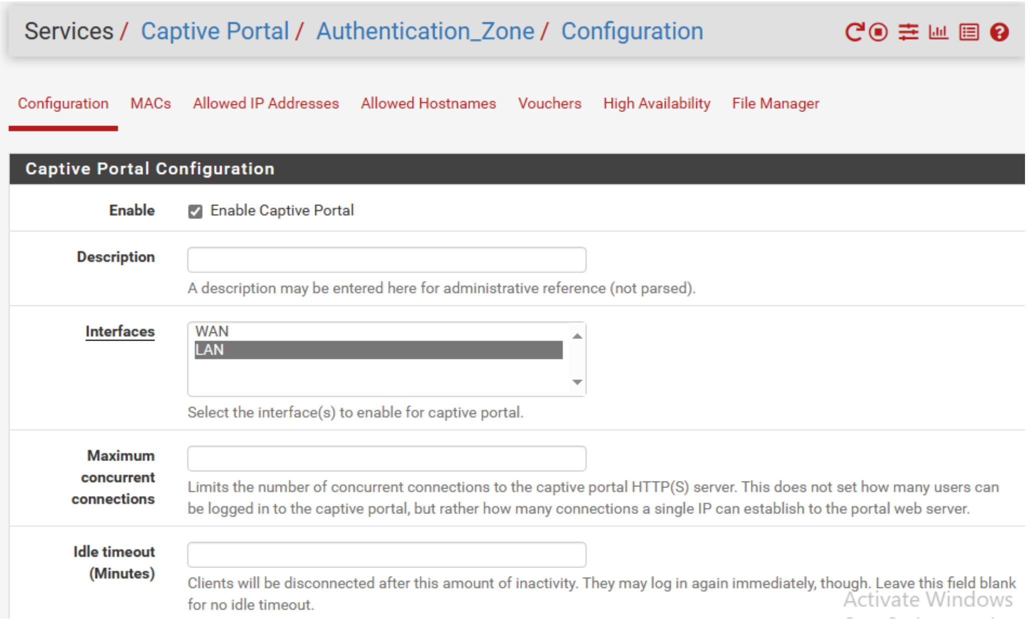
SunToWater Project

RADIUS Authentication Procedure

Sun
ToWater
TECHNOLOGIES, LLC

Captive Portal Creation



Services / Captive Portal / Authentication_Zone / Configuration

Captive Portal Configuration

Enable ☑ Enable Captive Portal

Description

A description may be entered here for administrative reference (not parsed).

Interfaces WAN LAN

Select the interface(s) to enable for captive portal.

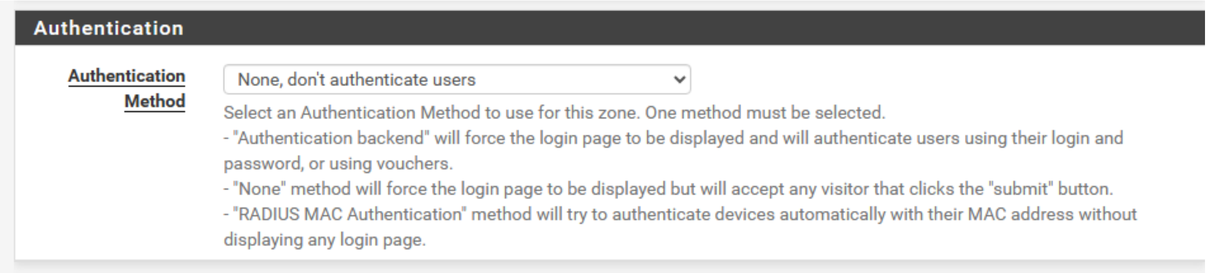
Maximum concurrent connections

Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

Idle timeout (Minutes)

Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

We start creating a captive portal by going to "Services / Captive Portal".
Click the green button "+ Add"
Give it a name in this case we called it "Authentication_Zone"
From there we go to it's configuration, click the checkbox "enable captive portal" to enable it and select in interfaces "LAN"



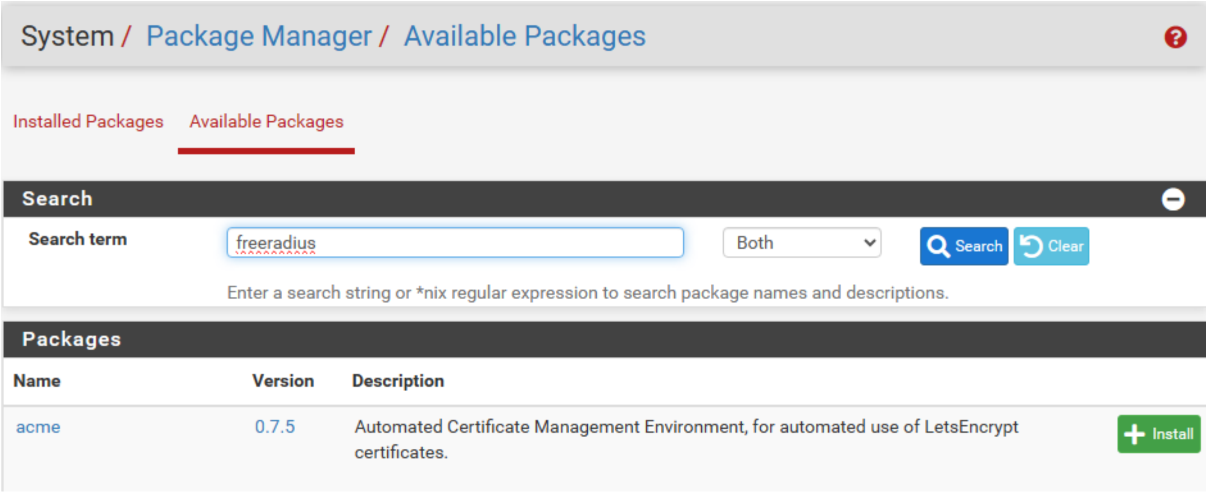
Authentication

Authentication Method: None, don't authenticate users

Select an Authentication Method to use for this zone. One method must be selected.
- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Next scroll down a bit and make sure the "None, don't authenticate users" is selected on the Authentication method, we will come back to this in a later step.
Click the blue save button to save.

FreeRadius Installation



System / Package Manager / Available Packages

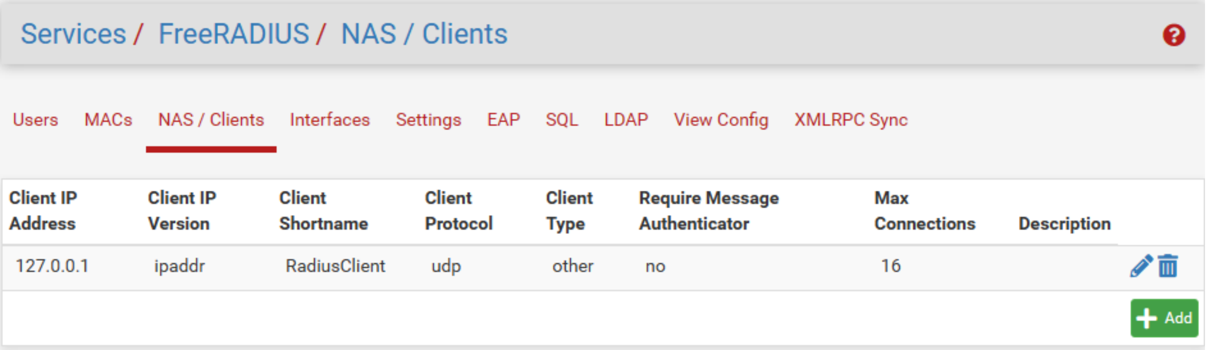
Search term: freeradius

Enter a search string or *nix regular expression to search package names and descriptions.

Name	Version	Description
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.

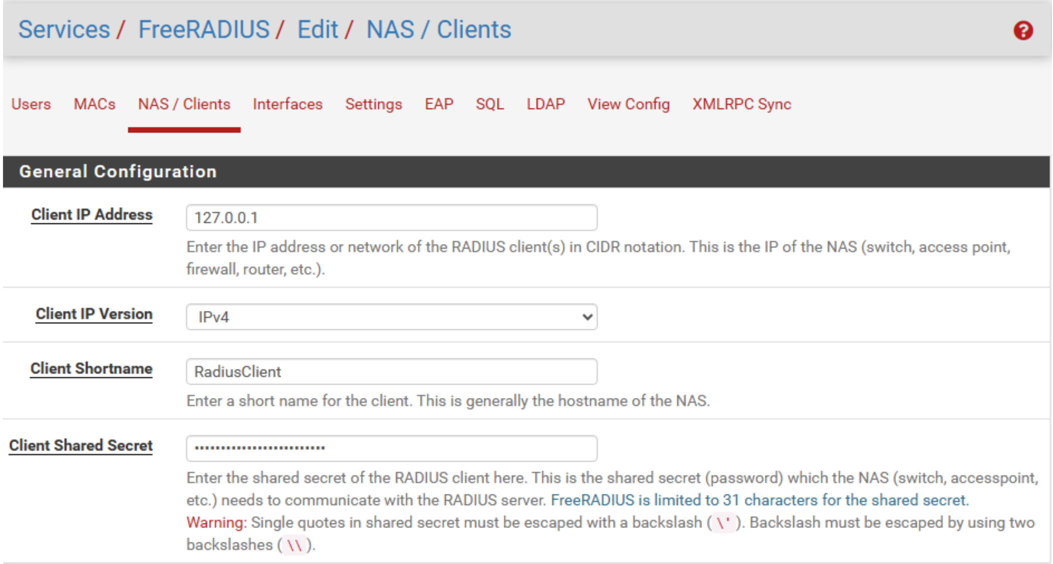
To install FreeRADIUS go to “System / Package Manager / Available Packages”
In the search term search freeradius and click the blue “search” button
The package will appear below (It’s already installed so it wont show up in the screenshot)
To install it, click the green “+ install” button

FreeRadius NAS/Clients Creation



Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description
127.0.0.1	ipaddr	RadiusClient	udp	other	no	16	

After installing FreeRADIUS, go to “Services / FreeRADIUS / NAS/Clients”, click the + Add button



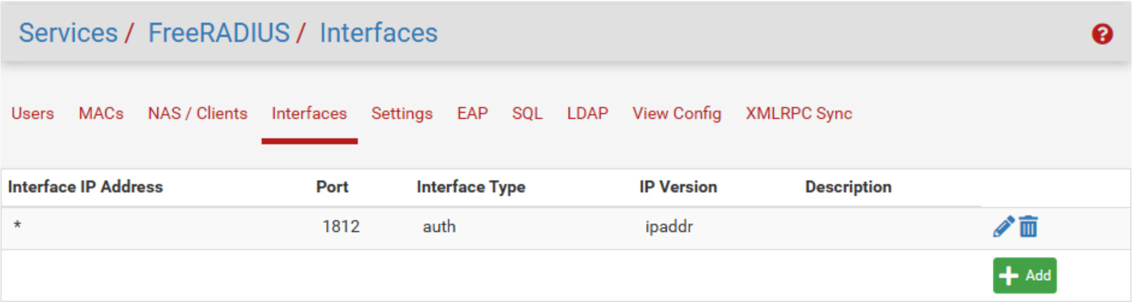
General Configuration

Client IP Address	127.0.0.1 Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).
Client IP Version	IPv4
Client Shortname	RadiusClient Enter a short name for the client. This is generally the hostname of the NAS.
Client Shared Secret	•••••••••••••••••••••••••••• Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret. Warning: Single quotes in shared secret must be escaped with a backslash (\'). Backslash must be escaped by using two backslashes (\\ ).

Here add the local host IP which is 127.0.0.1, give it a “shortname” and a “client shared secret” password

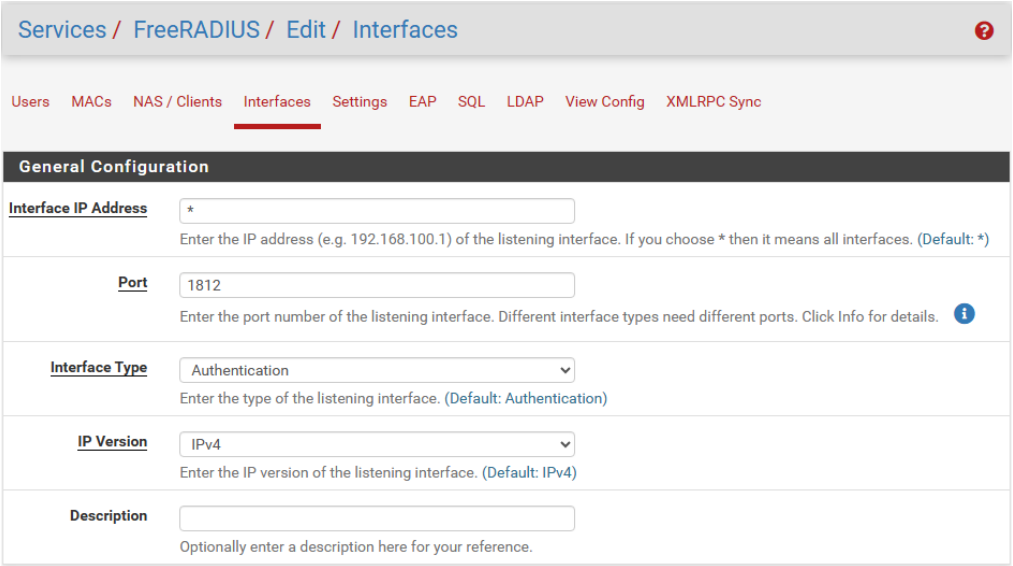
Make sure to write it down on a note for now because it will be used later.

FreeRadius Interface Creation



Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	

Next go to “Services / FreeRADIUS / Interfaces” and click the + Add green button



General Configuration

Interface IP Address: *
Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)

Port: 1812
Enter the port number of the listening interface. Different interface types need different ports. Click Info for details.

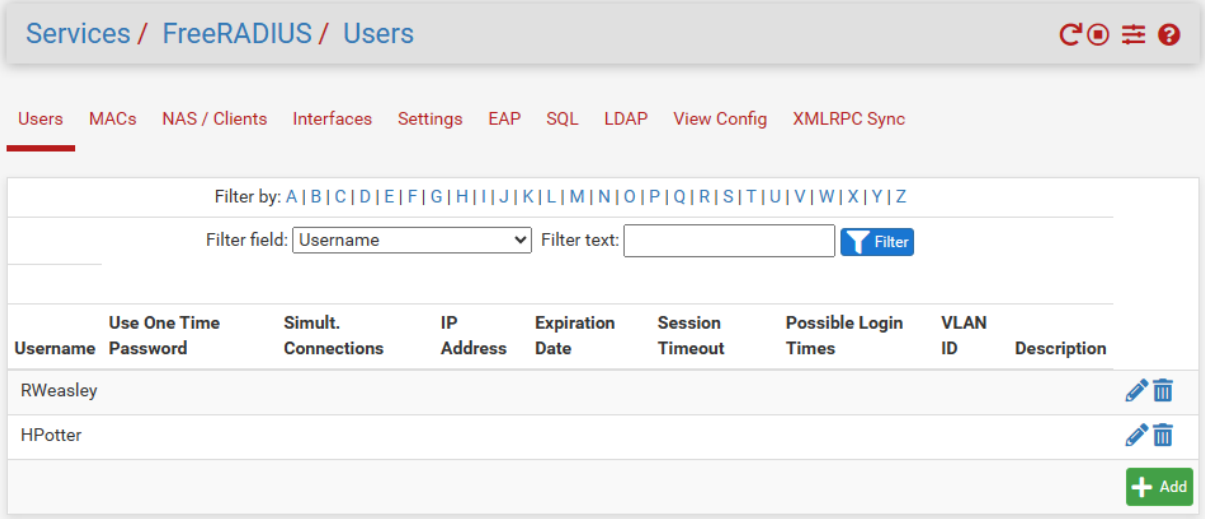
Interface Type: Authentication
Enter the type of the listening interface. (Default: Authentication)

IP Version: IPv4
Enter the IP version of the listening interface. (Default: IPv4)

Description:
Optionally enter a description here for your reference.

In here leave everything as default and save

FreeRadius User Creation

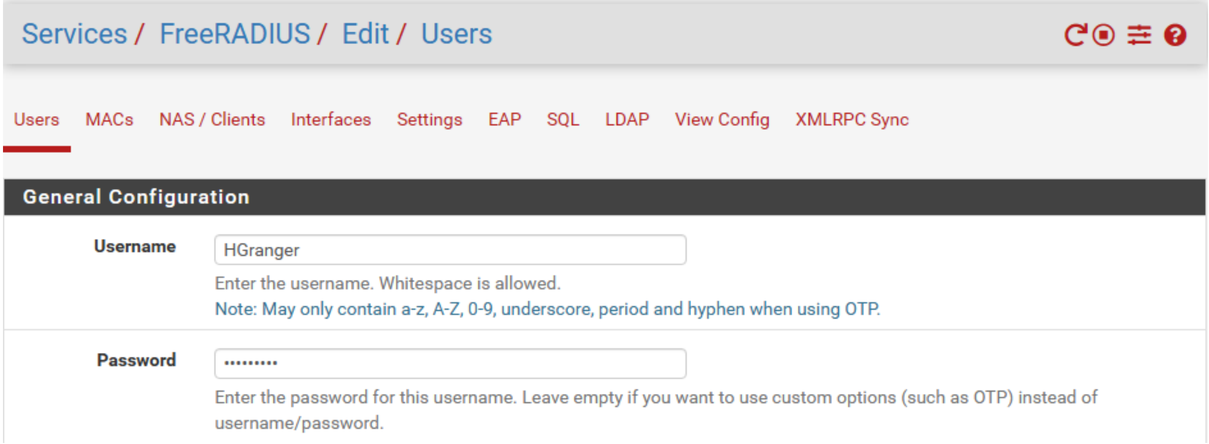

Services / FreeRADIUS / Users
Users
MACs
NAS / Clients
Interfaces
Settings
EAP
SQL
LDAP
View Config
XMLRPC Sync
Filter by: A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z
Filter
Add

Filter field: Username

Filter text:

Username	Use One Time Password	Simult. Connections	IP Address	Expiration Date	Session Timeout	Possible Login Times	VLAN ID	Description
RWeasley								
HPotter								

Next create a user by clicking the + Add green button



General Configuration

Username: HGranger

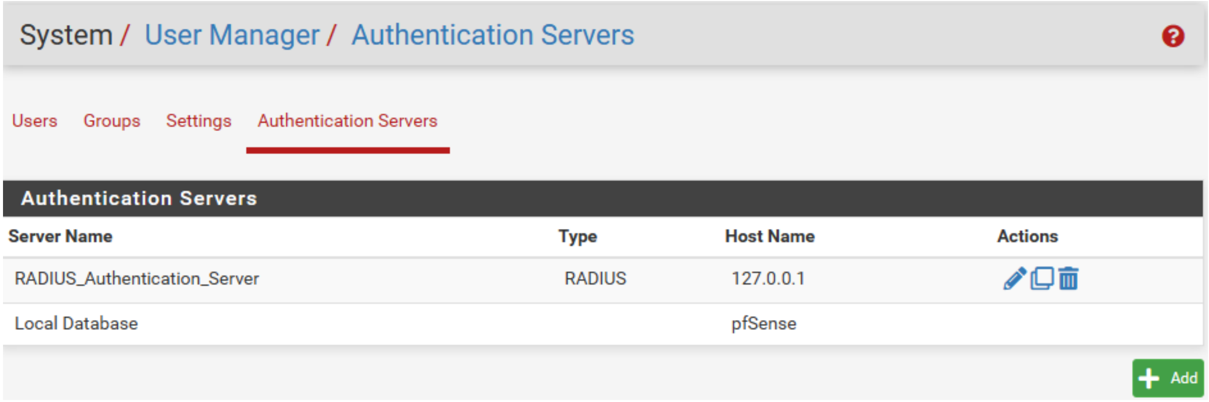
Enter the username. Whitespace is allowed.
Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP.

Password: •••••••••

Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password.

In here give a user name and a password, leave everything else on default and save

FreeRadius Authentication Server Creation

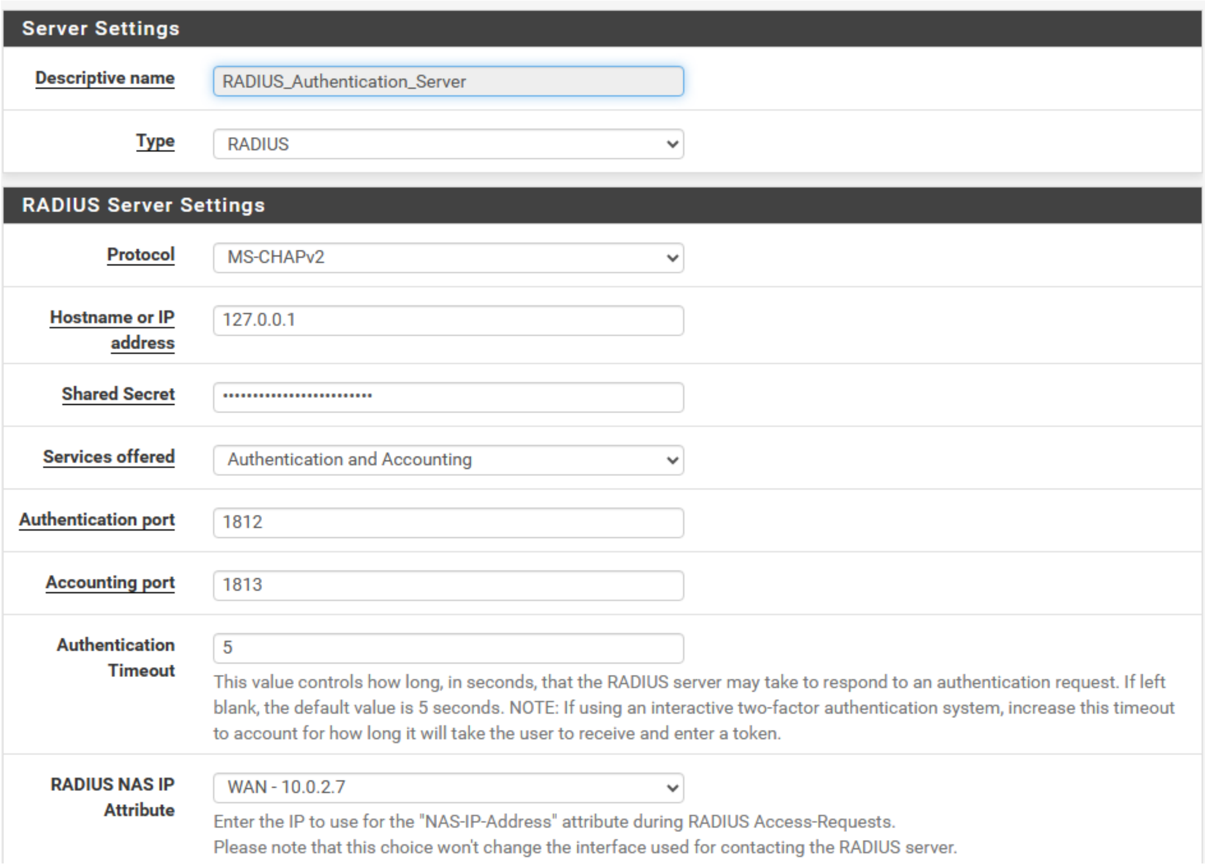


System / User Manager / Authentication Servers

Authentication Servers

Server Name	Type	Host Name	Actions
RADIUS_Authentication_Server	RADIUS	127.0.0.1	✎ ❐ 🗑
Local Database		pfSense	

Next go to “System / User Manager / Authentication Servers” and click the + Add green button



Server Settings

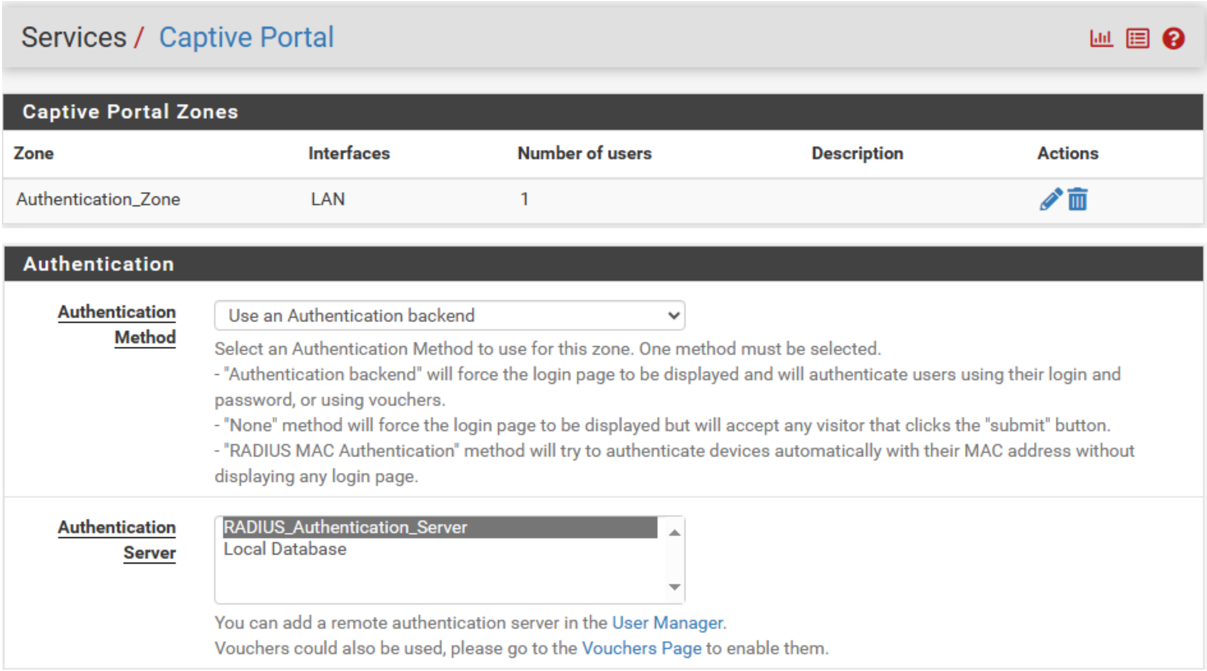
Descriptive name	RADIUS_Authentication_Server
Type	RADIUS

RADIUS Server Settings

Protocol	MS-CHAPv2
Hostname or IP address	127.0.0.1
Shared Secret	••••••••••••••••••••••••••
Services offered	Authentication and Accounting
Authentication port	1812
Accounting port	1813
Authentication Timeout	5 This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.
RADIUS NAS IP Attribute	WAN - 10.0.2.7 Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

Give it a descriptive name, change the type to “RADIUS”, give it the local host ip address and the “shared secret” password created on a previous step
Leave everything else at default and save.

Captive Portal Edit to use FreeRadius



Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
Authentication_Zone	LAN	1		✎🗑

Authentication

Authentication Method: Use an Authentication backend

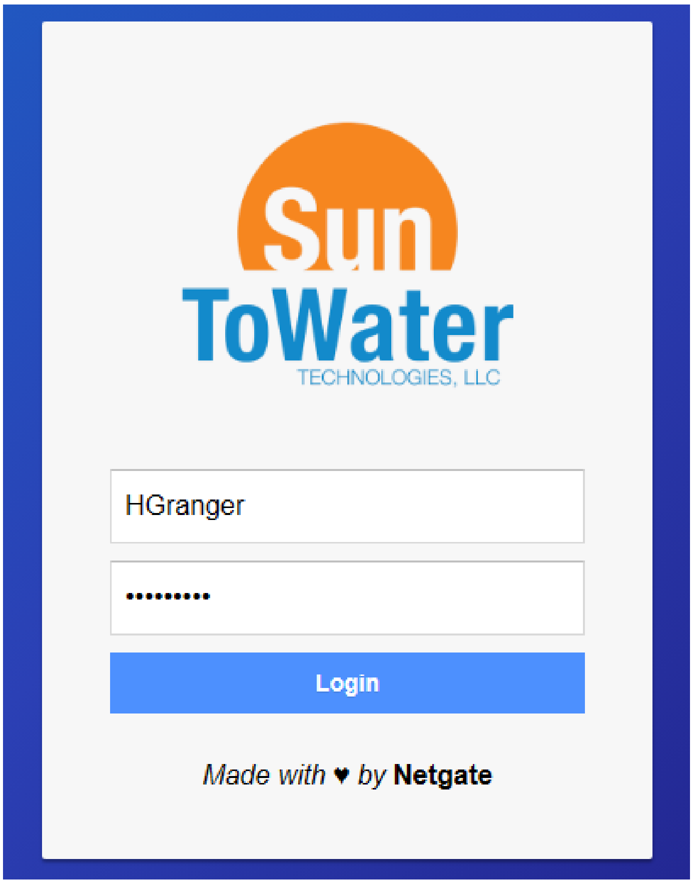
Select an Authentication Method to use for this zone. One method must be selected.
- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server: RADIUS_Authentication_Server
Local Database

You can add a remote authentication server in the User Manager.
Vouchers could also be used, please go to the Vouchers Page to enable them.

Go back to “Services / Captive Portal” click the pencil button to edit the portal zone. In its configuration scroll down until Authentication is found, change the method to “Use an Authentication backend” and choose the previous authentication server created and save.

Authentication Portal

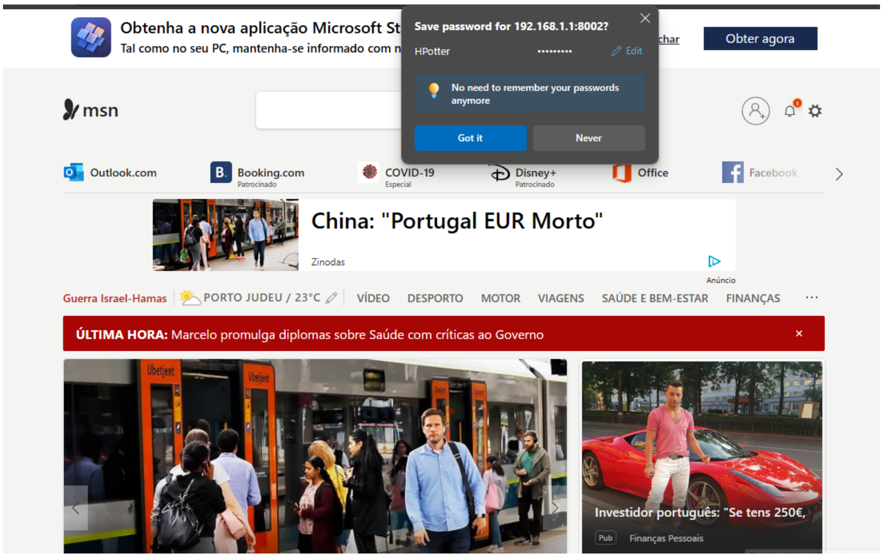


HGranger

•••••••••

Made with ♥ *by* **Netgate**

Now restart the pfSense machine and open a browser
It will show the Authentication portal and it will ask for credentials
Use the credentials from the user created in a previous step to login



Obtenha a nova aplicação Microsoft St
Tal como no seu PC, mantenha-se informado com n

Save password for 192.168.1.1:8002?

HPotter ••••••••••

No need to remember your passwords anymore

China: "Portugal EUR Morto"

Zinodas

ÚLTIMA HORA: Marcelo promulga diplomas sobre Saúde com críticas ao Governo

Investidor português: "Se tens 250€,

And If the credentials are correct it will redirect to a webpage!