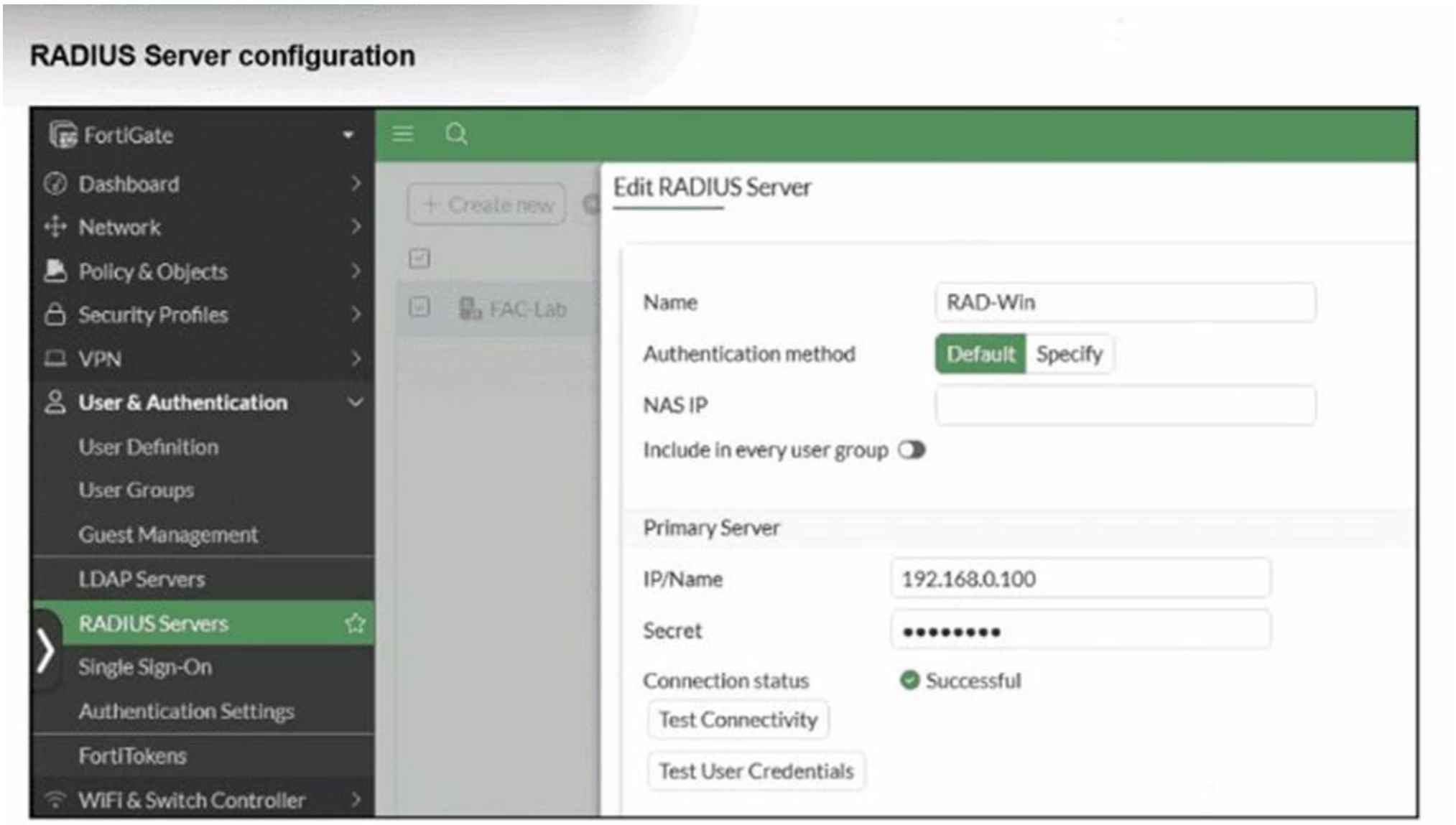
Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect

https://www.2passeasy.com/dumps/FCSS_LED_AR-7.6/

NEW QUESTION 1
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 2
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

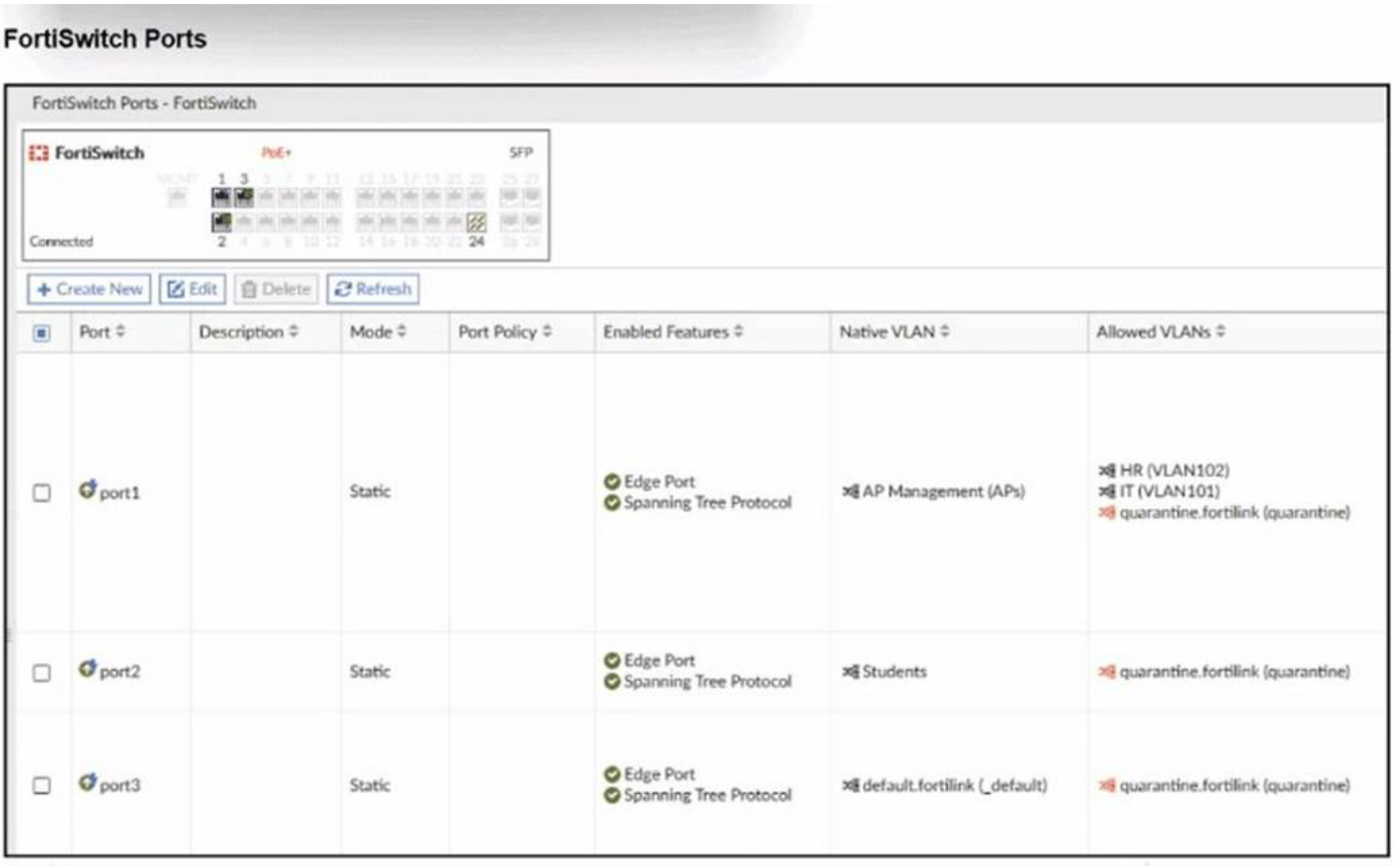
NEW QUESTION 3
What is the expected behavior when enabling auto TX power control on a FortiAP interface?

A. FortiGate monitors the signal strength of nearby AP interfaces and adjusts its own transmit power every 30 seconds to match the signal strength of the adjacent AP
B. FortiGate measures the signal strength of nearby FortiAP interfaces every 30 seconds and adjusts their transmit power to ensure they remain detectable at -70 dBm.
C. FortiGate periodically measures the signal strength of the weakest associated client and adjusts the AP radio power to align with the detected signal strength of that client.
D. The AP periodically evaluates the signal strength of its own transmission from the client perspective and adjusts its power to ensure the signal is detected at -70 dBm.

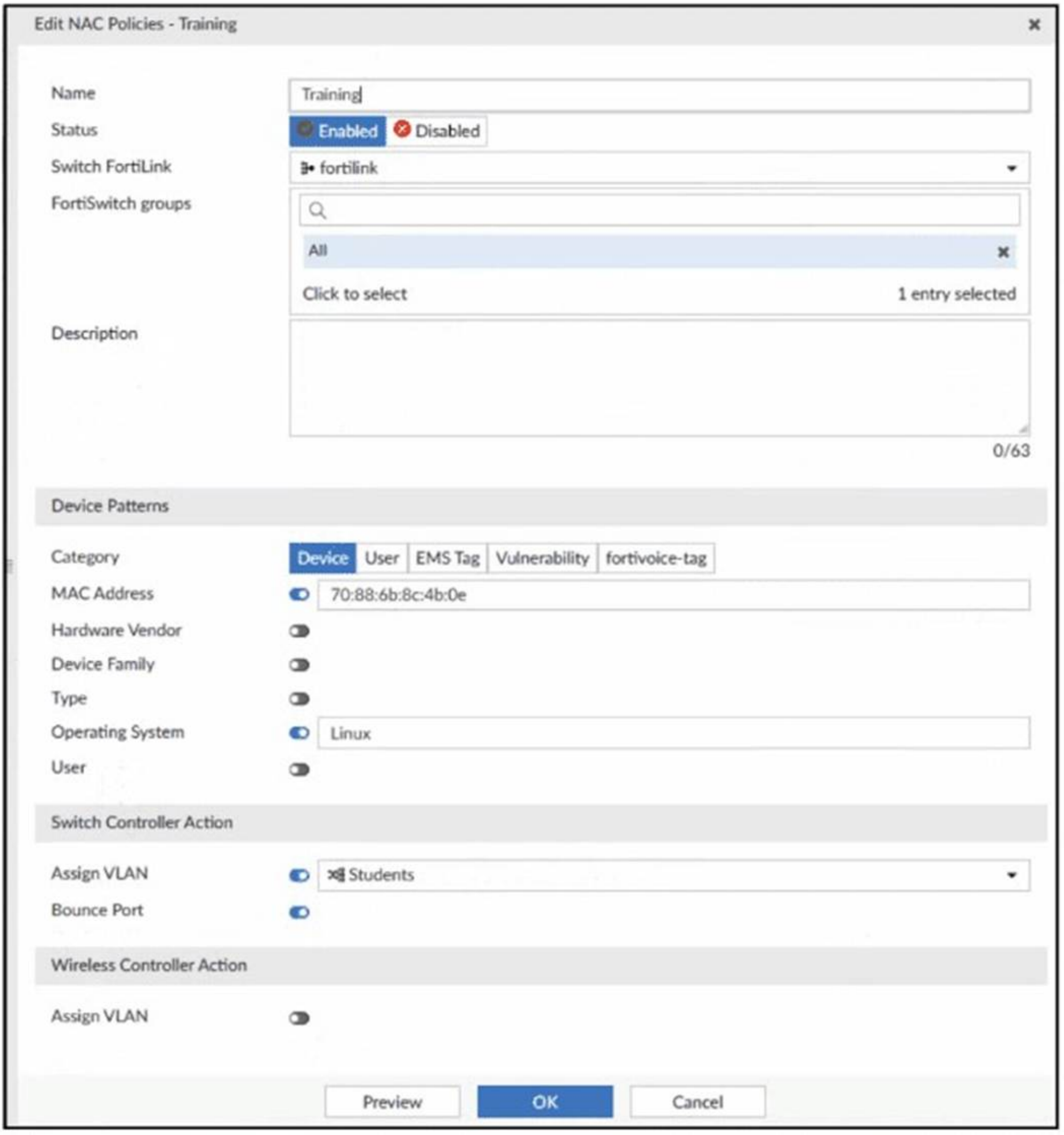
Answer:

C

NEW QUESTION 4
Refer to the exhibits.



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 5
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 6
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 7
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 8
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 9
What is the primary function of FortiLink NAC in a LAN environment?

A. To extend security policies across FortiGate firewalls only
B. To automate device onboarding and verify security posture
C. To manage FortiSwitch devices and apply manual firewall rules
D. To ensure devices are manually placed in VLANs based on their user roles

Answer: B

NEW QUESTION 10
You are setting up a captive portal to provide Wi-Fi access for visitors. To simplify the process, your team wants visitors to authenticate using their existing social media accounts instead of creating new accounts or entering credentials manually.
Which two actions are required to enable this functionality? (Choose two.)

A. Set up a remote open authorization (OAuth) server for each selected social media platform.
B. Configure only the email login option because a social media login cannot be used with captive portals.
C. Enable Account Login as the authentication type and configure a remote LDAP server.
D. Set up the FortiAuthenticator internal database as the primary source for user credentials

E. Configure the social login profiles for the supported platforms.

Answer: AD

NEW QUESTION 10
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 14
Refer to the exhibits.

VAP configuration

```
config wireless-controller vap
    edit "Corporate"
        set ssid "Corp"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "FAC-Lab"
        set intra-vap-privacy enable
        set schedule "always"
        set vlan-pooling wtp-group
        config vlan-pool
            edit 101
                set wtp-group "Floor_1"
            next
            edit 102
                set wtp-group "Office"
            next
        end
    next
end
```

Wi-Fi zone table

WiFi SSID 7				
	Corp (Corporate)	WiFi SSID		0.0.0.0/0.0.0.0
	Corp.101	VLAN		0.0.0.0/0.0.0.0
	Corp.102	VLAN		10.0.20.1/255.255.255.0
	wqtn.5.Corporat	VLAN		0.0.0.0/0.0.0.0
	Guest (Guest)	WiFi SSID		0.0.0.0/0.0.0.0
	Student01 (Student01)	WiFi SSID		0.0.0.0/0.0.0.0
Zone 1				
	Corp.zone	Zone	Corp.101 Corp.102	

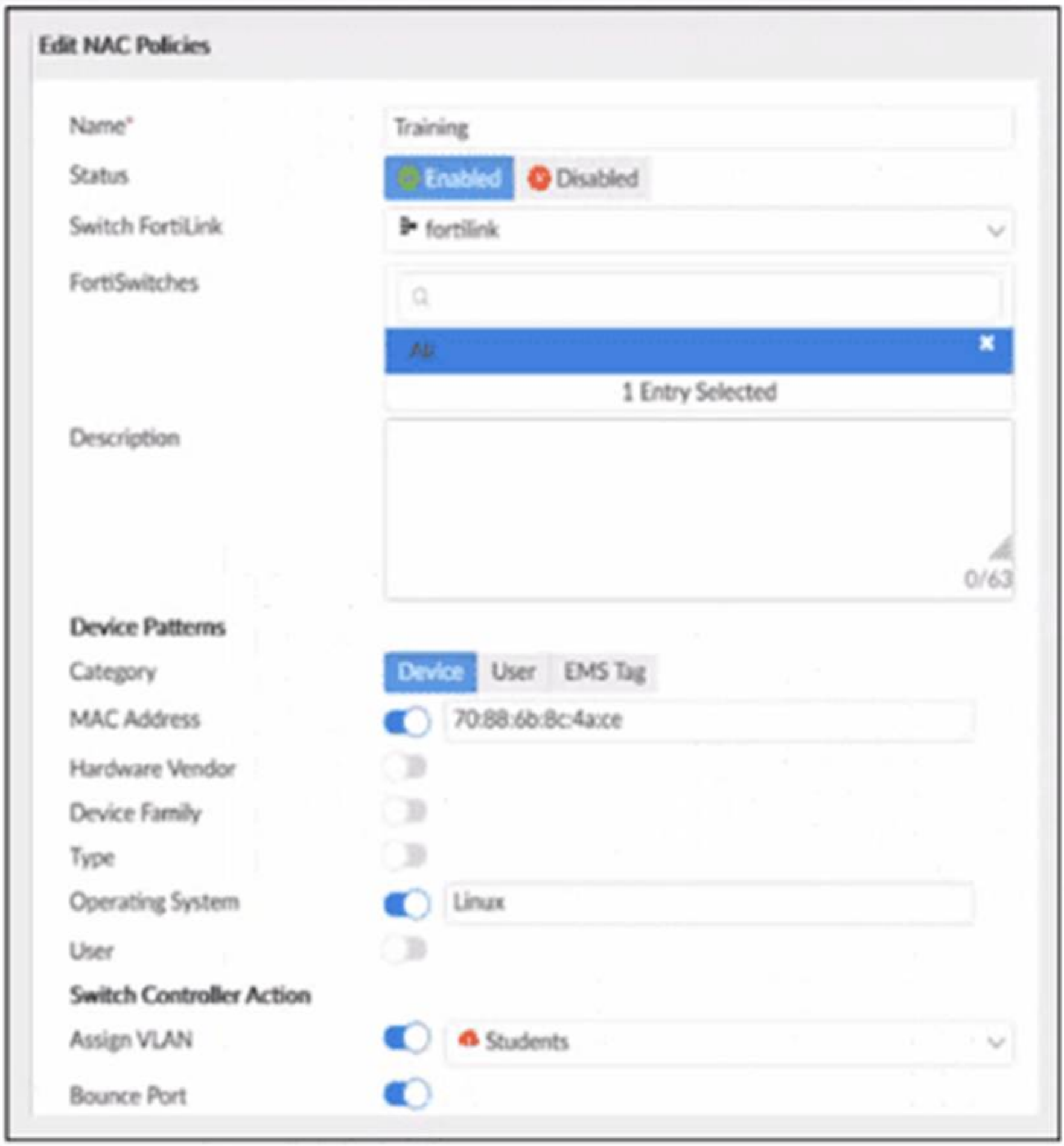
The exhibits show the VAP configuration. Wi-Fi SSIDs. and zone table.
Which two statements describe how FortiGate handles VLAN assignment for wireless clients? (Choose two.)

A. FortiGate will load balance clients using VLAN 101 and VLAN 102 and assign them an IP address from the 10.0.3.0/24 subnet.
B. All clients connecting to the Corp Zone will receive an IP address from the 10.0.20.0/24 subnet.
C. Clients connecting to APs in the Floor 1 group will not be able to receive an IP address.
D. Clients connecting to APs in the Office group will be assigned to VLAN 102.

Answer: CD

NEW QUESTION 19
Refer to the exhibits.

FortiManager configuration



FortiGate CLI output

```
FortiGate# diagnose switch-controller switch-info mac-table S224EPTF19005867
vdom: root

Managed Switch : S224EPTF19005867 0

MAC: 00:0c:29:e6:ea:d2 VLAN: 4089 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 1 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native I

MAC: 00:0c:29:e6:ea:d2 VLAN: 4093 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 4094 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 70:88:6b:8c:4a:ce VLAN: 4089 Port: port2(port-id 2)
   Flags: 0x00010441 ( hit dynamic src-hit native )

MAC: 04:d5:90:3e:e7:80 VLAN: 1 Port: port1(port-id 1)
   Flags: 0x00010441 ( hit dynamic src-hit native )

MAC: 00:0c:29:06:ea:d2 VLAN: 4088 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 10 Trunk:  GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

Total Displayed: 8

FortiGate# diagnose switch-controller mac-device nac onboarding
vdom: root
VLAN        MAC                 LAST-SEEN    TYPE    LOCATION
4089        70:88:6b:8c:4a:ce   4            SW      S224EPTF19005867      port2

FortiGate# diagnose switch-controller mac-device nac known
vdom: root
MAC        LAST-KNOWN-SWITCH     LAST-KNOWN-PORT       MATCHED-NAC-POLICY MAC-POLICY-ACTION   FSW-ID  COMMENTS
```

Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit.
The NAC feature is being tested with a device connected to port2 on managed FortiSwitch S224SPTF19005867. The NAC policy has been applied to port2, and traffic was generated from the test device. However, the traffic from the test device does not match the NAC policy and remains in the onboarding VLAN.
What are two possible reasons why the test device is not being correctly classified by the NAC policy? (Choose two.)

A. Device detection is not enabled on VLAN 4089.
B. The device operating system detected by FortiGate is not Linux.
C. Management communication between FortiGate and FortiSwitch is down.
D. The MAC address configured on the NAC policy is incorrect.

Answer: AB

NEW QUESTION 24
Refer to the exhibits.

Network topology

FortiSwitch status

Name	Switch Group	Status	Model
FortiLink: fortilink 1			
FortiSwitch		Offline	FortiSwitch 224E-PO

Fortilink interface settings in FortiGate

```
FortiGate (fortilink) # show
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.0.13.254 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "port4"
        set device-identification enable
        set lldp-reception enable
        set lldp-transmission enable
        set role lan
        set snmp-index 14
        set auto-auth-extension-device enable
        set ip-managed-by-fortiipam disable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
        set lacp-mode static
    next
end
```

DHCP server setting for fortilink

```
config system dhcp server
    edit 1
        set dns-service default
        set ntp-service local
        set default-gateway 10.0.13.254
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.0.13.1
                set end-ip 10.0.13.253
            next
        end
        set vci-match enable
        set vci-string "FortiExtender"
    next
end
```

You are adding a new FortiSwitch to FortiGate for management. All necessary settings have been configured on FortiGate, but FortiSwitch remains offline. The cabling has been verified and is correctly connected.
Which misconfiguration might be preventing FortiGate from detecting FortiSwitch?

A. The Fortilink interface setting ip-managed-by-fortiipam must be enabled.
B. The Fortilink interface has the wrong interface member.
C. The Fortilink interface setting cype must be physical.
D. The DHCP server setting vci-string is misconfigured.

Answer: D

NEW QUESTION 27
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_LED_AR-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_LED_AR-7.6 Product From:

https://www.2passeasy.com/dumps/FCSS_LED_AR-7.6/

Money Back Guarantee

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