



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

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?

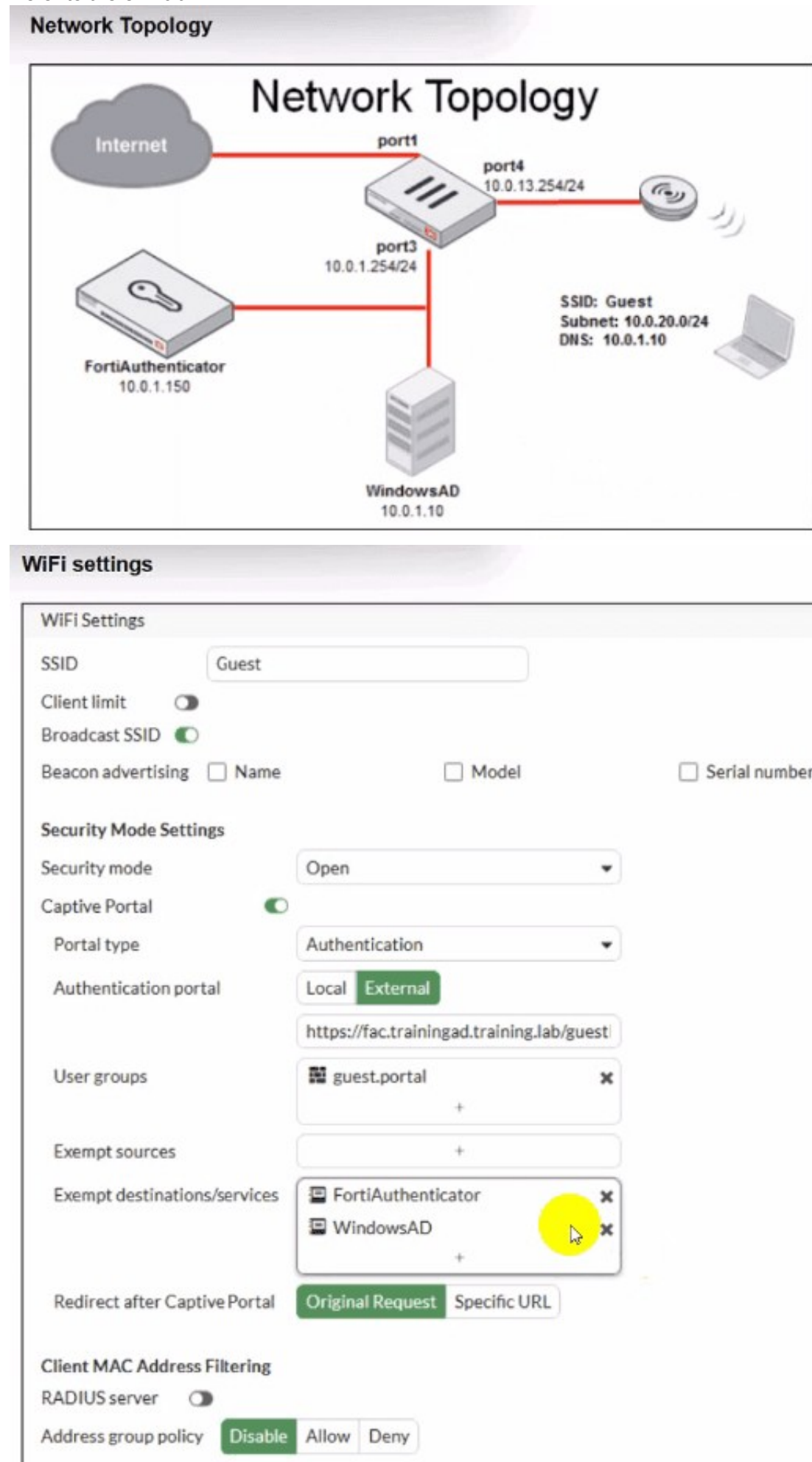
- A. The first AP 2.4 GHz interface provides a stronger signal, which clients often prioritize.

- 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.



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	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 4

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	

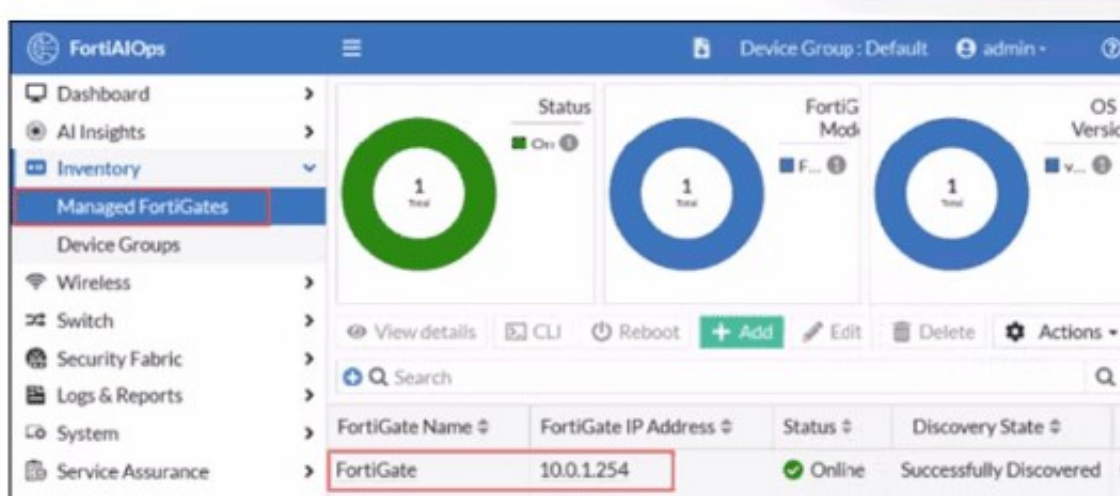
An LDAP server has been successfully configured on FortiGate, which forwards LDAP authentication requests to a Windows Active Directory (AD) server. Wireless users report that they are unable to authenticate. Upon troubleshooting, you find that authentication fails when using MSCHAPv2. What is the most 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 5

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 6

Refer to the exhibits.

FortiSwitch Ports

FortiSwitch Ports - FortiSwitch							
FortiSwitch PoE+ SFP 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							
+ 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

Refer to the exhibits.

SSID Profiles

SSIDs (4)				
☐	CompanyPrinters	Guest-01	Tunnel	WPA2 Personal
☐	Employees-Red	Student01	Local Bridge	WPA2 Enterprise
☐	Guest-CorpPort	fortinet	Tunnel	WPA2 Personal
☐	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 8
Refer to the exhibit.

FortiGate Radius Server

FortiGate

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

User Definition

User Groups

Guest Management

LDAP Servers

RADIUS Servers

Single Sign-On

Authentication Settings

FortiTokens

WiFi & Switch Controller

Create new

FAC-Lab

Edit RADIUS Server

Name

RAD-Win

Authentication method

Default Specify

NAS IP

Include in every user group

Primary Server

IP/Name

192.168.0.100

Secret

.....

Connection status

Successful

Test Connectivity

Test User Credentials

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:

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 9
Refer to the exhibits.

FortiGate VLAN AP settings

```
config system interface
    edit "APs"
        set vdom "root"
        set ip 10.10.100.254 255.255.255.0
        set allowaccess ping
        set alias "AP Management"
        set device-identification enable
        set role lan
        set snmp-index 118
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 100
    next
end
```

DHCP configuration

```
config system dhcp server
    edit 7
        set dns-service default
        set default-gateway 10.10.100.254
        set netmask 255.255.255.0
        set interface "APs"
        config ip-range
            edit 1
                set start-ip 10.10.100.1
                set end-ip 10.10.100.253
            next
        end
    next
end
```

FortiSwitch port1 VLAN AP assignment

```
config switch-controller managed-switch
  edit "FortiSwitch"
    set sn "S224EPTF19006016"
    set fsw-wan1-peer "fortilink"
    set fsw-wan1-admin enable
    set poe-detection-type 2
    set version 1
    set max-allowed-trunk-members 8
    set pre-provisioned 1
    set dynamic-capability 0x0000000000000001551027757dddfff7
  config ports
    edit "port1"
      set poe-capable 1
      set vlan "APs"
      set allowed-vlans "VLAN102" "VLAN101" "quarantine"
      set untagged-vlans "quarantine"
      set export-to "root"
      set mac-addr 04:d5:90:39:7d:8e
    next
  next
```

A FortiSwitch is successfully managed by a FortiGate. FortiAP is connected to port1 of the managed FortiSwitch. On FortiGate, the VLAN AP is configured to detect and manage FortiAP, along with a DHCP server for the VLAN AP. Additionally, the VLAN AP is assigned to port1 of FortiSwitch. However, FortiGate is unable to detect or manage FortiAP.

Which FortiGate misconfiguration is preventing the detection of FortiAP?

- A. Security Fabric is disabled in the administrative access options of the VLAN.
- B. The FortiAP firmware is incompatible with the FortiGate firmware version.
- C. The VLAN is not tagged correctly on the FortiSwitch uplink port.
- D. The CAPWAP ports (UDP 5246 and 5247) are not open on FortiGate.

Answer: A

NEW QUESTION 10

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 10

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 14

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 15

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 FortiSwitches 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 17

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 18

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 19

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 20

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 22

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

- 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

NEW QUESTION 23

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 24

.....

Relate Links

100% Pass Your FCSS_LED_AR-7.6 Exam with ExamBible 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/>