uses community strings for authentication. These strings function as passwords to grant read-only or read-write access to the SNMP data.
Understanding Other Options:
Create an SNMP user (A) is necessary for SNMP v3, not v2c, as it involves user-based authentication and encryption.
Specify an SNMP host (B) is typically a part of SNMP configuration but not a requirement just to enable SNMP.
Enable SNMP v3 (C) is not related to enabling SNMP v2c.
Reference: For detailed instructions on configuring SNMP on FortiSwitch, you can refer to the SNMP configuration section in the FortiSwitch administration guide available on: Fortinet Product Documentation

5.Which two statements about managing a FortiSwitch stack on FortiGate are true? (Choose two.)
A. A FortiLink interface must be enabled on FortiGate.
B. The switch controller feature must be enabled on FortiGate.
C. Only a hardware-based FortiGate can manage a FortiSwitch stack.
D. FortiSwitch must be operating in standalone mode before authorization.
Answer: A, B
Explanation:
A FortiLink interface must be enabled on FortiGate (A): To manage a FortiSwitch stack, a dedicated FortiLink interface on the FortiGate is required. This interface is used to manage the communication between FortiGate and the FortiSwitch stack, enabling centralized control and configuration of the switches directly from the FortiGate.
The switch controller feature must be enabled on FortiGate (B): Enabling the switch controller feature on FortiGate allows it to manage connected FortiSwitch units. This feature provides tools and interfaces on the FortiGate for overseeing FortiSwitch configurations, monitoring switch status, and managing network policies across the stack.