Fortinet

Exam Questions FCSS_LED_AR-7.6

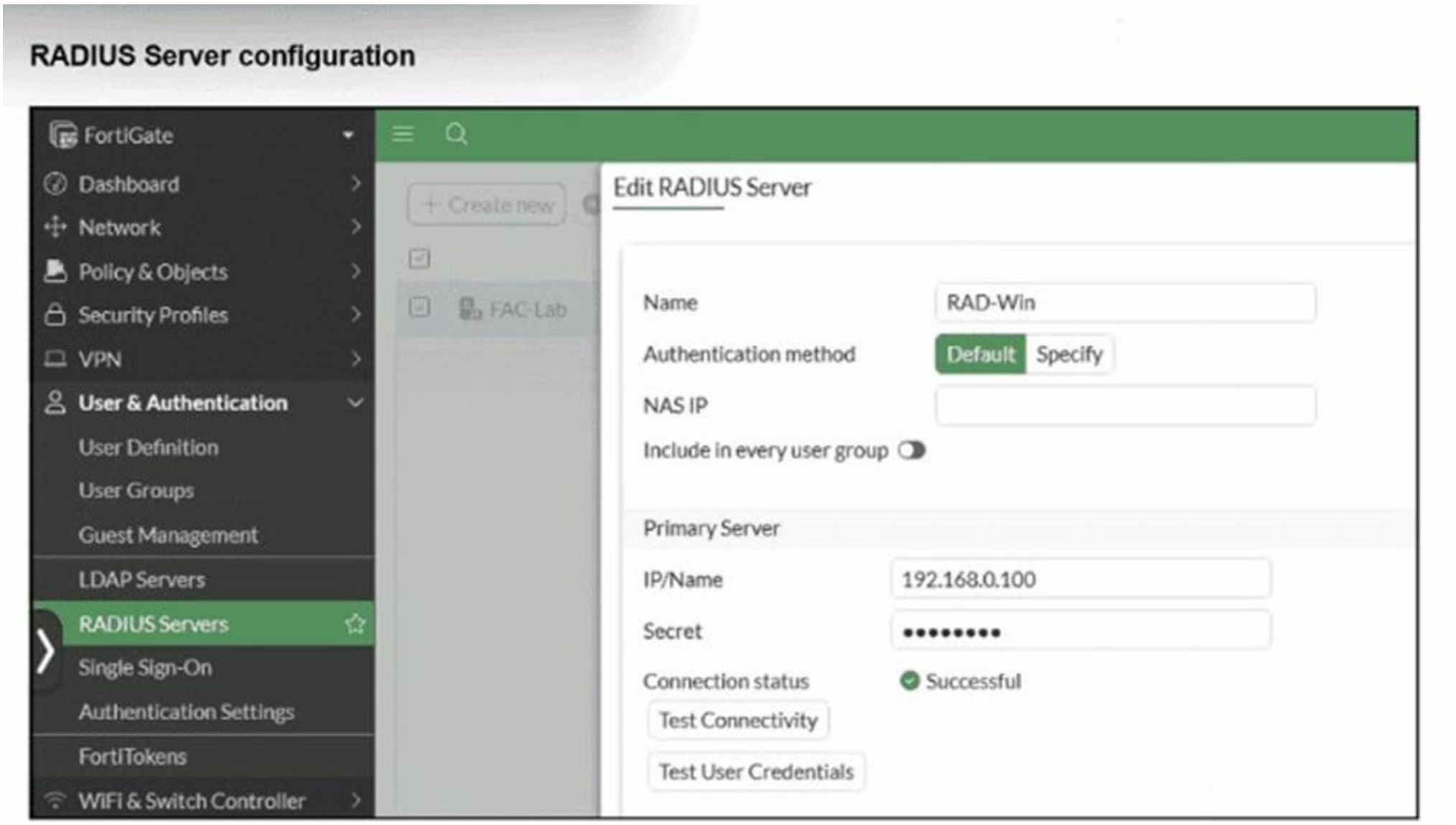
FCSS - LAN Edge 7.6 Architect

NEW QUESTION 1
Which FortiGuard licenses are required for FortiLink device detection to enable device identification and vulnerability detection?

A. FortiGuard Vulnerability Management and FortiGuard Endpoit Protection
B. FortiGuard Threat Intelligence and FortiGuard loT Detection
C. FortiGuard Threat Intelligence and FortiGuard Endpoint Protection
D. FortiGuard Attack Surface Security and FortiGuard loT Detection

Answer: D

NEW QUESTION 2
Refer to the exhibit.



On FortiGate, a RADIUS server is configured to forward authentication requests to FortiAuthenticator, which acts as a RADIUS proxy. FortiAuthenticator then relays these authentication requests to a remote Windows AD server using LDAP.
While testing authentication using the CLI command diagnose test authserver. the administrator observed that authentication succeeded with PAP but failed when using MS- CHAFV2.
Which two solutions can the administrator implement to enable MS-CHAPv2 authentication? (Choose two.)

A. Change the FortiGate authentication method to CHAP instead of MS-CHAPv2.
B. Enable Windows Active Directory domain authentication on FortiAuthenticator.
C. Enable RADIUS attribute filtering on FortiAuthenticator.
D. Configure FortiAuthenticator to use RADIUS instead of LDAP as the back-end authentication server

Answer: AD

NEW QUESTION 3
You are configuring FortiAuthenticator to integrate with FSSO for user identification. To enable FortiAuthenticator to extract user information from syslog messages and inject it into FSSO, you have configured syslog matching rules.
What is the role of syslog matching rules in the process of injecting user information into FSSO?

A. To automatically update user group memberships in FSSO based on syslog events
B. To enforce user authentication policies based on syslog message contents
C. To define how syslog messages are parsed and extract user information, such as usernames and IP addresses
D. To filter and block irrelevant syslog messages from being processed by the FortiAuthenticator

Answer: C

NEW QUESTION 4

Refer to the exhibit.

WTP profile configuration

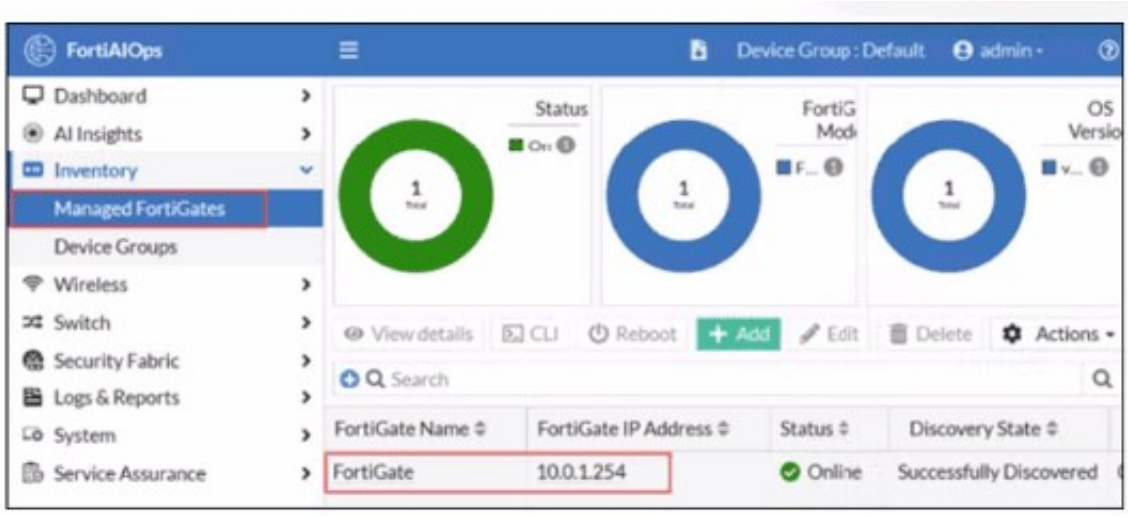
```
config wireless-controller wtp-profile
    edit "S231F"
        config platform
            set type 231F
        end
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set ap-country US
        config radio-1
            set band 802.11n-2G
            set wids-profile "default-wids-apscan-enabled"
            set vap-all manual
            set vaps "Student01"
            set channel "1" "6" "11"
        end
        config radio-2
            set band 802.11ac-5G
            set channel-bonding 40MHz
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set arrp-profile "arrp-default"
            set vap-all manual
            set vaps "Student01"
            set channel "36" "44" "52"
        end
        config radio-3
            set mode disabled
        end
    next
end
```

Which shows the WTP profile configuration.
The AP profile is assigned to two FAP-231F APs that are installed in an open plan area. The first AP has 32 clients associated with the 5 GHz radios and 22 clients associated with the 2.4 GHz radio. The second AP has 12 clients associated with the 5 GHz radios and 20 clients associated with the 2.4 GHz radio.
A dual-band-capable client enters the area near the first AP and the first AP measures the new client at - 3 3 dBm signal strength. The second AP measures the new client at -43 dBm signal strength.
If the new client attempts to conned to the student 01 wireless network, which AP radio will the client be associated with?

A. The first AP 2.4 GHz interface provides a stronger signal, which clients often prioritize.
B. The first AP 5 GHz interface because it has a stronger signal.
C. The second AP 5 GHz interface has fewer clients, which ensures better performance despite the weaker signal.
D. The second AP 2.4 GHz interface is preferred over 5 GHz for better speed and lower interference.

Answer: C

NEW QUESTION 5
FortiGate has been added to FortiAIOps for management.



Which step must be performed on FortiAIOps to add a FortiSwitch device connected to the recently added FortiGate?

A. Add the FortiSwitch device by submitting its serial number.
B. FortiAIOps requires that the FortiSwitch IP address is submitted.
C. FortiSwitch is added automatically.
D. Configure the FortiSwitch IP address, user ID, and password

Answer: C

NEW QUESTION 6
Refer to the exhibits.

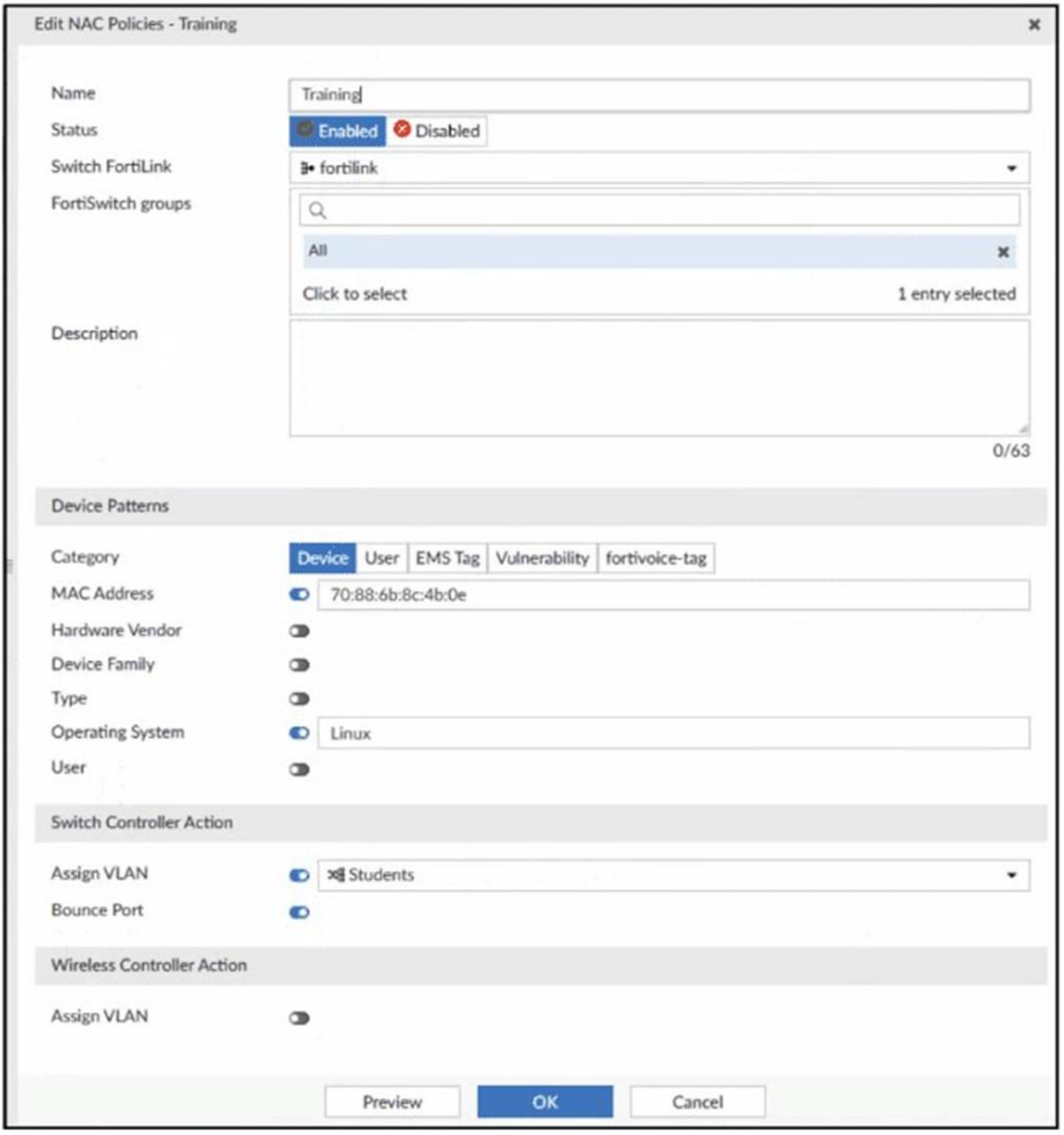
FortiSwitch Ports

FortiSwitch Ports - FortiSwitch

+ Create New | Edit | Delete | Refresh

Port	Description	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs
port1		Static		Edge Port Spanning Tree Protocol	AP Management (APs)	HR (VLAN102) IT (VLAN101) quarantine.fortilink (quarantine)
port2		Static		Edge Port Spanning Tree Protocol	Students	quarantine.fortilink (quarantine)
port3		Static		Edge Port Spanning Tree Protocol	default.fortilink (_default)	quarantine.fortilink (quarantine)

NAC policy



A NAC policy has been configured to apply traffic that flows through FortiSwitch port 2. Traffic that meets the NAC policy criteria will be assigned to the Students VLAN. However, the NAC policy does not seem to be taking effect.
Which configuration is missing?

A. Port2 Access mode should be set to NAC mode.
B. The MAC address or OS might be misconfigured for the connected device.
C. Port2 Access mode should be set to Port Policy mode.
D. The Students VLAN should be set to Allowed VLANs instead of Native VLAN.

Answer: A

NEW QUESTION 7
You are troubleshooting a Syslog-based single sign-on (SSO) issue on FortiAuthenticator, where user authentication is not being correctly mapped from the syslog messages. You need a tool to diagnose the issue and understand the logs to resolve it quickly.
Which tool in FortiAuthenticator can you use to troubleshoot and diagnose a Syslog SSO issue?

A. Debug logs > Remote Servers > Syslog Viewer
B. Parsing Test Tool

C. Debug logs > SSO Sessions page
D. Debug logs > Single Sign-On > Syslog SSO

Answer: D

NEW QUESTION 8
Refer to the exhibits.

FortiGate VLAN AP settings

```
config system interface
    edit "APs"
        set vdom "root"
        set ip 10.10.100.254 255.255.255.0
        set allowaccess ping
        set alias "AP Management"
        set device-identification enable
        set role lan
        set snmp-index 118
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 100
    next
end
```

DHCP configuration

```
config system dhcp server
    edit 7
        set dns-service default
        set default-gateway 10.10.100.254
        set netmask 255.255.255.0
        set interface "APs"
        config ip-range
            edit 1
                set start-ip 10.10.100.1
                set end-ip 10.10.100.253
            next
        end
    next
end
```

FortiSwitch port1 VLAN AP assignment

```
config switch-controller managed-switch
    edit "FortiSwitch"
        set sn "S224EPTF19006016"
        set fsw-wan1-peer "fortilink"
        set fsw-wan1-admin enable
        set poe-detection-type 2
        set version 1
        set max-allowed-trunk-members 8
        set pre-provisioned 1
        set dynamic-capability 0x00000000000000001551027757ddfff7
        config ports
            edit "port1"
                set poe-capable 1
                set vlan "APs"
                set allowed-vlans "VLAN102" "VLAN101" "quarantine"
                set untagged-vlans "quarantine"
                set export-to "root"
                set mac-addr 04:d5:90:39:7d:8e
            next
```

A FortiSwitch is successfully managed by a FortiGate. FortiAP is connected to port1 of the managed FortiSwitch. On FortiGate, the VLAN AP is configured to detect and manage FortiAP, along with a DHCP server for the VLAN AP. Additionally, the VLAN AP is assigned to port1 of FortiSwitch. However. FortiGate is unable to detect or manage FortiAP.
Which FortiGate misconfiguration is preventing the detection of FortiAP?

A. Security Fabric is disabled in the administrative access options of the VLAN.
B. The FortiAP firmware is incompatible with the FortiGate firmware version.
C. The VLAN is not tagged correctly on the FortiSwitch uplink port.
D. The CAPWAP ports (UDP 5246 and 5247) are not open on FortiGate.

Answer: A

NEW QUESTION 9
Which VLAN is used by FortiGate to place devices that fail to match any configured NAC policies? CRSPAN

A. NAC
B. segment
C. Quarantine
D. Onboarding

Answer: D

NEW QUESTION 10
Connectivity tests are being performed on a newly configured VLAN. The VLAN is configured on a FortiSwitch device that is managed by FortiGate. During testing, it is observed that devices within the VLAN can successfully ping FortiGate. and FortiGate can also ping these devices.
Inter-VLAN communication is working as expected. However, devices within the same VLAN are unable to communicate with each other.
What could be causing this issue?

A. Access VLAN is enabled on the VLAN.
B. The FortiSwitch MAC address table is missing entries.
C. The FortiGate ARP table is missing entries.
D. The native VLAN configured on the ports is incorrect.

Answer: A

NEW QUESTION 10
Your office wants to set up a Wi-Fi network for visitors. Your company would like to require them to log in for (racking purposes. Which two types of captive portals could be enabled on an interface? (Choose two.)

A. Terms Acknowledgment Without Authentication
B. Email Notification Only
C. Disclaimer + Authentication
D. Guest Pass Access
E. Authentication

Answer: AE

NEW QUESTION 14
A FortiSwitch is not appearing in the FortiGate management interface after being connected via FortiLink. What could be a first troubleshooting step?

A. Ensure that the FortiGate security policies allow traffic from the FortiSwitch.
B. Manually assign a static IP to the FortiSwitch.
C. Verify that FortiGate device DHCP server is assigning an IP to the FortiSwitch.
D. Ensure the FortiSwitch has internet access.

Answer: C

NEW QUESTION 17
Which statement about generating a certificate signing request (CSR) for a CER certificate is true?

A. Inaccurate or missing fields in the CSR will prevent the CA from validating the request, leading to the rejection of the certificate and possible delays in the deployment process.
B. If key fields like the common name (CN) and organization (O) are incorrect, the certification authority (CA) will still issue the certificate, but it may not be trusted by certain applications or systems that rely on accurate field information for validation.
C. CSR fields are primarily used for internal recordkeeping by the requesting organization, and only the public key in the CSR must be accurate for successful certificate signing.
D. The fields in the CSR are primarily for documentation purposes; any missing or incorrect information will be automatically corrected by the CA during the signing process.

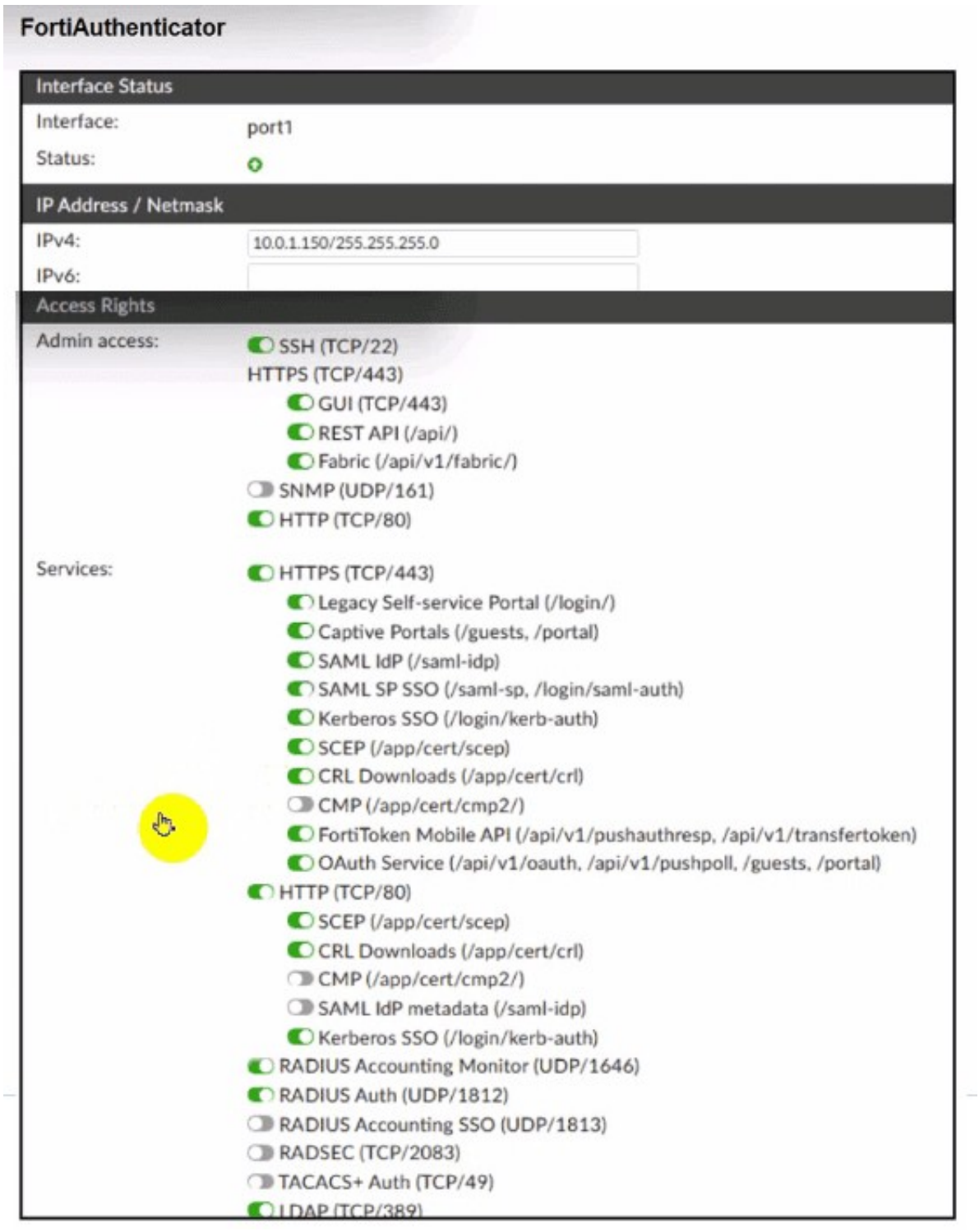
Answer: A

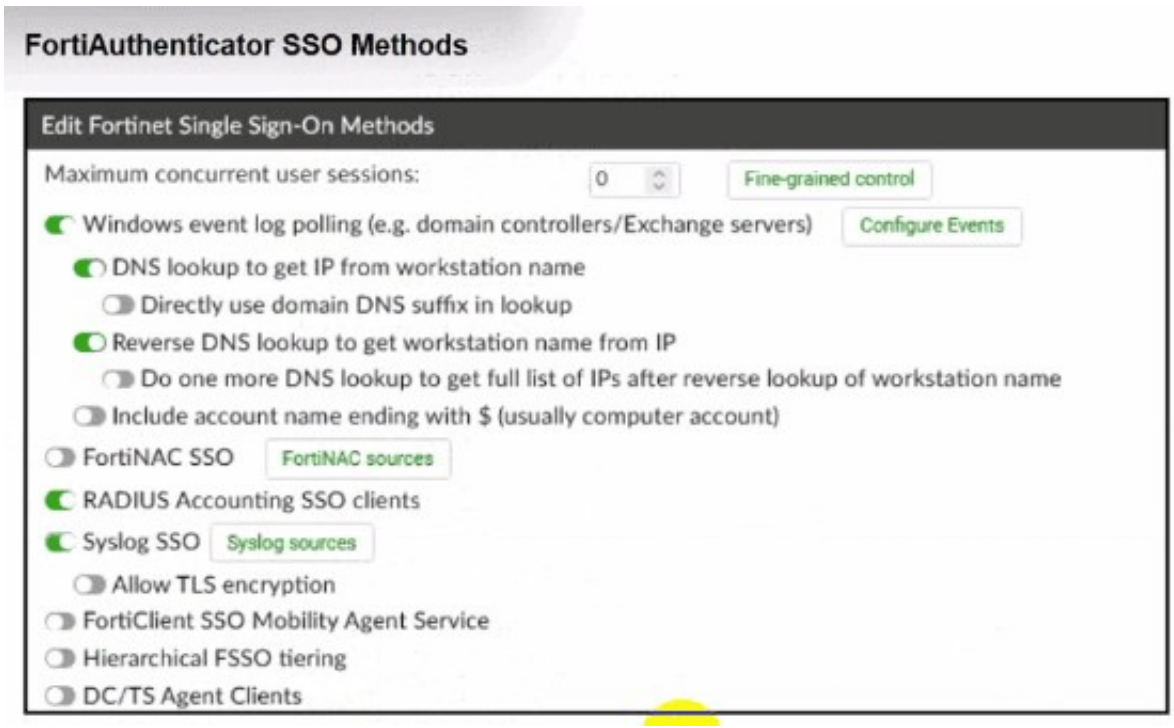
NEW QUESTION 19
A conference center wireless network provides guest access through a captive portal, allowing unregistered users to self-register and connect to the network. The IT team has been tasked with updating the existing configuration to enforce captive portal authentication over a secure HTTPS connection. Which two steps should the administrator take to implement this change? (Choose two.)

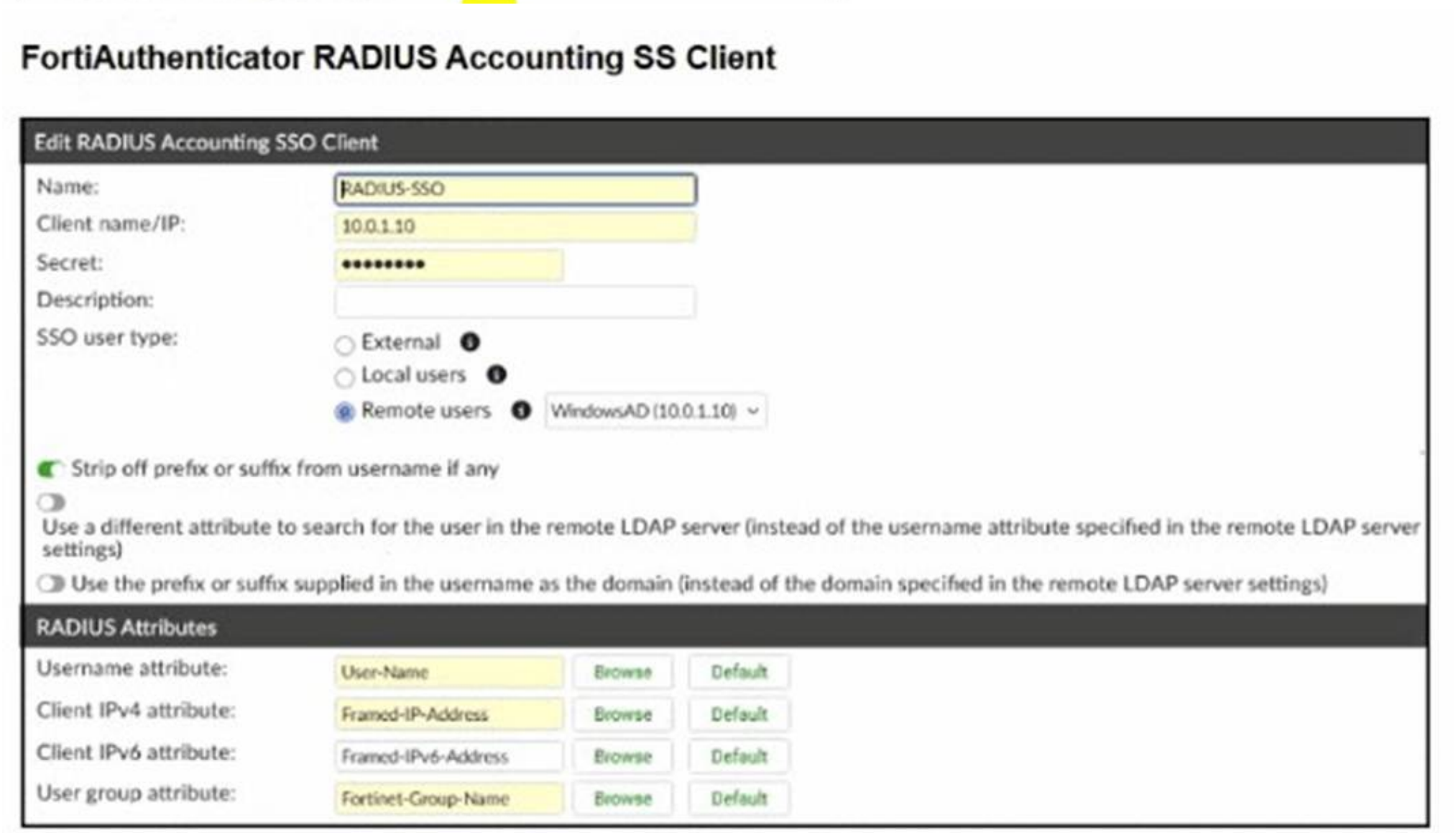
A. Enable HTTP redirect in the user authentication settings.
B. Create a new SSID with the HTTPS captive portal URL.
C. Disable HTTP administrative access on the guest SSID to enforce HTTPS connection.
D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator.

Answer: AD

NEW QUESTION 23
Refer to the exhibits.







A company has multiple FortiGate devices deployed and wants to centralize user authentication and authorization. The administrator decides to use FortiAuthenticator to convert RSSO messages to FSSO, allowing all FortiGate devices to receive user authentication updates.
After configuring FortiAuthenticator to receive RADIUS accounting messages, users can authenticate, but FortiGate does not enforce the correct policies based on user groups. Upon investigation, the administrator discovers that FortiAuthenticator is receiving RADIUS accounting messages from the RADIUS server and successfully queries LDAP for user group information. But, FSSO updates are not being sent to FortiGate devices and FortiGate firewall policies based on FSSO user groups are not being applied.
What is the most likely reason FortiGate is not receiving FSSO updates?

A. The RADIUS Username and Client IPv4 attributes are not defined on FortiAuthenticator.
B. The LDAP server is not configured to retrieve group memberships for RSSO users.
C. FortiAuthenticator is missing the FSSO user group attribute in the configuration.
D. The FortiAuthenticator interface is not enabled to receive RADIUS accounting messages.

Answer: A

NEW QUESTION 26
A network administrator connects a new FortiGate to the network, allowing it to automatically discover andI register with FortiManager.
What occurs after FortiGate retrieves the FortiManager address?

A. FortiGate establishes a secure tunnel to FortiManager over TCP port 541.
B. The device needs to be manually authorized on FortiManager.
C. FortiGate configures its interface settings based on a DHCP response from FortiManager.
D. FortiGate sends a discovery request to all devices on the local network using UDP port 1068.

Answer: A

NEW QUESTION 31
How can FortiAIOps help optimize network performance in an SD-Branch deployment with FortiGate, FortiSwitch, and FortiAP?

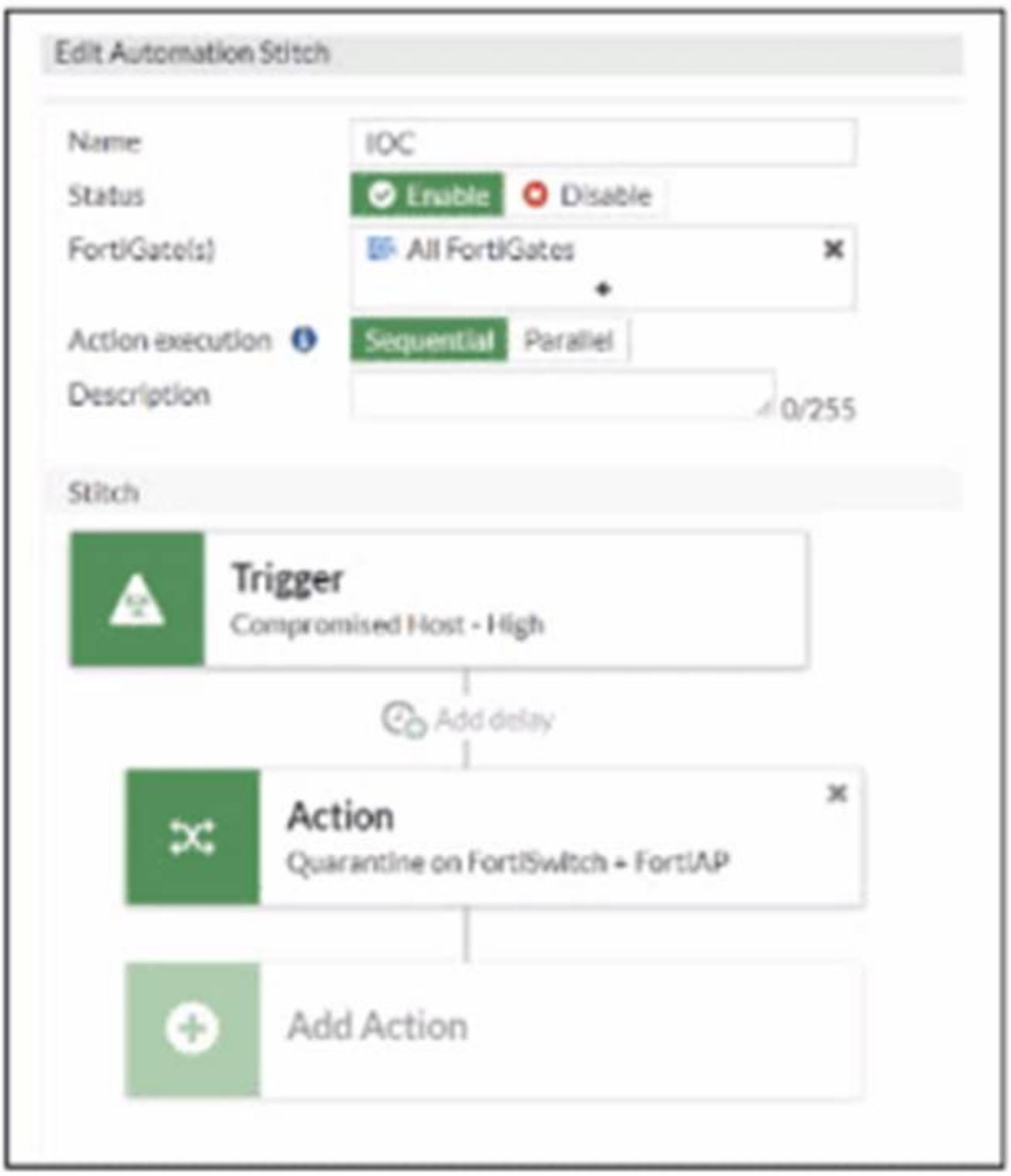
A. It disables low-performing APs and switches automatically.
B. It uses AI-driven analytics to identify network issues and provide optimization recommendations.
C. It removes the need for SD-WAN configuration by automating all routing decisions.
D. It predicts and resolves all network issues without any human intervention.

Answer: B

NEW QUESTION 32
Refer to the exhibits.

FortiGate Security Fabric widget

Security Fabric Automation Stitch



Quarantine widget

FortiGate firewall policy

FortiAnalyzer log

Examine the FortiGate configuration, FortiAnalyzer logs, and FortiGate widget shown in the exhibits.
Security Fabhc quarantine automation has been configured to isolate compromised devices automatically. FortiAnalyzer has been added to the Security Fabric, and an automation stitch has been configured to quarantine compromised devices.
To test the setup, a device with the IP address 10.0.2.1 that is connected through a managed FortiSwitch attempts to access a malicious website. The logs on FortiAnalyzer confirm that the event was recorded, but the device does not appear in the FortiGate quarantine widget.
Which two reasons could explain why FortiGate is not quarantining the device? (Choose two.)

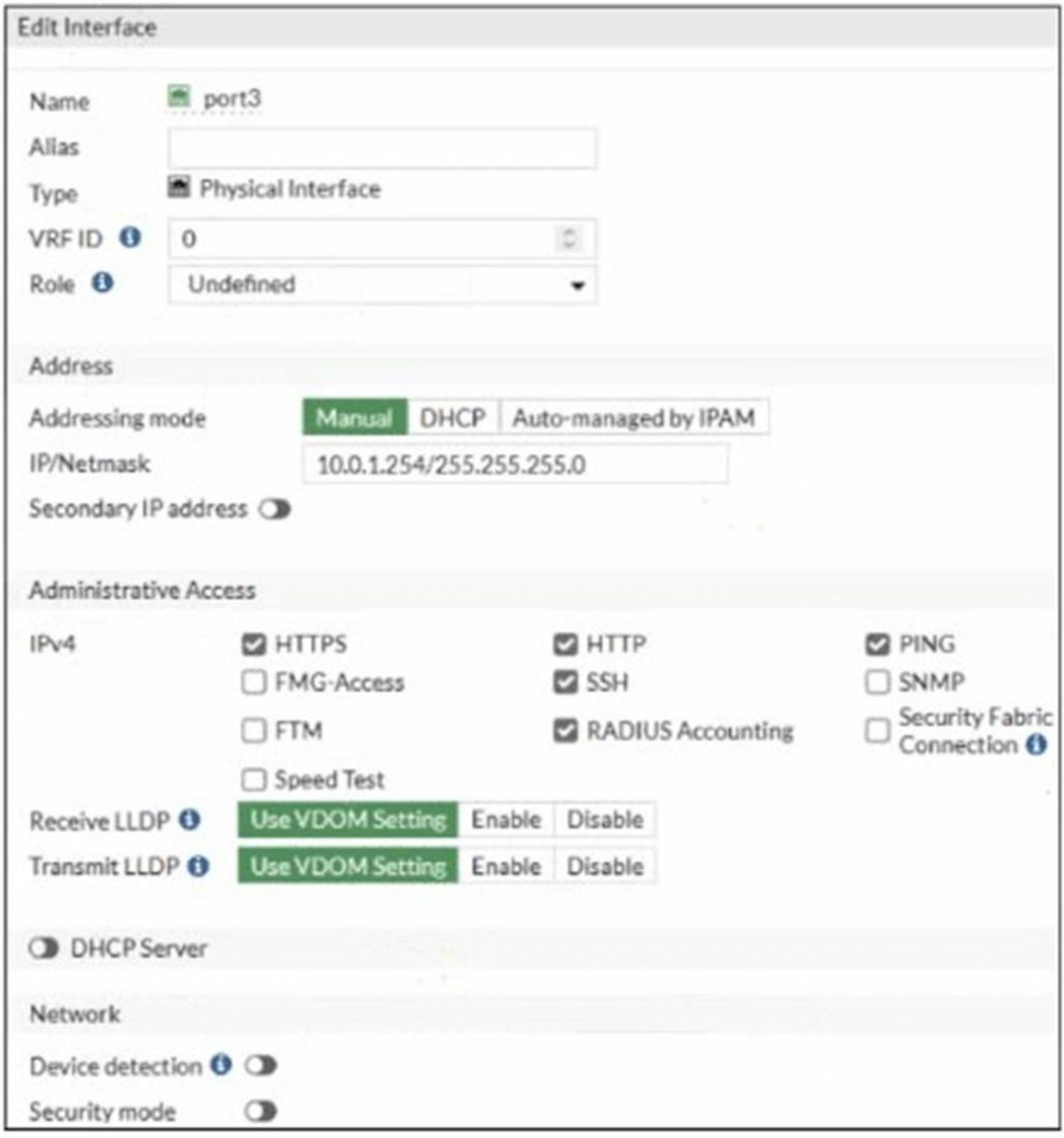
A. The IOC action should include only the FortiSwitch in the quarantine.
B. The SSL inspection should be set to deep-Inspection
C. The malicious website is not recognized as an indicator of compromise (IOC) byFortiAnalyzer.
D. The threat detection services license is missing or invalid under FortiAnalyzer.

Answer: CD

NEW QUESTION 33
Refer to the exhibits.


FortiGate RSSO configuration
Edit External Connector
Endpoint/Identity
RADIUS Single
Sign-On Agent
Connector Settings
Name
RSSO Agent
Use RADIUS Shared Secret
Send RADIUS Responses

FortiGate interface configuration



Examine the FortiGate RSSO configuration shown in the exhibit.
FortiGate is set up to use RSSO for user authentication. It is currently receiving RADIUS accounting messages through port3. The incoming RADIUS accounting messages contain the username in the User-Name attribute and group membership in the Class attribute. You must ensure that the users are authenticated through these RADIUS accounting messages and accurately mapped to their respective RSSO user groups.
Which three critical configurations must you implement on the FortiGate device? (Choose three.)

A. The RADIUS Attribute Value setting configured for an RSSO user group should match the class RADIUS attribute value in the RADIUS accounting message.
B. RSSO user groups should be assigned to all firewall policies.
C. Device detection and Security Fabric Connection should be enabled on port3
D. The sso-attribute CLI setting in the RSSO agent configuration should be set to Class.
E. The rsso-endpoint-attribute CLI setting in the RSSO agent configuration should be set toUser-Name.

Answer: ADE

NEW QUESTION 35

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCSS_LED_AR-7.6 Practice Exam Features:

* FCSS_LED_AR-7.6 Questions and Answers Updated Frequently

* FCSS_LED_AR-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_LED_AR-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_LED_AR-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year