Seattle-ops-301d10: Lab 08

Zachariah Woodbridge Dec 6, 2023

# 

# **Lab: RADIUS Authentication**

## **Overview**

RADIUS (Remote Authentication Dial-In User Service ) is a network management protocol facilitating AAA (Authentication, Authorization, and Accounting) management for network users. In this type of configuration, the NAS (Network Access Server) brokers authentication requests and acts as the network’s gatekeeper.

## **Scenario**

GlobeX’s MSSP, Secutronix, informed you this morning that a network intrusion was detected. “You’ve got someone poking around your network!” the Secutronix rep, Sarah, explained. “Traffic logs indicate this was a wired connection. Somebody got onsite and used a wallport. We’ll have to perform a deeper investigation. Until then, as a precaution, I recommend deploying additional network security systems. Have you tried TACACS+ or RADIUS? You might be able to implement wired network authentication that way.”

## **Prerequisites**

* ~~A pfSense VM in VirtualBox, free from configuration settings from previous labs~~
* ~~A user endpoint VM in VirtualBox (any existing Windows 10 or Linux VM)~~

## **Objectives**

* Enable a Captive Portal on pfSense
* Create a local user and group on pfSense which can login through the Captive Portal
* Install the FreeRADIUS package on pfSense
* Configure FreeRADIUS and connect it to a local Authentication Server
* Reconfigure the Captive Portal to authenticate using FreeRADIUS
* Provide detailed documentation of your configuration

## **Resources**

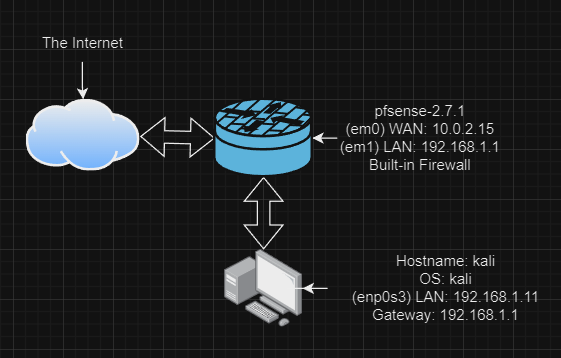
* [Video - Advanced Captive Portal on pfSense](https://www.netgate.com/resources/videos-advanced-captive-portal-on-pfsense)
* [Video - How to configure captive portal and freeRadius on pfsense 2.4.2 server](https://www.youtube.com/watch?v=qCTsyW65WbA)
* [Netgate - RADIUS Authentication Servers](https://docs.netgate.com/pfsense/en/latest/usermanager/radius.html#authservers-radius-config)
* [How to Set Up a Radius Server on pfSense](https://turbofuture.com/internet/How-to-Set-Up-a-Radius-Server-on-pfSense-Using-the-FreeRadius-Package)

## **Tasks**

Be sure to carefully document all configuration settings and passwords used in this lab.

### **Part 1: Topology 1/2**

* ~~Read through the entire lab and use Draw.io to create an appropriate topology of the network you expect to construct. Include as many details as you can such as computer names, OS types, IP addresses, etc. Include a screenshot of this initial topology.~~

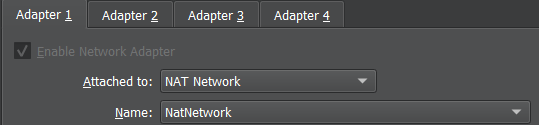


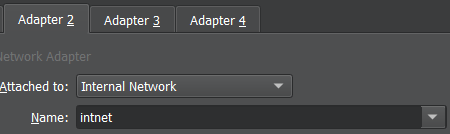
### **Part 2: Staging**

Submit detailed documentation regarding all of the configurations in this section.

* ~~First you will need a fresh pfSense VM, free from configuration settings from previous labs. You can reset an existing instance to factory settings (Diagnostics / Factory Defaults), revert to a baseline snapshot, import a fresh instance from a baseline OVA backup, or install pfSense on a new VM. However you achieve this, it is important to start from a clean baseline to avoid complications.  
  On the pfSense VM, configure the WAN network adapter to NAT Network and the LAN adapter to Internal Network.~~

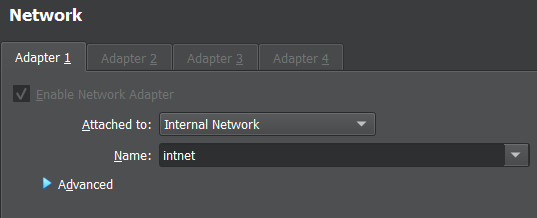
**As you can see, my pfsense is setup as per your instructions:**





* ~~Second you will need a user endpoint VM with a GUI (Windows 10 or Kali) for configuring pfSense and testing the Captive Portal.  
  On the user endpoint VM, configure the network adapter to match the LAN adapter of pfSense (should be set to the same Internal Network).~~

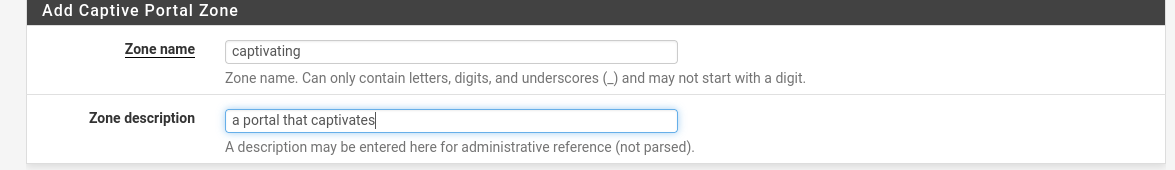
**This is my Kali VM:**



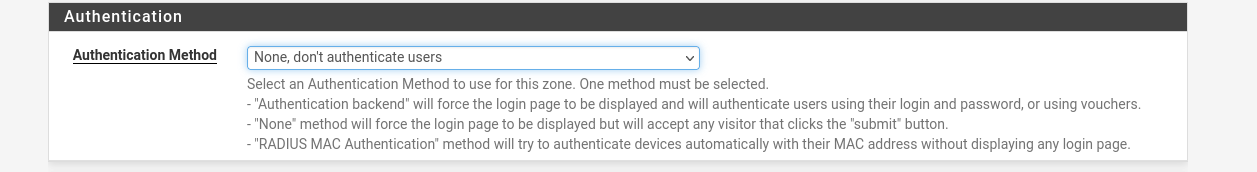
### **Part 3a: Captive Portal**

Submit detailed documentation regarding all of the configurations in this section.

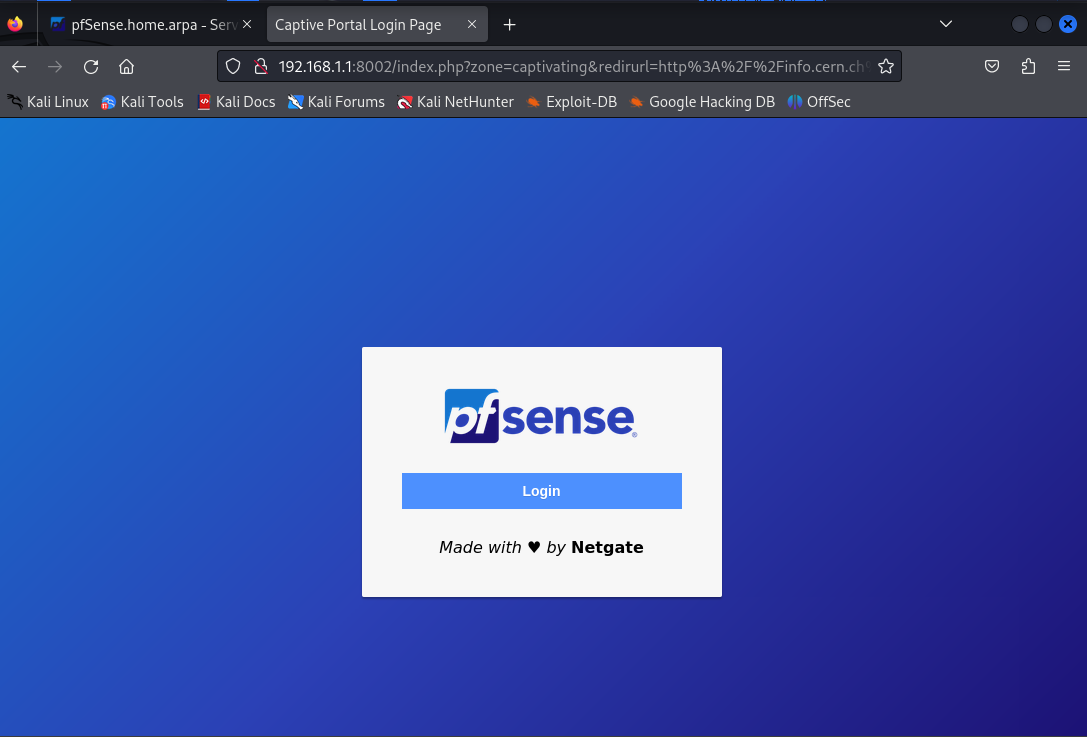
* ~~In Services > Captive Portal, add a new captive portal zone~~



* ~~Enable the captive portal and configure it as follows:~~
  + ~~Interfaces: LAN~~
  + ~~Authentication Method: None~~

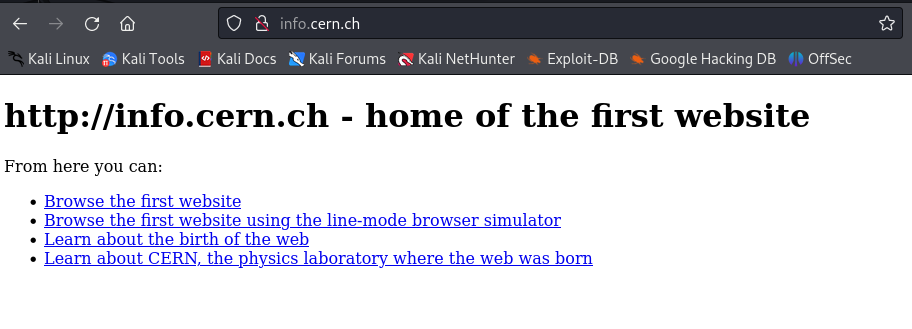


* ~~On the same VM that you are using to access the pfSense GUI, use your browser to navigate to~~ **~~http://info.cern.ch~~** ~~and observe what happens~~*~~Please note that we have not enabled https for the captive portal, so it will work best with http addresses~~*

**

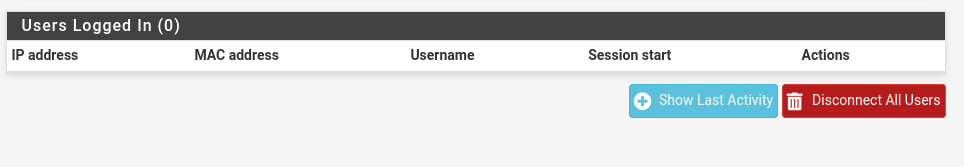
* ~~Attempt to login to the portal~~

**It allows login without authentication as per our setup.**



* ~~Navigate to Status / Captive Portal and disconnect the host~~

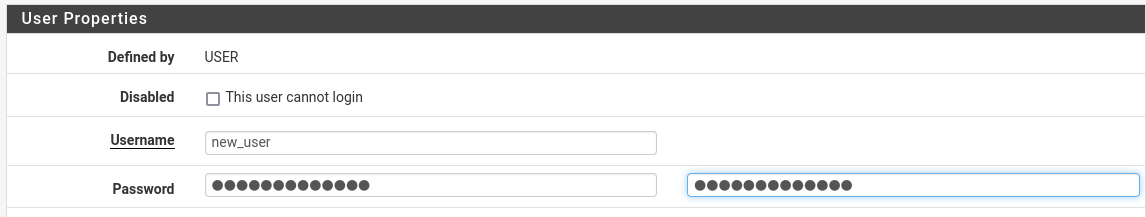
**Disconnected!**



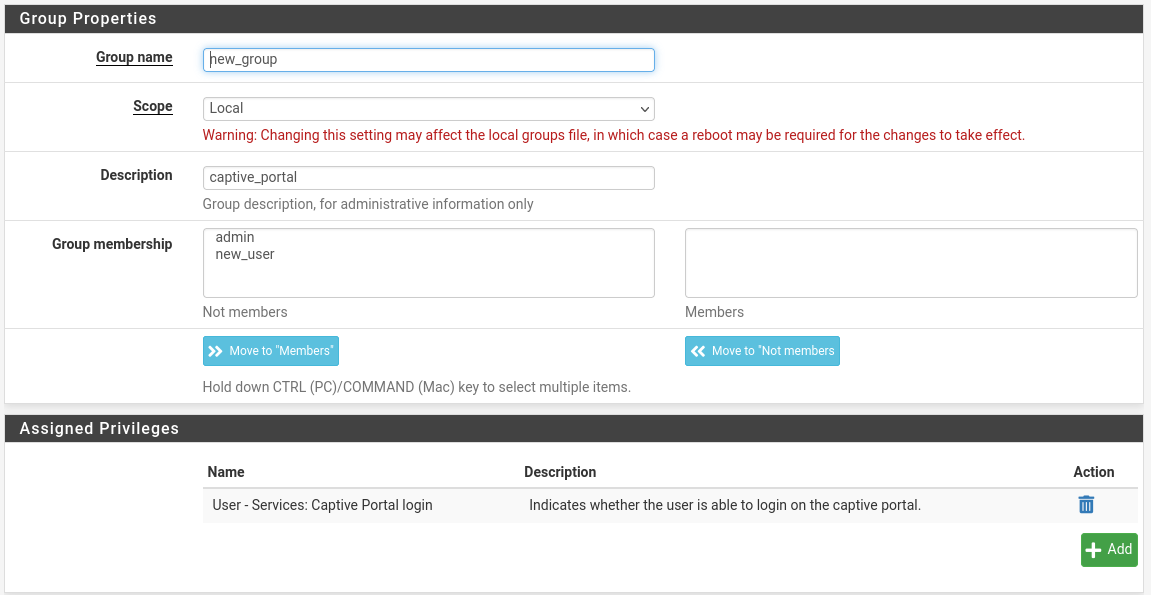
### **Part 3b: Captive Portal Authentication**

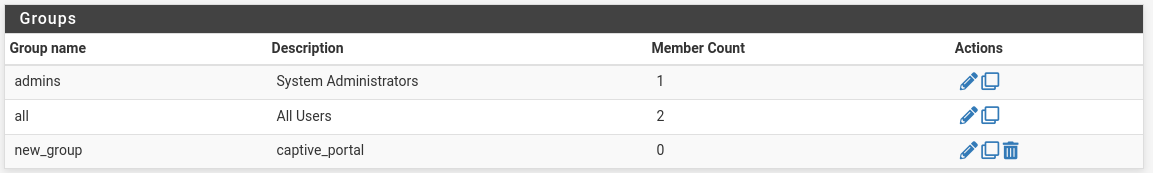
Submit detailed documentation regarding all of the configurations in this section.

* ~~In System > User Manager:~~
  + ~~Create a new user~~

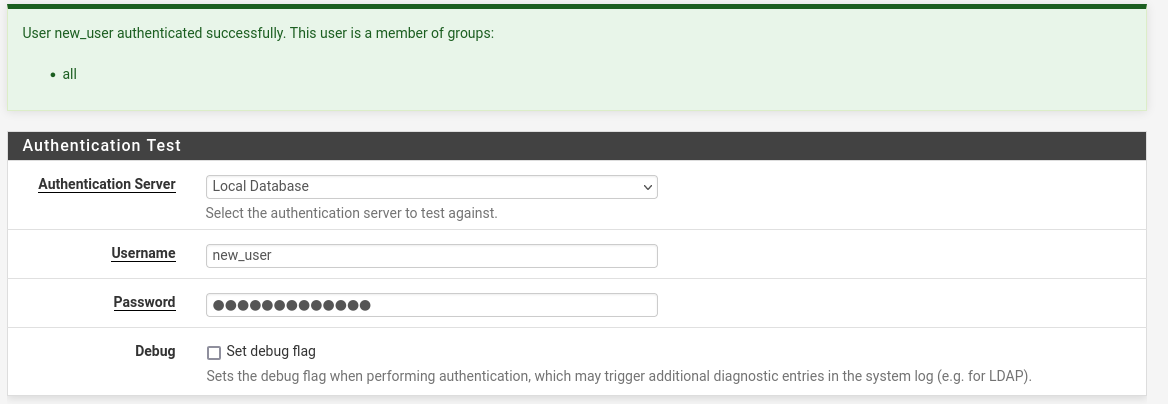


* + ~~Create a new group and grant it only captive portal privileges~~

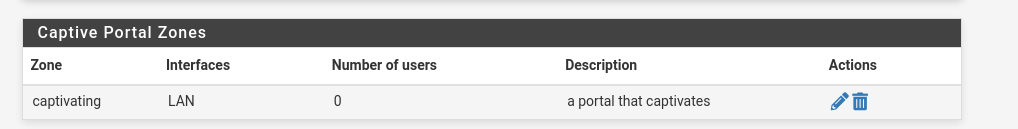




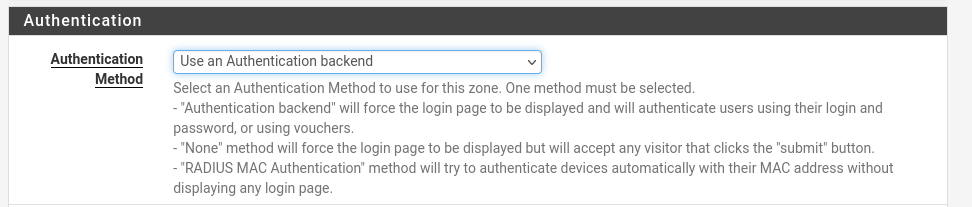
* ~~Use Diagnostics > Authentication with the Local Database to test that the account is usable~~



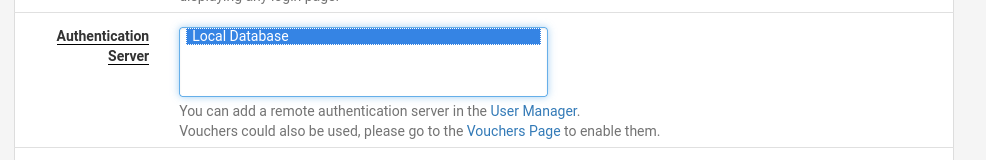
* ~~Return to Services > Captive Portal and make the following changes to the zone:~~



* + ~~Authentication Method: Use an Authentication Backend~~

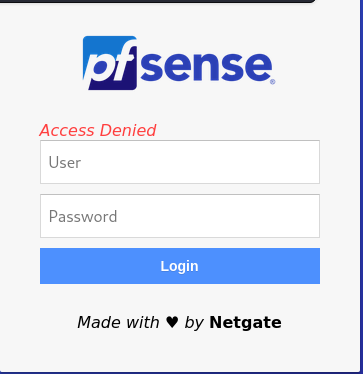


* + ~~Authentication Server: Local Database (the only option, but you still must select it)~~



* ~~Navigate back to~~ **~~http://info.cern.ch~~** ~~and login with the new user you just created~~*~~If the CERN website remains in the browser instead of loading the authentication portal, try opening your browser’s settings and clearing the cached web content~~*

**

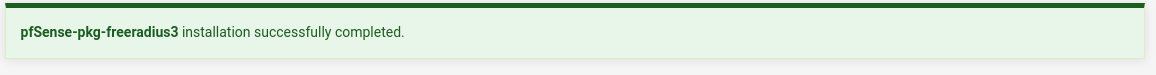
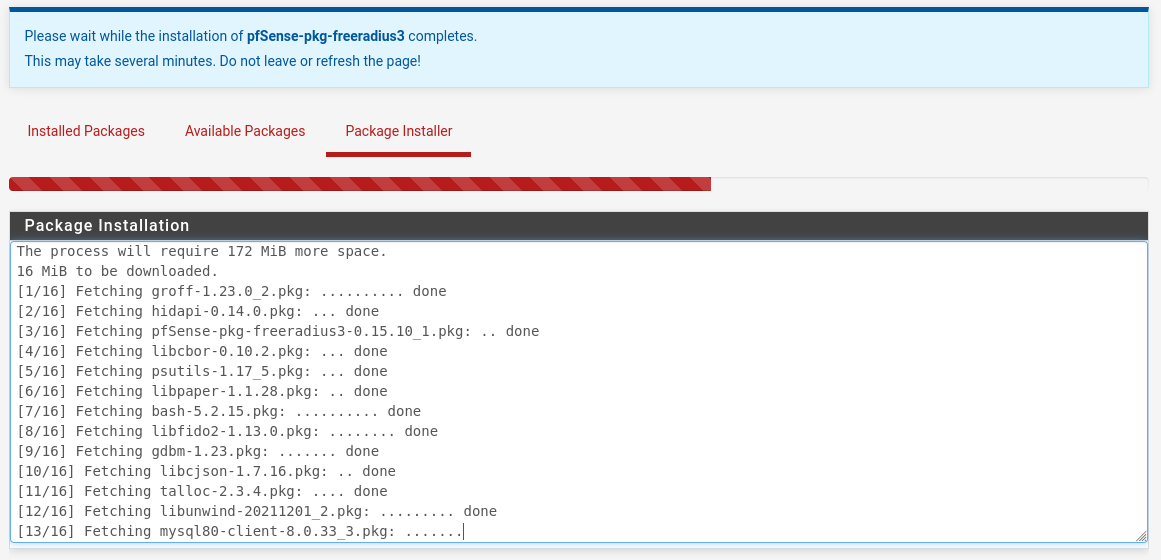
**

* ~~Why did the captive portal change?~~ 
  + **Because the instructions told me to change the authentication**
* ~~How is pfSense authenticating this user?~~
  + **Because I didn’t assign ‘new\_user’ to ‘new\_group’ pfsense is authenticating ‘new\_user’ as per the local database - in this case ‘new\_user’ is only assigned to group ‘all’**
* ~~Can you use the pfSense admin user to access the portal as well? Why or why not?~~
  + **Nope, because when assigning privileges the instructions said to ONLY allow ‘new\_group’ authentication, and by default admin doesn’t have that privilege. It can be changed easily.**

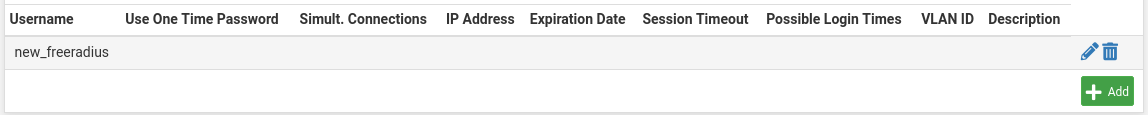
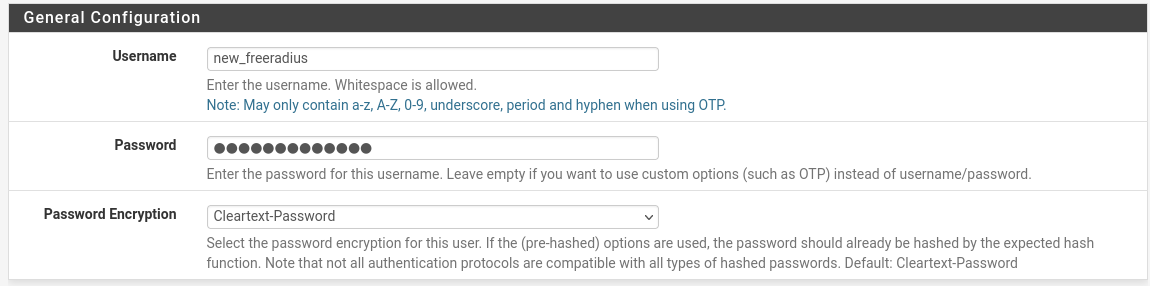
### **Part 4: Deploy FreeRADIUS**

Submit detailed documentation regarding all of the configurations in this section.

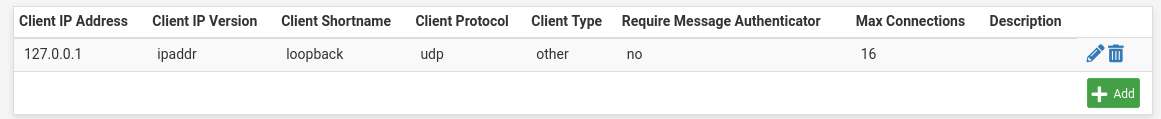
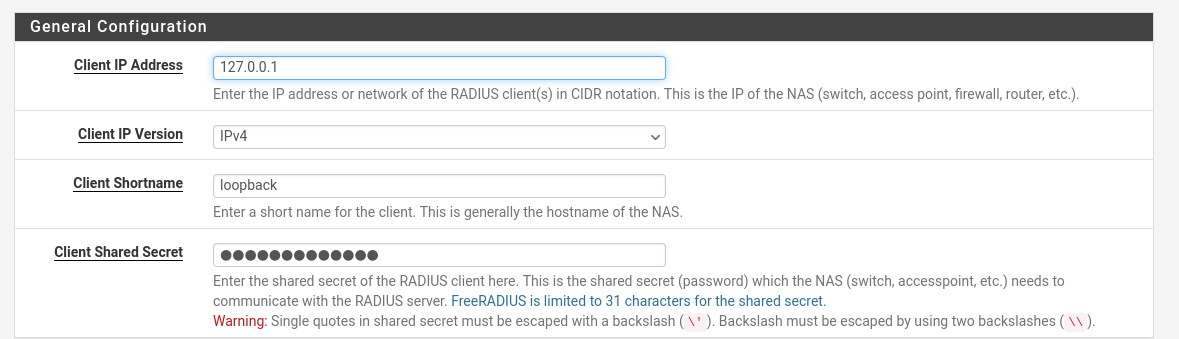
* ~~Navigate to System > Package Manager and install the FreeRADIUS package.~~



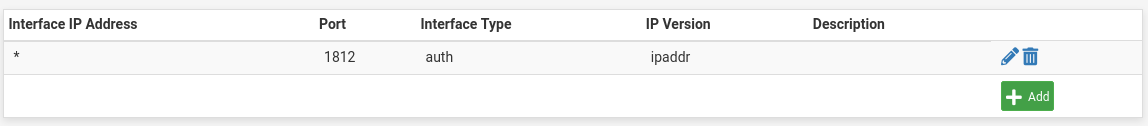
* In Services > FreeRADIUS, do the following:
  + ~~Create a User~~



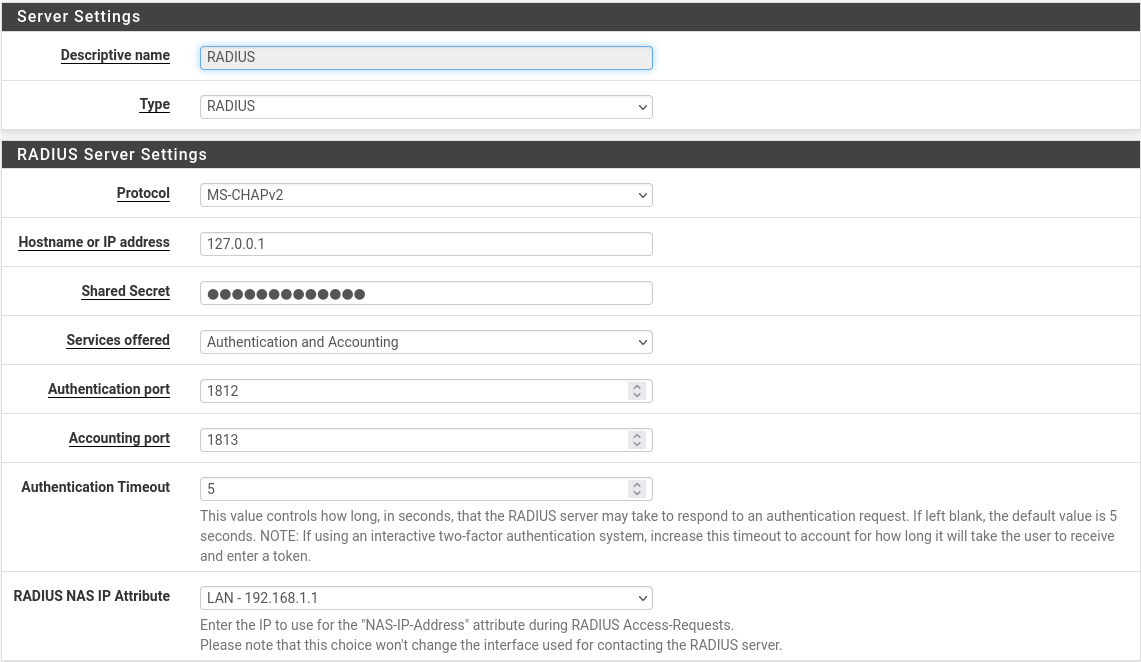
* + ~~Create a Client with the loopback address as its IP address~~
    - ~~Choose a Client Shared Secret and include it here (you’ll need it in a moment)~~



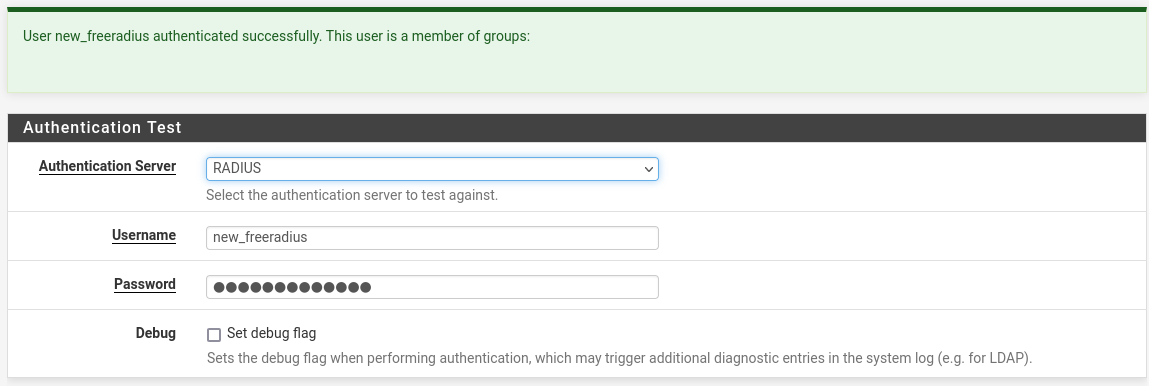
* + ~~Create an Interface (default settings are fine)~~



* ~~Under System > User Manager, select the Authentication Server tab and create a server with the following settings:~~
  + ~~Type: RADIUS~~
  + ~~IP address: the loopback address, the same as with the FreeRADIUS Client~~
  + ~~Shared Secret: the same as above~~



* ~~In Diagnostics > Authentication, test the new FreeRADIUS user you just created to confirm it is working~~

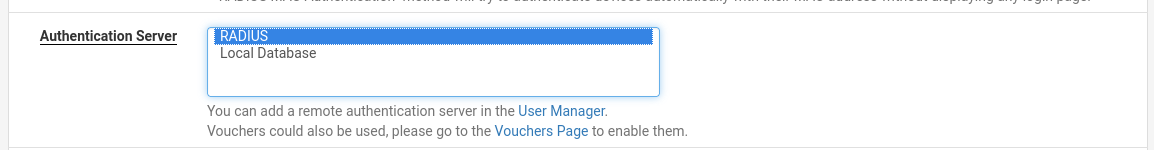


**I fat-fingered the password - but it works. I also changed the NAS to the internal LAN - but IDK if that matters or not.**

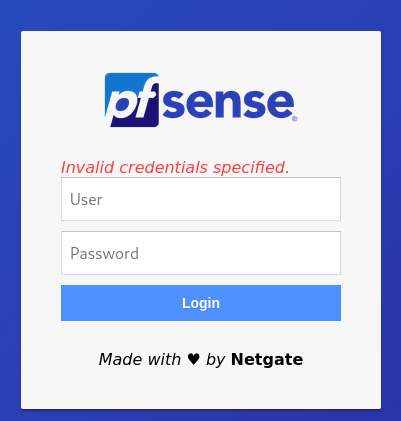
### **Part 5: Integrating FreeRADIUS with Captive Portal**

Next, let’s try and integrate FreeRADIUS. Submit detailed documentation regarding all of the configurations in this section.

* ~~Return to Services > Captive Portal and change Authentication Server from Local Database to the new server you just created~~

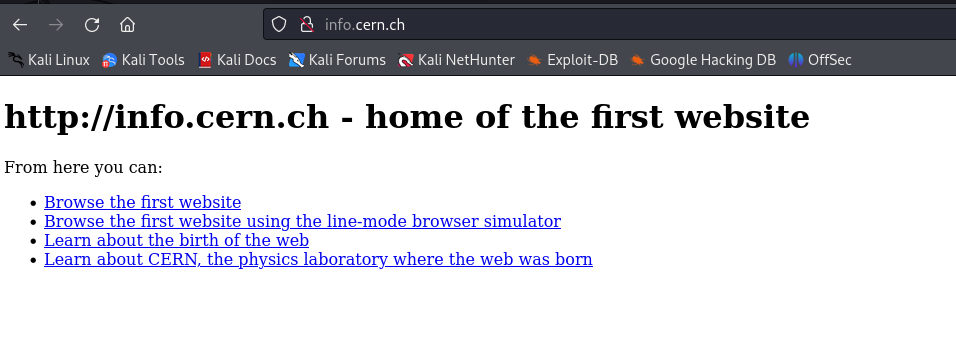


* ~~Try logging in with the pfSense local user you created in Part 2b – were you able to log in? Why or why not?~~



**Of course not, the instructions told me to change the login authenticator to freeRADIUS.**

* ~~Try logging in with the FreeRADIUS user you just created – did it work? Why or why not?~~

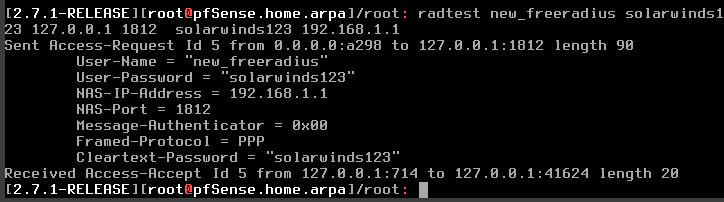


**Of course it did, I already validated the authentication.**

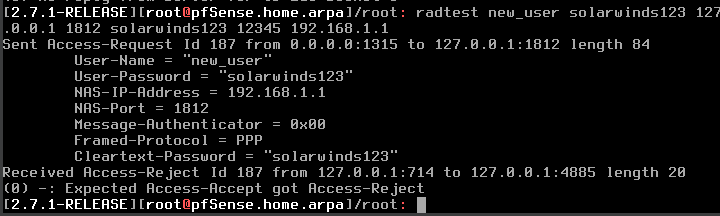
### **Part 6: Logs**

As with any system you deploy be prepared to troubleshoot it!

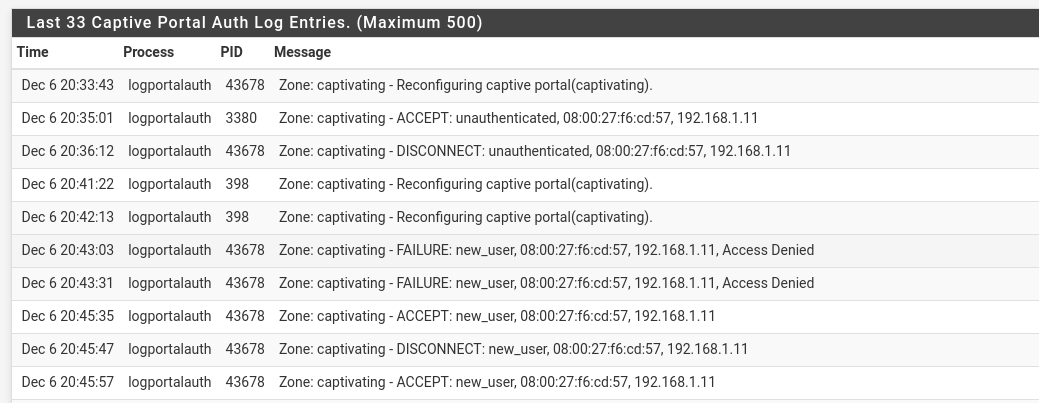
* Look up the FreeRADIUS **radtest** command
  + ~~What is the command used for?~~
    - **The radtest command is used to test the authentication process against a RADIUS (Remote Authentication Dial-In User Service) server, particularly the FreeRADIUS server.**
  + ~~What is the command’s syntax?~~
    - **[radtest <username> <password> <radius-server>[:<port>] <radius-secret> <nas-port> <nas-ip-address>]**
    - **<username>: The username you want to test.**
    - **<password>: The corresponding password for the username.**
    - **<radius-server>: The IP address or hostname of the RADIUS server.**
    - **<port>: (Optional) The UDP port on which the RADIUS server is listening. The default is usually 1812.**
    - **<radius-secret>: The shared secret between the RADIUS server and the client.**
    - **<nas-port>: The NAS (Network Access Server) port.**
    - **<nas-ip-address>: The NAS IP address.**
      * **\* Brought to you by chatGPT**
  + ~~Include a screenshot of using~~ **~~radtest~~** ~~to test your FreeRADIUS user~~



* + ~~Can you use~~ **~~radtest~~** ~~to check a pfSense local user?~~
    - **Yes, in this case the pfsense local user does NOT have access, which we proved when trying their credentials earlier.**



* ~~Identify the system logs in pfSense~~
  + ~~Include a screenshot of logs related to FreeRADIUS and/or the Captive Portal~~

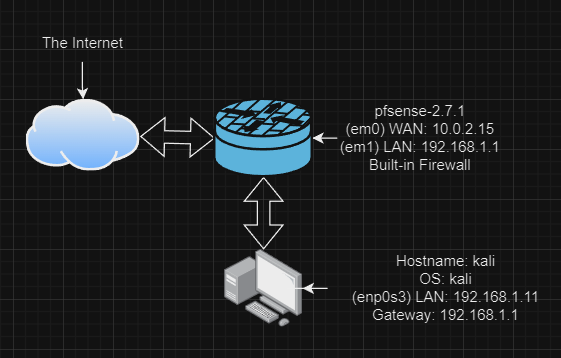


* + ~~What events do you think these logs recorded?~~
    - **My authorization attempts to login to the cern website**
  + ~~Do the system logs include authentication attempts? How about failed authentication attempts?~~
    - **Yes and Yes**
* ~~Look up AAA Management as it relates to computer security~~
  + ~~What does it mean?~~
    - **Authentication, authorization, and accounting (AAA) is a security framework that controls access to computer resources.**
      * **https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting**
  + ~~Explain in your own words how this RADIUS configuration facilitates AAA management~~
    - **Authentication: RADIUS servers verify the user's credentials (username and password) against its authentication database.**
    - **Authorization: RADIUS servers provide information on the privileges of users**
    - **Accounting: RADIUS servers track and record user's activities and resource consumption during a network session.**

Submit detailed documentation regarding all of the above configurations.

### **Part 7: Topology 2/2**

When the other tasks are complete:



* ~~review the topology and update, revise, extend, or add details as necessary.~~
* ~~Was your initial topology accurate to the finished product?~~ 
  + **Yes**
* ~~Why or why not?~~
  + **Because it was literally connecting a vm to a pfsense, which had access to the interwebs.**