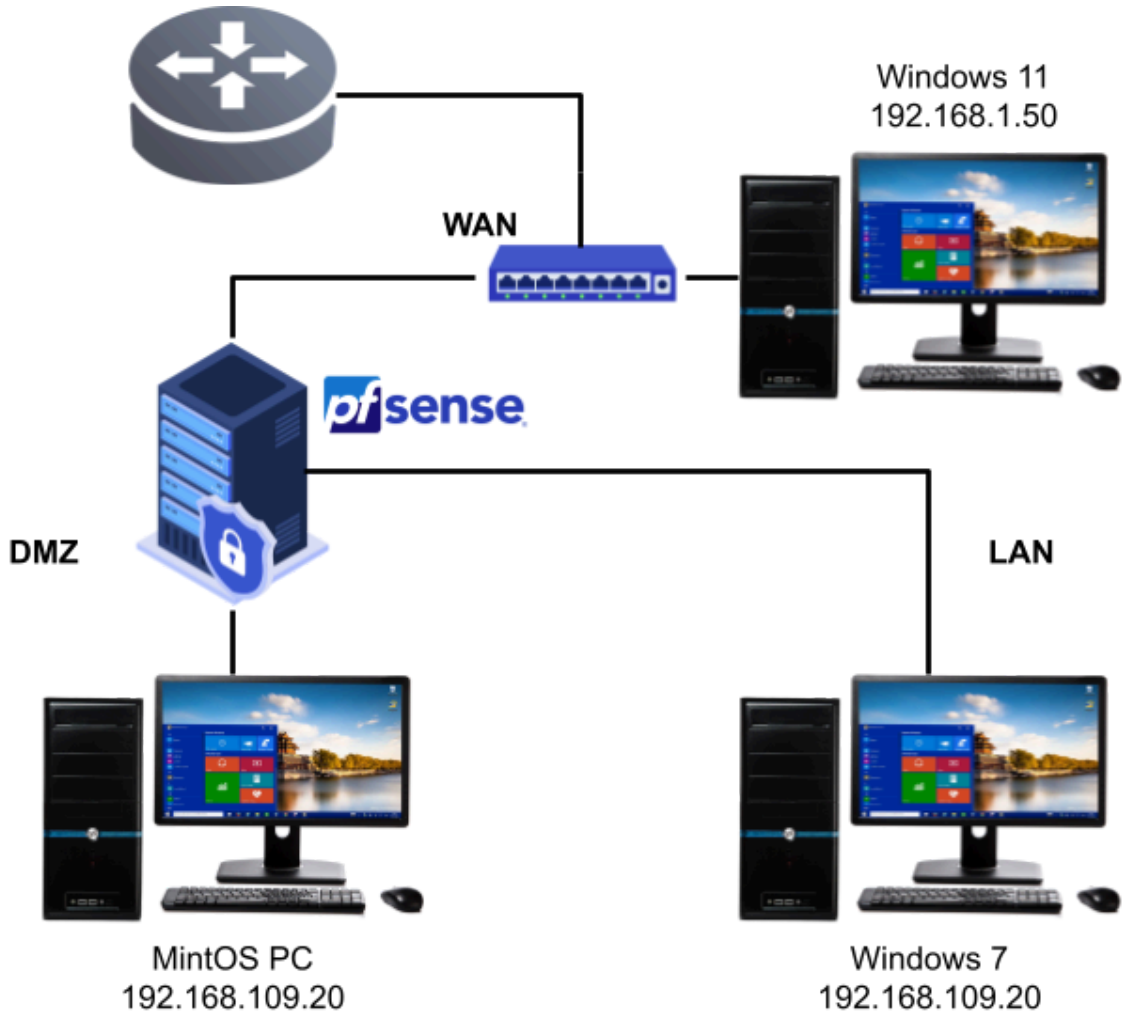
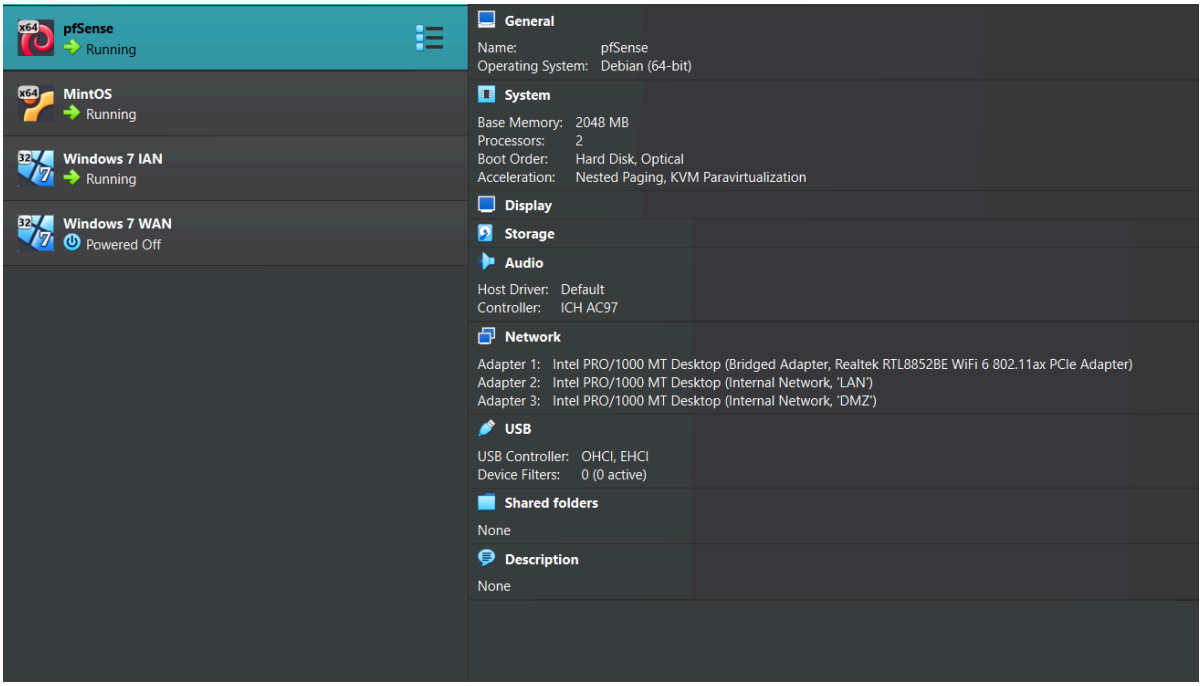
Module : Sécurité Informatique
Workshop - Fascicule 4
Installation et Configuration de pfSense

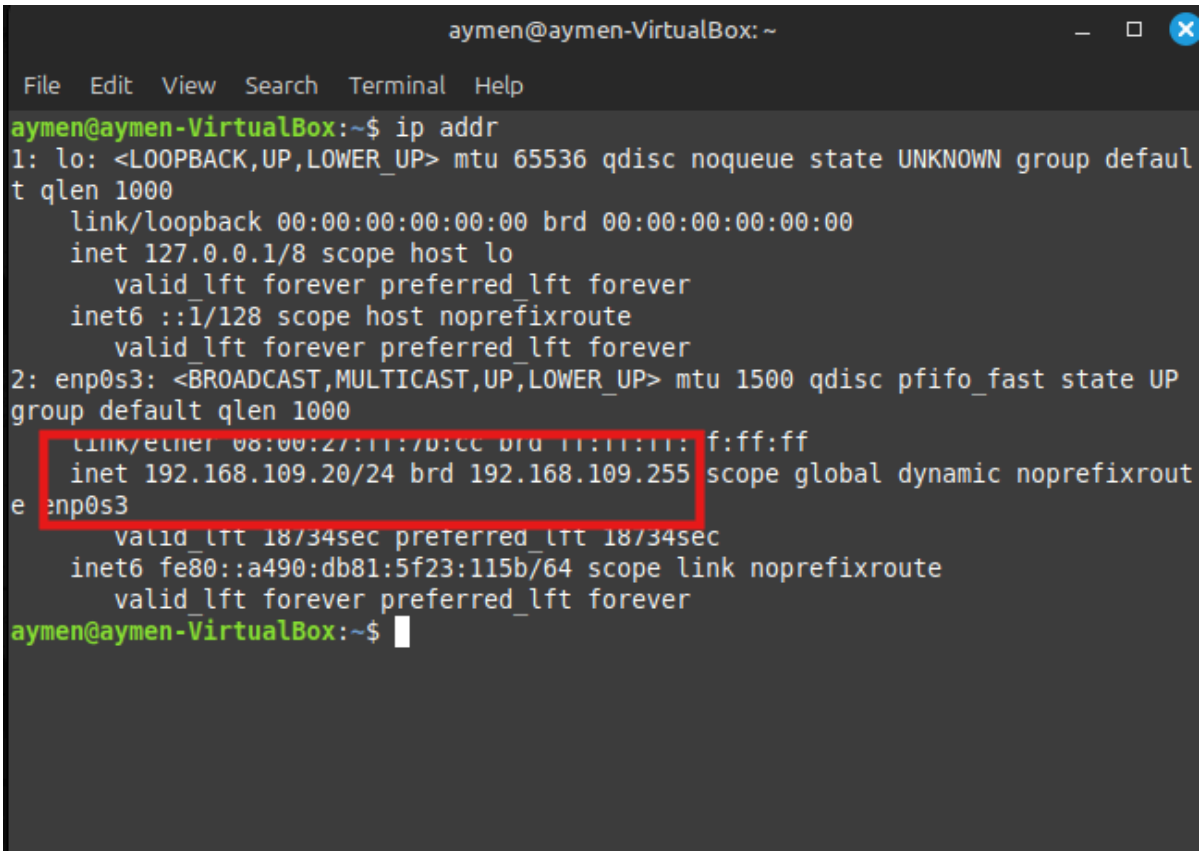
Voici notre architecture:



Voici notre architecture a niveau de VirtualBox:



Voici l'adress ip de la machine linux à niveau de réseau DMZ:



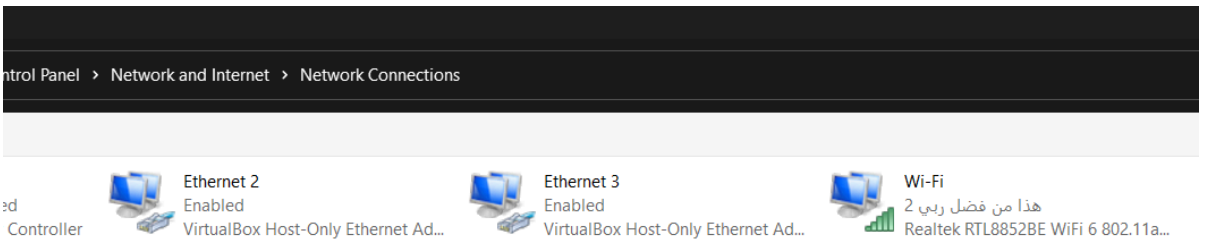
Voici l'adress ip de la machine windows à niveau de réseau LAN:

```
C:\Windows\system32\cmd.exe

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : home.arpa
   Link-local IPv6 Address . . . . . [redacted]32c0:d4cc%11
   IPv4 Address. . . . . . . . . . . 192.168.108.21
   Subnet Mask . . . . . . . . . . . [redacted]
   Default Gateway . . . . . . . . . : 192.168.108.1

Tunnel adapter isatap.home.arpa:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home.arpa

Tunnel adapter isatap.{70B6AE1B-EDC6-4B82-9379-F71629D037CD}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{99F66C79-F867-468C-BEFC-402770B57A47}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\vboxuser>
```

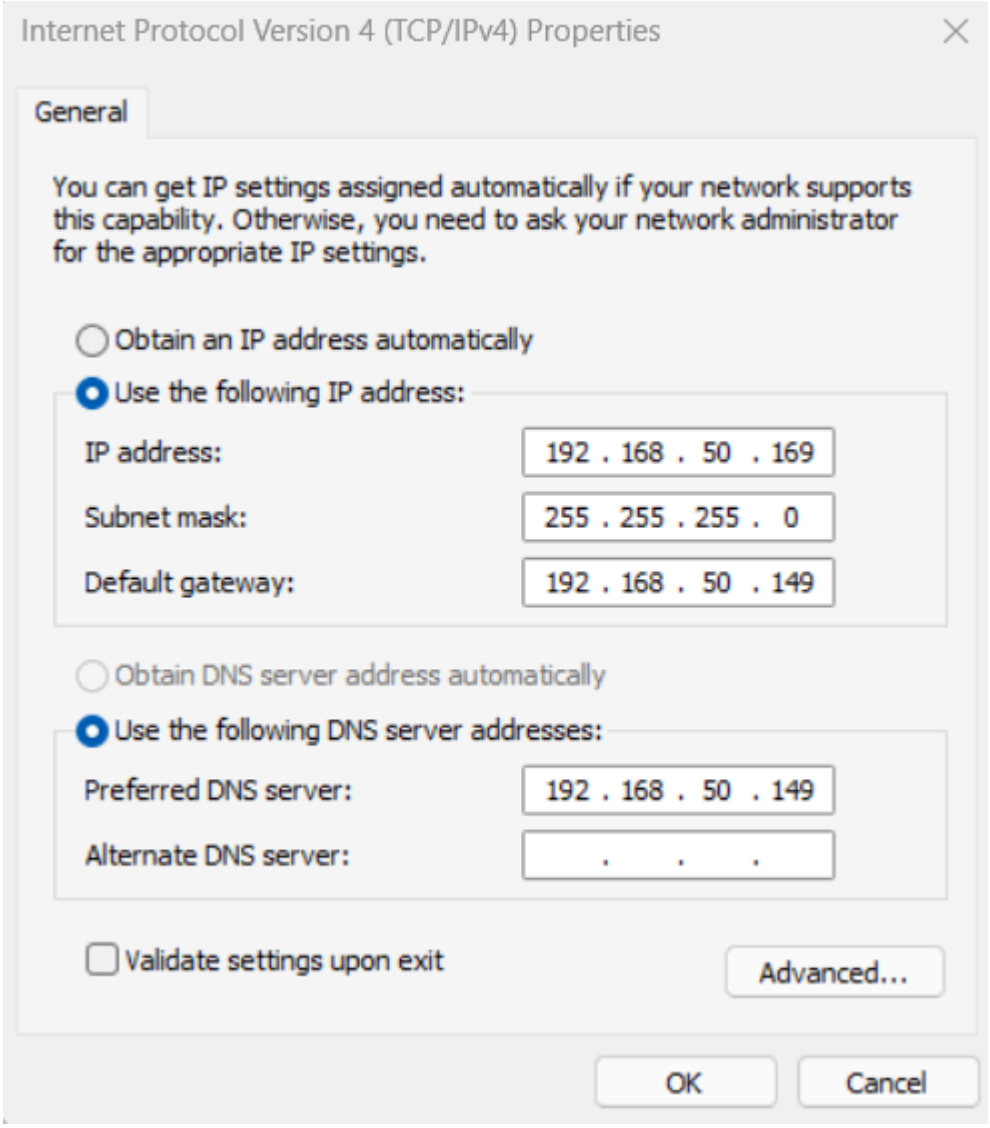
Voici la terminal de la machine pfSense qui indique que on bien configuré les trois réseaux (WAN, LAN, DMZ):

```
Enter an option:


FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 21cdff461d85c41ee247

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.60/24
 LAN (lan)       -> em1        -> v4: 192.168.108.1/24
 OPT1 (opt1)     -> em2        -> v4: 192.168.109.1/24

 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:
```

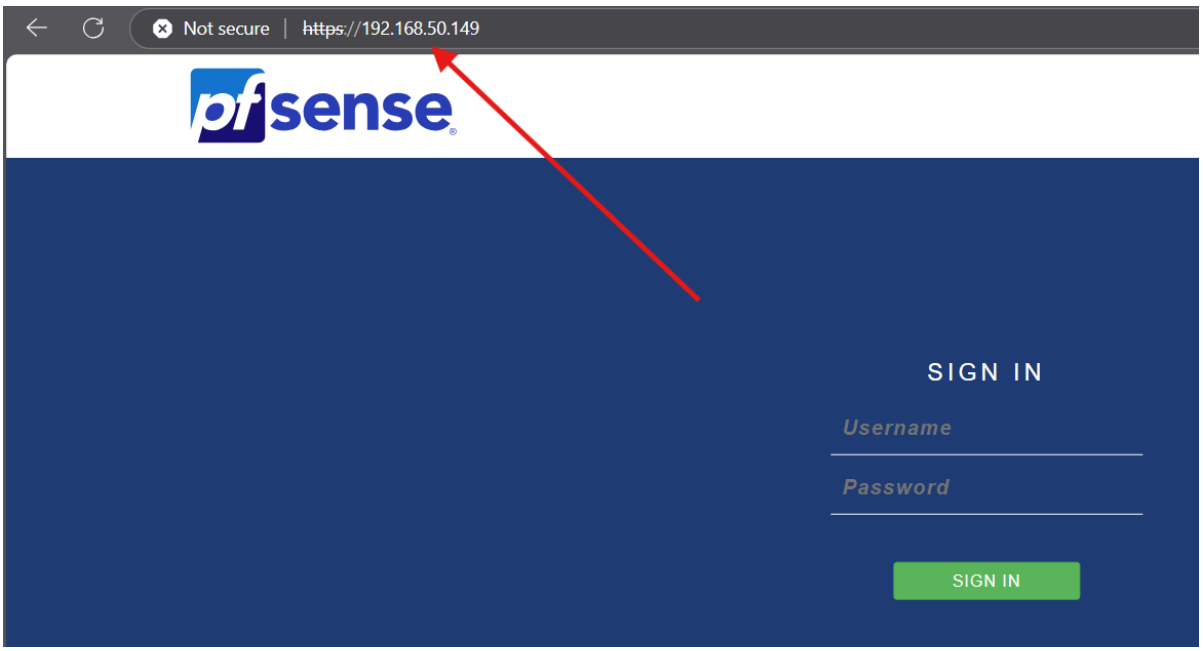
Voici notre liste des connection réseaux au niveau de panneau de configuration:



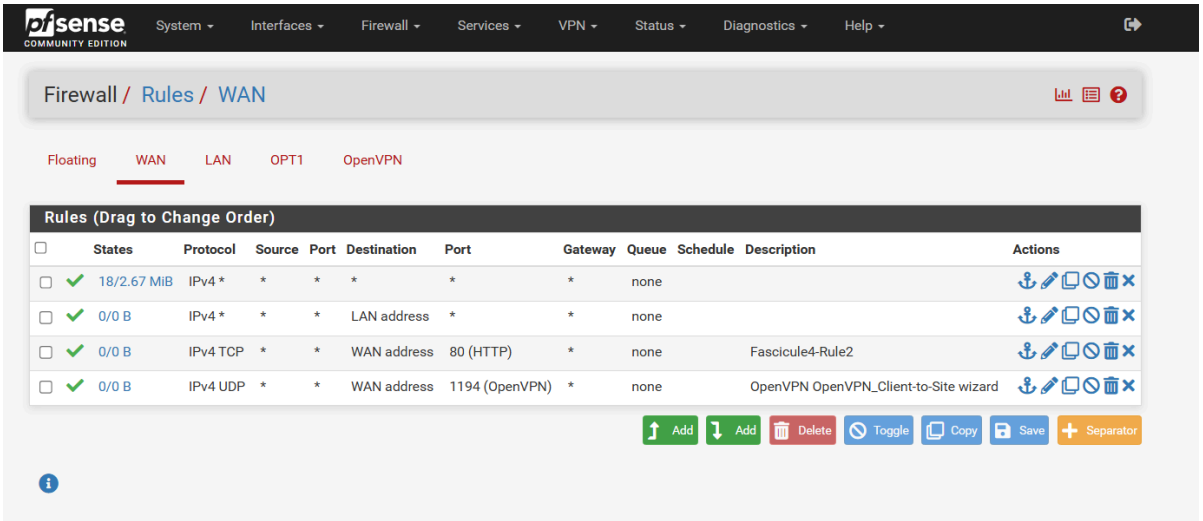
Voici notre configuration réseau de la machine windows 11 (WAN) pour que l'on peut accéder au pfSense.



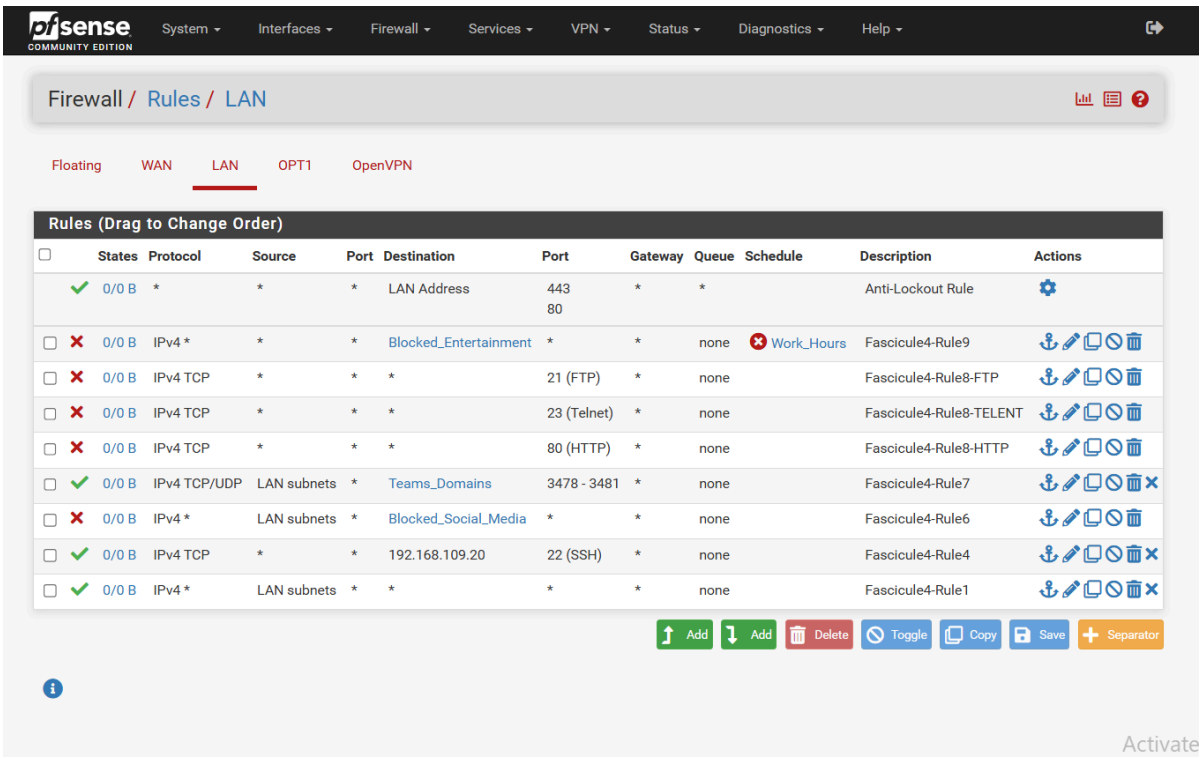
Voici l'interface de pfSense au niveau de la pc windows 10 lorsque on tape l'adresse du passerelle par défaut dans le navigateur:



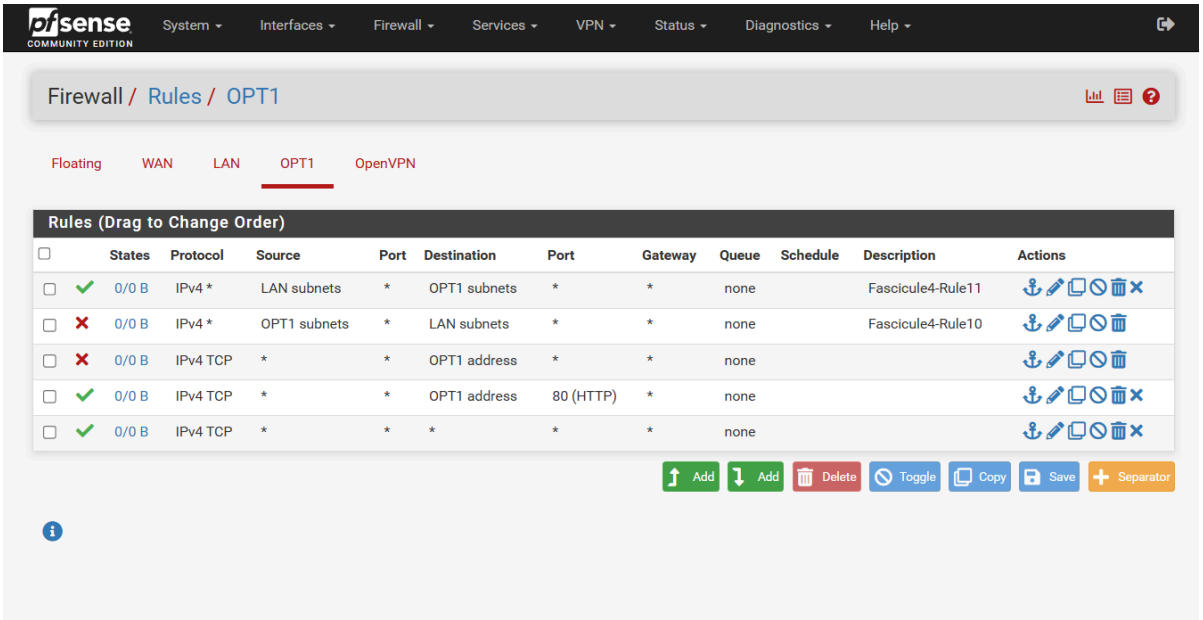
Voici la liste de rules au niveau de l'interface WAN:



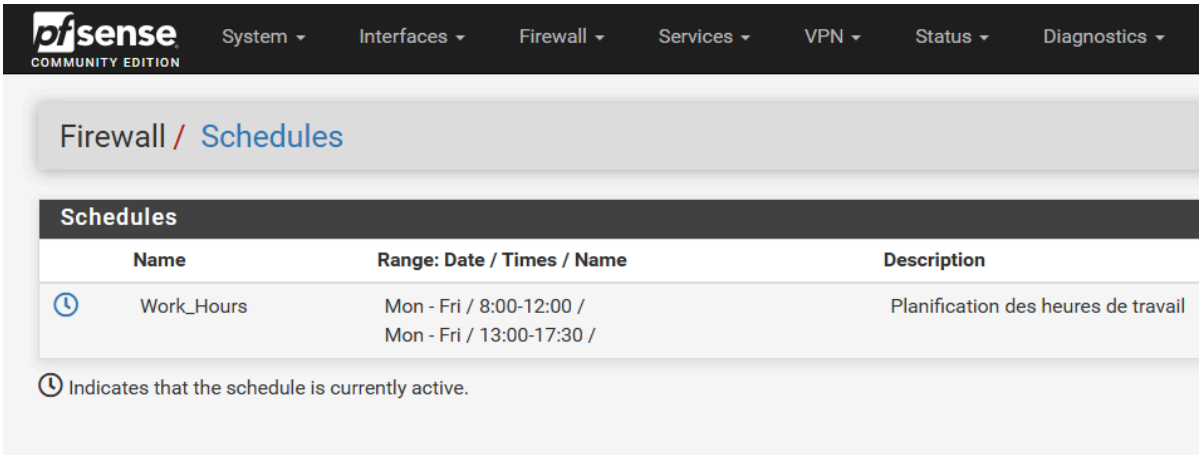
Voici la liste de rules au niveau de l'interface LAN:



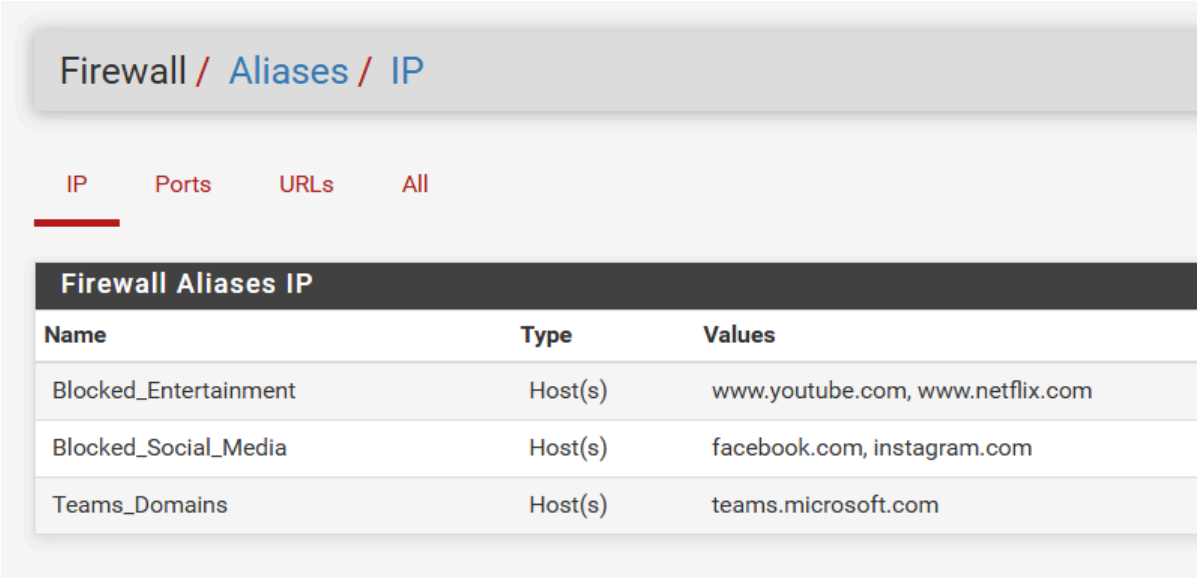
Voici la liste de rules au niveau de l'interface DMZ:



Voici la liste de schedules du notre firewall:



Voici la liste de hostnames alias utilisé dans notre rules du notre firewall:



Workshop - Fascicule 5
Sécurité Informatique
Mettre en place une solution IDS et Mettre en place une solution VPN

Voici la liste packages installe au niveau de pfSense:

System / Package Manager / Installed Packages

Installed Packages | Available Packages

Installed Packages

	Name	Category	Version	Description	Actions
✔	openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software. Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01	
✔	snort	security	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.20_8	

= Update ✔ = Current

= Remove = Information = Reinstall

Newer version available

Package is configured but not (fully) installed or deprecated

Voici notre configuration Snort:

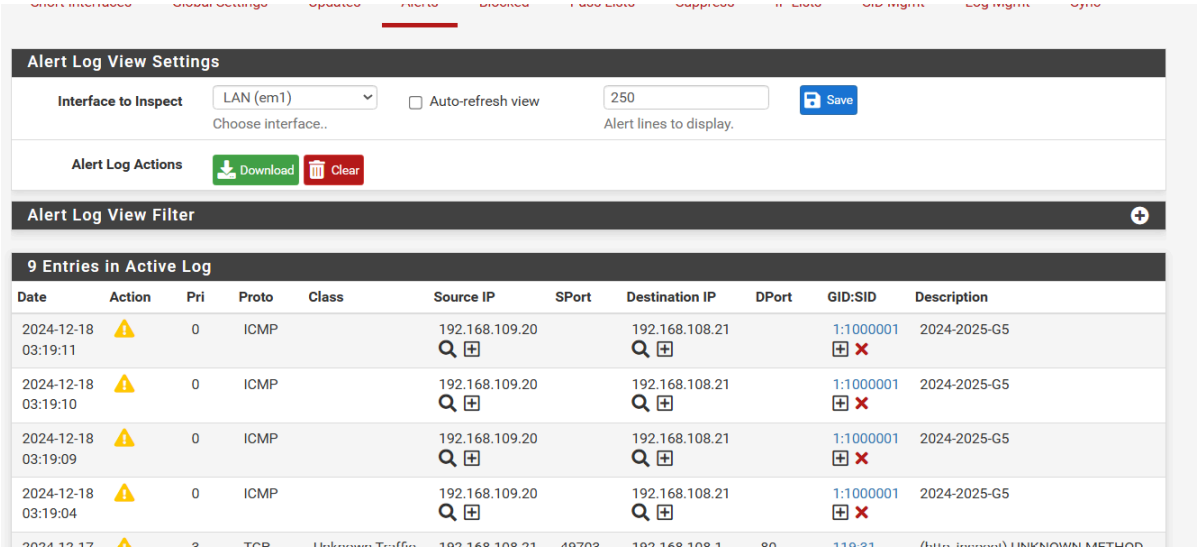
Services / Snort / Interfaces

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress

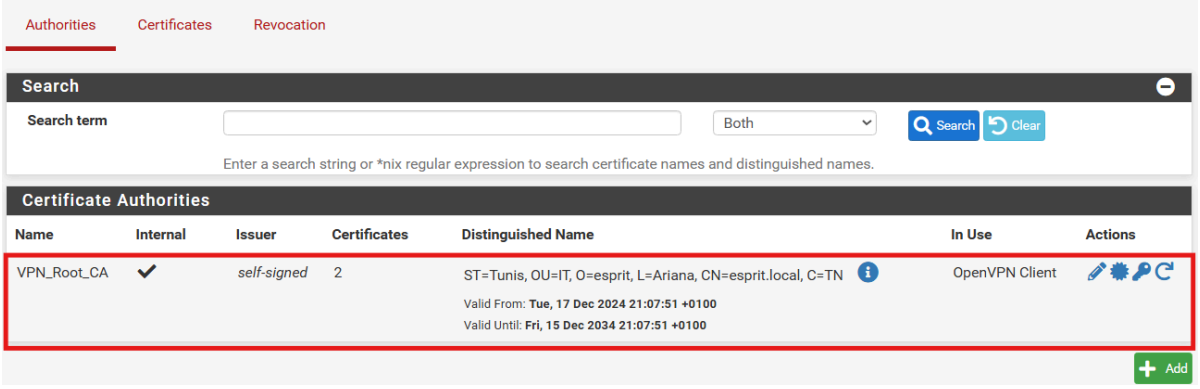
Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode
☐	LAN (em1)		AC-BNFA	DISABLED

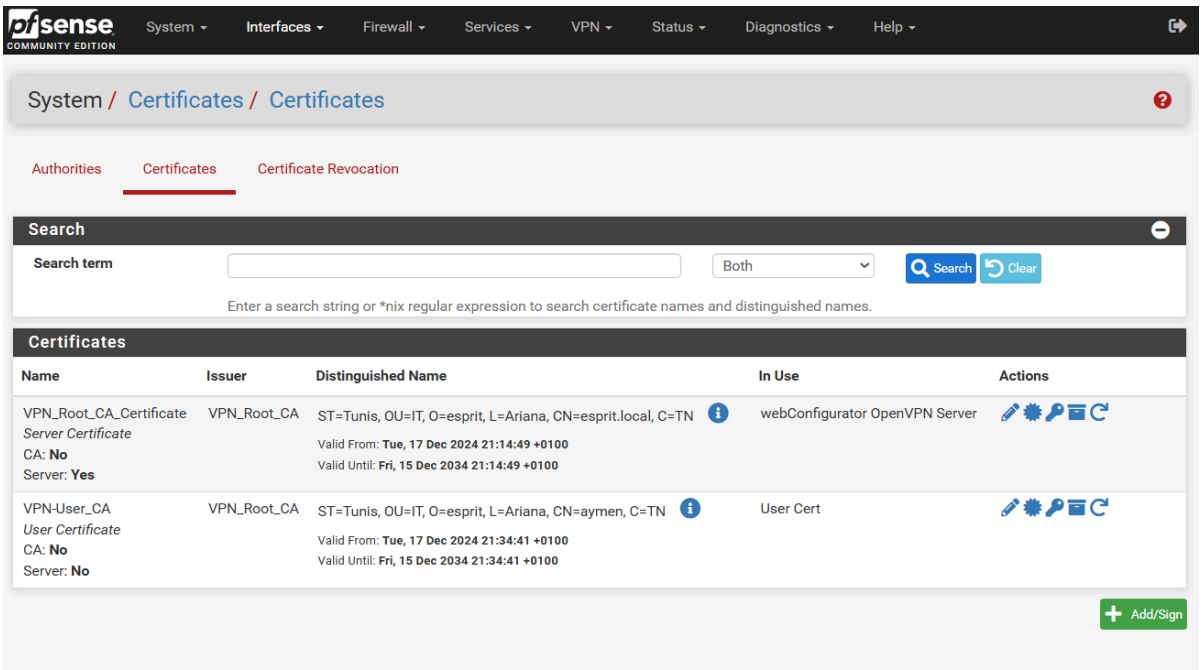
Voici la liste des alerts après le test:



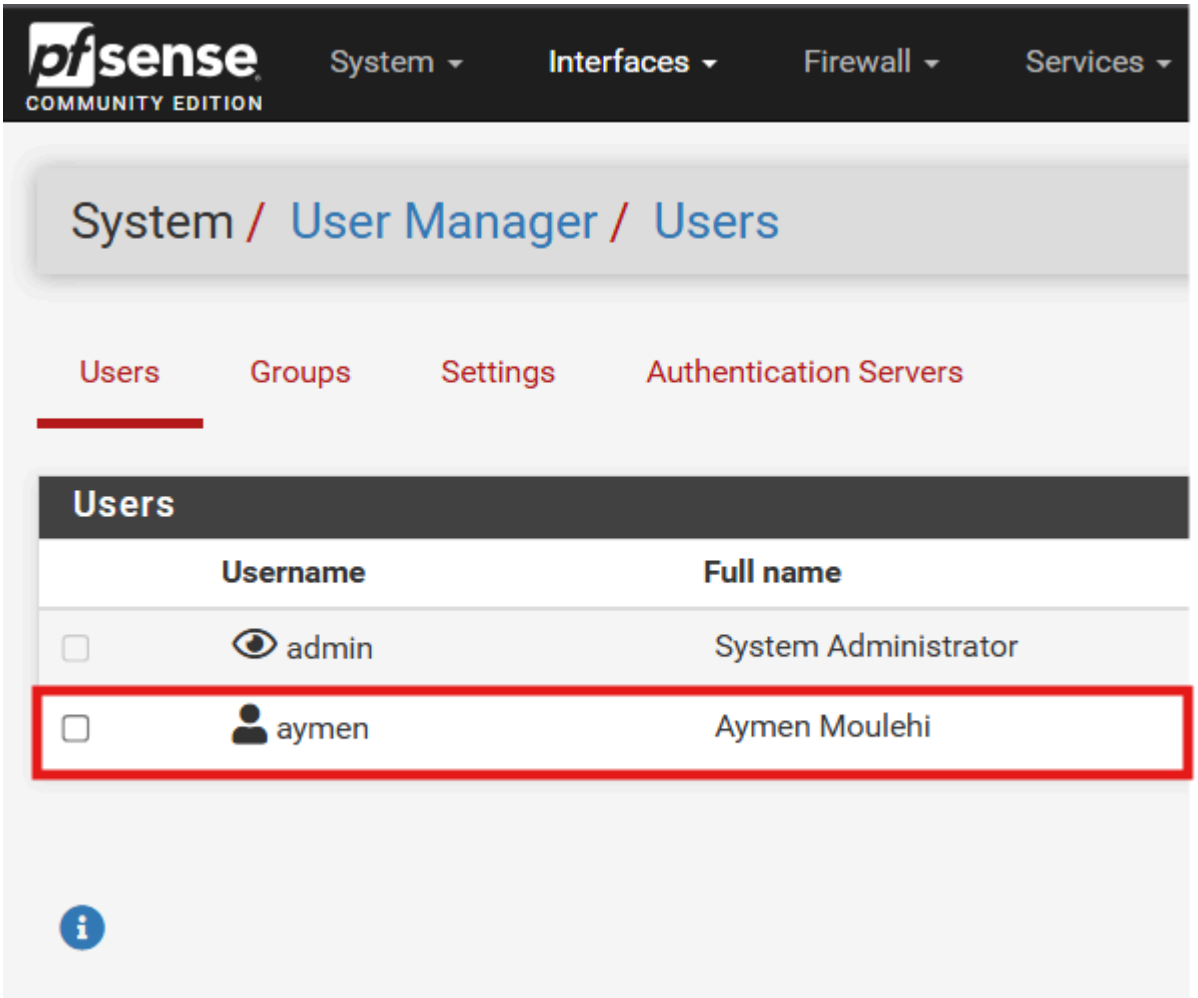
Voici notre Authoritiy pour la certification:



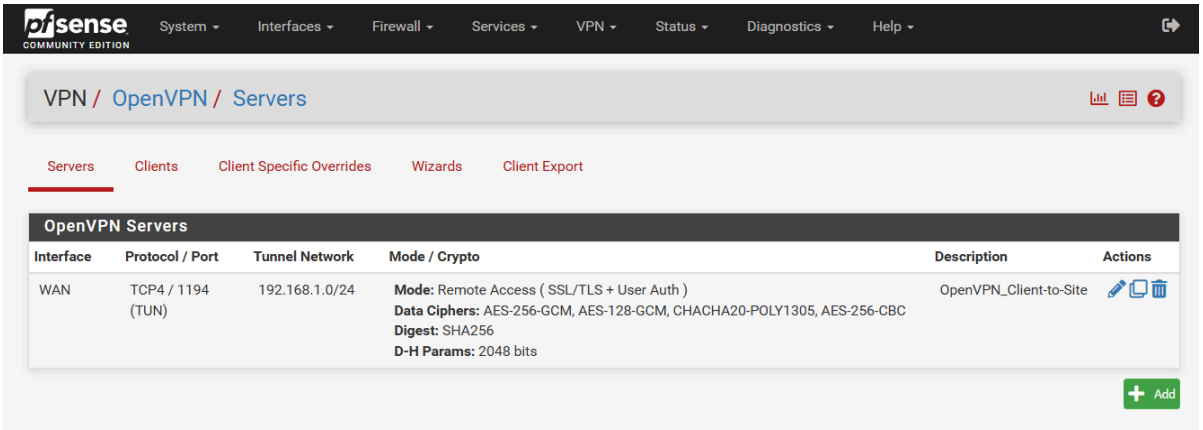
Voici notre certification server et user pour OpenVPN:



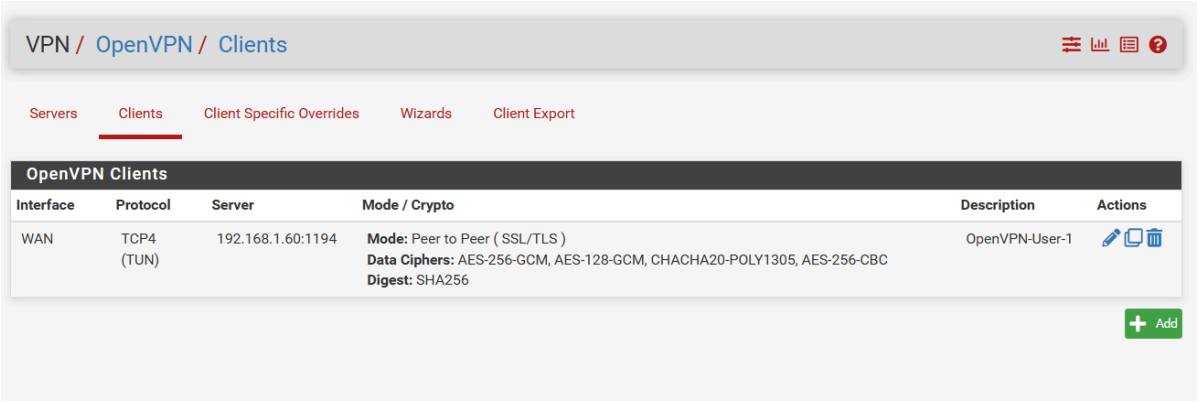
Voici notre user pour OpenVPN:



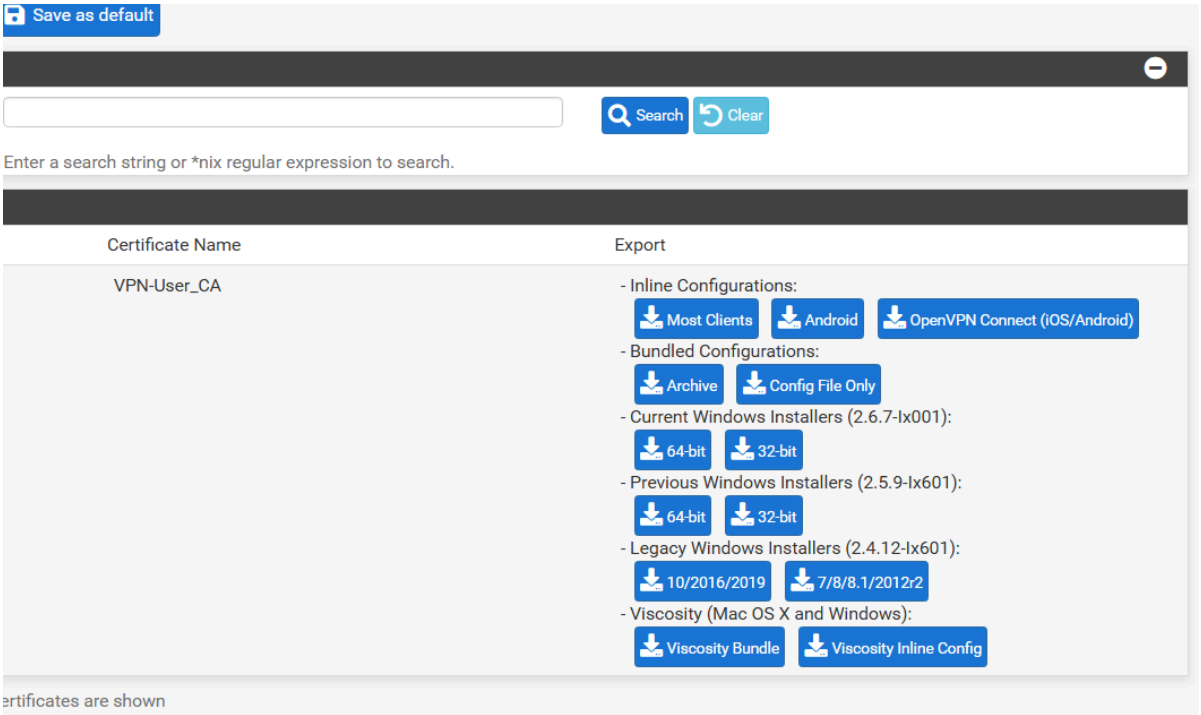
Voici la configuration server pour OpenVPN:



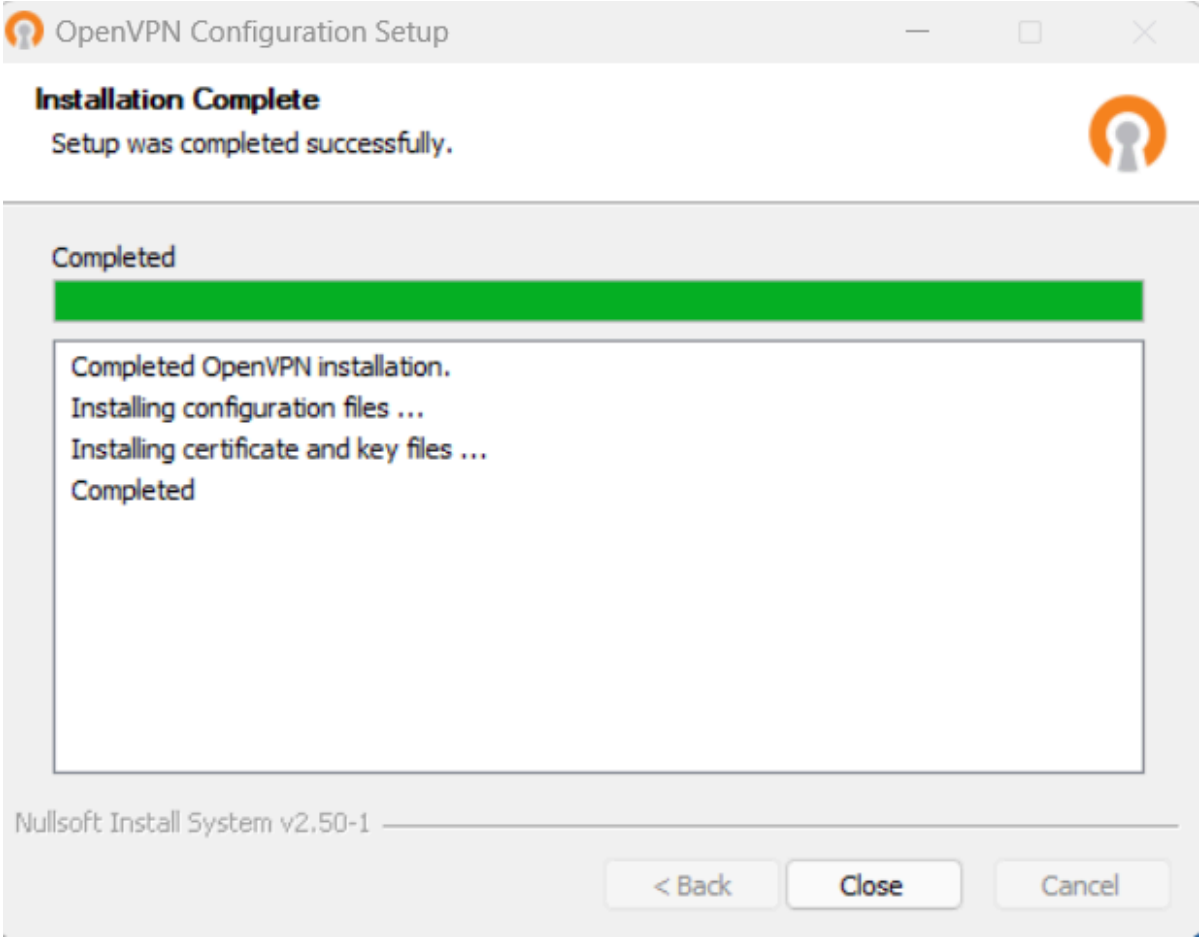
Voici la configuration client pour OpenVPN:



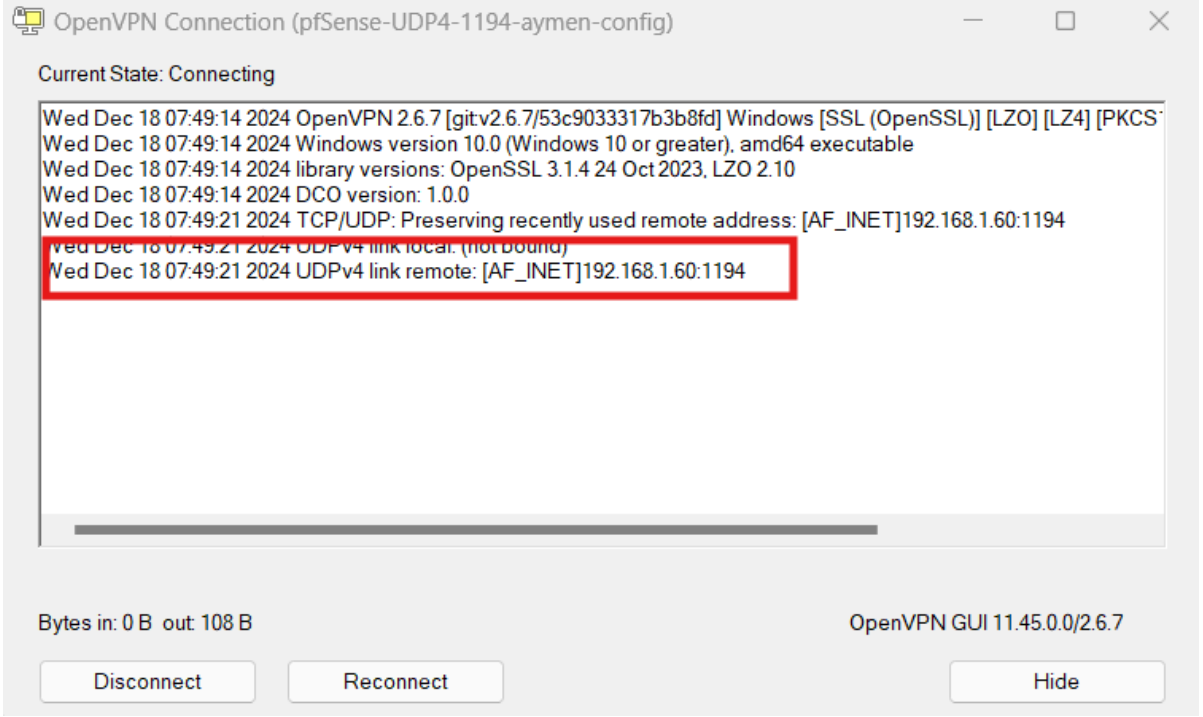
Voici la page du export dans pfSense:



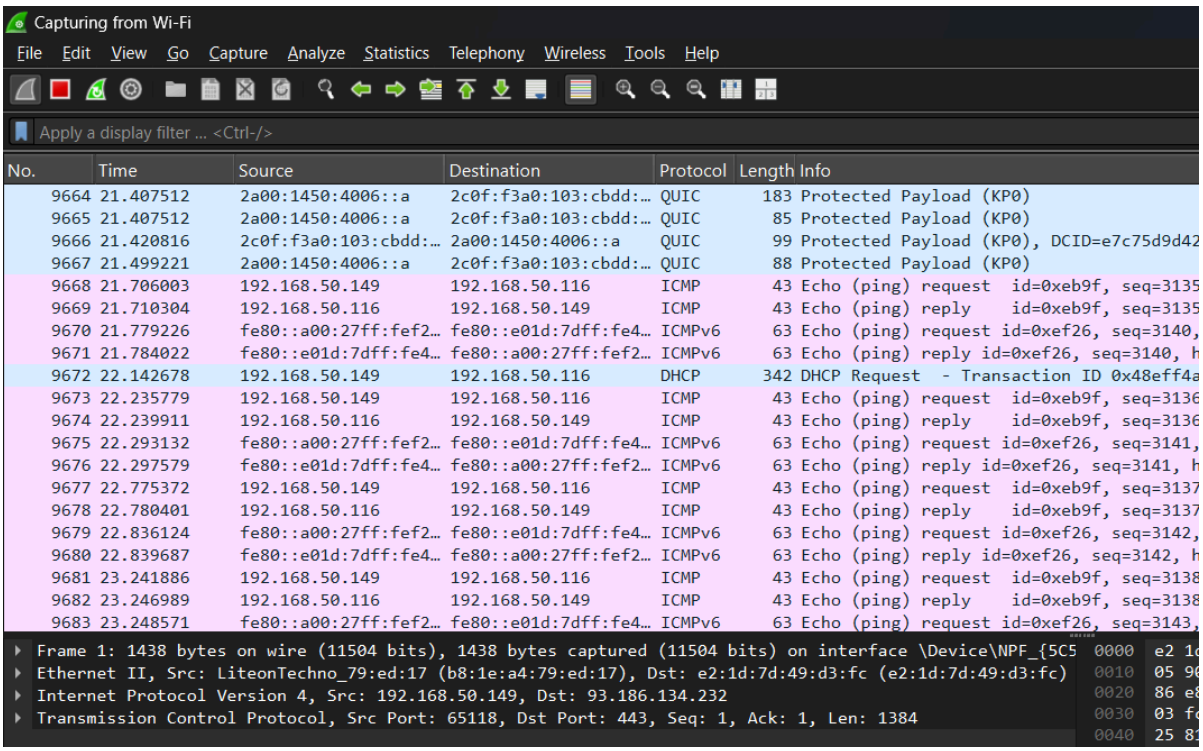
Voici l' application OpenVPN bien installé dans la machine windows 11:



Voici la machine windows est bien connecté au serveur VPN:



Voici une capture wireshark pour le trafic au niveau l'interface Wifi (Bridge - WAN):



Workshop - Fascicule 6
Sécurité Informatique
Réaliser deux attaques Web

Installer Docker sur Linux:

```
┌──(moataz㉿kali)-[~]
└─$ sudo apt install docker-cli
```

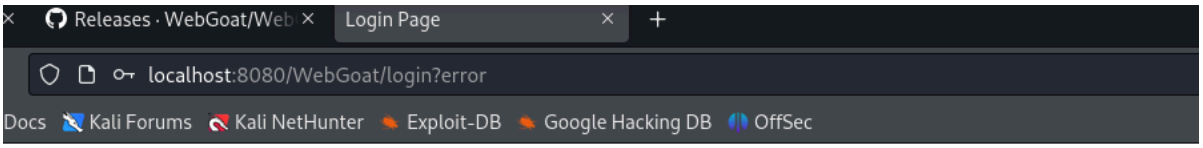
Installation de Webgoat:

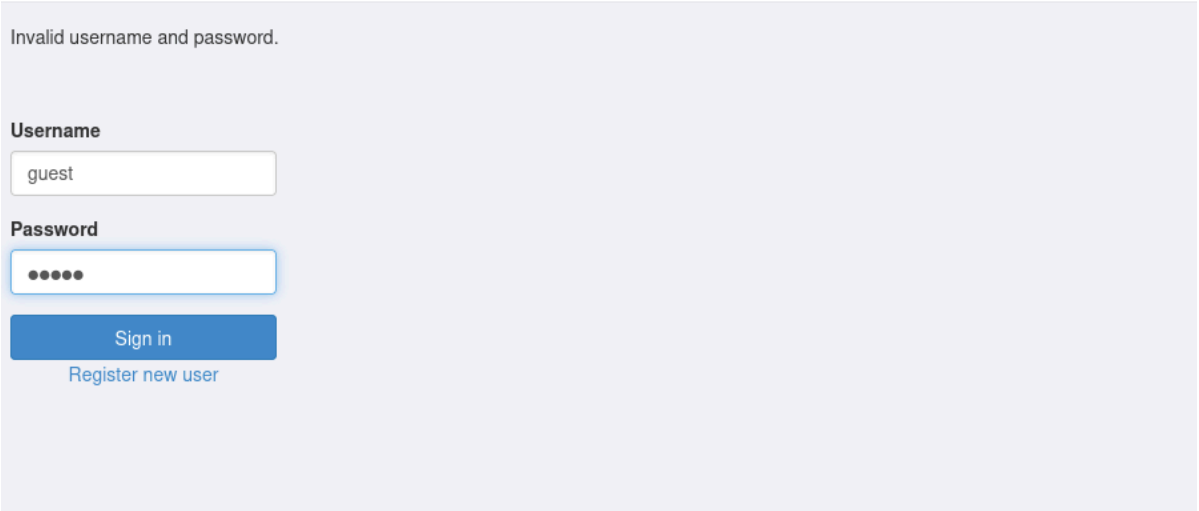
```
┌──(moataz㉿kali)-[~]
└─$ sudo docker pull webgoat/goatandwolf
Using default tag: latest
latest: Pulling from webgoat/goatandwolf
f8416d8bac72: Downloading  642.3kB/31.37MB
86ae0b0c4c13: Downloading  736.5kB/1.582MB
7333045f8c26: Downloading  540.7kB/185.2MB
8a5f0348f955: Waiting
a553e7433d6c: Waiting
ddda7d9cdca5: Waiting
4cca113b9964: Waiting
e4e2f5270c00: Waiting
e535ddd94a9f: Waiting
48cd64625d9e: Waiting
ba3693fa8f49: Waiting
```

Ensuite, exécuter le container:

```
┌──(moataz㉿kali)-[~]
└─$ sudo docker run -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 -e TZ=Europe/Amsterdam we
bgoat/goatandwolf

[sudo] password for moataz:
Starting nginx: nginx.
Starting WebGoat ...
Starting WebWolf ...
16:28:07.842 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args: --web
goat.build.version=8.2.2,--server.address=0.0.0.0

  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::                (v2.4.3)

2024-12-15 16:28:11.170  INFO 23 --- [           main] org.owasp.webgoat.StartWebGoat
     : Starting StartWebGoat v8.2.2 using Java 16.0.2 on 41292a79ddda with PID 23 (/home/we
bgoat/webgoat.jar started by webgoat in /home/webgoat)
2024-12-15 16:28:11.172 DEBUG 23 --- [           main] org.owasp.webgoat.StartWebGoat
     : Running with Spring Boot v2.4.3, Spring v5.3.4
2024-12-15 16:28:11.173  INFO 23 --- [           main] org.owasp.webgoat.StartWebGoat
     : No active profile set, falling back to default profiles: default
Browse to http://localhost to get started
       main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repos
itories in DEFAULT mode.
2024-12-15 16:28:17.970  INFO 23 --- [           main] .s.d.r.c.RepositoryConfigurationDele
gate : Finished Spring Data repository scanning in 690 ms. Found 2 JPA repository interface
```

Voici l'interface de notre application web:





Exécution de l'attaque SQL injection:

What is SQL?

SQL is a standardized (ANSI in 1986, ISO in 1987) programming language which is used for managing relational databases and performing

A database is a collection of data. The data is organized into rows, columns and tables, and indexed to make finding relevant information mo

Example SQL table containing employee data; the name of the table is 'employees':

Employees Table

userid	first_name	last_name	department	salary	auth_tan
32147	Paulina	Travers	Accounting	$46.000	P45JSI
89762	Tobi	Barnett	Development	$77.000	TA9LL1
96134	Bob	Franco	Marketing	$83.700	LO9S2V
34477	Abraham	Holman	Development	$50.000	UU2ALK
37648	John	Smith	Marketing	$64.350	3SL99A

A company saves the following employee information in their databases: a unique employee number ('userid'), last name, first name, departr company.

SQL queries can be used to modify a database table and its index structures and add, update and delete rows of data.

There are three main categories of SQL commands:

- Data Manipulation Language (DML)
- Data Definition Language (DDL)
- Data Control Language (DCL)

Each of these command types can be used by attackers to compromise the confidentiality, integrity, and/or availability of a system. Proceed

If you are still struggling with SQL and need more information or practice, you can visit http://www.sqlcourse.com/ for free and interactive onli

It is your turn!

Look at the example table. Try to retrieve the department of the employee Bob Franco. Note that you have been granted full administrator pri

SQL query: SELECT * FROM Employees WHERE last_name = 'Smith';

Submit

You have succeeded!

SELECT * FROM Employees WHERE last_name = 'Smith';

USERID	FIRST_NAME	LAST_NAME	DEPARTMENT	SALARY	AUTH_TAN
37648	John	Smith	Marketing	64350	3SL99A

Exécution de l'attaque XSS Cross Site Scripting:

Cross Site Scripting

Show hints | Reset lesson

1 2 3 4 5 6 7 8 9 10 11 12

Try It! Reflected XSS

The goal of the assignment is to identify which field is susceptible to XSS.

It is always a good practice to validate all input on the server-side. XSS can occur when unvalidated user input gets used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with the attack script and post it to another website, email it, or otherwise get a victim to click on it.

An easy way to find out if a field is vulnerable to an XSS attack is to use the `alert()` or `console.log()` methods. Use one of them to find out which field is vulnerable.

Shopping Cart

Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	$0.00
Dynex - Traditional Notebook Case	27.99	1	$0.00
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	$0.00
3 - Year Performance Service Plan $1000 and Over	299.99	1	$0.00

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: 11<script>alert(1)</script>

Purchase

Seems like you tried to compromise our shop with an reflected XSS attack.
We do our... "best"... to prevent such attacks. Try again!