Prepare Smart for Success Free Fortinet FCSS_LED_AR-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 6 - LAN Edge 7.6 Architect exam PDF questions now. Get authentic FCSS_LED_AR-7.6 dumps packed with verified answers and secure your certification success with PrepBolt FCSS_LED_AR-7.6 exam pdf questions and answers.

Thank you for Downloading FCSS_LED_AR-7.6 exam PDF Demo

https://prepbolt.com/FCSS_LED_AR-7.6.html

Question 1

Question Type: MultipleChoice

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.)

Options:

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:

A, D

Explanation:

Goal: enforce captive portal authentication overHTTPSfor guests.

On FortiGate/FortiAuthenticator captive portal setups:

HTTP redirectis used so that when a guest browses to any HTTP site, their request is redirected to theportal URL.

Theportal URLitself must beHTTPSif you want a secure login page.

FortiOS captive portal and firewall authentication guidelines recommend:

EnablingHTTP redirectso unauthenticated HTTP traffic is transparently sent to the portal.

Configuring theportal URL with HTTPS, often referencing a certificate on FortiGate or FortiAuthenticator.

Therefore:

A . Enable HTTP redirect in the user authentication settings.This ensures unauthenticated HTTP requests are redirected to the (now HTTPS) portal.

D . Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator.This makes the login itself secure (TLS-protected).

Incorrect:

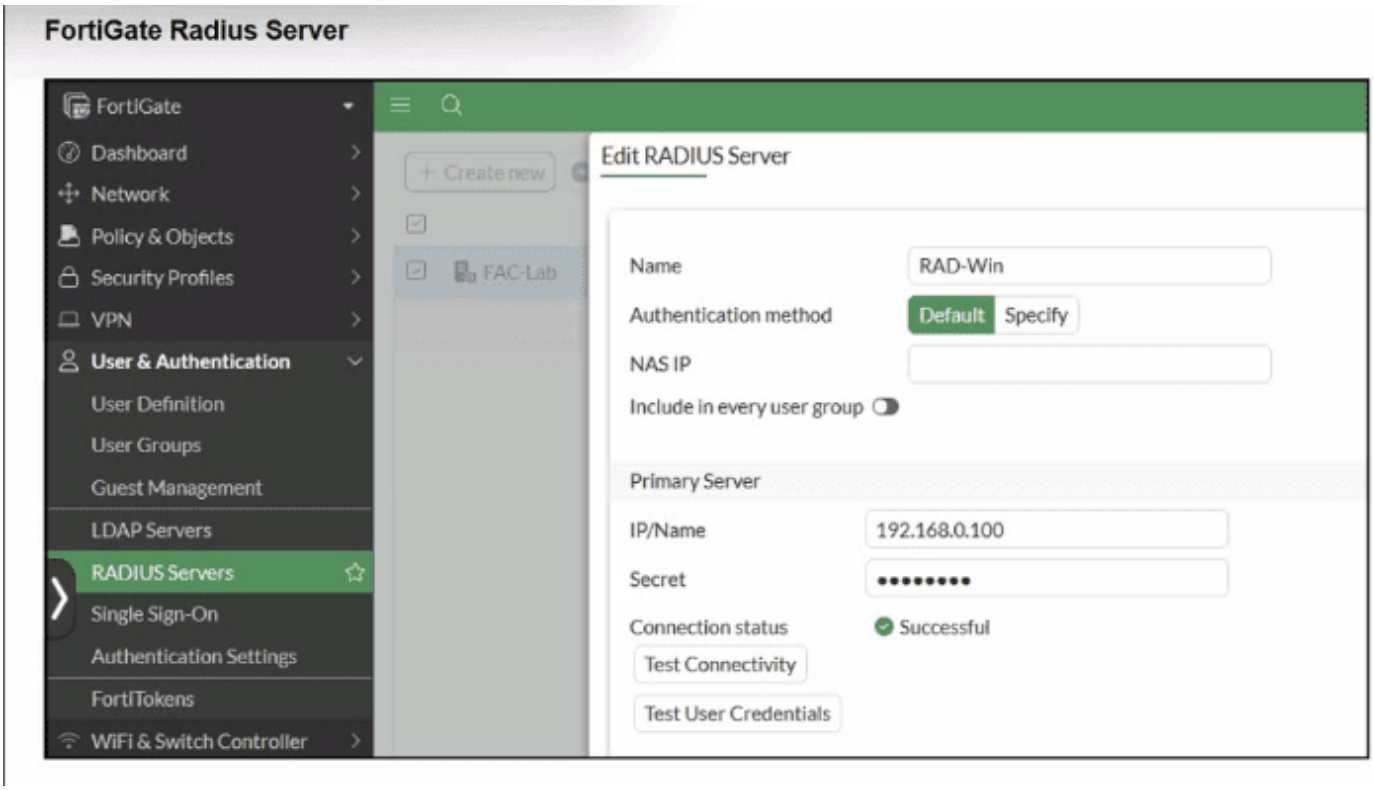
B-- You don't need a new SSID; the same SSID can use HTTPS portal.

C-- Disabling HTTP admin access on the SSID doesn't control the captive portal scheme; HTTPS enforcement is done by the portal configuration and redirect, not by admin-access flags.

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

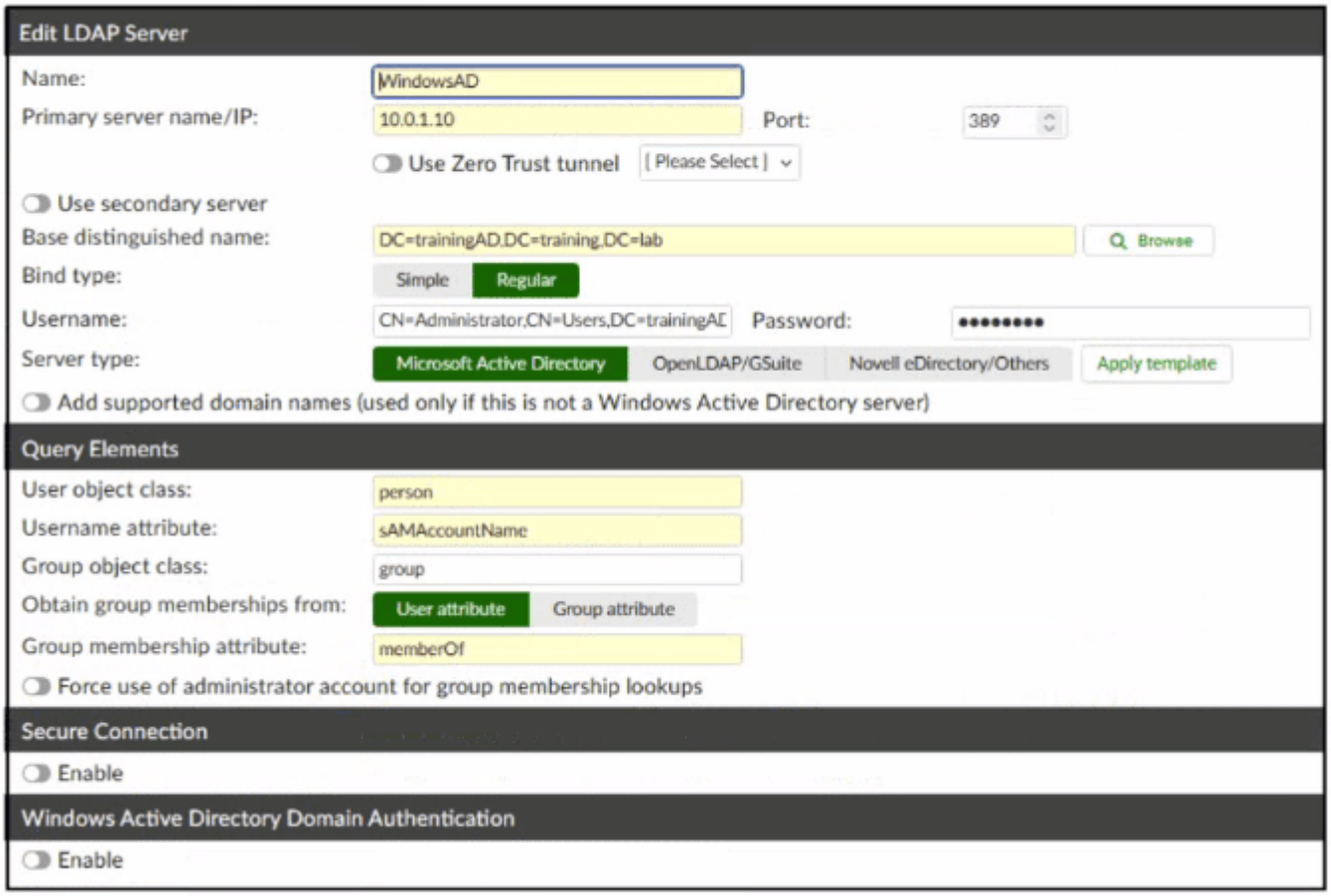


FortuiGate CLI RADIUS server test

```
FortiGate #
FortiGate # diagnose test authserver radius FAC-Lab pap wifi101 password
authenticate 'wifi101' 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 wifi101 password
authenticate 'wifi101' against 'mschap2' failed, assigned_rad_session_id=19718280638474 session_timeout=0 secs idle_timeout=0 secs!
```

FortiAuthenticator - Remote LDAP server configuration



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?

Options:

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

Explanation:

From the exhibits and text:

FortiGate RADIUS FortiAuthenticator

FortiAuthenticator LDAP Windows AD

diagnose test authserver radius ... papsucceeds

diagnose test authserver radius ... mschap2fails

This behavior matches a classic limitation documented in FortiOS:

When usingLDAPas the back-end, the RADIUS server must usePAP. CHAP/MS-CHAPv2 arenot supportedwith plain LDAP because the server cannot validate the challenge--response without access to password hashes.

In the Remote LDAP server config on FortiAuthenticator, the option''Windows Active Directory Domain Authentication'' is disabled.When this feature isenabled, FortiAuthenticator can talk to AD usingKerberos/NTLMinstead of a simple LDAP bind, whichdoes support MS-CHAPv2for incoming RADIUS authentications.

So to allow MS-CHAPv2 all the way from FortiGate to AD, you must:

Keep FortiGate using RADIUS with MS-CHAPv2 FortiAuthenticator

EnableWindows Active Directory Domain Authenticationso FortiAuthenticator can properly validate MS-CHAPv2 against AD.

Why the other options are wrong:

A . Change to CHAP-- CHAP still cannot be validated over LDAP; docs say LDAP back-ends must usePAP.

C . Manually add users to local DB-- That would allow local-DB auth but does not fix MS-CHAPv2 against AD.

D . Use RADIUS attributes on FortiGate-- Attributes do not influence the EAP inner method; they don't fix MS-CHAPv2 failures.

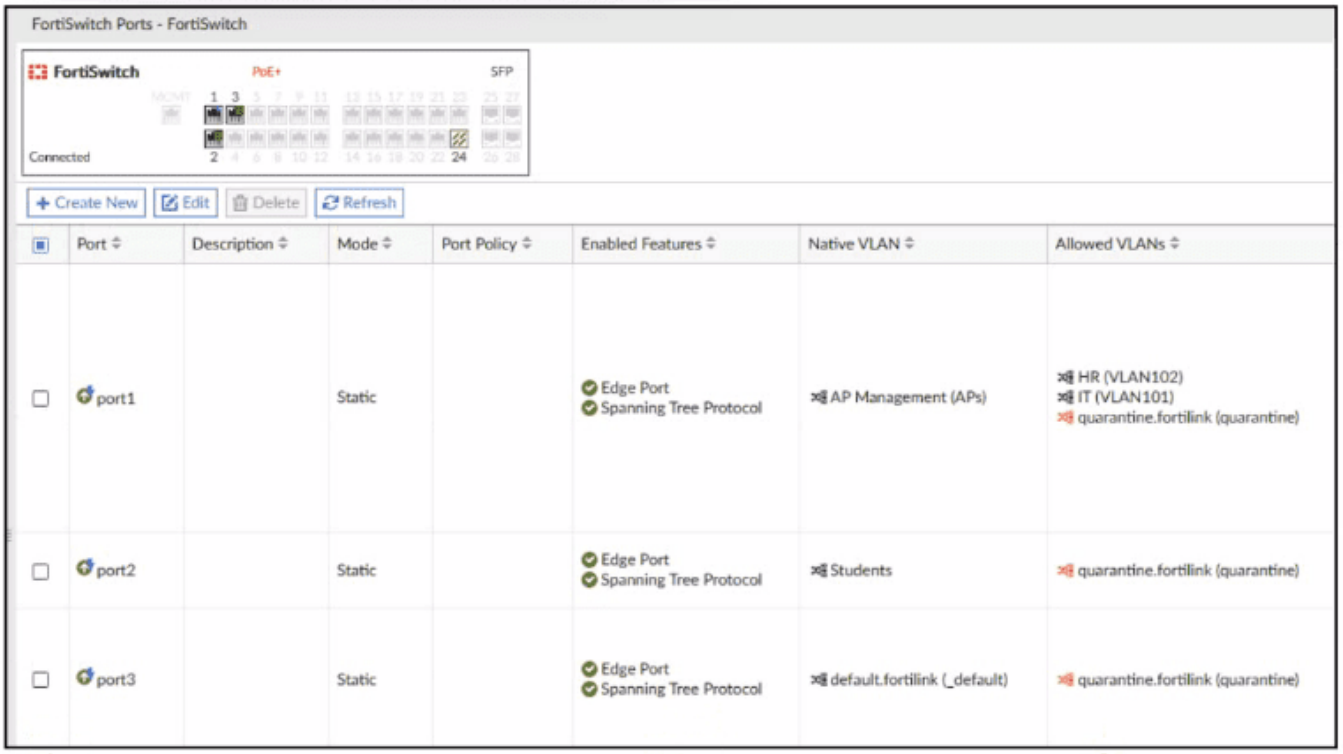
Therefore the configuration change that can realistically fix the MS-CHAPv2 problem isenabling Windows Active Directory Domain Authentication on FortiAuthenticator (B).

Question 3

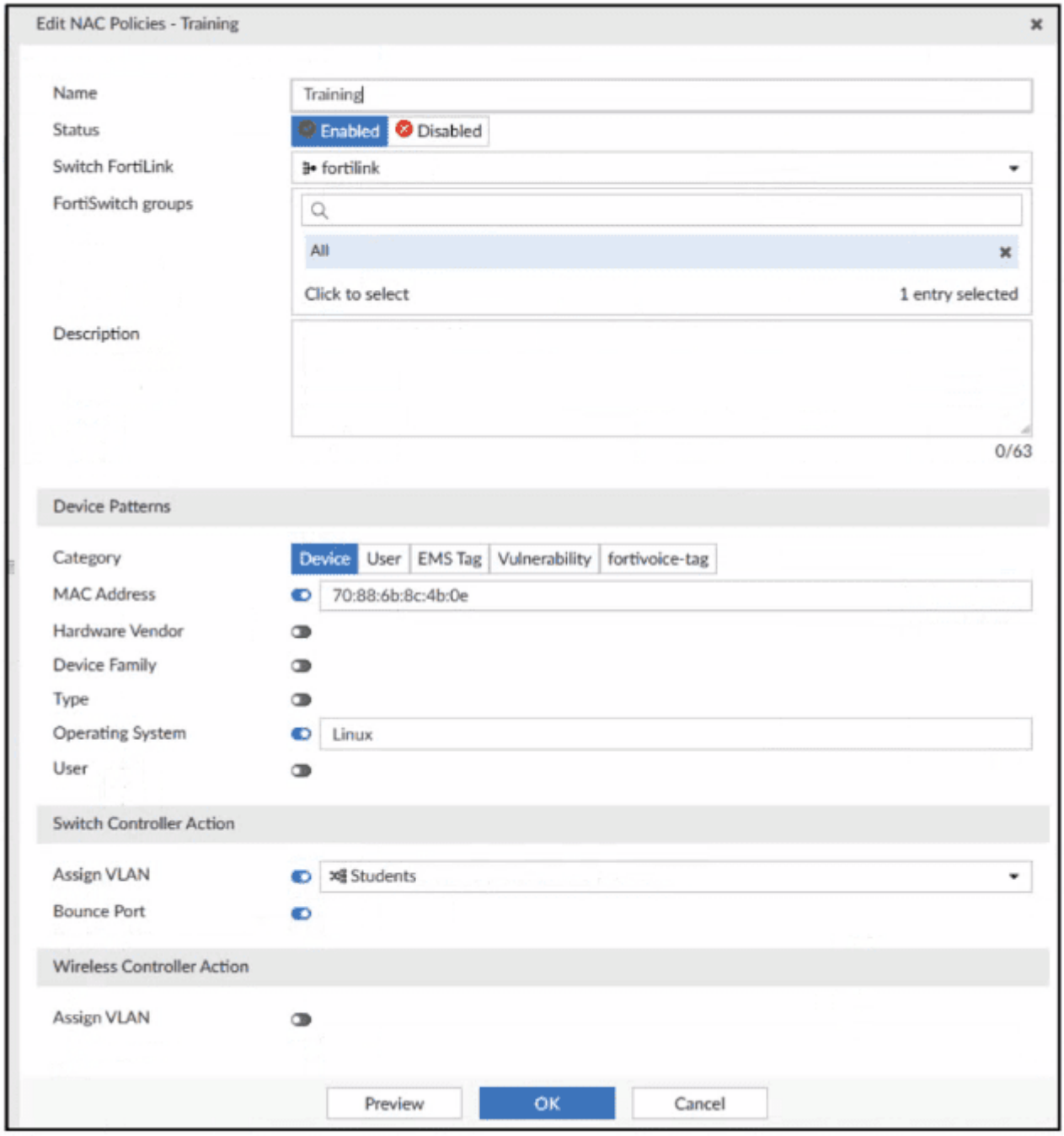
Question Type: MultipleChoice

Refer to the exhibits.

FortiSwitch Ports



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?

Options:

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

Explanation:

From the exhibits:

FortiSwitch Ports viewshows:

port2

Mode: Static

Native VLAN: Students

Allowed VLANs: quarantine.fortilink (quarantine)

NAC policy ''Training'':

Switch FortiLink: fortilink

Category:Device

Matching criteria:

MAC Address: 70:88:6b:8c:4b:0e (enabled)

Operating System:Linux(enabled)

Switch Controller Action:

Assign VLAN = Students

Bounce Port = enabled

Design intent:

Device with that MAC + OS Linux, when plugged intoport2, should be dynamically moved to VLANStudentsby the NAC policy.

Why it doesn't work now

On FortiLink NAC,dynamic NAC decisions only apply on ports whose ''Access Mode'' is set to NAC:

NAC mode = FortiGate controls theonboarding VLAN, evaluates NAC policies, and then dynamically reassigns the switch port VLAN (access, quarantine, etc.).

Static mode(what we see on port2) means the port just uses its configurednative/allowed VLANs, andno NAC classificationhappens.

Right now:

port2 is astatic access portwith Native VLAN = Students.

The NAC policy exists, butFortiSwitch is not in NAC enforcement mode on that port, so the policy is never evaluated for traffic on port2.

Therefore, themissing configurationis:

Setport2toNAC mode(sometimes called ''Access mode: NAC'' or ''NAC LAN edge port'').

Once port2 is changed to NAC mode:

Device initially lands in the onboarding/quarantine VLAN.

FortiGate collects device info (MAC, OS, etc.).

NAC policy ''Training'' matches MAC + Linux.

Switch controller actionAssign VLAN = Studentsis applied.

Port is bounced (if configured), bringing the device back up in VLAN Students.

Why the other options are wrong

B . MAC or OS misconfigured

Possible in general, but the question asks forwhich configuration is missing, and the exhibits clearly focus on port mode. Also, even with wrong MAC/OS, the port would still be in NAC mode; here NAC isn't even active.

C . Port Policy mode

Port policy (edge/trunk) is separate from NAC; NAC requires the specificNAC access mode.

D . Students VLAN should be Allowed VLANs instead of Native VLAN

For an access port, having Students as thenative VLANis correct. NAC policy's Assign VLAN will set that as access VLAN; no need to make it an allowed trunk VLAN.

Question 4

Question Type: MultipleChoice

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

Options:

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

Explanation:

In an SD-Branch deployment (FortiGate + FortiSwitch + FortiAP),FortiAIOps:

Collects telemetry and logs from Fabric devices

Usesmachine-learning / AI analyticsto:

Spot anomalies (latency, packet loss, RF issues, misconfigurations)

Highlight root causes

Proposeoptimization recommendations(e.g., channel changes, power tuning, config fixes)

It doesnot:

Automatically disable devices (Afalse)

Replace SD-WAN config or all routing (Cfalse)

Fixallissues with zero human input (Dis marketing fantasy, not reality)

Question 5

Question Type: MultipleChoice

APs have been manually configured to connect to FortiGate over an IPsec network, and FortiGate successfully detects and authorizes them. However, the APs remain unmanaged because FortiGate is unable to establish a CAPWAP tunnel with them.

What configuration change can resolve this issue and enable FortiGate to establish the CAPWAP tunnel over the IPsec connection?

Options:

A- Configure a static route on FortiGate to reach the APs over the IPsec tunnel.
B- Assign a custom AP profile for the remote APs with the set mpls-connection option enabled.
C- Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.

D- Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version.

Answer:

B

Explanation:

When FortiAPs connect to FortiGate overIPsec tunnels, this is treated similarly to WAN/MPLS deployments.

In these scenarios, FortiGate must know that CAPWAP must traverse anon-L2transport.

FortiAP profiles include:

set mpls-connection enable

This setting is required so that:

FortiGate can encapsulate CAPWAP inside the transport tunnel

Remote FortiAPs can establish CAPWAP even when behind routed/IPsec networks

Without this option, the FortiGate detects the AP butcannot bring CAPWAP UP, leaving the AP in ''discovered/unauthorized'' or ''offline'' state.

Why others are wrong

A . Static route Discovery already succeeds, so routing is not the issue.

C . Reduce MTU Sometimes useful for IPsec, but not required for CAPWAP establishment.

D . Firmware upgrade Firmware mismatch would show ''Managed (upgrade required),'' not CAPWAP tunnel failure.

Therefore,set mpls-connection enableis the required fix.

Thank You for trying FCSS_LED_AR-7.6 PDF Demo

To try our FCSS_LED_AR-7.6 practice exam software visit link below

https://prepbolt.com/FCSS_LED_AR-7.6.html

Start Your FCSS_LED_AR-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your FCSS_LED_AR-7.6 preparation with actual exam questions.