

Fortinet

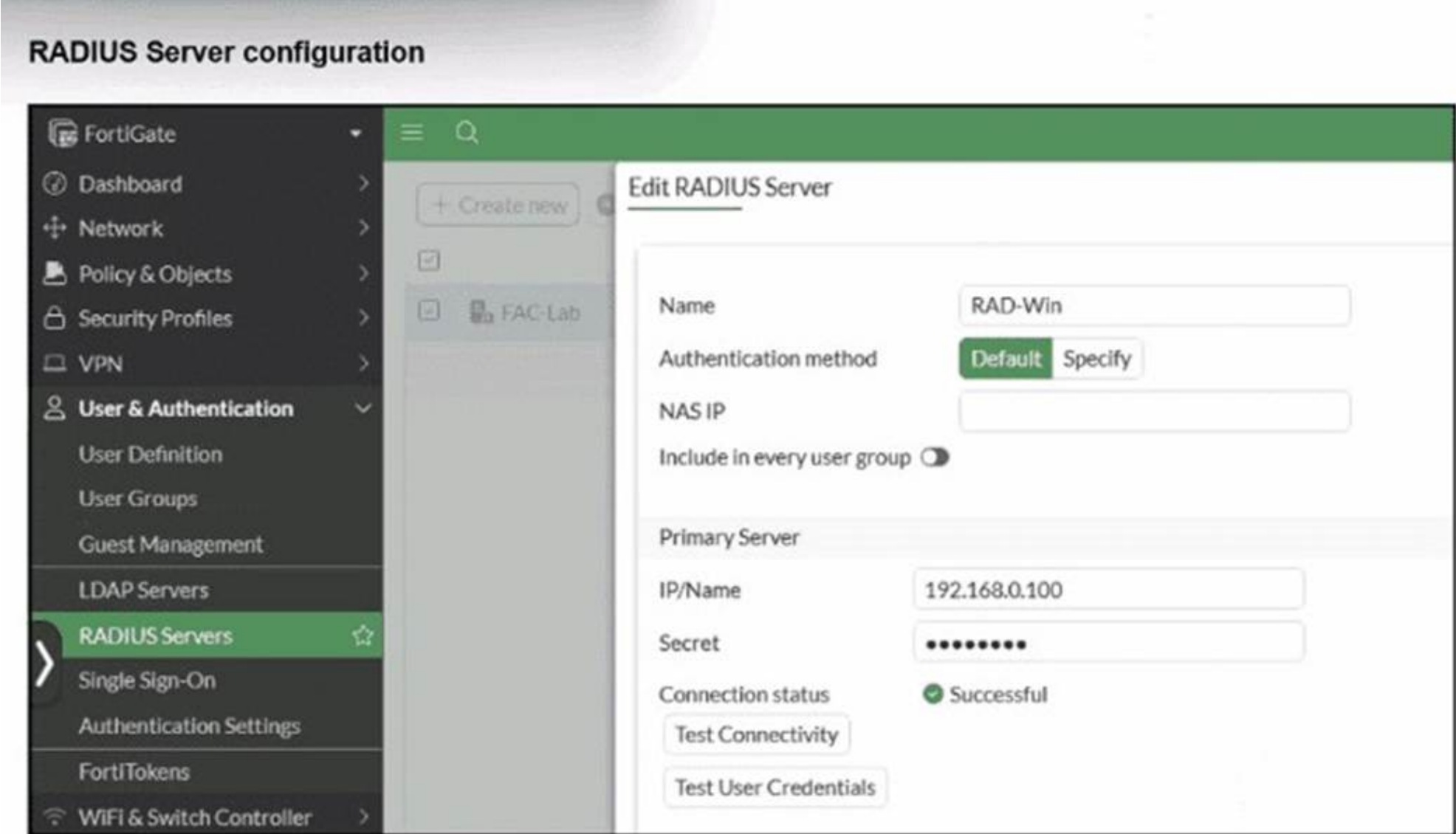
Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect



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-CHAPV2. 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

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
  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 -33 dBm signal strength. The second AP measures the new client at -43 dBm signal strength.

If the new client attempts to connect 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 3

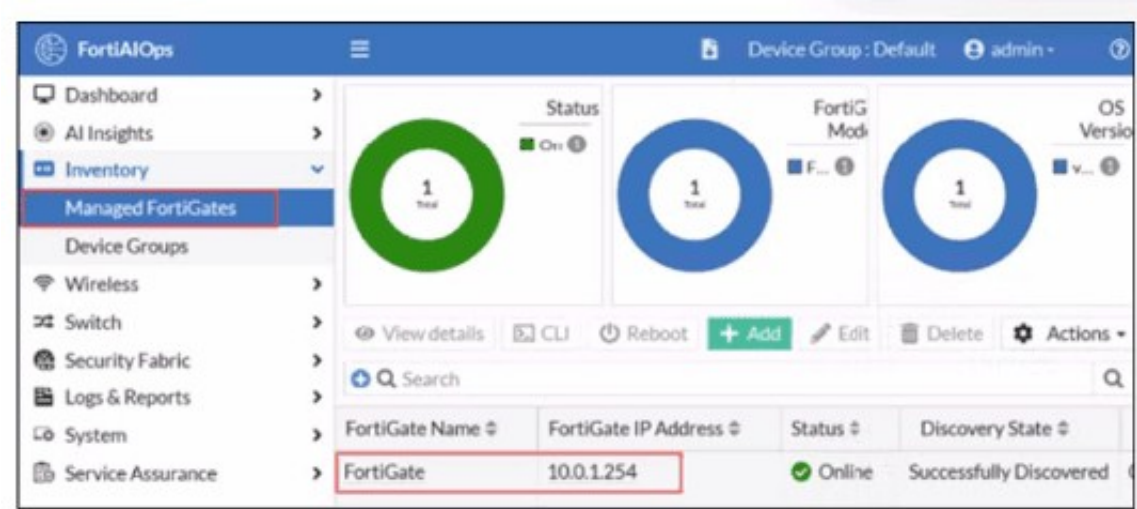
When the MAC address of a device is placed in quarantine on FortiSwitch, what happens to its egress traffic?

- A. Traffic is sent to an access VLAN.
- B. Traffic is assigned to the native VLAN.
- C. Traffic is sent as untagged traffic.
- D. Traffic is sent to an allowed VLAN.

Answer: A

NEW QUESTION 4

FortiGate has been added to FortiAIOps for management.



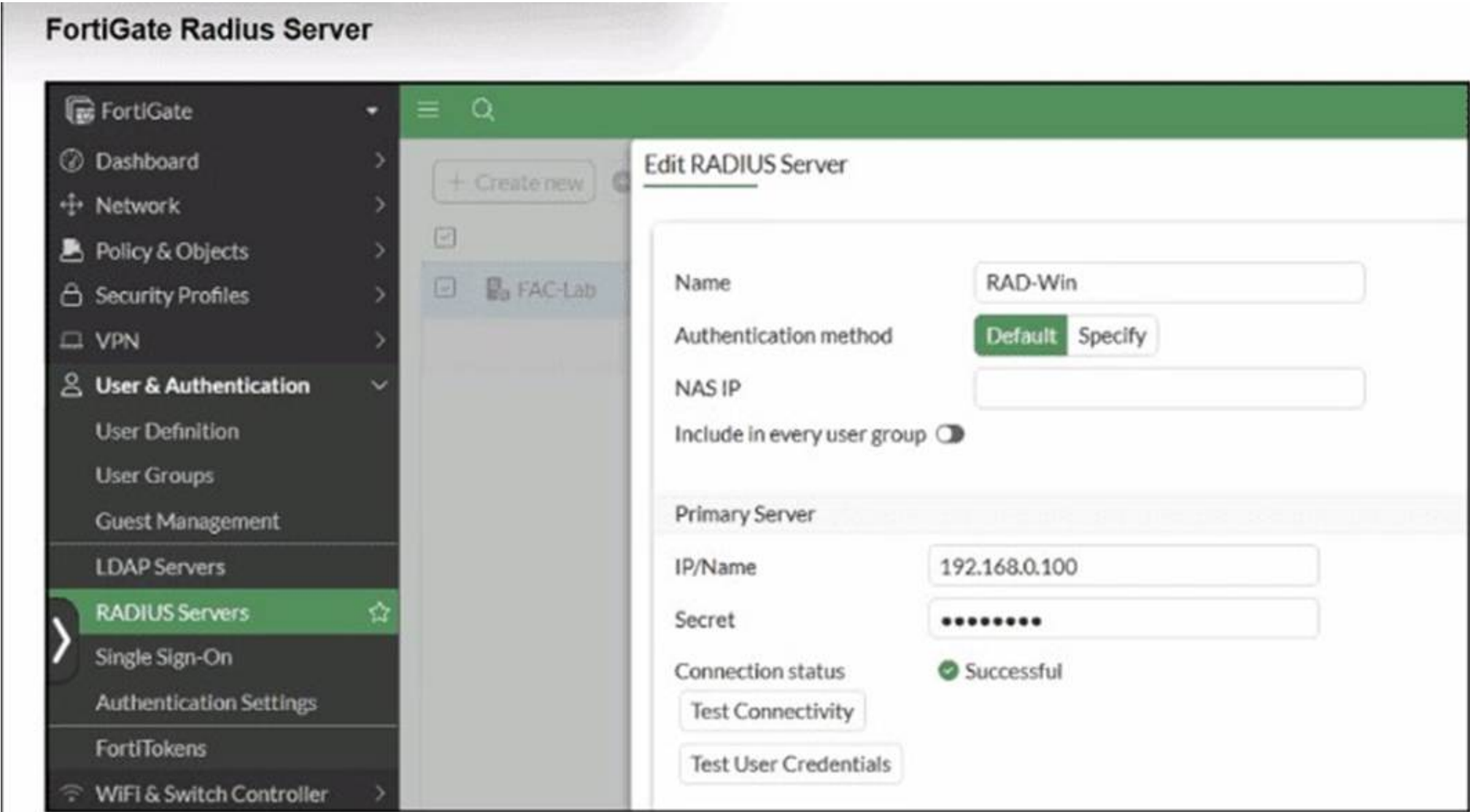
Which step must be performed on FortiAIOps to add a FortiSwitch device connected to the recently added FortiGate?

- 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 5

Refer to the exhibit.



FortuiGate CLI RADIUS server test

```
FortiGate #
FortiGate # diagnose test authserver radius FAC-Lab pap wifil01 password
authenticate 'wifil01' against 'pap' succeeded, server=primary assigned_rad_session_id=19718280638473 session_timeout=0 secs idle_timeout=0 secs!

FortiGate # diagnose test authserver radius FAC-Lab mschap2 wifil01 password
authenticate 'wifil01' against 'mschap2' failed, assigned_rad_session_id=19718280638474 session_timeout=0 secs idle_timeout=0 secs!
```

FortiAuthenticator - Remote LDAP server configuration

Edit LDAP Server

Name:

WindowsAD

Primary server name/IP:

10.0.1.10

Port:

389

☐ Use Zero Trust tunnel

[Please Select]

☐ Use secondary server

Base distinguished name:

DC=trainingAD,DC=training,DC=lab

Q Browse

Bind type:

Simple

Regular

Username:

CN=Administrator,CN=Users,DC=trainingAC

Password:

Server type:

Microsoft Active Directory

OpenLDAP/GSuite

Novell eDirectory/Others

Apply template

☐ Add supported domain names (used only if this is not a Windows Active Directory server)

Query Elements

User object class:

person

Username attribute:

sAMAccountName

Group object class:

group

Obtain group memberships from:

User attribute

Group attribute

Group membership attribute:

memberOf

☐ Force use of administrator account for group membership lookups

Secure Connection

☐ Enable

Windows Active Directory Domain Authentication

☐ Enable

A RADIUS server has been successfully configured on FortiGate, which sends RADIUS authentication requests to FortiAuthenticator. FortiAuthenticator, in turn, relays the authentication using LDAP to a Windows Active Directory server. It was reported that wireless users are unable to authenticate successfully. The FortiGate configuration confirms that it can connect to the RADIUS server without issues. While testing authentication on FortiGate using the command `diagnose test authserver radius`, it was observed that authentication succeeds with PAP but fails with MSCHAPv2. Additionally, the Remote LDAP Server configuration on FortiAuthenticator was reviewed. Which configuration change might resolve this issue?

- A. Change the RADIUS authentication protocol to CHAP
- B. Enable Windows Active Directory Domain Authentication.
- C. Manually add user credentials to the FortiAuthenticator local database
- D. Use RADIUS attributes under the FortiGate configuration.

Answer: B

NEW QUESTION 6

In a Windows environment using AD machine authentication, how does FortiAuthenticator ensure that a previously authenticated device is maintaining its network access once the device resumes operating after sleep or hibernation?

- A. It temporarily assigns the device to a guest VLAN until full reauthentication is completed.
- B. It sends a wake-on-LAN packet to trigger reauthentication.
- C. It uses machine authentication based on the device IP address.
- D. It caches the MAC address of authenticated devices for a configurable period of time.

Answer: D

NEW QUESTION 7

In addition to requiring a FortiAnalyzer device to configure the Security Fabric, which license must be added to FortiAnalyzer to use Indicators of Compromise (IOC) rules?

- A. IoT Security Add-on license
- B. IOC Subscription license
- C. IOC detection is included on FAZ-Basic license
- D. Threat Detection Service license

Answer: D

NEW QUESTION 8

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 9

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 10

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 10

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 12

A network administrator connects a new FortiGate to the network, allowing it to automatically discover and 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 16

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 19

When troubleshooting a captive portal issue, which POST parameter in the redirected HTTPS request can be used to track the user's session and ensure that the request is valid?

- A. username

- B. redir
- C. magic
- D. email

Answer: C

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 29

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_LED_AR-7.6 Practice Test Here](#)