

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 Endpoint Protection
- B. FortiGuard Threat Intelligence and FortiGuard IoT Detection
- C. FortiGuard Threat Intelligence and FortiGuard Endpoint Protection
- D. FortiGuard Attack Surface Security and FortiGuard IoT Detection

Answer: D

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
  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.

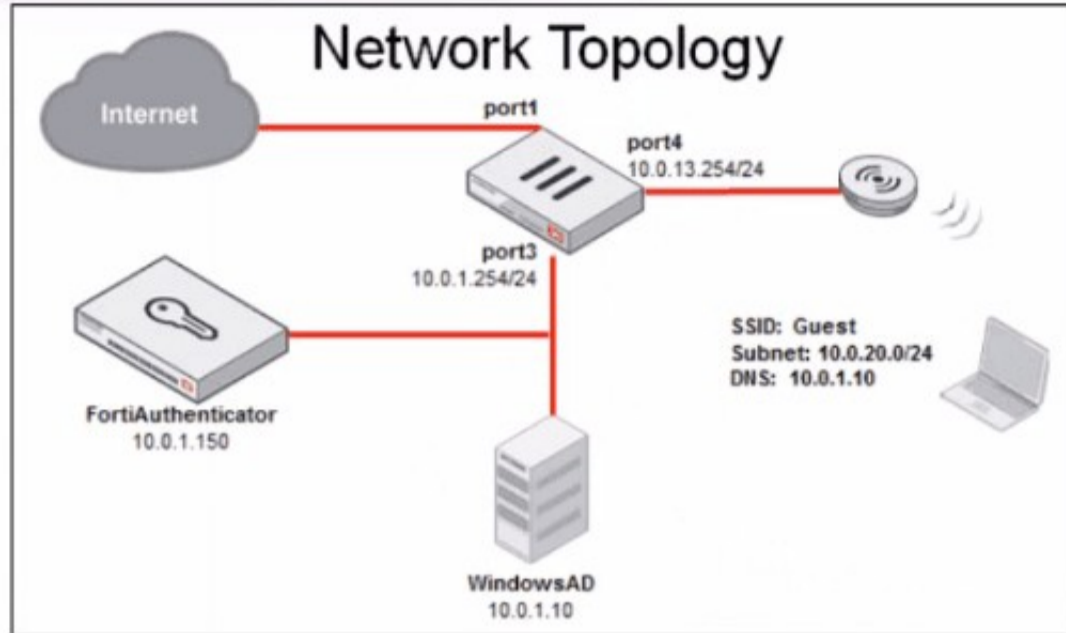
- B. The first AP 5 GHz interface because it has a stronger signal.
- C. The second AP 5 GHz interface has fewer clients, which ensures better performance despite the weaker signal.
- D. The second AP 2.4 GHz interface is preferred over 5 GHz for better speed and lower interference.

Answer: C

NEW QUESTION 3

Refer to the exhibit.

Network Topology



WiFi settings

WiFi Settings

SSID:

Client limit:

Broadcast SSID:

Beacon advertising: Name Model Serial number

Security Mode Settings

Security mode:

Captive Portal:

Portal type:

Authentication portal: Local External

User groups:

Exempt sources:

Exempt destinations/services:

Redirect after Captive Portal: Original Request Specific URL

Client MAC Address Filtering

RADIUS server:

Address group policy: Disable Allow Deny

Firewall policy settings

ID	Name	Source	Destination	Schedule	Service	Action	NA
Guest01 (Guest-Access) → port1							
12	guest internet access	all guest.portal	all	always	ALL	ACCEPT	Enabled
port2 → port1							
port2 → port3							
port3 → port1							
port3 → port2							
port3 → Students							

Review the exhibits to analyze the network topology, SSID settings, and firewall policies.

FortiGate is configured to use an external captive portal for authentication to grant access to a wireless network. During testing, it was found that users attempting to connect to the SSID cannot access the captive portal login page.

What configuration change should be made to resolve this issue to allow users to access the captive portal?

- A. Change the SSID security mode to WPA2-Enterprise for authentication.
- B. Disable HTTPS redirection for the captive portal authentication page.
- C. Exclude FortiAuthenticator and Windows AD address objects from filtering.
- D. A firewall policy allowing Guest SSID traffic to reach FortiAuthenticator and Windows AD.

Answer: D

NEW QUESTION 4

Refer to the exhibits.

FortiSwitch Ports

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

Edit NAC Policies - Training ✕

Name:

Status: Enabled Disabled

Switch FortiLink:

FortiSwitch groups: ✕
 Click to select 1 entry selected

Description:

0/63

Device Patterns

Category: Device User EMS Tag Vulnerability fortivoice-tag

MAC Address:

Hardware Vendor:

Device Family:

Type:

Operating System:

User:

Switch Controller Action

Assign VLAN:

Bounce Port:

Wireless Controller Action

Assign VLAN:

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

Refer to the exhibits.

SSID Profiles

SSIDs (4)				
<input type="checkbox"/>	CompanyPrinters	Guest-01	Tunnel	WPA2 Personal
<input type="checkbox"/>	Employees-Red	Student01	Local Bridge	WPA2 Enterprise
<input type="checkbox"/>	Guest-CorpPort	fortinet	Tunnel	WPA2 Personal
<input type="checkbox"/>	PSK	fortinet	Tunnel	WPA2 Personal

Platform: FAP231F

Dedicated Scan:

Indoor / Outdoor: Default (Indoor) | Indoor | Outdoor

Country / Region: United States

FortiAP Configuration Profile:

AP Login Password: Set | Leave Unchanged | Set Empty

Administrative Access: HTTPS SNMP SSH

Client Load Balancing: Frequency Handoff AP Handoff

Bluetooth Profile:

802.1X Authentication:

Radio 1

Mode: Disabled | Access Point | Dedicated Monitor | SAM | Packet Sniffer

WIDS Profile:

Radio Resource Provision:

Band: 2.4 GHz | Click to select

Channel Width: []

Transmit Power Mode: **Percent**

Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

dBm
Power is setting using a dBm value.

Auto
Set a range of dBm values and the power is set automatically.

Transmit Power: [] 100 %

SSIDs: Tunnel | Bridge | Manual

Monitor Channel Utilization:

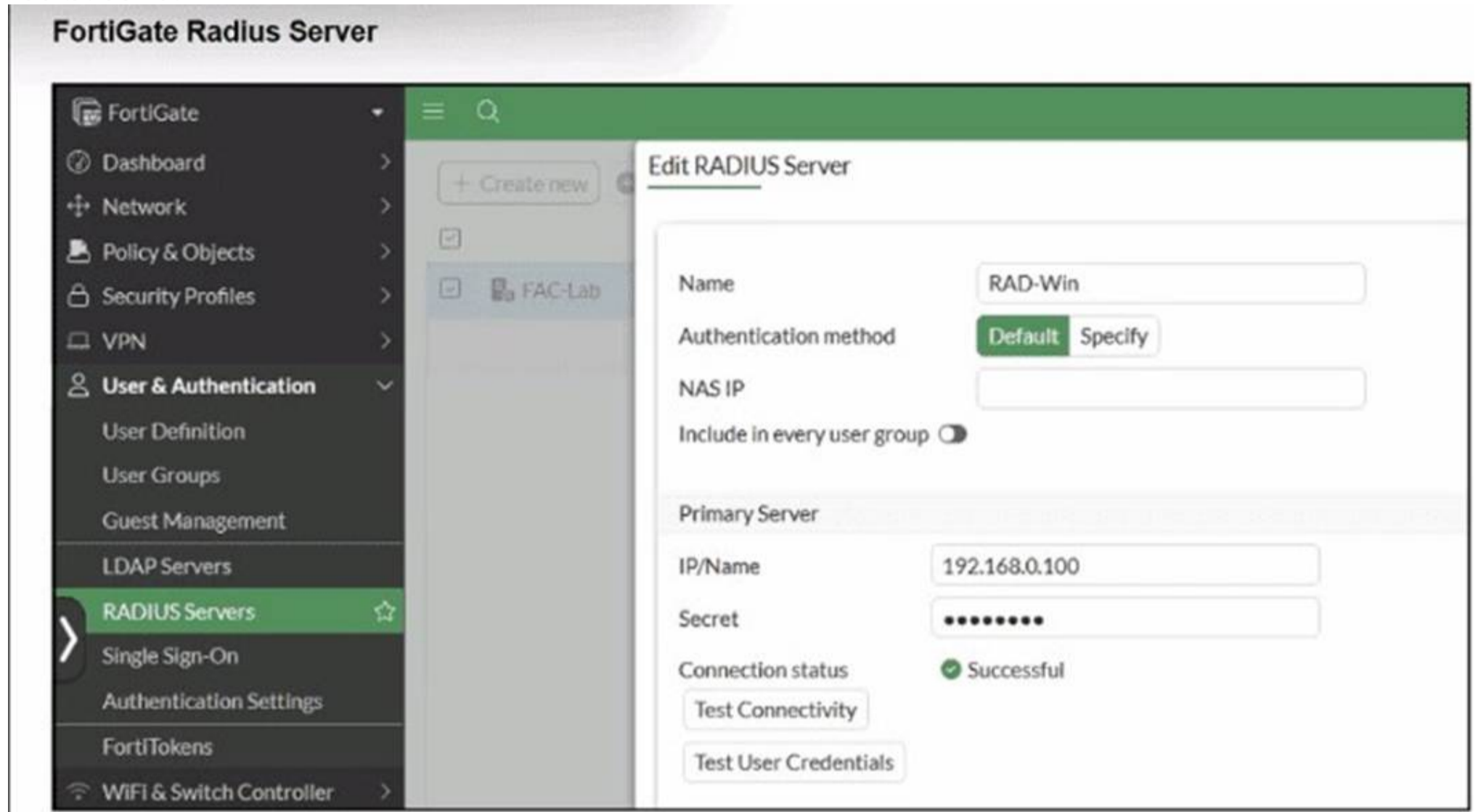
A set of SSID profiles has been configured on FortiManager, and an AP profile has been assigned to a group of AP managed by FortiGate. However, none of the designated SSIDs are being broadcast by these APs.

Which configuration change is required to make the APs broadcast these SSIDs as intended?

- A. Adjust the AP profile to ensure all SSIDs are configured in a supported mode, either bridge or tunnel, but not a mix of both.
- B. Change the AP profile to use a platform that supports the configured mix of SSIDs.
- C. Choose Manual in the SSIDs setting and select the SSIDs to broadcast.
- D. Set the Transmit Power Mode to Auto.

Answer: C

NEW QUESTION 6
 Refer to the exhibit.



FortiGate 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:

Primary server name/IP: Port:

Use Zero Trust tunnel [Please Select] v

Use secondary server

Base distinguished name:

Bind type:

Username: Password:

Server type:

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

Query Elements

User object class:

Username attribute:

Group object class:

Obtain group memberships from:

Group membership attribute:

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 7

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 8

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 9

Refer to the exhibits.

FortiAuthenticator

Interface Status

Interface: port1
 Status: 

IP Address / Netmask

IPv4: 10.0.1.150/255.255.255.0
 IPv6:

Access Rights

Admin access:


- SSH (TCP/22)
- HTTPS (TCP/443)
 - GUI (TCP/443)
 - REST API (/api/)
 - Fabric (/api/v1/fabric/)
- SNMP (UDP/161)
- HTTP (TCP/80)

Services:

- HTTPS (TCP/443)
 - Legacy Self-service Portal (/login/)
 - Captive Portals (/guests, /portal)
 - SAML IdP (/saml-idp)
 - SAML SP SSO (/saml-sp, /login/saml-auth)
 - Kerberos SSO (/login/kerb-auth)
 - SCEP (/app/cert/scep)
 - CRL Downloads (/app/cert/crl)
 - CMP (/app/cert/cmp2/)
 - FortiToken Mobile API (/api/v1/pushauthresp, /api/v1/transfertoken)
 - OAuth Service (/api/v1/oauth, /api/v1/pushpoll, /guests, /portal)
- HTTP (TCP/80)
 - SCEP (/app/cert/scep)
 - CRL Downloads (/app/cert/crl)
 - CMP (/app/cert/cmp2/)
 - SAML IdP metadata (/saml-idp)
 - Kerberos SSO (/login/kerb-auth)
- RADIUS Accounting Monitor (UDP/1646)
- RADIUS Auth (UDP/1812)
- RADIUS Accounting SSO (UDP/1813)
- RADSEC (TCP/2083)
- TACACS+ Auth (TCP/49)
- LDAP (TCP/389)

FortiAuthenticator SSO Methods

Edit Fortinet Single Sign-On Methods

Maximum concurrent user sessions: 0  Fine-grained control

- Windows event log polling (e.g. domain controllers/Exchange servers) Configure Events
- DNS lookup to get IP from workstation name
 - Directly use domain DNS suffix in lookup
 - Reverse DNS lookup to get workstation name from IP
 - Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name
 - Include account name ending with \$ (usually computer account)
- FortiNAC SSO FortiNAC sources
- RADIUS Accounting SSO clients
- Syslog SSO Syslog sources
 - Allow TLS encryption
- FortiClient SSO Mobility Agent Service
- Hierarchical FSSO tiering
- DC/TS Agent Clients

FortiAuthenticator RADIUS Accounting SS Client

Edit RADIUS Accounting SSO Client

Name:

Client name/IP:

Secret:

Description:

SSO user type:

External ⓘ

Local users ⓘ

Remote users ⓘ

Strip off prefix or suffix from username if any

Use a different attribute to search for the user in the remote LDAP server (instead of the username attribute specified in the remote LDAP server settings)

Use the prefix or suffix supplied in the username as the domain (instead of the domain specified in the remote LDAP server settings)

RADIUS Attributes

Username attribute:

Client IPv4 attribute:

Client IPv6 attribute:

User group attribute:

A company has multiple FortiGate devices deployed and wants to centralize user authentication and authorization. The administrator decides to use FortiAuthenticator to convert RADIUS 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 RADIUS 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 10

Refer to the exhibits.

Network topology



FortiSwitch status

<input type="checkbox"/>	Name ↕	Switch Group ↕	Status ↕	Model ↕
<input type="checkbox"/>	FortiLink:  fortalink ①			
<input type="checkbox"/>	 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 fortalink

```

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 10

Refer to the exhibits.

FortiGate RSSO configuration

Edit External Connector

Endpoint/Identity




RADIUS Single Sign-On Agent

Connector Settings


Name	<input type="text" value="RSSO Agent"/>
Use RADIUS Shared Secret	<input checked="" type="checkbox"/> <input type="text" value="●●●●●●●●"/>
Send RADIUS Responses	<input checked="" type="checkbox"/>


FortiGate interface configuration


Edit Interface

Name  port3

Alias

Type  Physical Interface

VRF ID 

Role 

Address


Addressing mode Manual DHCP Auto-managed by IPAM


IP/Netmask


Secondary IP address

Administrative Access

IPv4


<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
<input type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
<input type="checkbox"/> FTM	<input checked="" type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection 
<input type="checkbox"/> Speed Test		

Receive LLDP  Use VDOM Setting Enable Disable

Transmit LLDP  Use VDOM Setting Enable Disable

DHCP Server

Network

Device detection 

Security mode

Examine the FortiGate RSO configuration shown in the exhibit.

FortiGate is set up to use RSO 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 RSO user groups.

Which three critical configurations must you implement on the FortiGate device? (Choose three.)

- A. The RADIUS Attribute Value setting configured for an RSO user group should match the class RADIUS attribute value in the RADIUS accounting message.
- B. RSO 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 RSO agent configuration should be set to Class.
- E. The rso-endpoint-attribute CLI setting in the RSO agent configuration should be set to User-Name.

Answer: ADE

NEW QUESTION 15

.....

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 First Try
- * FCSS_LED_AR-7.6 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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