Fortinet NSE5_FSW_AD-7.6 NSE 5 Practice Questions

Shared by Mccarty on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What can an administrator do to maintain the existing standalone FortlSwltch configuration while changing the management mode to FortLink?

Options:

A- Use a migration tool based on python script to convert the configuration
B- Enable the Forti-link setting on FortiSwitch before the authorization process
C- FortiGate will automatically save the existing FortiSwitch configuration during the Forti-link management process.
D- Register FortiSwitch to For1ISwitch Cloud to save a copy before managing by Forti-Gate.

Answer:

A

Explanation:

'The tool is a Python script that converts the supported settings in a FortiSwitch standalone configuration file to the equivalent FortiOS settings for a managed switch.'Reference: FortiSwitch 7.6 Study Guide, page 349

Question 2

Question Type: MultipleChoice

(Full question statement start from here)

How does enabling an IGMP snooping proxy on FortiSwitch help reduce the number of IGMP reports processed by the IGMP querier? (Choose one answer)

Options:

A- By converting IGMP reports into broadcast packets to reach all VLAN members
B- By converting IGMP traffic to unicast
C- By suppressing duplicate IGMP reports within the VLAN
D- By forwarding IGMP reports only when the first member joins and the last member leaves

Answer:

D

Explanation:

In FortiSwitchOS 7.6,IGMP snooping proxyis an enhancement to standard IGMP snooping that optimizes multicast control-plane traffic between hosts, switches, and the upstream IGMP querier. Its primary purpose is toreduce the number of IGMP membership reportsthat the querier must process, thereby improving scalability and efficiency in multicast-enabled networks.

Without an IGMP snooping proxy, every multicast receiver on a VLAN independently sends IGMP membership reports to the querier. In environments with many hosts subscribing to the same multicast groups, this behavior can generate a large volume of redundant IGMP reports, unnecessarily increasing control-plane load on both the querier and intermediate network devices.

When the IGMP snooping proxy feature is enabled, the FortiSwitch acts as anIGMP proxy agenton behalf of hosts within the VLAN. The switch tracks multicast group membership locally andsuppresses individual IGMP reports from downstream hosts. Instead, the FortiSwitch forwards an IGMP report upstreamonly when the first host joins a multicast group. Likewise, when hosts leave the group, the switch sends an IGMP leave message or reportonly when the last remaining member leaves.

This aggregation mechanism dramatically reduces IGMP signaling traffic while preserving correct multicast forwarding behavior. Importantly, the switch does not alter IGMP packet types or convert them to broadcast or unicast traffic. It simply optimizes reporting behavior based on group membership state.

Therefore, the correct explanation is that IGMP snooping proxy reduces IGMP report processingby forwarding IGMP reports only when the first member joins and the last member leaves, makingOption Dthe correct and fully verified answer according to FortiSwitchOS 7.6 documentation.

Question 3

Question Type: MultipleChoice

On supported FortiSwitch models, which access control list (ACL) stage is recommended for applying actions before the switch performs any layer 2 or layer 3 processing? (Choose one answer)

Options:

A- Ingress
B- Forwarding
C- Egress
D- Prelookup

Answer:

D

Explanation:

According to theFortiSwitchOS 7.6 Administration Guideand theNSE 5 FortiSwitch 7.6 Administrator Study Guide, FortiSwitch supports a multi-stage ACL pipeline that allows for granular traffic control at different points in a packet's journey through the switch.1The documentation identifies three primary stages for ACL application:Prelookup,Ingress, andEgress.

Prelookup (Option D):This is the earliest stage in the switching pipeline. The documentation explicitly states thatPrelookup ACLsare processedbefore any Layer 2 or Layer 3 lookupsare performed by the switch hardware. This stage is highly recommended for high-performance security actions, such as dropping unwanted traffic immediately upon arrival, because it prevents the switch from wasting internal resources (CPU and ASIC lookup cycles) on frames that are destined to be discarded anyway.

Ingress (Option A):This stage occursafterthe switch has completed its Layer 2 (MAC table) and Layer 3 (routing table) lookups butbeforethe packet is queued for the egress port. While powerful, actions here occur after initial processing has already taken place.

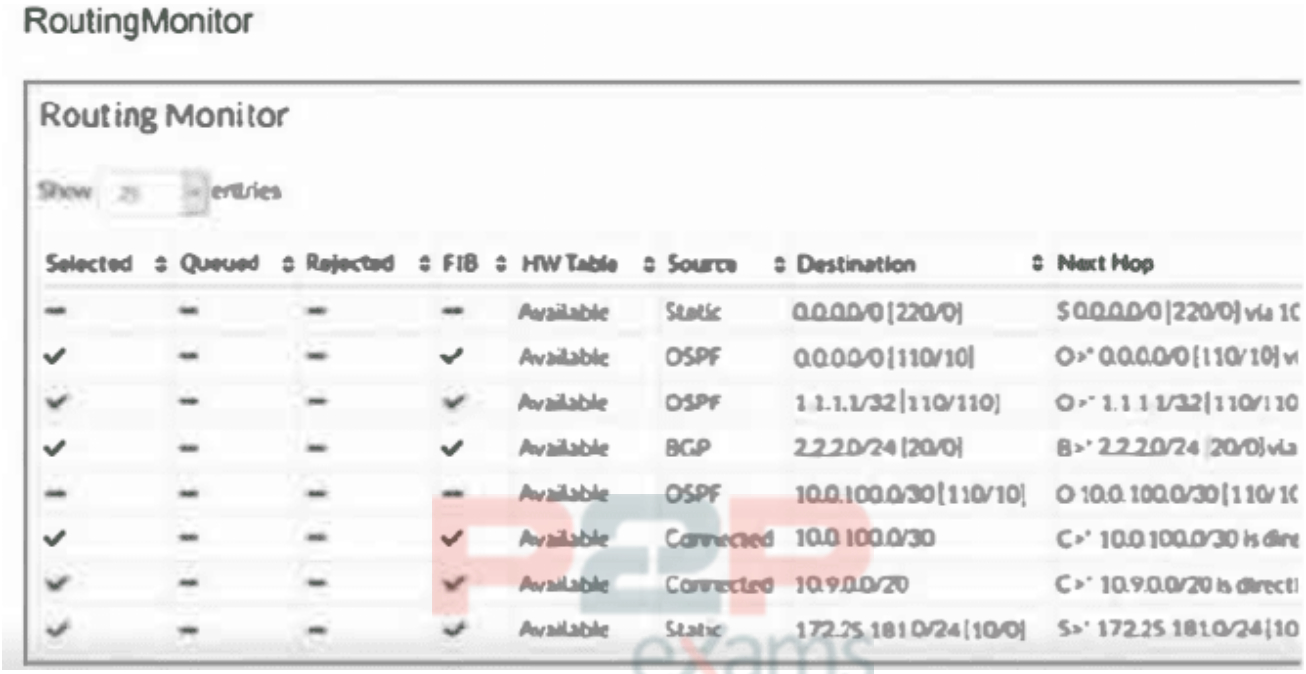
Egress (Option C):This stage is processed just before the frame leaves the switch through the destination port. It is typically used for final modifications or filtering based on the outgoing interface context.

Therefore, to achieve the goal of applying actionsbeforeany Layer 2 or Layer 3 processing occurs, thePrelookupstage is the technically correct and recommended choice in FortiSwitchOS 7.6.Forwarding (Option B)is a general functional stage of a switch but is not a specific ACL stage type in the FortiSwitch configuration hierarchy.

Question 4

Question Type: MultipleChoice

Exhibit.



Two routes are not installed in the forwarding information base (FIB) as shown in the exhibit. Which two statements about these two route entries are true? (Choose two.)

Options:

A- These two routes have a higher administrative distance value available to the destination networks.
B- These two routes will become primary, if the best routes are removed.
C- These two routes will be used as load-balancing routes.
D- These two routes are available in the hardware routing table.

Answer:

A, B

Explanation:

From the exhibit and the details given about the routes not installed in the FIB:

These two routes have a higher administrative distance value available to the destination networks (Option A): Administrative distance is a measure used by routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. A higher administrative distance means that the route is considered less trustworthy, thus not selected for the FIB unless the more preferred routes fail.

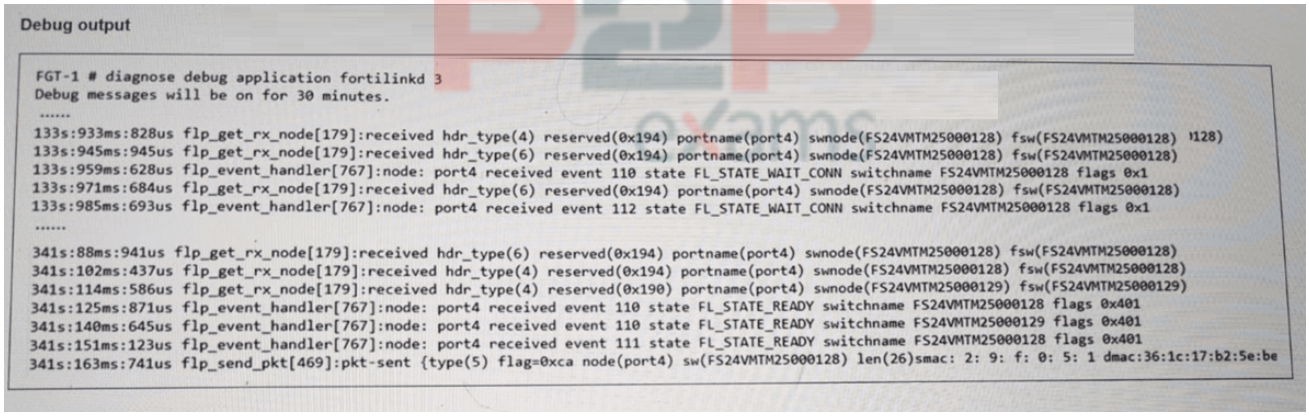
These two routes will become primary, if the best routes are removed (Option B): In routing, if the currently installed routes (which are considered the best due to reasons like lower administrative distance) are removed or become unavailable, the next best routes based on administrative distance will be used. This behavior ensures redundancy and maintains network connectivity in diverse scenarios.

This approach is aligned with standard routing protocol behavior as documented in networking protocols and Fortinet's routing mechanisms which prioritize routes based on administrative distance and other metrics to maintain efficient and reliable network routing.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



You have just authorized a new FortiSwitch on your FortiGate, and it appears online in the GUI. To verify that FortiLink connectivity is healthy, what should you check next? (Select one answer)

Options:

A- Check that the switch automatically disables all unused ports.
B- Look for FortiLink heartbeat messages sent from FortiSwitch to FortiGate every few seconds and confirm FortiGate acknowledges them.
C- Verify that FortiGate has pushed a new firmware image to FortiSwitch immediately.
D- Ensure the FortiSwitch is automatically sending log events to FortiAnalyzer.

Answer:

B

Explanation:

According to theFortiOS 7.6 Study Guideand theFortiSwitch 7.6 FortiLink Guide, the health and stability of the control plane between a FortiGate and a managed FortiSwitch are maintained through a continuous keepalive mechanism. Once a FortiSwitch is authorized and transitions to theFL_STATE_READYstate (as shown in the debug output in the exhibit), the devices must ensure the management tunnel remains active.

The primary mechanism for this is theFortiLink heartbeat. The documentation specifies that a managed FortiSwitch sends heartbeat messages to the FortiGate every few seconds over the FortiLink interface. The FortiGate, acting as the controller, must acknowledge these heartbeats to confirm that the switch is still reachable and responding to management commands. If the FortiGate fails to receive a certain number of consecutive heartbeats, it will consider the switch 'offline' in the GUI, even if physical link lights remain green.

Checking for these heartbeat exchanges is a critical troubleshooting step to verify that theCAPWAP(Control and Provisioning of Wireless Access Points) based management tunnel is functioning correctly without intermittent drops. Option A is incorrect as port disabling is a configuration choice, not a health check. Option C is incorrect because firmware updates are manual or scheduled, not automatic upon authorization. Option D is a logging function that relies on a healthy management tunnel but is not a direct measure of the FortiLink's operational health.

Question 6

Question Type: MultipleChoice

What can an administrator do to maintain a FortiGate-compatible FortiSwitch configuration when changing the management mode from standalone to FortiLinK?

Options:

A- Use a migration tool based on Python script to convert the configuration.
B- Enable the FortiLink setting on FortiSwitch before the authorization process.
C- FortiGate automatically saves the existing FortiSwitch configuration during the FortiLink management process.
D- Register FortiSwitch to FortiSwitch Cloud to save a copy before managing with FortiGate.

Answer:

C

Explanation:

When transitioning the management of a FortiSwitch from standalone mode to being managed by FortiGate via FortiLink, it is critical to ensure that the existing configurations are preserved. The best practice involves:

FortiGate's Role in Configuration Preservation:FortiGate has the capability to automatically preserve the existing configuration of a FortiSwitch when it is integrated into the network via FortiLink. This feature helps ensure that the transition does not disrupt the network's

operational settings.

Configuration Integration:As FortiSwitch is integrated into FortiGate's management via FortiLink, FortiGate captures and integrates the existing switch configuration, enabling a seamless transition. This process involves FortiGate recognizing the FortiSwitch and its current setup, then incorporating these settings into the centralized management interface without the need for manual reconfiguration or the use of additional tools.

Question 7

Question Type: MultipleChoice

Which feature should you enable to reduce the number or unwanted IGMP reports processed by the IGMP querier?

Options:

A- Enable the IGMP flood setting on the static port for all multicast groups.
B- Enable the IGMP flood reports setting on the mRouter port.
C- Enable IGMP snooping proxy.
D- Enable IGMP flood unknown multicast traffic on the global setting.

Answer:

C

Explanation:

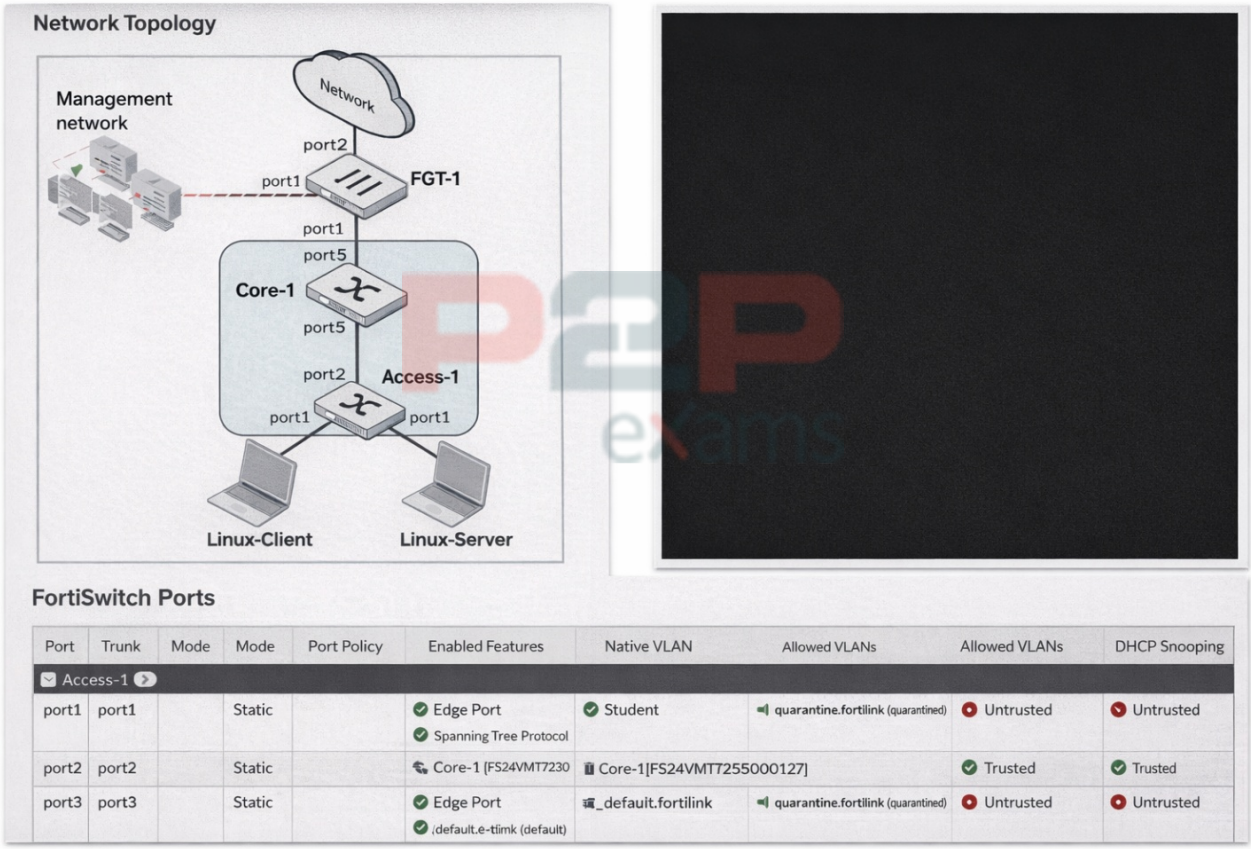
Enable IGMP snooping proxy (C): To reduce the number of unwanted IGMP reports processed by the IGMP querier, enabling IGMP snooping proxy is effective. This feature acts as an intermediary between multicast routers and hosts, optimizing the management of IGMP messages by handling report messages locally and reducing unnecessary IGMP traffic across the network. This minimizes the processing load on the IGMP querier and improves overall network efficiency.

Question 8

Question Type: MultipleChoice

(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)

Options:

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) 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.

Question 9

Question Type: MultipleChoice

What happens when a routed VLAN interface (RVI) is configured on a FortiSwitch port or trunk? (Choose one answer)

Options:

A- VLAN 1 is automatically assigned for management.
B- The port becomes a layer 3 interface with VLAN 4095 assigned automatically.1
C- All VLANs on the port are terminated in a trunk by default.
D- The port becomes a layer 3 interface and assigned to VLAN 1.

Answer:

B

Explanation:

According to theFortiSwitchOS 7.6 Administration Guideand theFortiSwitch 7.6.1

Administration Guide---Standalone Mode, aRouted VLAN Interface (RVI)is a physical port or trunk interface that is converted to support Layer 3 routing protocols.2This transformation changes the fundamental nature of the interface from a switching component to a routing component.

When an RVI is enabled on a specific physical port or trunk, the system automatically assignsVLAN 4095to that interface at the backend.3This specific VLAN ID is reserved across the FortiSwitch platform to signal that the interface is no longer operating as a standard Layer 2 switch port.4Once configured as an RVI, the interface supports advanced Layer 3 features such asOSPF, BGP, RIP, IS-IS, and static routing, as well asVirtual Routing and Forwarding (VRF)for routing isolation.5

Importantly, the documentation states that upon enabling RVI,Layer 2 protocols(such as Spanning Tree Protocol or 802.1X port-based security) and most standard switch interface features aredisabledon that port.6This is because the port is now treated as a dedicated Layer 3 'routed' interface rather than a member of the Layer 2 switching fabric.7Additionally, if the underlying physical port or trunk interface is administratively shut down, the associated RVI will also transition to a 'down' state.

Question 10

Question Type: MultipleChoice

How are the 'by VLAN redirect MAC address quarantine' mode and the 'by redirect MAC address quarantine' mode on FortiGate similar?

Options:

A- Both modes move quarantined devices to the quarantine VLAN.
B- Both modes require firewall policies to block inter-VLAN traffic.
C- Both modes add quarantined device MAC addresses to the blocked firewall address group.
D- Both modes block intra-VLAN traffic by FortiGate automatically.

Answer:

A

Explanation:

The 'by VLAN redirect MAC address quarantine' mode and the 'by redirect MAC address quarantine' mode on FortiGate share specific similarities:

Quarantine VLAN Assignment (A):

Common Feature:Both modes utilize a designated quarantine VLAN to isolate quarantined devices. This helps in mitigating the risk of spreading potential security threats within the network.

Operational Impact:Moving devices to a specific quarantine VLAN restricts their network access, effectively isolating them until further action or remediation is taken.

Question 11

Question Type: MultipleChoice

How does FortiGate handle configuration of flow tracking sampling if you export the settings to a managed FortiSwitch stack with sampling mode set to perimeter is true?

Options:

A- FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces.
B- FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces, except ICL and ISL interfaces.
C- FortiGate configures and enables flow sampling on FortiSwitch but does not change existing sampling settings of interfaces.
D- FortiGate configures and enables egress sampling on all management interfaces.

Answer:

B

Explanation:

When FortiGate exports configuration settings to a managed FortiSwitch stack with sampling mode set to 'perimeter is true,' the behavior is:

B . FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces, except ICL and ISL interfaces.This setting ensures that all incoming traffic on normal operational ports is sampled for monitoring and analysis purposes, but it excludes the inter-chassis link (ICL) and inter-switch link (ISL) interfaces from sampling. These exclusions are typically made to prevent the duplication of sampled data and to reduce unnecessary load on the monitoring system, as these links often carry traffic already monitored at other points.

Options A and D are incorrect because they either generalize the sampling across all interfaces without exceptions or incorrectly specify egress sampling on management interfaces. Option C is also incorrect as FortiGate can modify existing sampling settings to fit the perimeter-based configuration requirement.