

# Rendu Projet Infra/SI

*MODOLO Thomas / MATAS Lucas*

## Mise en place d'une architecture réseau sécurisée

### Sommaire

I - Introduction.....	p.2
I.1 Maquettes et schéma réseau.....	p.3-4
II - Installation de pfSense.....	p.5-6
III - Configuration des adresses.....	p.6-8
IV - Accès a l'interface.....	p.9-10
V - Configuration du portail.. ..	p.11-12
VI - Configuration des groupes.....	p.13-16
VII - Configuration DMZ.....	p.17-19
VIII - Installation T-Pot.....	p.20-22
IX - Conclusion.....	p.23



# I - Introduction

Dans ce document, je vais vous apprendre à faire une architecture réseau sécurité. Pour réaliser ce projet nous allons avoir besoin d'une machine FreeBSD (Pfsense) , deux machine Ubuntu : Une machine pour la configuration de l'interface pfSense et la seconde pour la DMZ. Et une dernière machine sera sous Debian 10 pour l'installation de l'Honeypot : T-Pot qui va nous créer une interface locale pour l'analyse du trafic des données.

A noter que de base le projet devait être fait sur GNS3 et par manque de cours et de connaissance nous avons dû nous en passer. De ce fait nous n'avons pas pu mettre en place la redondance réseau et les VLANs. Pour remédier à ça que nous travaillons avec des machines virtuelles sur VMWARE qui seront dans un même réseau.

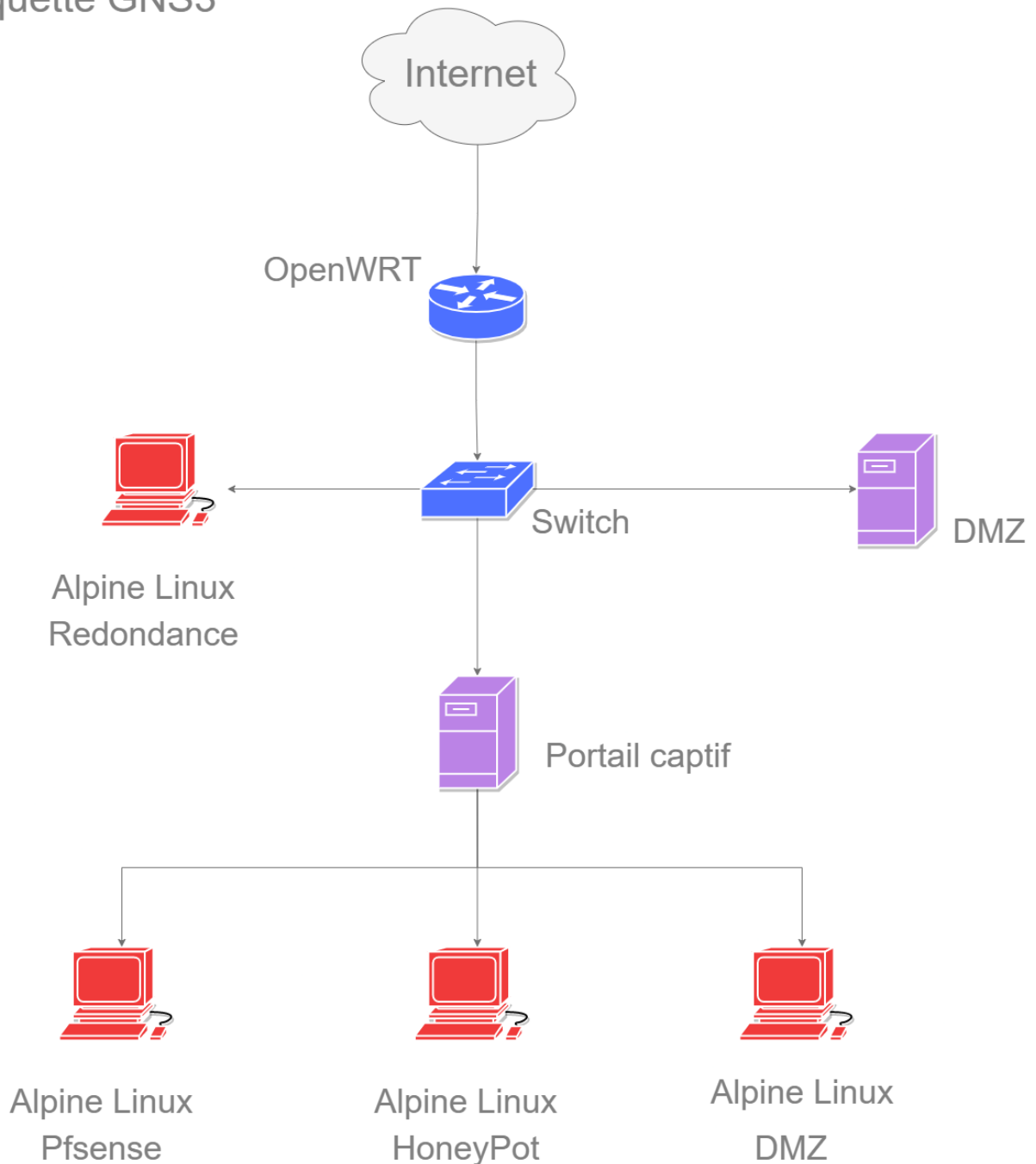
Bonne lecture !



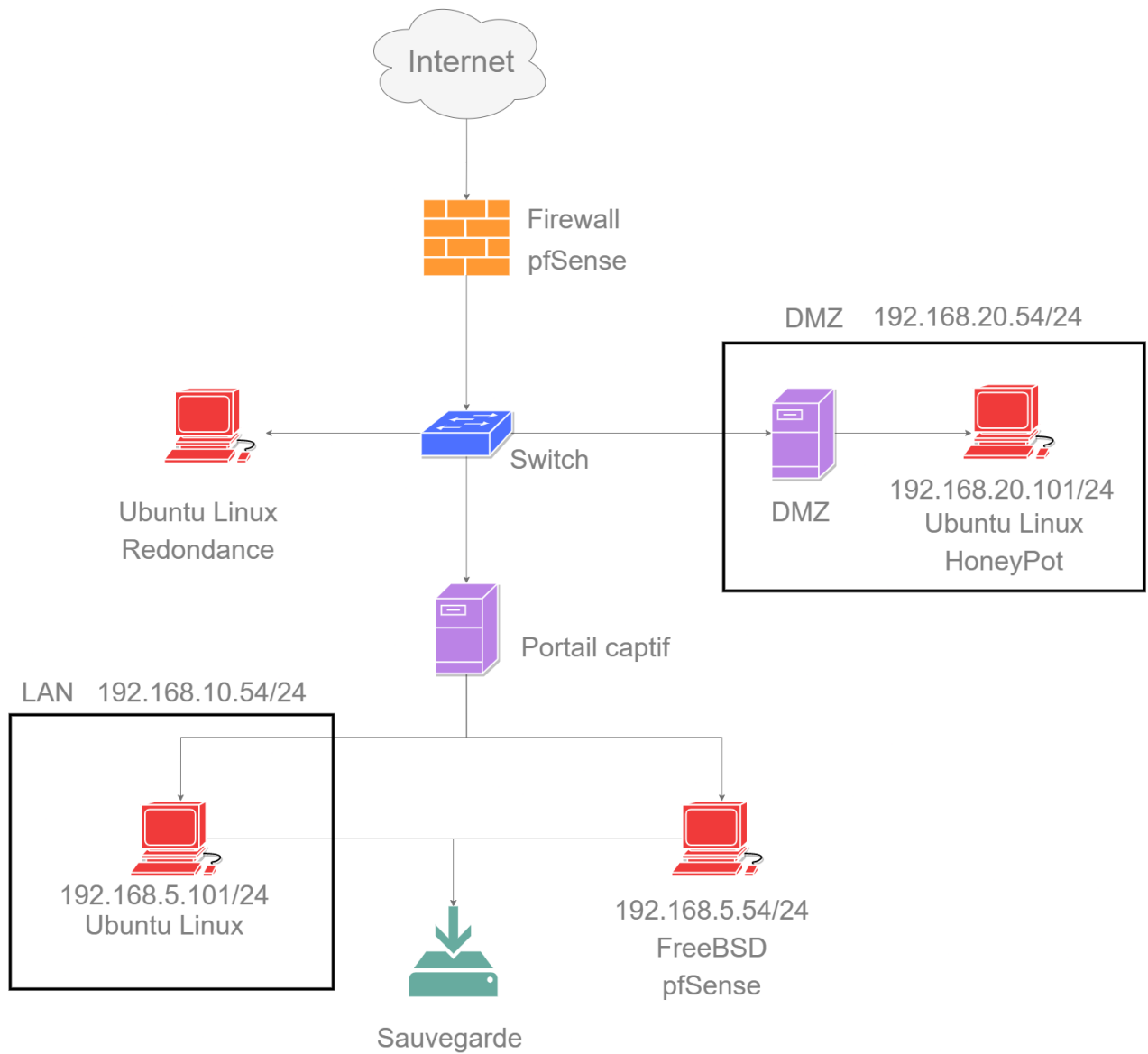
## I.1 Maquette et schéma réseau

### Maquette GNS3 (De base)

Maquette GNS3



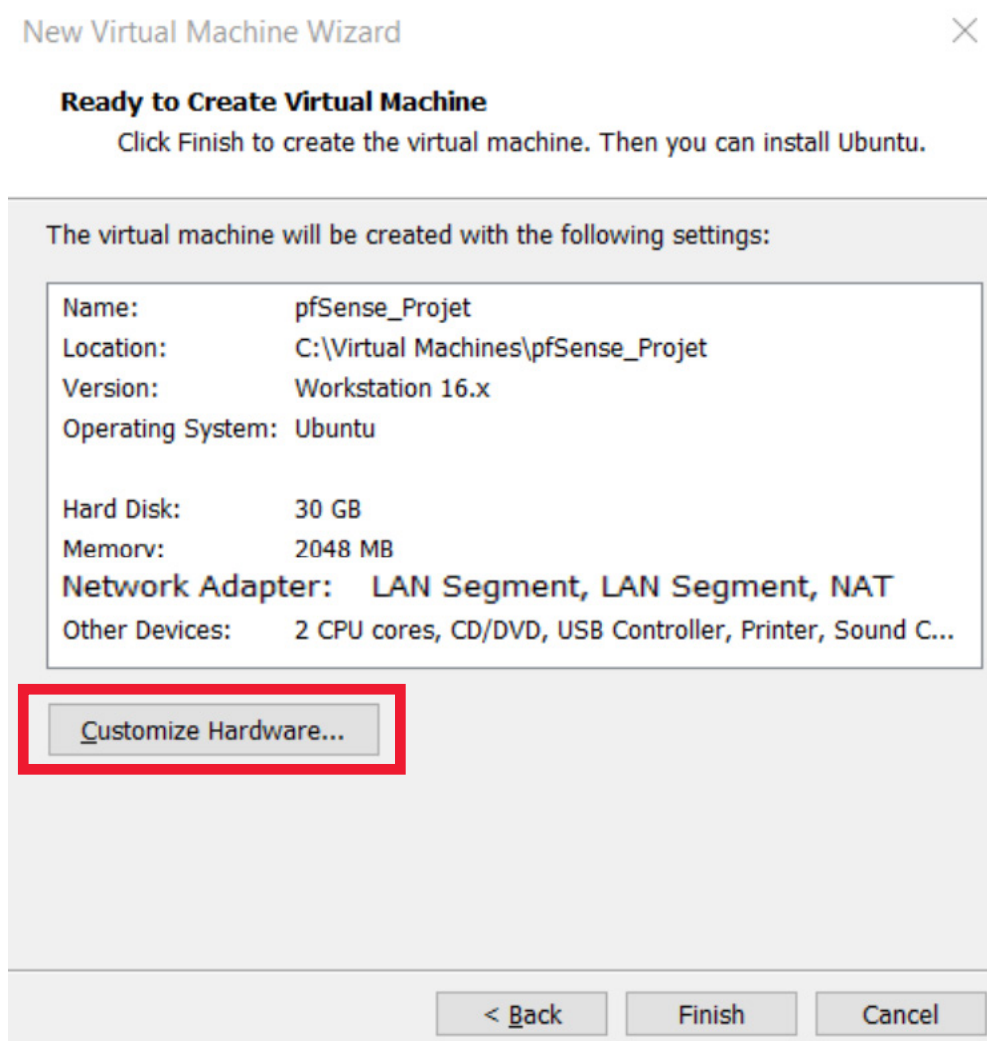
# Schéma réseau (Adaptation)



## II - Installation de pfSense

Nous allons d'abord commencer par télécharger l'iso FreeBSD de pfSense disponible ici : <https://www.pfsense.org/download/>

Après une installation avancée, arrivé à cette étape, nous allons ajouter 3 «Network Adapters».



On aura un NAT, un DMZ et un LAN.

Device	Summary
Memory	512 MB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file D:\Travaux_Ynov\...
Network Adapter	NAT
Network Adapter 2	LAN Segment <b>DMZ</b>
Network Adapter 3	LAN Segment <b>LAN</b>
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Ensuite on ajoute l'iso pour procéder à l'installation de notre machine.

Je vais passer les étapes de l'installation, un tuto est dispo ici : <https://techexpert.tips/fr/pfsense-fr/installation-du-serveur-pfsense/>

## III - Configuration des adresses

Pour cette étape, je vais montrer la configuration d'une carte. Cela sera pareil pour les autres, nous aurons simplement l'adresse ip qui changera.

On va choisir l'option : 2

```

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

```

Enter an option: 2

Pour cet exemple je vais configurer la carte WAN.

```
Available interfaces:
```

```
1 - WAN (em0 - static)
2 - LAN (em2 - static)
3 - DMZ (em1 - static)
```

```
Enter the number of the interface you wish to configure: 1
```

On ne veut pas de DHCP donc option : n

```
Configure IPv4 address WAN interface via DHCP? (y/n) n
```

L'adresse IP sera 192.168.5.54 (cela sera la seule chose à changer pour les autres cartes).

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.5.54
```

On sélectionne le CIDR 24.

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
```

```
Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24
```

En passerelle nous allons mettre l'adresse configurée dans virtual network editor, donc : 192.168.5.2

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.5.2
```

On ne veut pas d'IPv6 .

```
Configure IPv6 address WAN interface via DHCP6? (y/n) n
```

Nous laissons donc ce champ vide.

```
Enter the new WAN IPv6 address. Press <ENTER> for none:  
>
```

On veut garder notre HTTPS donc non.

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Et voilà ! Nous avons notre première carte qui est configurée. Il reste plus qu'à faire pareil avec les autres.

A la fin vous devriez vous retrouver avec une configuration comme celle-ci.

```
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on srv-pfsense ***

WAN (wan)      -> em0      -> v4: 192.168.5.54/24
LAN (lan)      -> em2      -> v4: 192.168.10.54/24
DMZ (opt1)     -> em1      -> v4: 10.0.0.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

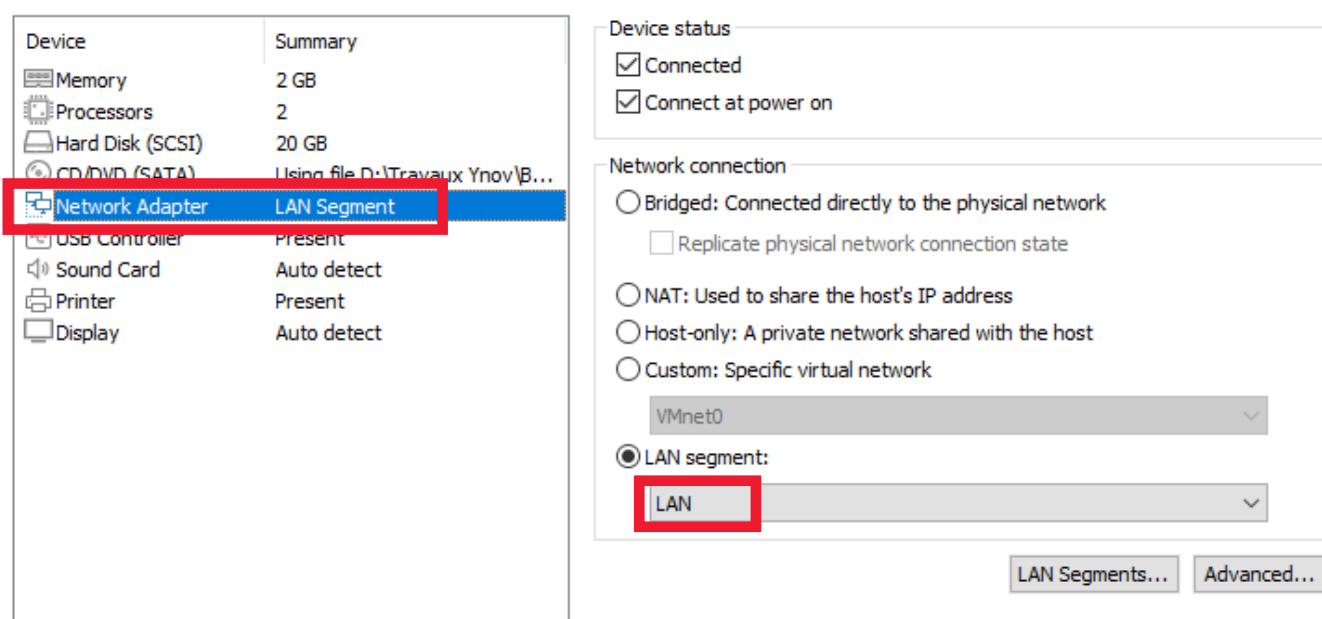
Enter an option:
```



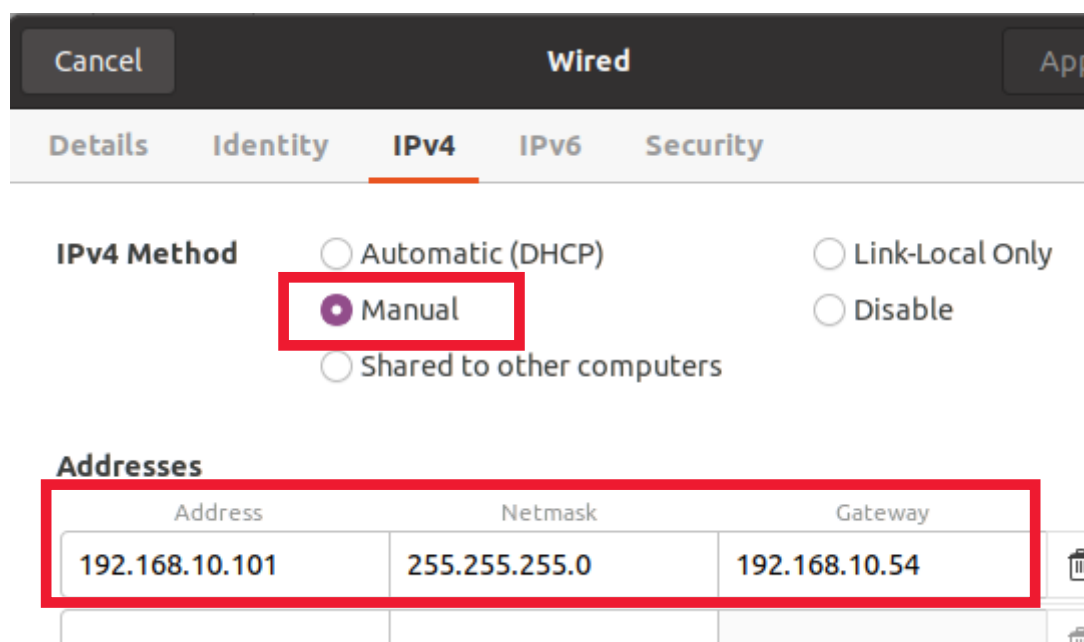
## IV - Accès à l'interface pfSense

Pour accéder à l'interface pfSense, nous allons utiliser une machine client. Pour ma part je vais utiliser une machine Ubuntu (Tuto dispo ici : [shorturl.at/uzGY3](https://shorturl.at/uzGY3)).

Dans les paramètres virtuels de la machine, on vérifie bien qu'on est sur le segment LAN que nous avons créé précédemment.



Dans les paramètres réseau on va configurer les adresse IP comme ceci.



**DNS**

Automatic ☐

192.168.10.54

Separate IP addresses with commas

Pour ensuite accéder à l'interface pfSense, il ne nous reste plus qu'à entrer l'adresse IP LAN configurée précédemment : 192.168.10.54 dans un navigateur WEB. (login/pass admin/pfsense)

pfSense - Login

https://192.168.10.54

**pf**sense

SIGN IN

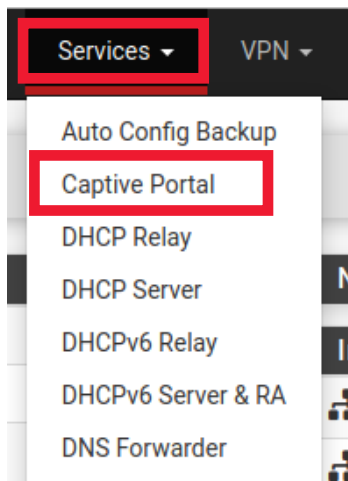
pfSense

Password

SIGN IN

Vous avez maintenant accès à votre interface pfSense

# V - Configuration du portail captif




Dans les services nous allons accéder aux paramètres du portail captif.

On va ensuite choisir un nom et une description.

Services / Captive Portal / Add Zone

### Add Captive Portal Zone

<b>Zone name</b>	<input type="text" value="Portail EKIP"/>
<small>Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.</small>	
<b>Zone description</b>	<input type="text" value="Portail"/>
<small>A description may be entered here for administrative reference (not parsed).</small>	

 Save & Continue

Suivez la configuration suivante.

## Captive Portal Configuration

**Enable** ☒ Enable Captive Portal

**Description** Portail

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

**Interfaces**

LAN

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

**Maximum concurrent connections**

3

Limits the number of concurrent connections to the captive portal HTTP(S) server, but rather how many connections a single IP can establish to the portal.

**Idle timeout (Minutes)**

6

Clients will be disconnected after this amount of inactivity. They may log in again.

**After authentication Redirection URL**

https://www.google.com/

Set a forced redirection URL. Clients will be redirected to this URL instead of the default.

**Authentication Server**

Local Database

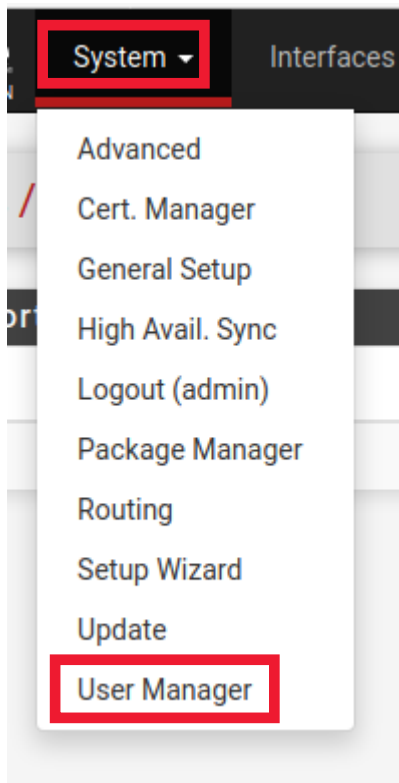
You can add a remote authentication server in the [User Manager](#). Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

**Secondary authentication Server**

Local Database

You can optionally select a second set of servers to authenticate users. This setting is useful if you want to provide multiple authentication methods. If this setting is empty, it will use the primary server.

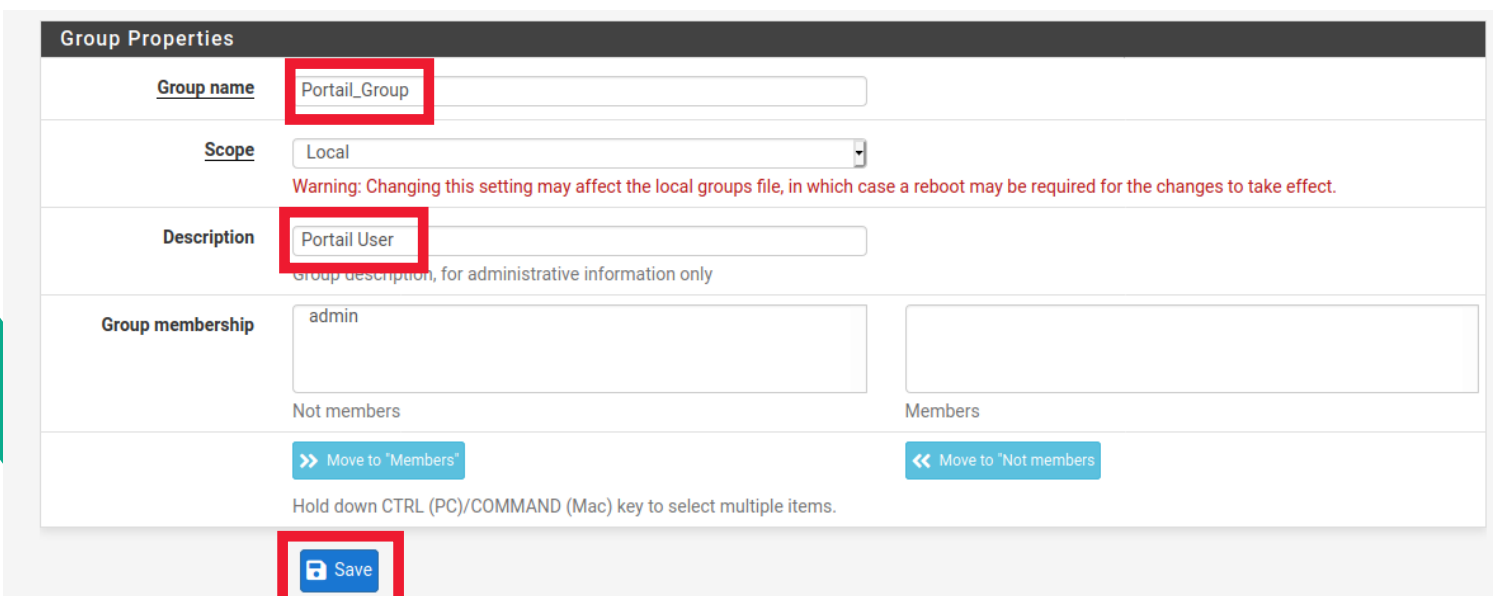
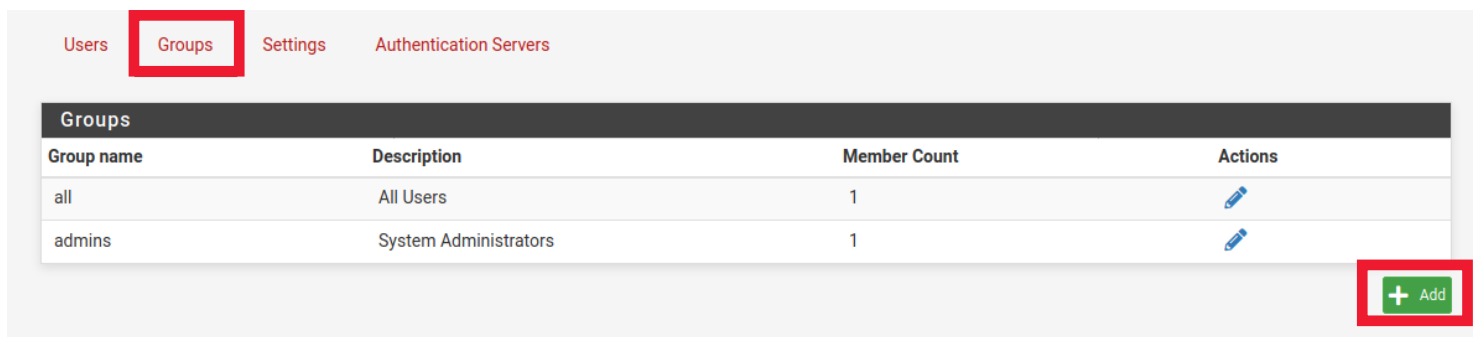
# VI - Configuration des groupes et User



On va ajouter un groupe de user pour le portail dans «User Management»

On va ajouter un groupe de user pour le portail dans «User Management»

Comme d'habitude on va y ajouter un nom, une description...ect.



On retourne ensuite modifier le groupe pour assigner les privilèges

Assigned Privileges		
Name	Description	Action
		<a href="#">+ Add</a>

### Group Privileges

Group	Portail_Group
<u>Assigned privileges</u>	<div><div>System - HA node sync</div><div>User - Config: Deny Config Write</div><div>User - Notices: View</div><div>User - Notices: View and Clear</div><div>User - Services: Captive Portal login</div><div>User - System: Copy files (scp)</div><div>User - System: Copy files to home directory (chrooted scp)</div><div>User - System: Shell account access</div><div>User - System: SSH tunneling</div><div>User - VPN: IPsec xauth Dialin</div><div>User - VPN: L2TP Dialin</div><div>User - VPN: PPPOE Dialin</div><div>WebCfg - AJAX: Get Queue Stats</div><div>WebCfg - AJAX: Get Service Providers</div><div>WebCfg - AJAX: Get Stats</div><div>WebCfg - All pages</div><div>WebCfg - Crash reporter</div><div>WebCfg - Dashboard (all)</div><div>WebCfg - Dashboard widgets (direct access).</div><div>WebCfg - Diagnostics: ARP Table</div></div>

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

On va autoriser le groupe a se connecter

Assigned Privileges		
Name	Description	Action
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	
		<a href="#">+ Add</a>
<a href="#">Save</a>		

On va ensuite ajouter l'utilisateur

Users Groups Settings Authentication Servers

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

+ Add Delete

User Properties

Defined by: USER

Disabled: ☐ This user cannot login

Username:

Password:

Full name:   
User's full name, for administrative information only

Expiration date:   
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings: ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership:

admins

Not member of

>> Move to "Member of" list

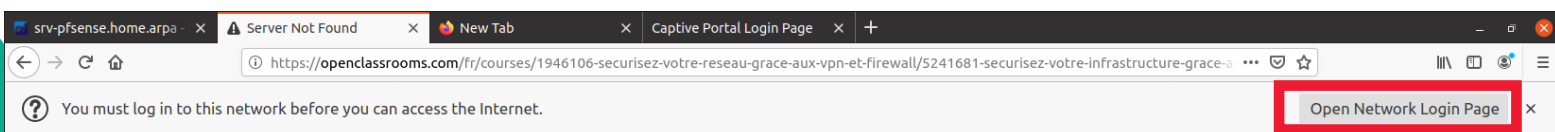
Portail\_Group

Member of

<< Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Après avoir sauvegarder les paramètres, vous n'aurez plus accès à internet. Il faudra donc vous connecter au portail à l'aide de la popup



Ici on va rentrer la config précédente c'est à dire User01/Passw0rd  
(le mot de passe que vous avez inséré)

srv-pfsense.home.arpa x Server Not Found x New Tab x Captive Portal Login Page x +

192.168.10.54:8002/index.php?zone=portail\_ekip&redirecturl=http%3A%2F%2Fdetectportal.firefox.com%2Fsuccess.txt

**DOR DADA**  
RECORDS

First Authentication Method

User

Password

Second Authentication Method

User

Password

☐ I agree with the terms & conditions

Login

Made with ♥ by Netgate

Et voilà !

srv-pfsense.home.arpa x Server Not Found x Sécurisez votre infrastructure x +

https://openclassrooms.com/fr/courses/1946106-securisez-votre-reseau-grace-aux-vpn-et-firewall/5241681-securisez-votre-infrastructure

OPENCLASSROOMS Formations Alternance Financements Pour les entreprises

Accueil > Cours > Sécurisez votre réseau grâce aux VPN et Firewall > Sécurisez votre infrastructure grâce à pfSense

## Sécurisez votre réseau grâce aux VPN et Firewall

6 heures Facile Licence CC BY NC ND

Mis à jour le 14/05/2021

Sécurisez votre infrastructure grâce à pfSense

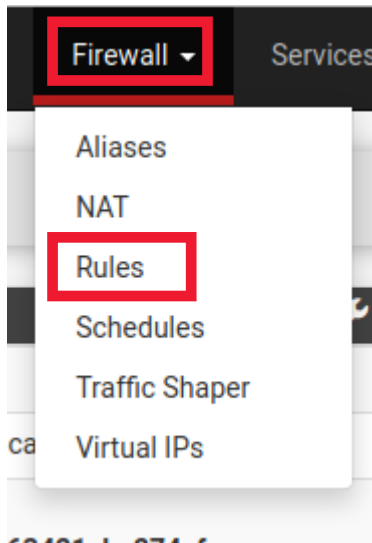
- 1. Sécurisez votre infrastructure grâce à pfSense
- 2. Rendez votre serveur accessible tout en le sécurisant
- 3. Filtrez les applications indésirables

ACCÉDER AU FORUM

Looked up f.vimeocdn.com...



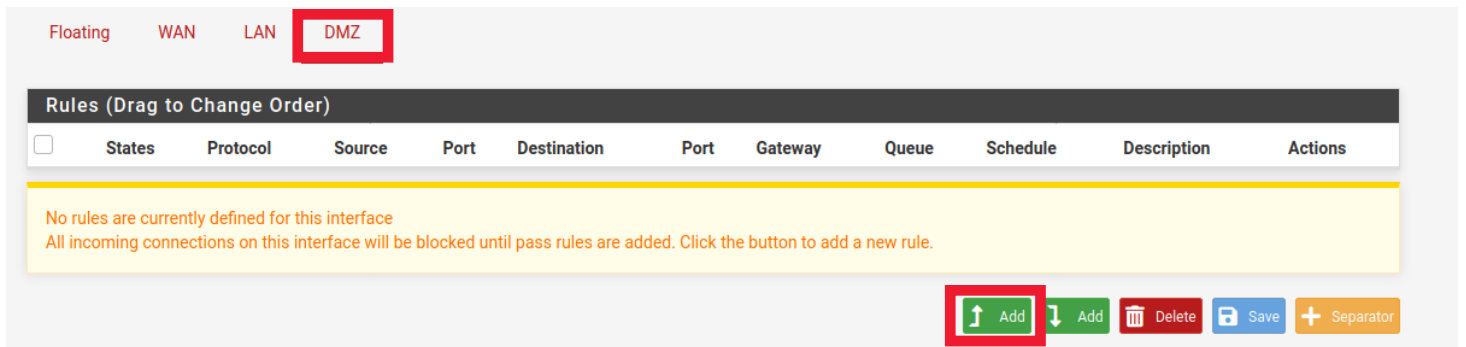
# VII - Configuration de la DMZ



La DMZ sera un clone de ma première machine Ubuntu

On va se retrouver sur pfSense dans Firewall > Rules

Et on va configurer nos règles pour lui donner accès à internet



La première règle sera pour laisser passer l'ICMP :

A screenshot of the pfSense 'Rule' configuration form. The form is for creating a new rule. The 'Interface' is set to 'DMZ' (highlighted with a red box). The 'Address Family' is 'IPv4' (highlighted with a red box). The 'Protocol' is 'ICMP' (highlighted with a red box). The 'ICMP Subtypes' are set to 'any' (highlighted with a red box). The 'Source' is set to 'DMZ net' (highlighted with a red box). The 'Destination' is set to 'any'. The 'Description' is 'ICMP' (highlighted with a red box). The 'Save' button is highlighted with a red box. The 'Advanced Options' section is expanded, showing 'Log' and 'Display Advanced' options.

## Ensuite on créer une autre règle pour les DNS

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP/UDP  
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match DMZ net Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

**Destination** ☐ Invert match any Destination Address /

**Destination Port Range** DNS (53) Custom To DNS (53) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** DMZ  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

[Save](#)

## On fait de meme pour HTTP et HTTPS pour avoir un accès aux sites web

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match DMZ net Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

**Destination** ☐ Invert match any Destination Address /

**Destination Port Range** HTTP (80) Custom To HTTP (80) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** HTTP accept  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

[Save](#)

Address Family	IPv4		
	Select the Internet Protocol version this rule applies to.		
Protocol	TCP/UDP		
	Choose which IP protocol this rule should match.		
Source			
Source	<input type="checkbox"/> Invert match	DMZ net	Source Address /
<a href="#">Display Advanced</a>			
The <b>Source Port Range</b> for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, <b>any</b> .			
Destination			
Destination	<input type="checkbox"/> Invert match	any	Destination Address /
Destination Port Range	HTTPS (443)	Custom	HTTPS (443) Custom
	From	To	
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			
Extra Options			
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the <a href="#">Status: System Logs: Settings</a> page).		
Description	<div></div> <p>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.</p>		
Advanced Options	<a href="#">Display Advanced</a>		
<a href="#">Save</a>			

# VIII - Installation et Configuration de T-Pot

Pour cette étape, je vais installer et utiliser une machine Debian 10 avec une adresse ipv4 : 192.168.10.102

Installation de git pour cloner le projet

```
root@debian:~# sudo apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl patch
```

Commande suivante pour cloner T-pot : git clone https://github.com/dtag-dev-sec/tpotce

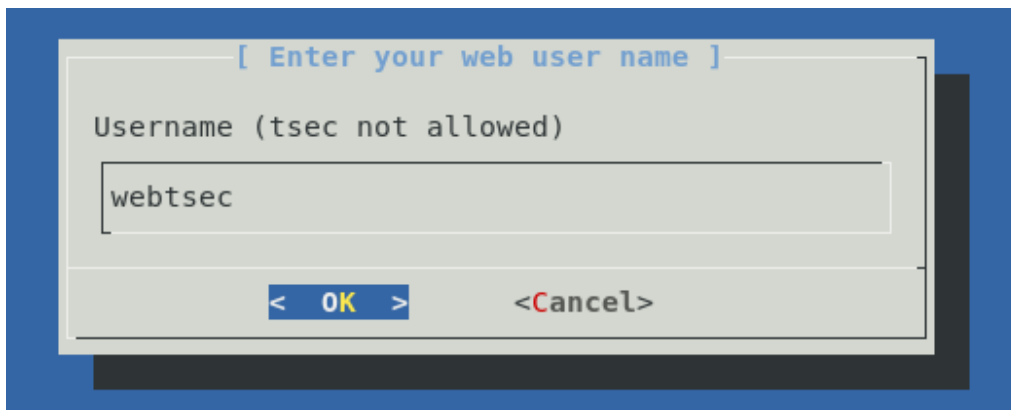
```
root@debian:~# sudo bash
root@debian:~# cd ~
root@debian:~# git clone https://github.com/dtag-dev-sec/tpotce
Cloning into 'tpotce'...
remote: Enumerating objects: 11392, done.
remote: Counting objects: 100% (162/162), done.
remote: Compressing objects: 100% (99/99), done.
Receiving objects: 80% (9114/11392), 58.72 MiB | 5.77 MiB/s
```

Et voici la commande pour l'installer : cd tpotce/iso/installer/ ./install.sh --type=user

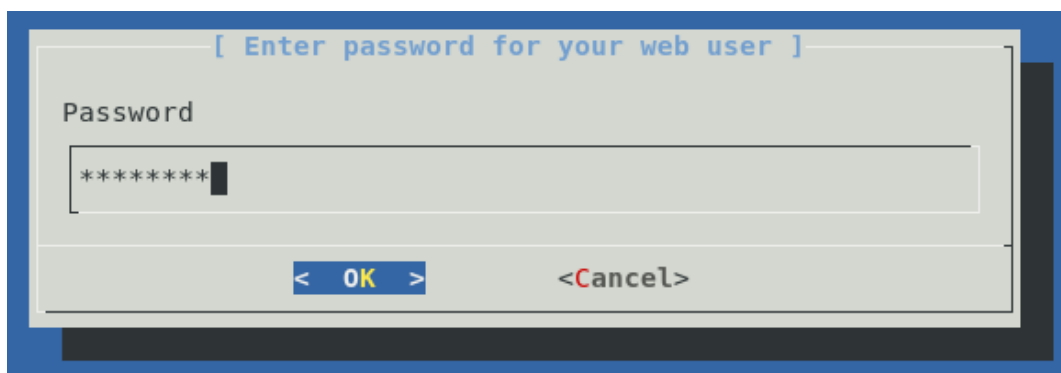
```
root@debian:~# cd tpotce/iso/installer/
root@debian:~/tpotce/iso/installer# ./install.sh --type=user

### Checking for root: [ OK ]
### Installing deps for apt-fast
```

Ensuite on tape «Y» pour continuer et on va choisir un nom d'utilisateur.



Ensuite il faut choisir un mot de passe.



Debian procedera ensuite a l'installation (C'est un peu long)



```
### Getting update information.
```

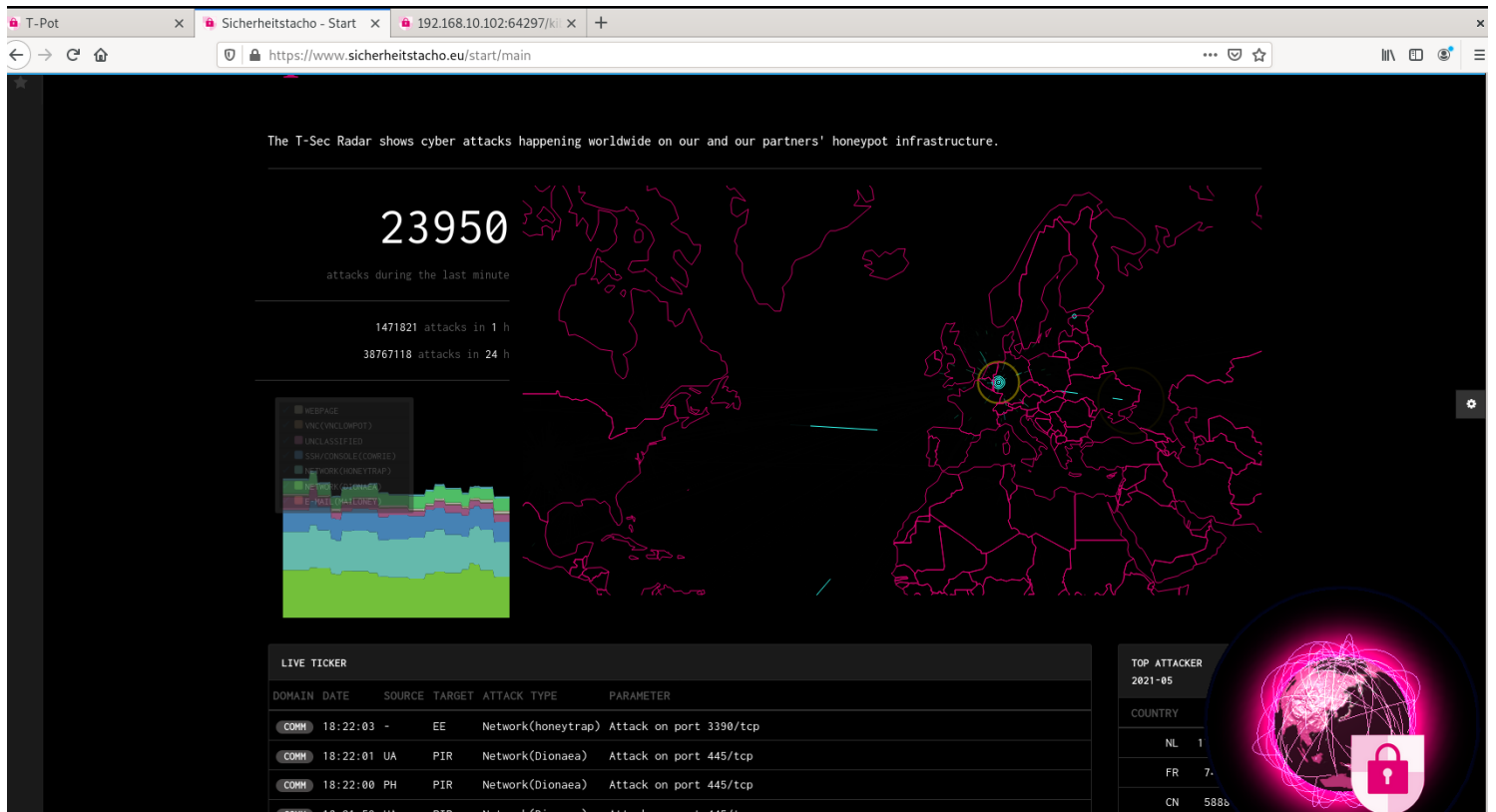
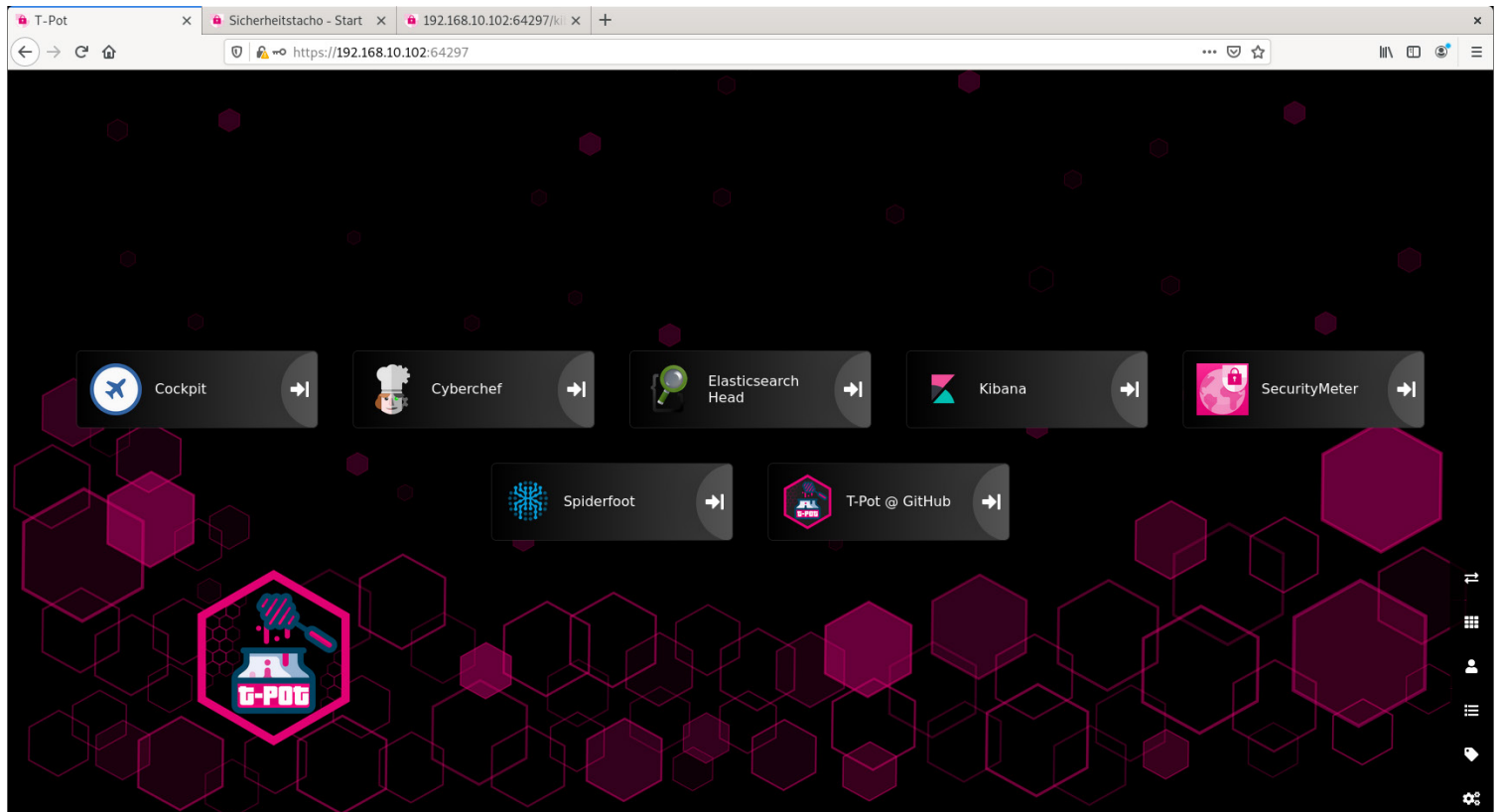
```
Hit:1 http://security.debian.org/debian-security buster/updates InRelease
Hit:2 http://deb.debian.org/debian buster InRelease
Hit:3 http://deb.debian.org/debian buster-updates InRelease
Reading package lists...
```

```
### Upgrading packages.
```

```
info: Trying to set 'docker.io/restart' [boolean] to 'true'
info: Loading answer for 'docker.io/restart'
info: Trying to set 'debconf/frontend' [select] to 'noninteractive'
info: Loading answer for 'debconf/frontend'
[apt-fast 16:25:18]
[apt-fast 16:25:18]Working... this may take a while.
```

Après installation, votre machine redemarrera et il vous suffira d'ouvrir votre navigateur web et entrer l'adresse suivante :  
`https://<votre adresse ip>:64297`

Vous aller devoir rentrer le login et le password rentré précédemment et voici l'interface suur laquelle vous aller arriver



# IX - Conclusion

Le document n'est malheureusement pas complet par faute de connaissances et de temps. On a essayé de faire le plus possible et voilà le document que cela donne. Je sais que certaines de ces installations ne fonctionnent pas forcément à 100% mais je ne pouvais laisser ce document vide.

Merci d'avoir lu.

Sources : Mr LAFAGE

<https://www.pc2s.fr/pfsense-installation-et-configuration/>

<https://github.com/telekom-security/tpotce>

<https://cyber-99.co.uk/t-pot-honeypot-framework-installation>

<https://computerz.solutions/pfsense-portail-captif/#:~:text=Mise%20en%20place%20du%20portail,actif%20puis%20configurer%20cette%20zone.>

