# AAA

Lab Goal:

1. Installation of CA Certificate Authority.
2. Installation and configuration of FreeRADIUS AAA server.
3. Configuration of WPA2 Enterprise Wi-Fi network.
4. Configuration of CISCO network devices to use AAA.

Lab Requirements:

1. Netgate FW appliance.
2. Debian client.
3. Internet Connection.

A blue and white logo

Description automatically generated



A red swirly circle with white background

Description automatically generated

Table of Contents

[AAA 1](#_Toc170219873)

[3](#_Toc170219874)

[FreeRADIUS 3](#_Toc170219875)

[History 3](#_Toc170219876)

[Technical Summary 3](#_Toc170219877)

[Task 1 – Configuration of CA 4](#_Toc170219878)

[Step 1: Click on System > Certificates. 4](#_Toc170219879)

[Step 2: Configure CA 4](#_Toc170219880)

[Task 2 – Configuring AAA Server certificates 6](#_Toc170219881)

[Step 1: Click on Certificates Tab 6](#_Toc170219882)

[Step 2: Configure Server Certificate 6](#_Toc170219883)

[Task 3 – Install Free Radius AAA server 7](#_Toc170219884)

[Step 1: Open System > Packet Manager 7](#_Toc170219885)

[Step 2: Select Available Packages Tab. 8](#_Toc170219886)

[Step 2: Create Wireless User Account in FreeRADIUS. 9](#_Toc170219887)

[Step 3: Create device account for Wi-Fi Access Point 9](#_Toc170219888)

[Task 4 – Create an interface. 10](#_Toc170219889)

[Step 1:  Create Authentication interface. 10](#_Toc170219890)

[Task 5 – Configure your Access Point 12](#_Toc170219891)

[Step 1:  Connect your AP. 12](#_Toc170219892)

[Step 2 -Switch mode to AP 12](#_Toc170219893)

[Step3: Changing Network Mode 13](#_Toc170219894)

[Step 4: Create SSID – name of Wi-Fi network 14](#_Toc170219895)

[Step 5: Disable DHCP as we are running one on Netgate. 14](#_Toc170219896)

[Step 6: Configure Wireless Security 14](#_Toc170219897)

[Task 6 – Connect to new Wi-Fi network 15](#_Toc170219898)

[Task 7 – Configure FreeRADIUS for Cisco devices. 15](#_Toc170219899)

[Step 1:   Create AAA Cisco Admin account. 15](#_Toc170219900)

[Step 2:  Create Device Account for SW1 and SW2 16](#_Toc170219901)

[Task 8 – Configure SW1 and SW2 to use AAA on FreeRADIUS. 17](#_Toc170219902)

[Step 1:  SW1 AAA configuration 17](#_Toc170219903)

[Step 2:  Configure VTY Lines 17](#_Toc170219904)

[Step 3:  Connect to SW1 using Debian client. 18](#_Toc170219905)

[Step 4:  Configure SW2. 19](#_Toc170219906)

[Step 2:  Configure VTY Lines 19](#_Toc170219907)

[Step 3:  Connect to SW2 using Debian client. 19](#_Toc170219908)

[Lab Challenge. 20](#_Toc170219909)

[References 20](#_Toc170219910)

## FreeRADIUS

## FreeRADIUS

FreeRADIUS is an open-source Remote Authentication Dial-In User Service (RADIUS) server widely used for network authentication, authorization, and accounting. Here’s a brief technical summary along with a bit of its history:

### History

* **Origins**: FreeRADIUS was initially developed in 1999 as a fork of the Cistron RADIUS server by Alan DeKok and Miquel van Smoorenburg. The goal was to create a more robust and extensible RADIUS server.
* **Development**: Over the years, FreeRADIUS has become the most popular and widely deployed RADIUS server, used by millions of users and organizations globally.
* **Community and Support**: FreeRADIUS is maintained by a community of developers and is supported by the FreeRADIUS Foundation.

### Technical Summary

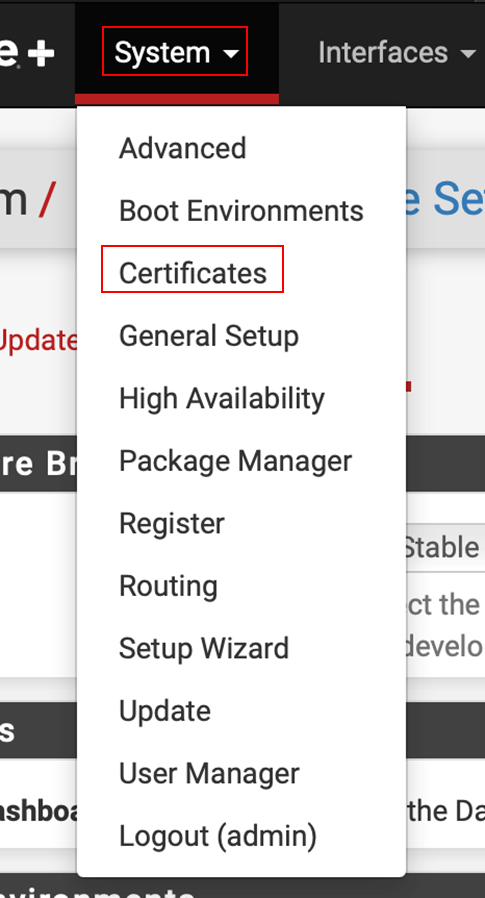
* **Authentication Protocols**: FreeRADIUS supports a wide range of authentication protocols, including PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP (TLS, TTLS, PEAP, LEAP, etc.), and others, making it suitable for various applications.
* **Authorization**: It can be integrated with various backends for authorization, such as SQL databases (MySQL, PostgreSQL, SQLite), LDAP directories, and even flat files.
* **Accounting**: FreeRADIUS provides comprehensive accounting features, logging all aspects of user sessions, which is crucial for auditing and billing purposes.
* **Extensibility**: The server is highly modular, allowing for customization and extension through modules. Modules can handle authentication, authorization, and accounting functions, or integrate with external systems.
* **Performance**: Known for its high performance, FreeRADIUS can handle thousands of authentication requests per second, making it suitable for large-scale deployments.
* **Compatibility**: FreeRADIUS works with a variety of network devices (routers, switches, access points) from numerous vendors, ensuring broad compatibility.
* **Security**: It supports advanced security features, including IPsec, TLS encryption, and the use of certificates for mutual authentication.
* **Configuration**: The configuration is managed through text-based files, providing flexibility and ease of automation. Policies and rules can be finely tuned to meet specific network requirements.
* **Community and Documentation**: A large user base and comprehensive documentation provide a wealth of resources for troubleshooting and extending functionality.

FreeRADIUS remains a critical component for organizations requiring secure, scalable, and reliable network authentication solutions, continuing to evolve with the needs of modern networking environments.

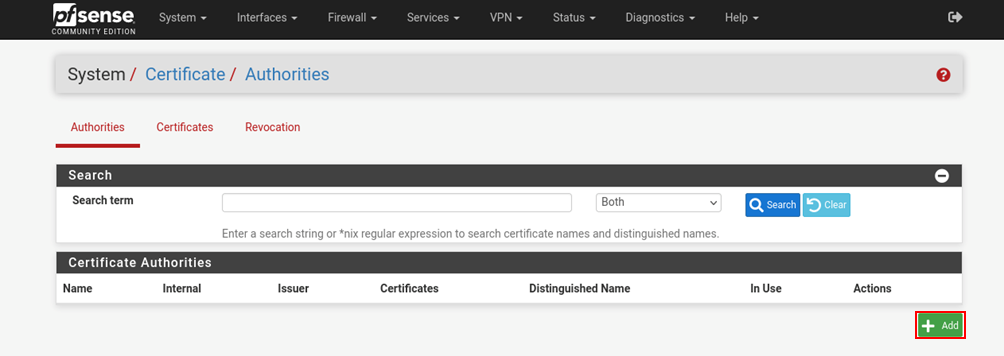
## Task 1 – Configuration of CA

In this task we will be configuring Certificate authority, and we will generate new Certificates we will use for our Wi-Fi WPA2 enterprise network.

### Step 1: Click on System > Certificates.



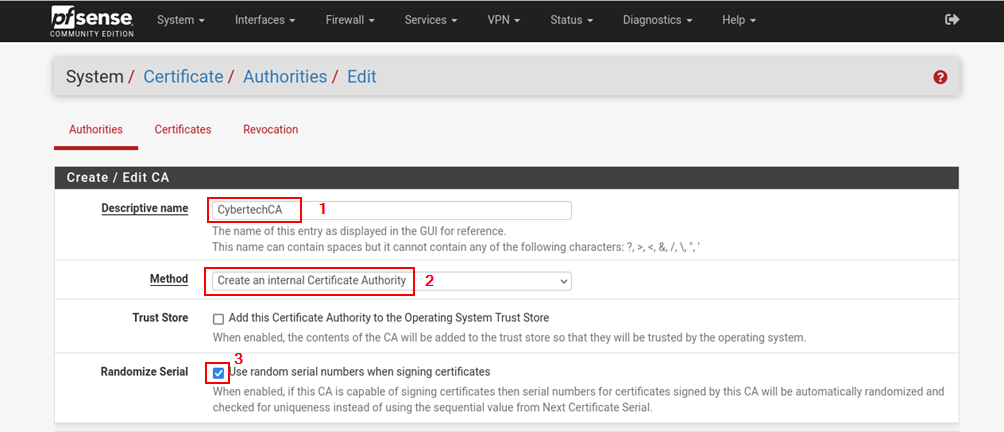
Click on **Add**



### Step 2: Configure CA

Configure CA as per specification:

* 1. Descriptive Name: **CybertechCA**
  2. Method: **Create an internal Certificate Authority**
  3. Randomize Serial: **Checked**



* 1. Country Code**: AU**
  2. State or Province**: Tasmania**
  3. City**: Hobart**
  4. Organization: **Cybertech**
  5. Organizational Unit: **SOC**
  6. Click on save.

A screenshot of a computer

Description automatically generated

Expected screenshot:

A screenshot of a computer

Description automatically generated

## Task 2 – Configuring AAA Server certificates

Open Server Certificate Tab

### Step 1: Click on Certificates Tab

A red text on a white background

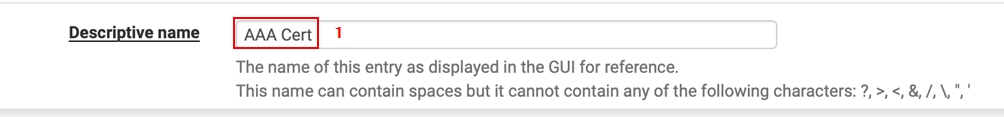
Description automatically generated

### Step 2: Configure Server Certificate

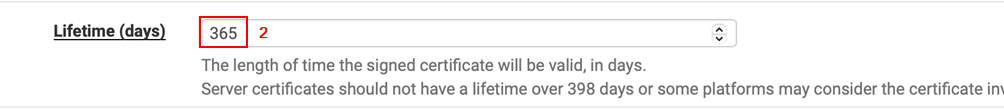
Click on add/sign at bottom of page.

Configure Server Certificate as per specification:

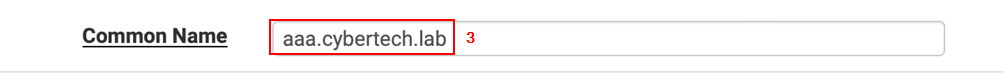
1. Descriptive Name: **AAA Cert**



1. Lifetime: **365**



1. Common Name: **aaa.cybertech.lab**



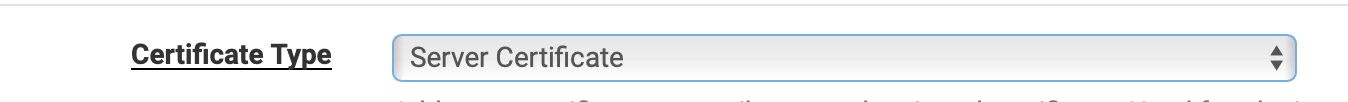
1. Certificate Type: **Server Certificate**

Change to Server Certificate from drop down list.

A screenshot of a computer

Description automatically generated

Screenshot of selection



1. Save.

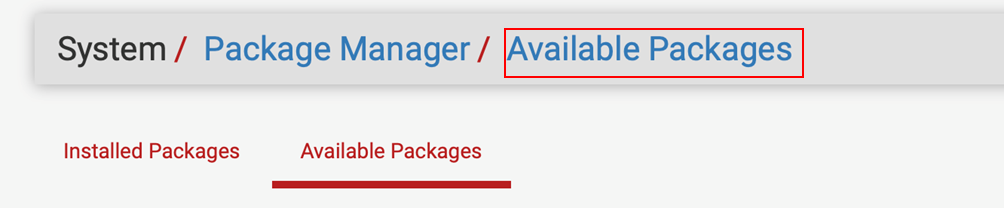
## Task 3 – Install Free Radius AAA server

### Step 1: Open System > Packet Manager

A screen shot of a computer

Description automatically generated

### Step 2: Select Available Packages Tab.



Search for radius (a) and click search button (b).

A screenshot of a computer

Description automatically generated

Add FreeRADIUS (a) by clicking on install button (b) on right.

A screenshot of a computer

Description automatically generated

Confirm

A screen shot of a computer

Description automatically generated

Expected screenshot:

A screenshot of a computer

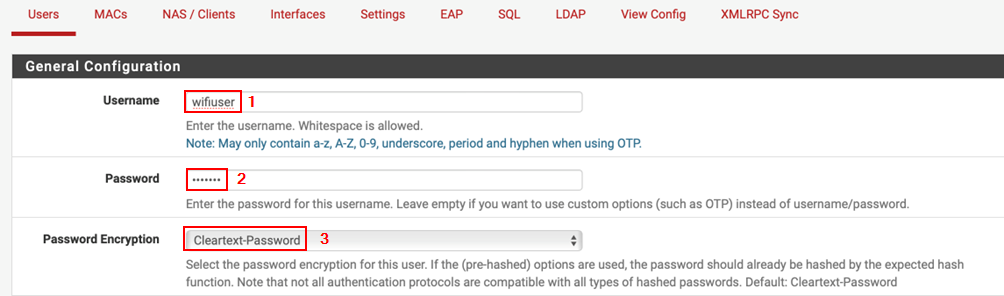
Description automatically generated

### Step 2: Create Wireless User Account in FreeRADIUS.

Click on Service > FreeRADIUS

Create a User by clicking on add.

1. Username: **wifiuser**
2. Password: **wifipass**
3. Password Encryption: **Cleartext-Password**



Note: As this is lab environment we will use clear text password, however we have learned that it is not best practice.

Research what is needed for non-clear text pass to be integrated.

1. Save

Expected screenshot:

A screenshot of a computer

Description automatically generated

### Step 3: Create device account for Wi-Fi Access Point

Click on NAS/Clients and click on Add button.

A screenshot of a computer

Description automatically generated

**Change IP accordingly to your group. If IP is used advise, please.**

1. Client IP Address: **10.1.1.254**
2. Client Version: **IPv4**
3. Client Shortname: **wifi\_ap**
4. Client Shared Secret: **aaasapsecret**
5. Save

A screenshot of a computer

Description automatically generated

Expected screenshot:

A screenshot of a computer

Description automatically generated

## Task 4 – Create an interface.

### Step 1:  Create Authentication interface.

This interface will be used by FreeRADIUS to listen for incoming Authentication requests.

Click on Add.

A screenshot of a computer

Description automatically generated

1. Interface IP Address: **\***
2. Port: **1812**
3. Interface Type: **Authentication**
4. IP Version: **IPv4**
5. Description: **Auth Interface**
6. Save

A screenshot of a computer

Description automatically generated

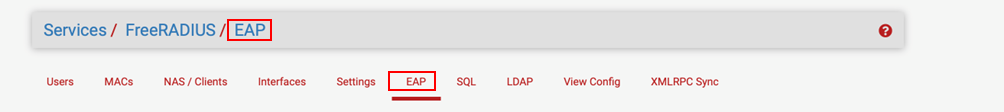
Expected screenshot:

A screenshot of a computer

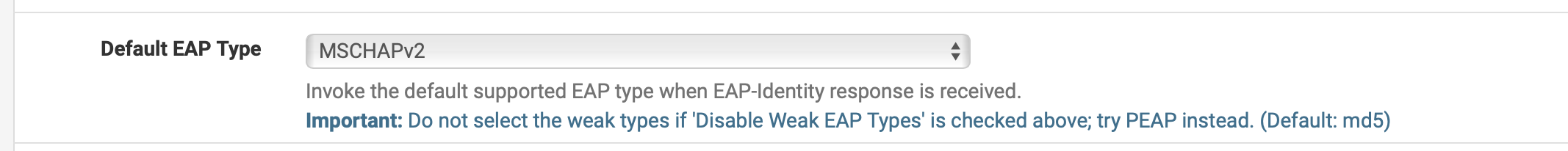
Description automatically generated

 Step 2:  Configure EAP.

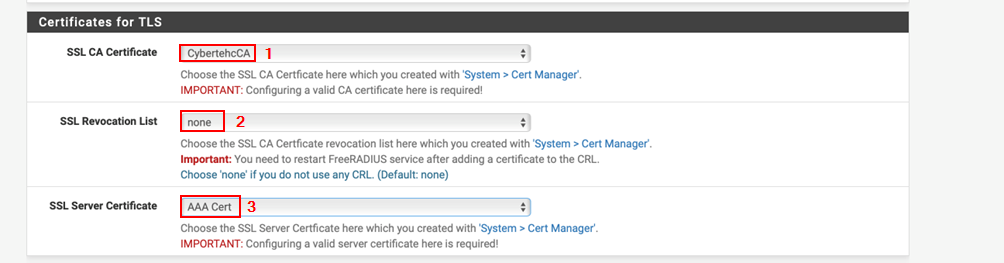
Select EAP Tab.



Default EAP Type: **MSHAPv2**



1. SSL CA Certificate: **CybertechCA**
2. SSL Revocation List: **none**
3. SSL Server Certificate: **AAA Cert**
4. Save.



**Note: You will not see new page.**

## Task 5 – Configure your Access Point

### Step 1:  Connect your AP.

1. Power up AP at your desk.
2. Start Debian VM
3. Configure Debian Network Adapter in VMware to be bridged.
4. Configure Ethernet Adapter to DHCP.
5. Connect PC Ethernet cable to LAN port of AP
6. Access web interface (find out your IP and what is DHCP address and access it as Web interface will be on same host)
7. Enter default credentials for model. You will need to research a bit

### Step 2 -Switch mode to AP

1. Select Operation mode
2. Select Access Point
3. Save

A screenshot of a computer

Description automatically generated

A close up of a sign

Description automatically generated

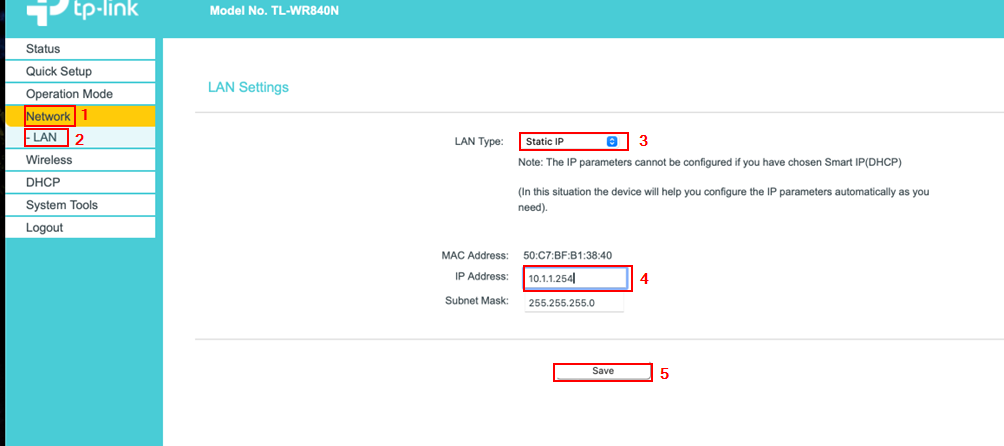
AP will reboot

.A screen shot of a computer error

Description automatically generated

### Step3: Changing Network Mode

1. Click on Network
2. LAN
3. Change to static IP
4. Assign correct IP based on your Group.
5. Save



AP will reboot.

A screenshot of a computer

Description automatically generated

### Step 4: Create SSID – name of Wi-Fi network

1. Under Wireless Tab
2. Wireless: **Enable**
3. Wireless Network Name: **GROUP1**

Name is example use your group name.

1. Save

A screenshot of a computer

Description automatically generated

### Step 5: Disable DHCP as we are running one on Netgate.

1. Under DHCP Tab
2. DHCP Server: **Disable**

A screenshot of a computer

Description automatically generated

### Step 6: Configure Wireless Security

Go to Wireless security and configure WPA2 Enterprise

Select

A close-up of a number

Description automatically generated

A close up of a logo

Description automatically generated pfsense ip

A black text on a white background

Description automatically generated **aaasapsecret**

**Save settings.**

## Task 6 – Connect to new Wi-Fi network

Use TasTAFE laptops to connect.

Note: There will be a warning with CA as it is self-signed.

## Task 7 – Configure FreeRADIUS for Cisco devices.

### Step 1:   Create AAA Cisco Admin account.

In this step we need to create CISCO AAA Admin account.

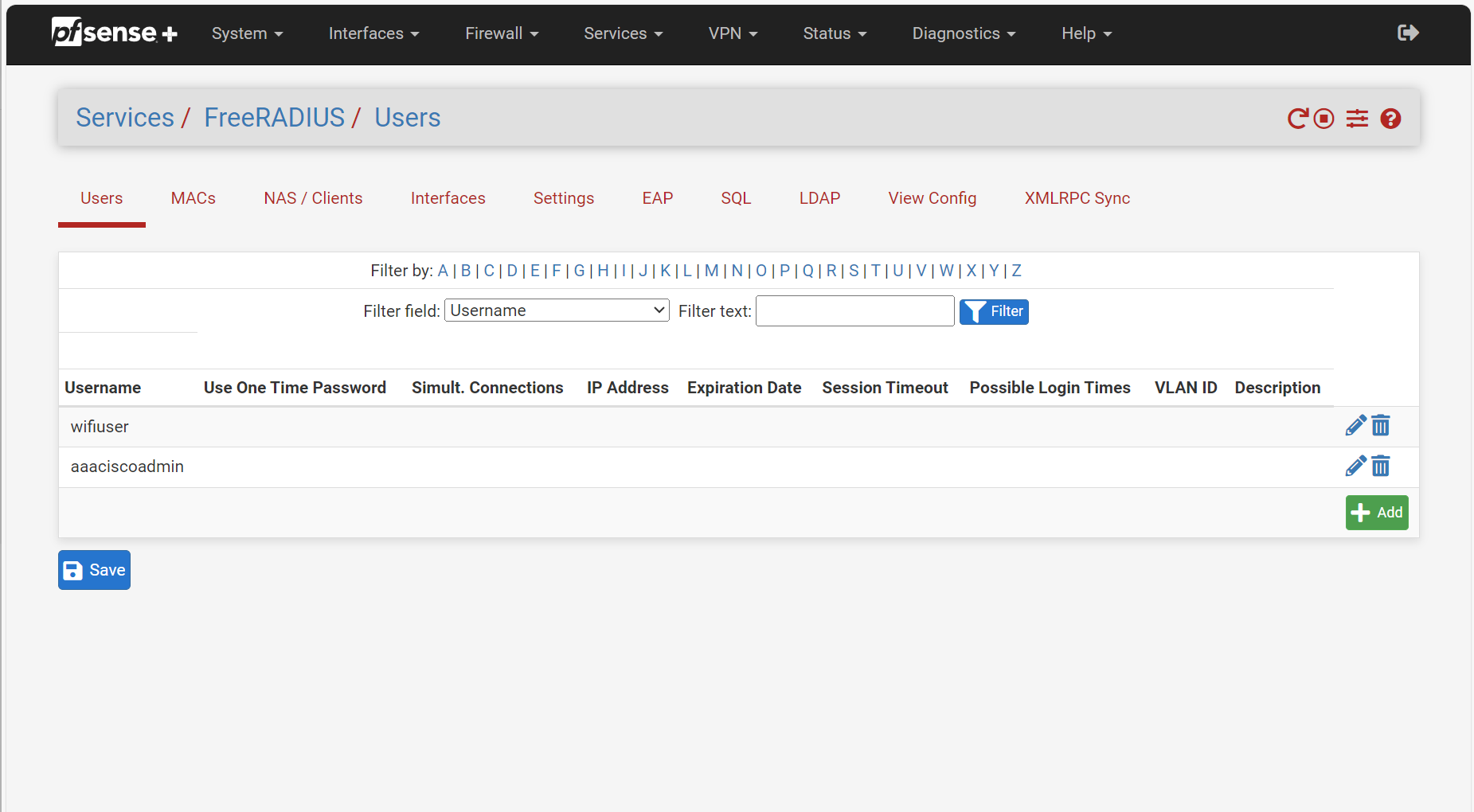
To achieve this, you can follow same steps as described in previous [Task](#_Step_2:_Create).

1. Username: **aaaciscoadmin**
2. Password: **aaaciscopass**
3. Password Encryption**: Cleartext-Password**
4. Save

A screenshot of a computer

Description automatically generated

Expected screenshot.



### Step 2:  Create Device Account for SW1 and SW2

In this step we need to create device account same way we did in previous Task for Wi-Fi AP.

[Link](#_Step_3:_Create)

**Example for G2SW1**

**Change IP accordingly to your group.** Client IP Address: **10.1.2.11**

1. Client Version: **IPv4**
2. Client Shortname: **G2SW1**
3. Client Shared Secret: **aaasw1secret**
4. Save

A screenshot of a computer

Description automatically generated

**Example for GSW2**

**Change IP accordingly to your group.**

1. Client IP Address: **10.1.2.12**
2. Client Version: **IPv4**
3. Client Shortname: **G2SW2**
4. Client Shared Secret: **aaasw2secret**
5. Save

A screenshot of a computer

Description automatically generated

### Task 8 – Configure SW1 and SW2 to use AAA on FreeRADIUS.

### Step 1:  SW1 AAA configuration

**NOTE: This is example use appropriate names and IPv4 addresses**

1. Enable AAA

G2SW1(config)#aaa new-model

1. Crete default login

G2SW1(config)#aaa authentication login default group radius local

1. Configure AAA Server connection

G2SW1(config)#radius server pfsense

G2SW1(config-radius-server)#address ipv4 10.1.2.1 auth-port 1812

G2SW1(config-radius-server)#key aaassw1secret

G2SW1(config-radius-server)#exit

G2SW1(config)#

1. Test connectivity using new AAA user.

SSH to SW1

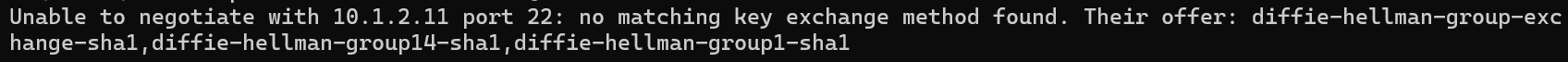
### Step 2:  Configure VTY Lines

G2SW1(config)#line vty 0 15

G2SW1(config-line)#login authentication default

### Step 3:  Connect to SW1 using Debian client.

NOTE: If you get error



You will need to edit ssh client to accept outdated cyphers offered by CISCO

1. Open ssh client configuration file.

sudo nano /etc/ssh/ssh\_config

1. Locate the line ‘ **# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc’** and remove the **Hash/Pound** sight from the beginning.
2. Locate the line **‘# MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160**′ and remove the **Hash/Pound #** sight from the beginning,
3. Then paste the following on the end;"

HostkeyAlgorithms ssh-dss,ssh-rsa

KexAlgorithms +diffie-hellman-group1-sha1,diffie-hellman-group14-sha1

A screenshot of a computer

Description automatically generated

### Step 4:  Configure SW2.

1. Enable AAA

G2SW2(config)#aaa new-model

1. Crete default login

G2SW2(config)#aaa authentication login default group radius local

1. Configure AAA Server connection

G2SW2(config)#radius server pfsense

G2SW2(config-radius-server)#address ipv4 10.1.2.1 auth-port 1812

G2SW2(config-radius-server)#key aaassw1secret

G2SW2(config-radius-server)#exit

G2SW2(config)#

1. Test connectivity using new AAA user.

SSH to SW2

### Step 2:  Configure VTY Lines

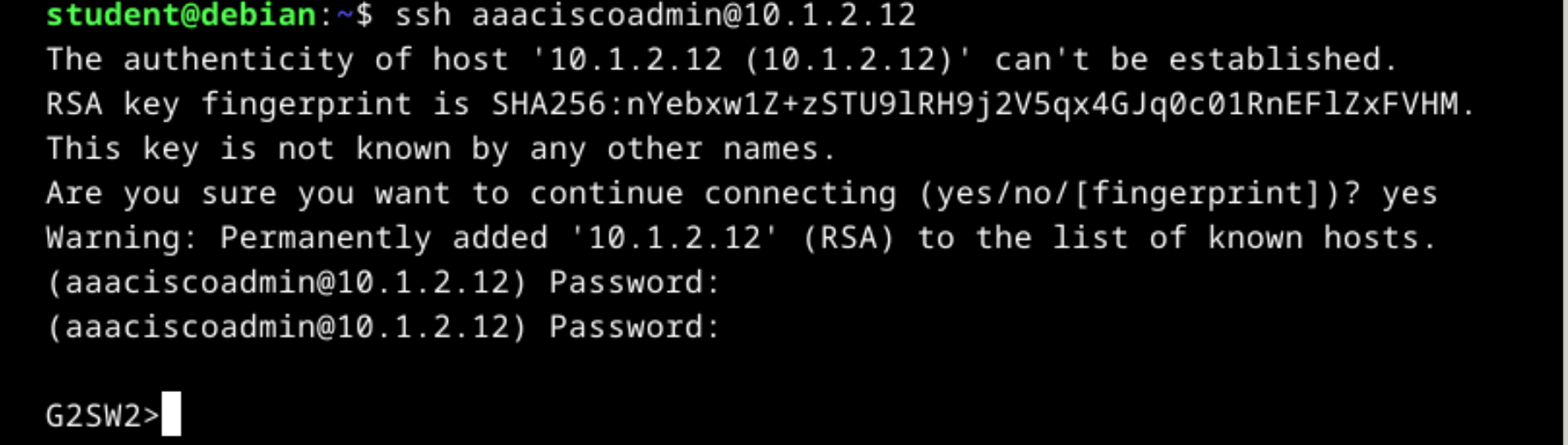
G2SW1(config)#line vty 0 15

G2SW1(config-line)#login authentication default

### Step 3:  Connect to SW2 using Debian client.

NOTE: If you get error refer to previous [Step](#_Step_3:_) how to solve it.

Expected screenshot:



### Lab Challenge.

As this Lab is challenging enough there will not be challenges this time.

### References

Official NetGate Documentation.

[RADIUS Authentication Servers | pfSense Documentation (netgate.com)](https://docs.netgate.com/pfsense/en/latest/usermanager/radius.html)

Official CISCO documentation