

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

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

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?

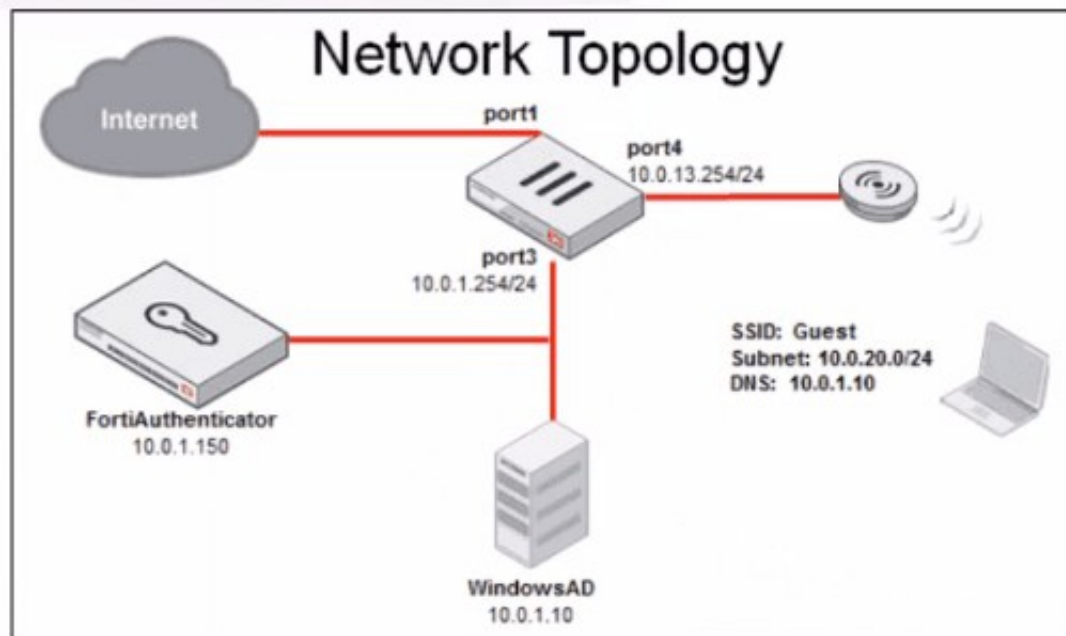
- A. The first AP 2.4 GHz interface provides a stronger signal, which clients often prioritize.
- B. The first AP 5 GHz interface because it has a stronger signal.
- C. The second AP 5 GHz interface has fewer clients, which ensures better performance despite the weaker signal.
- D. The second AP 2.4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

Answer: C

NEW QUESTION 4

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
12	guest internet access	all guest.portal	all	always	ALL	ACCEPT	Enab
	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 5

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+OJtf07y9+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 6

Refer to the exhibits.

FortiSwitch Ports

FortiSwitch Ports - FortiSwitch

FortiSwitch

1

3

5

7

9

11

13

15

17

19

21

23

25

27

2

4

6

8

10

12

14

16

18

20

22

24

26

28

Connected

24

25

26

+

Create New

✎

Edit

🗑

Delete

↻

Refresh

☐	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

Training

Status

Enabled

Disabled

Switch FortiLink

fortilink

FortiSwitch groups

All

×

Click to select

1 entry selected

Description

0/63

Device Patterns

Category

Device

User

EMS Tag

Vulnerability

fortivoice-tag

MAC Address

70:88:6b:8c:4b:0e

Hardware Vendor

Device Family

Type

Operating System

Linux

User

Switch Controller Action

Assign VLAN

Students

Bounce Port

Wireless Controller Action

Assign VLAN

Preview

OK

Cancel

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 7

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

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

- C. Debug logs > SSO Sessions page
- D. Debug logs > Single Sign-On > Syslog SSO

Answer: D

NEW QUESTION 8

A network engineer is deploying FortiGate devices using zero-touch provisioning (ZTP). The devices must automatically connect to FortiManager and receive their configurations upon first boot. However, after powering on the devices, they fail to register with FortiManager. What could be a possible cause of this issue?

- A. The FortiGate device requires manual intervention to accept the FortiManager connection.
- B. In this scenario, the ZTP process works only when devices are connected using a console cable.
- C. The FortiGate device must be preloaded with a configuration file before ZTP can function.
- D. The FortiManager IP address is not reachable over TCP port 541.

Answer: D

NEW QUESTION 9

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 10

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 13

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?

- 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

NEW QUESTION 18

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 21

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 25

You've configured the FortiLink interface, and the DHCP server is enabled by default.

```
config system dhcp server
  edit 1
    set ntp-service local
    set default-gateway 169.254.1.1
    set netmask 255.255.255.0
    set interface "fortilink"
    config ip-range
      edit 1
        set start-ip 169.254.1.2
        set end-ip 169.254.1.254
      next
    end
    set vci-match enable
    set vci-string "FortiSwitch" "FortiExtender"
  next
end
```

The resulting DHCP server settings are shown in the exhibit. What is the role of the vci-string setting in this configuration?

- A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices.
- B. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname.
- C. To connect, devices must match the VCI string; otherwise, they will not receive an IP address.
- D. To reserve IP addresses for FortiSwitch and FortiExtender devices.

Answer: C

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](#)