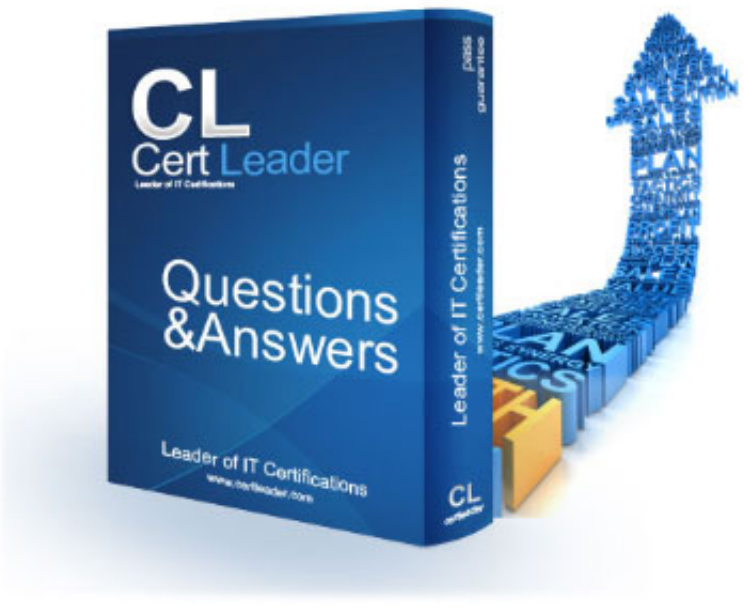
NSE6_FSW-7.2 Dumps

Fortinet NSE 6 - FortiSwitch 7.2

https://www.certleader.com/NSE6_FSW-7.2-dumps.html



NEW QUESTION 1
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 can grant each device a different access level based on the credentials provided
C. FortiSwitch performs faster when using this security mode on the ports.
D. FortiSwitch must communicate with the RADIUS server to authenticate devices

Answer: D

Explanation:
In the context of 802.1X security profiles using MAC-based authentication mode, the following statement is true:

FortiSwitch must communicate with the RADIUS server to authenticate devices (D):

Authentication Process:MAC-based authentication involves the switch forwarding the MAC address of a connecting device to a RADIUS server. The RADIUS server then checks this MAC address against a database of allowed addresses to determine whether the device should be granted access to the network.

RADIUS Server Role:The use of a RADIUS server is crucial because it centralizes the authentication process and allows for scalable management of connected devices across the network.
References:For comprehensive insights into 802.1X and MAC-based authentication on FortiSwitch, including the role of RADIUS servers, consult security configuration resources or the FortiSwitch security manual available at:Fortinet Product Documentation

NEW QUESTION 2
Exhibit.

```
config switch-controller security-policy local-access
    edit default
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
config switch-controller snmp-sysinfo
    set status enable
    set contact-info "Training"
    set location "Sunnyvale"
end
config switch-controller snmp-community
    edit 1
        set name "Training"
    next
end
```

Which configuration change will allow the managed FortiSwitch to accept SNMP requests from any source?

A. Create a new local access profile for SNMP only.
B. Enable SNMP on the internal interface of the switch.
C. Configure an SNMP host to send SNMP traps.

D. Add SNMP service on the management interface of the switch.

Answer: D

Explanation:
To enable a managed FortiSwitch to accept SNMP requests from any source, the relevant configuration would involve setting up access on the management interface specifically to permit SNMP traffic. Based on the provided options:

Add SNMP service on the management interface of the switch (Option D): This configuration change directly targets the interface responsible formanagement traffic, which includes SNMP communications. By enabling SNMP service on this interface, SNMP requests from any source can be processed, assuming no other restrictive ACLs or firewall rules are in place that would block such requests.
References:

Typically, enabling SNMP on a device??s management interface is straightforward and involves specifying the SNMP version, community strings, and permitted sources. This setting allows the device to process SNMP queries and send SNMP traps as configured.

NEW QUESTION 3
In which two ways can you assign a FortiSwitch port to a VDOM using multi-tenancy setup? (Choose two.)

A. Switch the FortiLink interface to the target VDOM.
B. Remove the managed FortiSwitch and allocate ports directly on FortiSwitch.
C. Create a virtual port pool on the FortiGate CLI.
D. Assign a port to a VDOM directly on the managed FortiSwitch.

Answer: AC

Explanation:
In a multi-tenancy setup on FortiGate, you can assign a FortiSwitch port to a VDOM in two primary ways:

Switch the FortiLink Interface to the Target VDOM (A): This method involves configuring the FortiLink interface, which is the dedicated interface used to manage FortiSwitch units from FortiGate, to operate within a specific VDOM. This effectively assigns all ports on the FortiSwitch, managed through that FortiLink interface, to the designated VDOM.

Create a Virtual Port Pool on the FortiGate CLI (C): Virtual port pools are created on FortiGate and allow ports from FortiSwitch to be grouped and assigned to a VDOM. This method is more granular and flexible, as it allows specific ports on the FortiSwitch to be dedicated to different VDOMs without requiring the entire switch or FortiLink interface to be dedicated to a single VDOM.

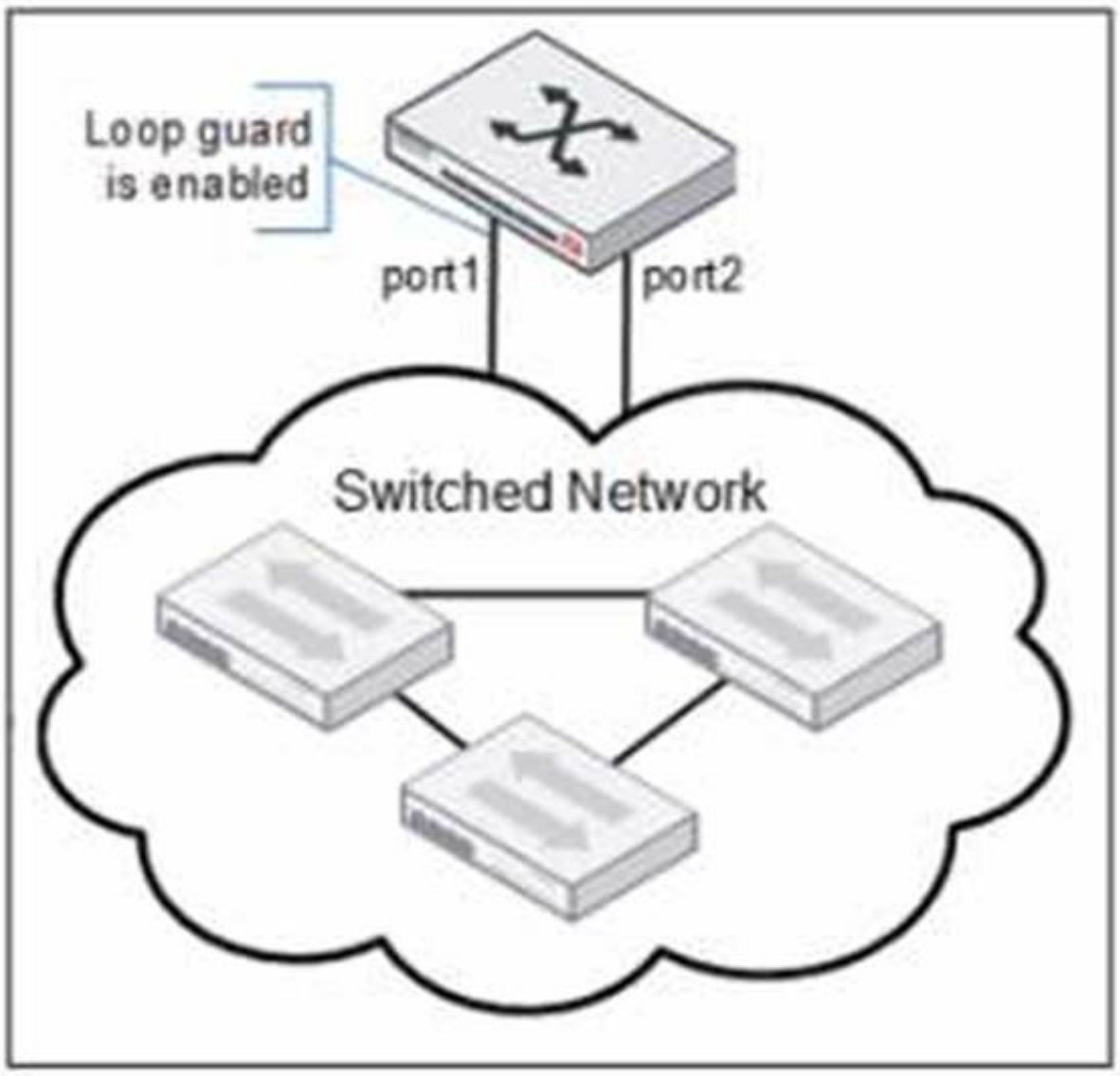
NEW QUESTION 4
Which statement about the configuration of VLANs on a managed FortiSwitch port is true?

A. Untagged VLANs must be part of the allowed VLANs: ingress and egress.
B. FortiSwitch VLAN interfaces are created only when FortiSwitch is managed by Forti-Gate.
C. The native VLAN is implicitly part of the allowed VLAN on the port.
D. Allowed VLANS expand the collision domain to the port.

Answer: C

Explanation:
The native VLAN is implicitly part of the allowed VLAN on the port (C): On a managed FortiSwitch port, the native VLAN, which is the VLAN assigned to untagged traffic, is implicitly included in the list of allowed VLANs. This means it does not need to be explicitly specified whenconfiguring VLAN settings on the port. This configuration simplifies VLAN management and ensures that untagged traffic is handled correctly without additional configuration steps.

NEW QUESTION 5
Refer to the exhibits.



LoopGuard-setup

```
# diagnose switch-controller switch-info loop-guard S108EF4N17000029
S108EF4N17000029:
  Portname          State     Status      Timeout(m)   MAC-Move   Count    Last-Event
  ________________  ________  __________  ___________  _________  _____  ___________________
  port1             enabled   Triggered      2            0         1     2021-02-19 15:50:35
  port2             disabled    -            -            -         -          -
  port3             disabled    -            -            -         -          -
  port4             disabled    -            -            -         -          -
  port5             disabled    -            -            -         -          -
  port6             disabled    -            -            -         -          -
  port9             disabled    -            -            -         -          -
  port10            disabled    -            -            -         -          -
  8EF4N17000030-0   disabled    -            -            -         -          -
  _FlInK1_MLAG0_    disabled    -            -            -         -          -
```

Port1 and port2 are the only ports configured with the same native VLAN 10. What are two reasons that can trigger port1 to shut down? (Choose two.)

A. port1 was shut down by loop guard protection.
B. STP triggered a loop and applied loop guard protection on port1.
C. An endpoint sent a BPDU on port1 that it received from another interface.
D. Loop guard frame sourced from port 1 was received on port 1.

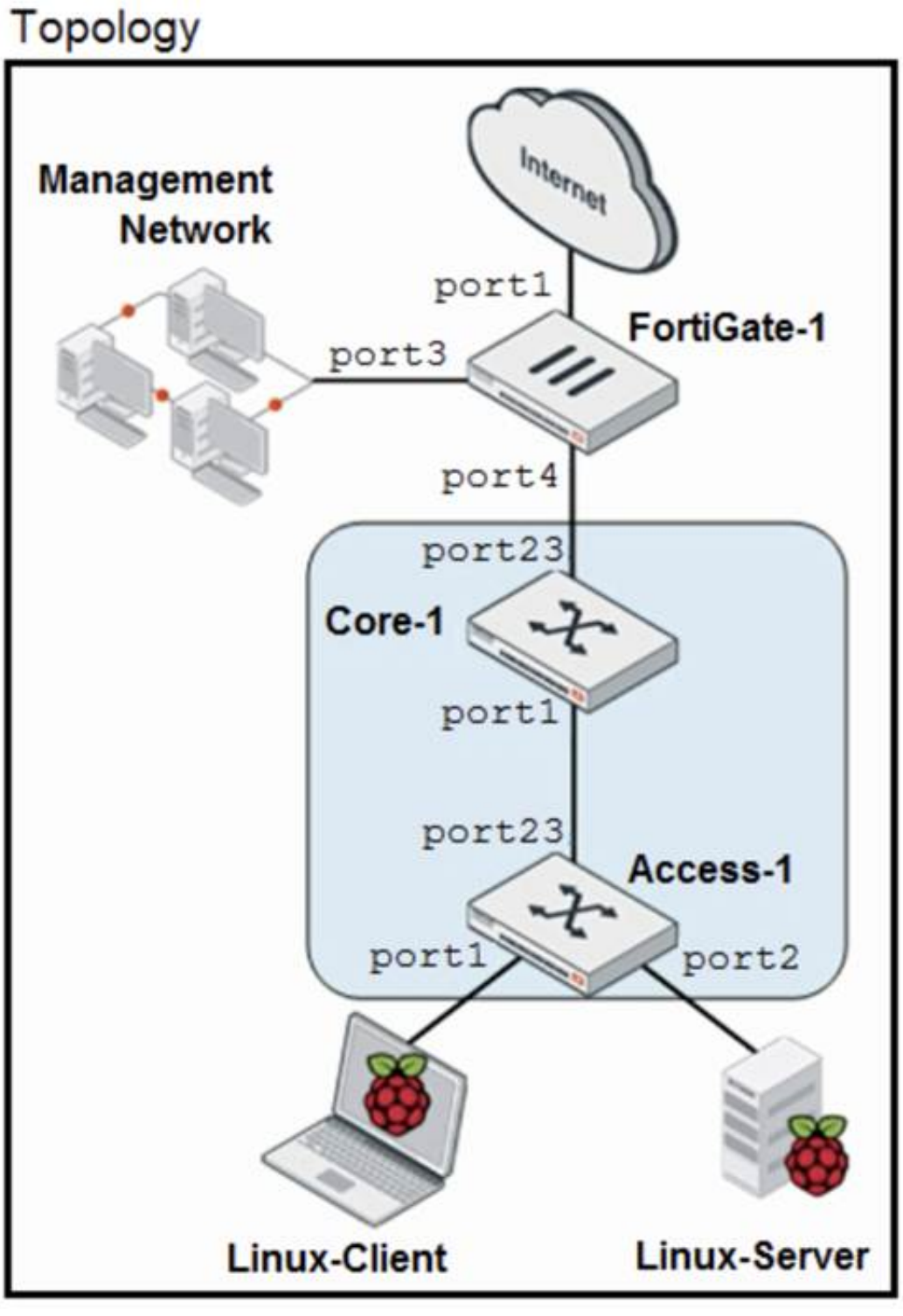
Answer: AB

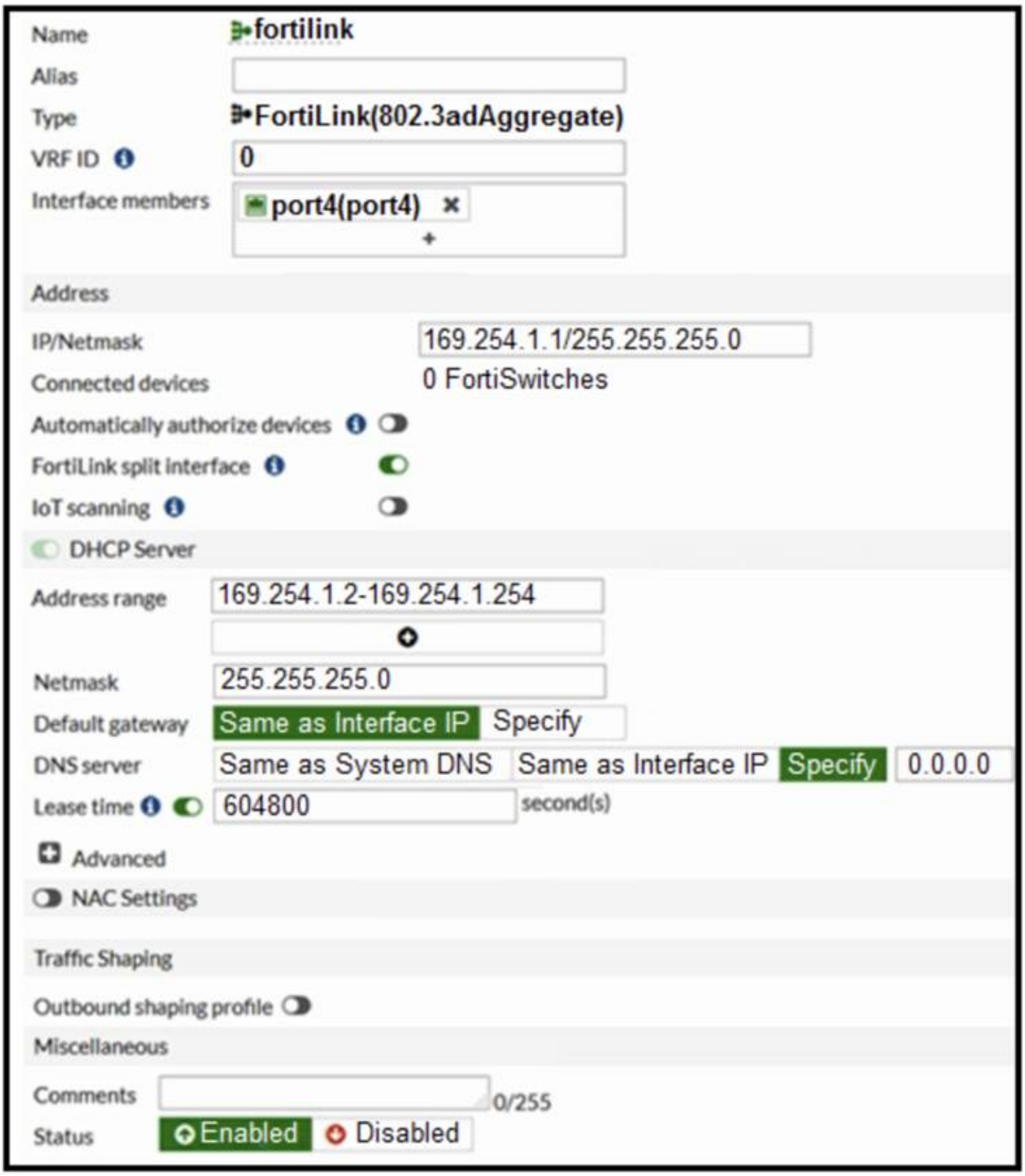
Explanation:
When loop guard is enabled on port1 and port2 configured with the same native VLAN (VLAN 10), there are specific scenarios under which port1 can be shut down due to loop guard operation:
A.port1 was shut down by loop guard protection.Loop guard is a specific feature used in network environments to prevent alternative or redundant loops. When loop guard is active, it can shut down a port if it stops receiving BPDU (Bridge Protocol Data Units) on a port that is expected to receive them, assuming a loop or link failure and putting the port into an inconsistent state to prevent potential loops.
B.STP triggered a loop and applied loop guard protection on port1.If the Spanning Tree Protocol (STP) detects a loop or loss of BPDU transmissions while loop guard is enabled, it will proactively shut down the port to prevent network instability or a broadcast storm. This is an essential function of loop guard within the

context of STP, providing additional protection against topology changes that could introduce loops.
References:

Additional details about loop guard functionality and STP interaction can be found in the FortiSwitch administration guides, accessible viaFortinet Documentation.

NEW QUESTION 6
Refer to the exhibits.





You are asked to ensure that managed FortiSwitch devices are reachable by other devices, such as SNMP and other management tools across your network.
Which setting must you configure to ensure traffic from other devices in the network reaches FortiSwitch?

A. Select a specific default gateway provided to FortiSwitch as an upstream device.
B. Change the FortiLink interface IP address and DHCP server address range.
C. Recreate the FortiLink interface with a nonaggregate setting.
D. Enable NAC settings to select the onboarding VLAN.

Answer: A

Explanation:
To ensure that the managed FortiSwitch devices are reachable by other devices across the network for management purposes, such as SNMP or other network management tools, configuring network connectivity correctly is essential. Here's the rationale for the suggested setting:
Select a Specific Default Gateway (A):
Why Other Options Are Less Applicable:
References:For a detailed explanation on configuring network settings on FortiSwitch, including how to set up default gateways and IP addresses for network management, refer to the FortiSwitch administration guides available on:Fortinet Product Documentation

NEW QUESTION 7
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.

NEW QUESTION 8
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: AB

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.

NEW QUESTION 9
Which two statements about the FortiLink authorization process are true? (Choose two.)

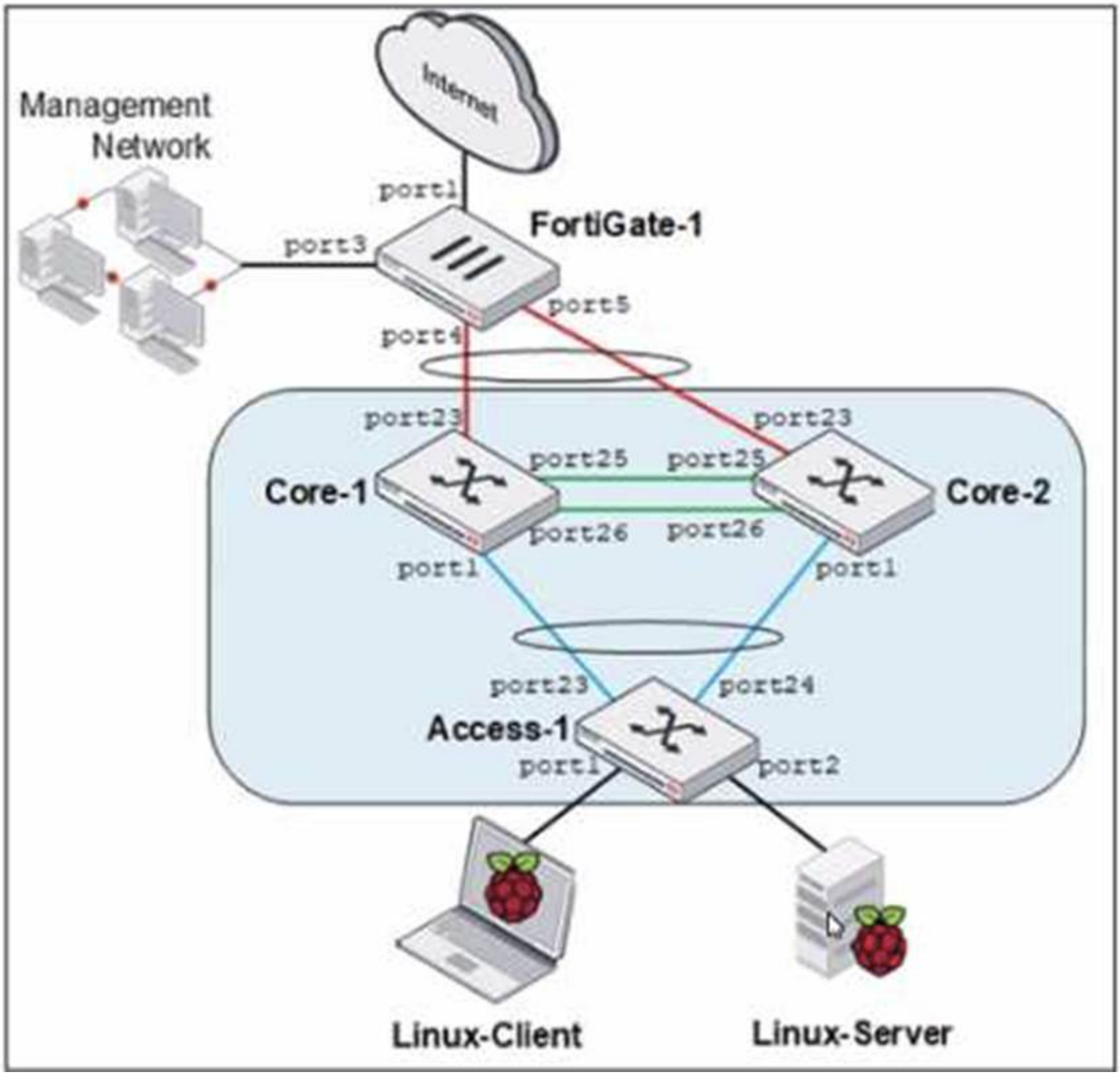
A. The administrator must manually pre-authorize FortiGate on FortiSwitch by adding the FortiGate serial number.
B. FortiSwitch requires a reboot to complete the authorization process.
C. A FortiLink frame is sent by FortiGate to FortiSwitch to complete the authorization.
D. FortiLink authorization sets the FortiSwitch management mode to FortiLink.

Answer: CD

Explanation:
Explanation
The FortiLink authorization process is an integral part of setting up FortiSwitch to be managed by FortiGate. The correct statements regarding the FortiLink authorization process are:
* C. A FortiLink frame is sent by FortiGate to FortiSwitch to complete the authorization.This is a part of the FortiLink protocol, where FortiGate communicates with the connected FortiSwitch to establish management and control. This frameinitiates the configuration and management process, allowing FortiGate to effectively control the switch.
* D. F tiLink authorization sets the FortiSwitch management mode to FortiLink.Once authorized, the management mode of FortiSwitch is set to FortiLink, indicating that it is being managed via a FortiLink
connection from a FortiGate appliance. This changes the operational mode of the switch to be under the control of the FortiGate for centralized management and policy application.
References:
Further details on the FortiLink setup and authorization process can be accessed through the FortiGate configuration guides available on theFortinet Documentation site.

NEW QUESTION 10
Refer to the exhibit.

MCL-Topology



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

Answer: B

Explanation:
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.

NEW QUESTION 10
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.)

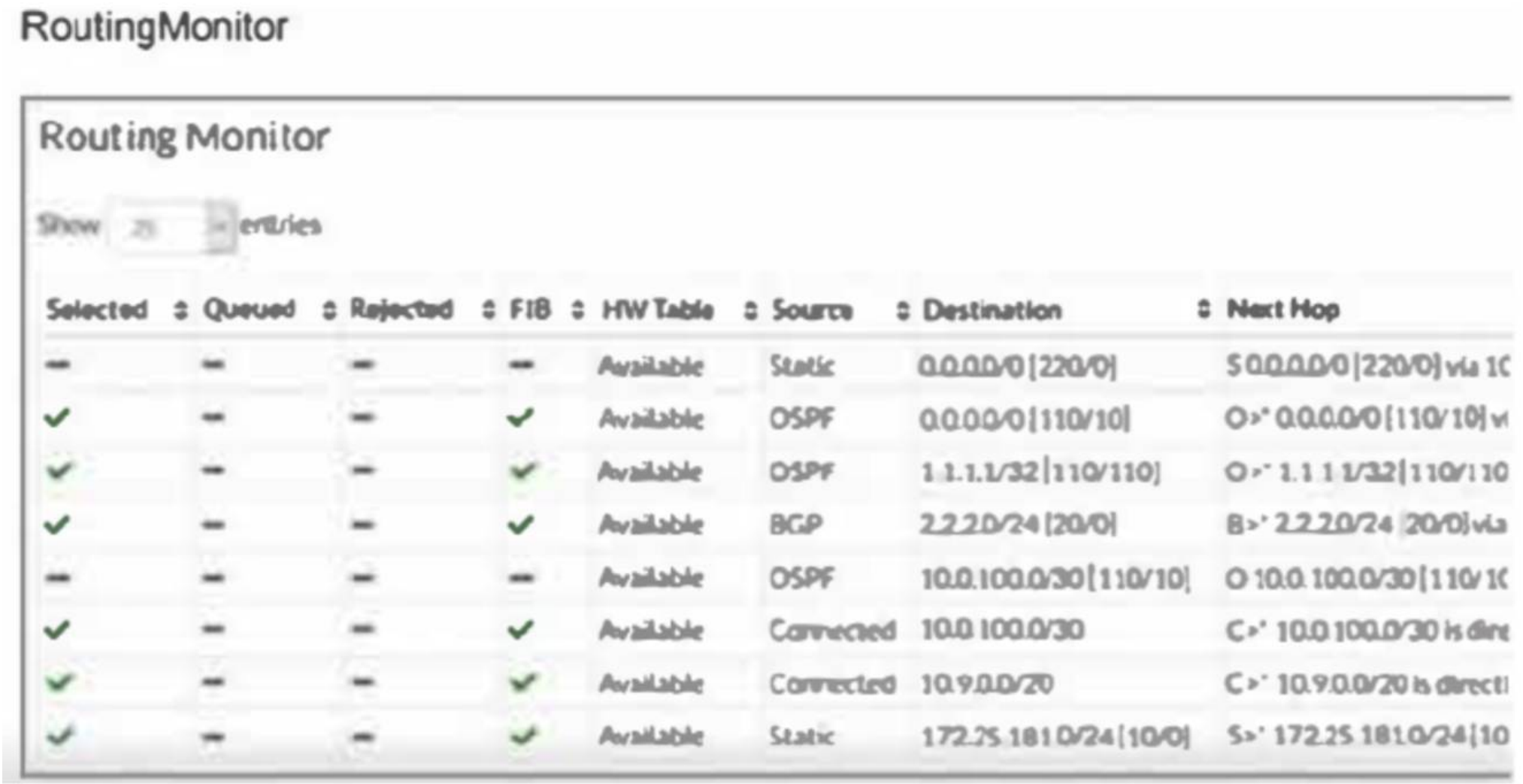
A. A FortiSwitch interface connected to the ISP router configured with fortilink-13-mode enabled.
B. FortiSwitch and FortiGate devices configured with VXLAN interfaces.

C. FortiSwitch devices configured with NAT disabled.
D. FortiSwitch devices that have the required internal hardware for this configuration.
E. FortiSwitch and FortiGate devices configured with IPsec interfaces.

Answer: BD

Explanation:
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):
Appropriate Hardware (D):
References:For specific information on VXLAN configuration and hardware requirements, refer to the technical documentation provided by Fortinet:Fortinet Product Documentation

NEW QUESTION 12
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.)

A. These two routes have a higher administrative distance value available to the destina-tion 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: AB

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.
References:
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.

NEW QUESTION 14
Refer to the exhibit.

Output

```
2021-07-23 12:13:19 573s:160ms:74us flp event handler[734]:node: port4
received event 101 state FL_STATE_WAIT_JOIN switchname S424DPTF20000029
flags 0x401

2021-07-23 12:13:21 575s:396ms:114us flp event handler[734]:node: port4
received event 110 state FL_STATE_READY switchname  flags 0x124a

2021-07-23 12:13:21 575s:398ms:724us flp event handler[734]:node: port4
received event 111 state FL_STATE_READY switchname  flags 0x124a

2021-07-23 12:13:21 575s:403ms:607us flp send pkt[445]:pkt-sent (type(5)
flag=0x18ca node(port4) sw(port4) len(26)smac: 0:50:56:96:d8: 2 dmac:
4:d5:90:c2:fa:ea

2021-07-23 12:13:22 576s:284ms:825us flp send pkt[445]:pkt-sent (type(3)
flag=0x8a node(port4) sw(S424DPTF20000029) len(26)smac: 0:50:56:96:d8: 2
dmac: 4:d5:90:c2:fb: b

2021-07-23 12:13:24 578s:411ms:316us flp event handler[734]:node: port4
received event 110 state FL_STATE_READY switchname  flags 0x124a

2021-07-23 12:13:24 578s:413ms:151us flp event handler[734]:node: port4
received event 111 state FL_STATE_READY switchname  flags 0x124a

2021-07-23 12:13:24 578s:415ms:255us flp send pkt[445]:pkt-sent (type(5)
flag=0x18ca node(port4) sw(port4) len(26)smac: 0:50:56:96:d8: 2 dmac:
4:d5:90:c2:fa:ea
```

Which two statements best describe what is displayed in the FortiLink debug output shown in the exhibit? (Choose two.)

A. FortiSwitch is sending FortiLink heartbeats to FortiGate.
B. FortiSwitch is discovered and authorized by FortiGate.
C. FortiSwitch is in a waiting state to join the stack group on FortiGate.
D. FortiSwitch is ready to push its new hostname to FortiGate.

Answer: AB

Explanation:
The provided debug output indicates that the FortiSwitch is sending FortiLink heartbeats to the FortiGate and is currently waiting to join the stack group. Here's a breakdown of the relevant lines:
Line 1:Shows the date, time, elapsed time since boot, and process ID for the FortiLink event handler.
Event 101:This indicates the FortiSwitch is in a "wait join" state (FL_STATE_WAIT_JOIN). This means it's discovered by the FortiGate and is awaiting further instructions to join the FortiLink stack group.
switchname S424DPTF20000029:This displays the serial number of the FortiSwitch.
flags 0x401:The specific flag meaning might depend on the FortiSwitch model and version, but it likely indicates general communication between the switch and FortiGate.
Lines 2 and onward:These lines show subsequent events with similar timestamps, suggesting a regular heartbeat interval. There are also instances of the FortiSwitch sending packets to the FortiGate (indicated bypkt-sent).
Why the Other Options Are Less Likely:
* C. FortiSwitch is discovered and authorized by FortiGate.While discovery might have happened before these lines, the "wait join" state suggests authorization hasn't necessarily completed yet.
* D. FortiSwitch is ready to push its new hostname to FortiGate.There's no explicit indication of hostname changes in this excerpt. The focus is on joining the stack group.
In Summary:
The key point is the "FL_STATE_WAIT_JOIN" state, which signifies the FortiSwitch is ready to be fully integrated but is waiting for further commands from the FortiGate to complete the process.

NEW QUESTION 17
Which drop policy mode, if assigned to a congested port, will drop incoming packets until there is no congestion on the egress port?

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

Answer: A

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 19

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

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.

NEW QUESTION 23
FortiGate is unable to establish a tunnel with the FortiSwitch device it is supposed to manage Based on the debug output shown in the exhibit, what is the reason for the failure?

A. The handshake process timed out before FortiSwitch responded.
B. DTLS client hello had the incorrect pre-shared key.
C. The CAPWAP tunnel failed to come up due to a mismatch in time.
D. FortiSwitch has disabled FortiLink and is only managed as a standalone.

Answer: C

Explanation:
The issue described pertains to the establishment of a tunnel (likely a CAPWAP tunnel for management purposes between FortiGate and FortiSwitch). Based on typical error analysis in tunnel setup scenarios:
The CAPWAP tunnel failed to come up due to a mismatch in time (Option C): This answer is plausible because time synchronization is crucial for security protocols that underpin tunnel establishments, such as DTLS (Datagram Transport Layer Security) used within CAPWAP tunnels. If the clocks on FortiGate and FortiSwitch are significantly out of sync, the security handshake (which can include timestamp validation) could fail, preventing the tunnel from coming up.
References:
Fortinet's technical documentation typically outlines the importance of time synchronization for secure communications. In CAPWAP/DLTS scenarios, precise time matching is crucial to ensure that the cryptographic parameters align correctly during the handshake process.

NEW QUESTION 26
Refer to the configuration:

```
config switch phy-mode
set port-configuration disable-port54
set port53-phy-mode 4x10G
end
```

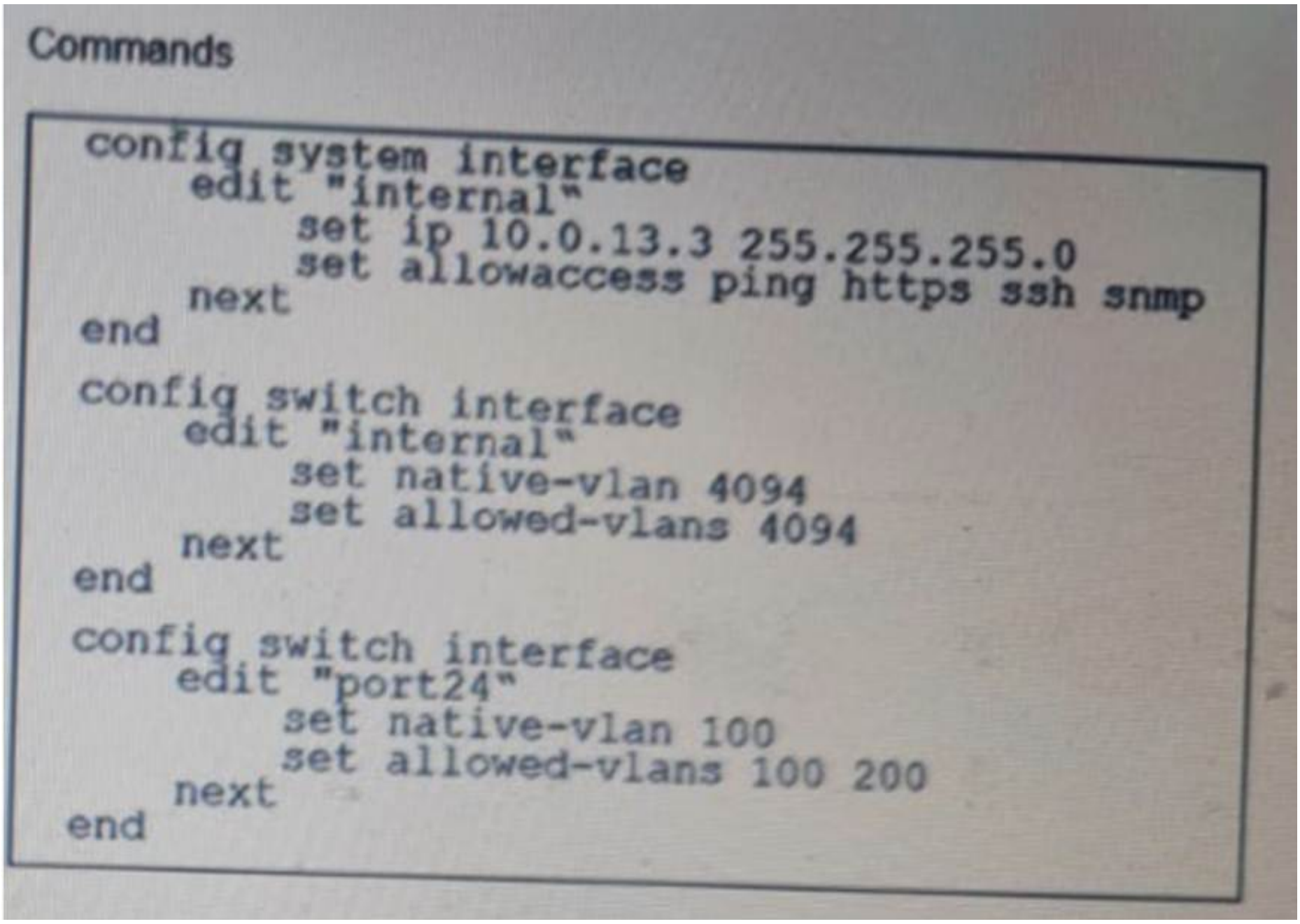
Which two conditions does FortiSwitch need to meet to successfully configure the options shown in the exhibit above? (Choose two.)

A. The FortiSwitch model is equipped with a maximum of 54 interfaces
B. FortiSwitch would need to be rebooted.
C. The split port can be assigned to a native VLAN.
D. The Dort full speed prior to the split was 100G QSFP+.

Answer: BD

Explanation:
The configuration provided involves adjusting the physical (PHY) mode of the ports on a FortiSwitch, including disabling a port and reconfiguring another for a different speed. The conditions needed for this configuration to be successful include:
FortiSwitch would need to be rebooted (B):
Reboot Requirement:Changes to the physical mode of ports, particularly when involving high-speed interfaces or changes that affect the operational mode of the hardware, typically require a reboot to apply the new configuration correctly.
The port full speed prior to the split was 100G QSFP+ (D):
Hardware Capabilities:Configuring port 53 to operate at 4x10G suggests that the original configuration supported a high throughput, such as 100GQSFP+. This configuration is typical in switches that support breaking down a high-capacity port into smaller units.
References:For more specific guidelines on port configuration and PHY mode settings in FortiSwitch devices, refer to the hardware installation and configuration manuals available at:Fortinet Product Documentation

NEW QUESTION 29
Exhibit.



port24 is the only uplink port connected to the network where access to FortiSwitch management services is possible. However, FortiSwitch is still not accessible on the management interface. Which two actions should you take to fix the issue and access FortiSwitch? (Choose two.)

A. You must add port24 native VLAN as an allowed VLAN on internal.
B. You must add VLAN ID 200 to the allowed VLANS on internal.
C. You must allow VLAN ID 4094 on port24, if management traffic is tagged.
D. You should use VLAN ID 4094 as the native VLAN on port24.

Answer: AC

Explanation:
To enable access to the FortiSwitch management interface from the network, certain configuration adjustments need to be made, particularly considering the VLAN settings displayed in the exhibit:
Adding port24 native VLAN to the allowed VLANs on internal (Option A): The management VLAN (VLAN 4094 in this case, as it is set as the native VLAN on the 'internal' interface of the FortiSwitch) must be included in the allowed VLANs on the interface that provides management connectivity. Since port24 is set with a different native VLAN (VLAN 100), VLAN 4094 (the management VLAN) should be allowed through to ensure connectivity.
Allow VLAN ID 4094 on port24 if management traffic is tagged (Option C): Management traffic is tagged on VLAN 4094. Since port24 is connected to thenetwork and serves as an uplink, allowing VLAN 4094 ensures that management traffic can reach the management interface of the FortiSwitch through this port.
The changes align with Fortinet??s best practices for setting up management VLANs and ensuring they are permitted on the relevant switch ports for proper management traffic flow.
References:
FortiGate Infrastructure and Security 7.2 Study Guides
Best practices for VLAN configurations in Fortinet??s technical documentation

NEW QUESTION 31
How are the 'by VLAN redirect MAC address quarantine' mode and the 'by redirect MAC address quarantine' mode on FortiGate similar?

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.

NEW QUESTION 32

Which two statements about VLAN assignments on FortiSwitch ports are true? (Choose two.)

A. Configure a native VLAN on the FortiLink
B. Assign an IP address and subnet mask to FortiSwitch VLANs
C. Only assign one native VLAN on a port
D. Assign untagged VLANs using FortiGate CLI

Answer: CD

Explanation:
VLAN assignments on FortiSwitch ports must follow certain rules and guidelines to ensure network integrity and proper traffic segregation:
Only Assign One Native VLAN on a Port (C):
Assign Untagged VLANs Using FortiGate CLI (D):
References:For detailed instructions and best practices on VLAN configuration on FortiSwitch, refer to the FortiSwitch administration guide available on:Fortinet Product Documentation

NEW QUESTION 33
Which packet capture method allows FortiSwitch to capture traffic on trunks and management interfaces?

A. SPAN
B. Sniffer profile
C. sFlow
D. TCP dump

Answer: C

NEW QUESTION 35
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE6_FSW-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE6_FSW-7.2-dumps.html