



Fortinet

Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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?

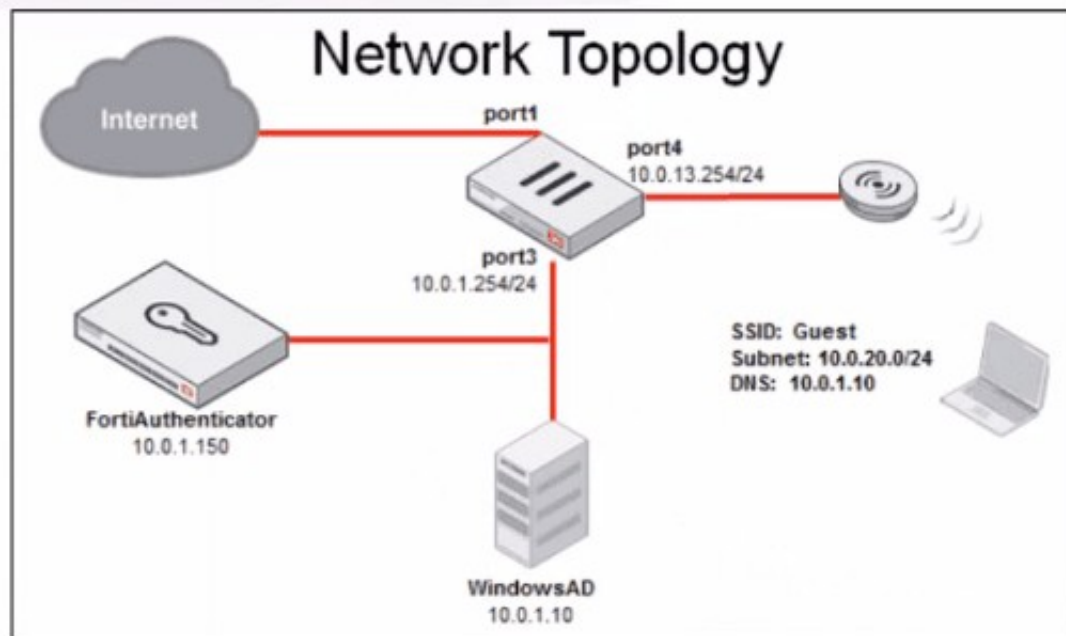
- A. The first AP 2.4 GHz interface provides a stronger signal, which clients often prioritize.
- B. The first AP 5 GHz interface because it has a stronger signal.
- C. The second AP 5 GHz interface has fewer clients, which ensures better performance despite the weaker signal.
- D. The second AP 2.4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

Answer: C

NEW QUESTION 2

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:

User groups:

Exempt sources:

Exempt destinations/services:

Redirect after Captive Portal:

Client MAC Address Filtering

RADIUS server: ☐

Address group policy:

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	✓ Enable
+ 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 3

Refer to the exhibits.

FortiGate LDAP server configuration and diagnostics

```
config user ldap
  edit "FAC-LDAP"
    set server "10.0.1.10"
    set cnid "sAMAccountName"
    set dn "DC=trainingAD,DC=training,DC=lab"
    set type regular
    set username "CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab"
    set password ENC MTAwNE2iciyoaiRa20HnjmgtQbCRYdI+OJtfO7y9+uW5V8ZxQ/Vj+mW4zPijgtCgrnAA
  next
end

FortiGate # diagnose test authserver ldap FAC-LDAP wifil01 password
authenticate 'wifil01' against 'FAC-LDAP' succeeded!
Group membership(s) - CN=Domain Users,CN=Users,DC=trainingad,DC=training,DC=lab
Domain of user is trainingad.training.lab
```

Wi-Fi Authentication

PEAP version	Automatic
Inner authentication	MSCHAPv2
Username	wifi101
Password	

An LDAP server has been successfully configured on FortiGate, which forwards LDAP authentication requests to a Windows Active Directory (AD) server. Wireless users report that they are unable to authenticate. Upon troubleshooting, you find that authentication fails when using MSCHAPv2. What is the most likely reason for this issue?

- A. A firewall policy is missing an LDAP authentication rule.
- B. The Windows AD server requires LDAPS (LDAP over SSL) for authentication.
- C. The FortiGate LDAP configuration is missing the correct Bind DN.
- D. FortiGate does not support MSCHAPv2 for LDAP authentication.

Answer: D

NEW QUESTION 4

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 5

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 6

Why is it critical to maintain NTP synchronization between FortiGate and FortiSwitch when FortiLink is configured?

- A. To facilitate synchronization of firmware updates across devices
- B. To allow FortiSwitch to communicate with other FortiSwitch devices in the network.
- C. To ensure accurate time for logs, authentication, and event correlation
- D. To allow FortiSwitch to function in standalone mode if FortiGate becomes unavailable

Answer: C

NEW QUESTION 7

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 8

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 9

Refer to the exhibits.

FortiManager configuration

Edit NAC Policies

Name*

Training

Status

Enabled

Disabled

Switch FortiLink

fortilink

FortiSwitches

Q

All

1 Entry Selected

Description

Device Patterns

Category

Device

User

EMS Tag

MAC Address

70:88:6b:8c:4a:ce

Hardware Vendor

Device Family

Type

Operating System

Linux

User

Switch Controller Action

Students

Assign VLAN

Bounce Port

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 10

.....

Relate Links

100% Pass Your FCSS_LED_AR-7.6 Exam with Exam Bible Prep Materials

https://www.exambible.com/FCSS_LED_AR-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>