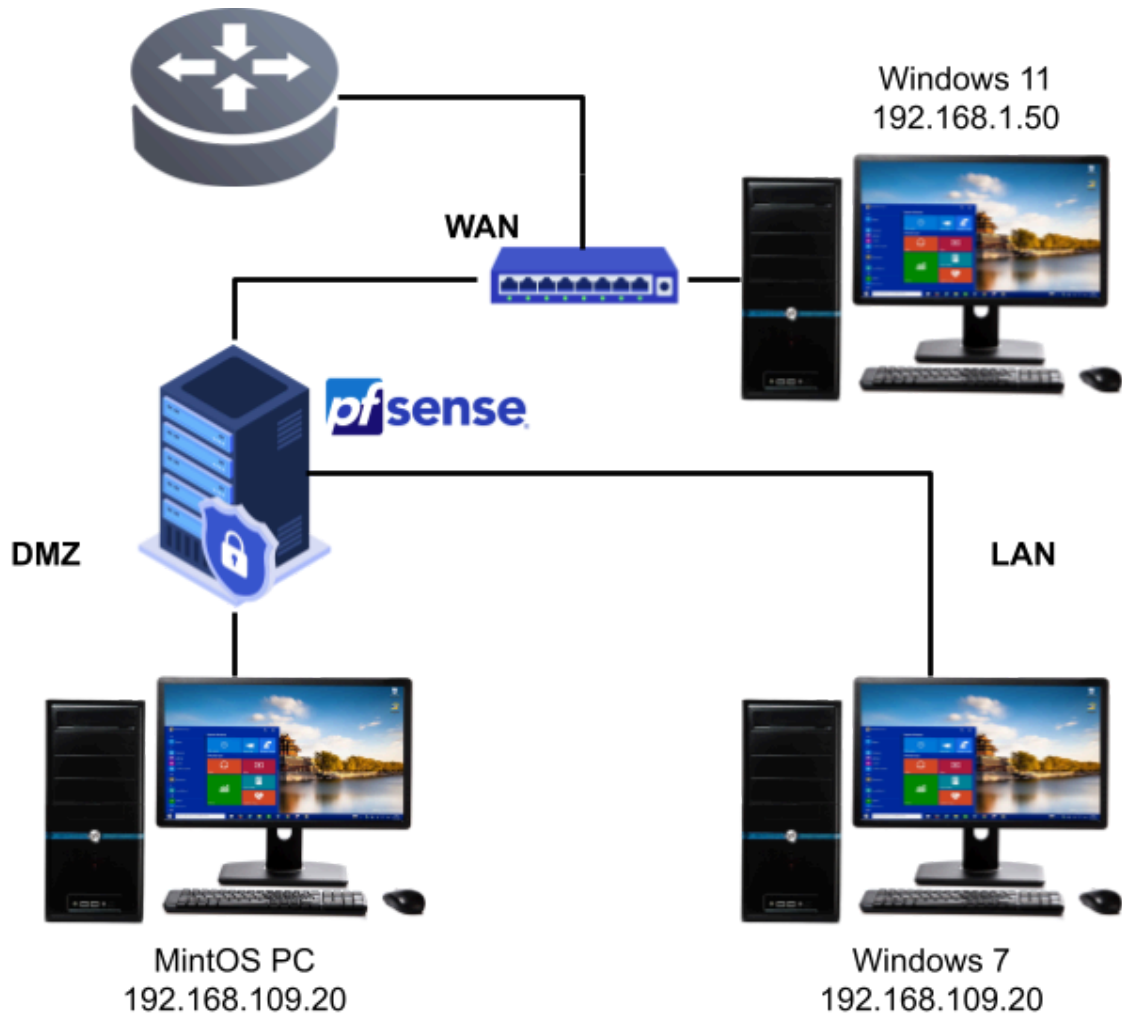
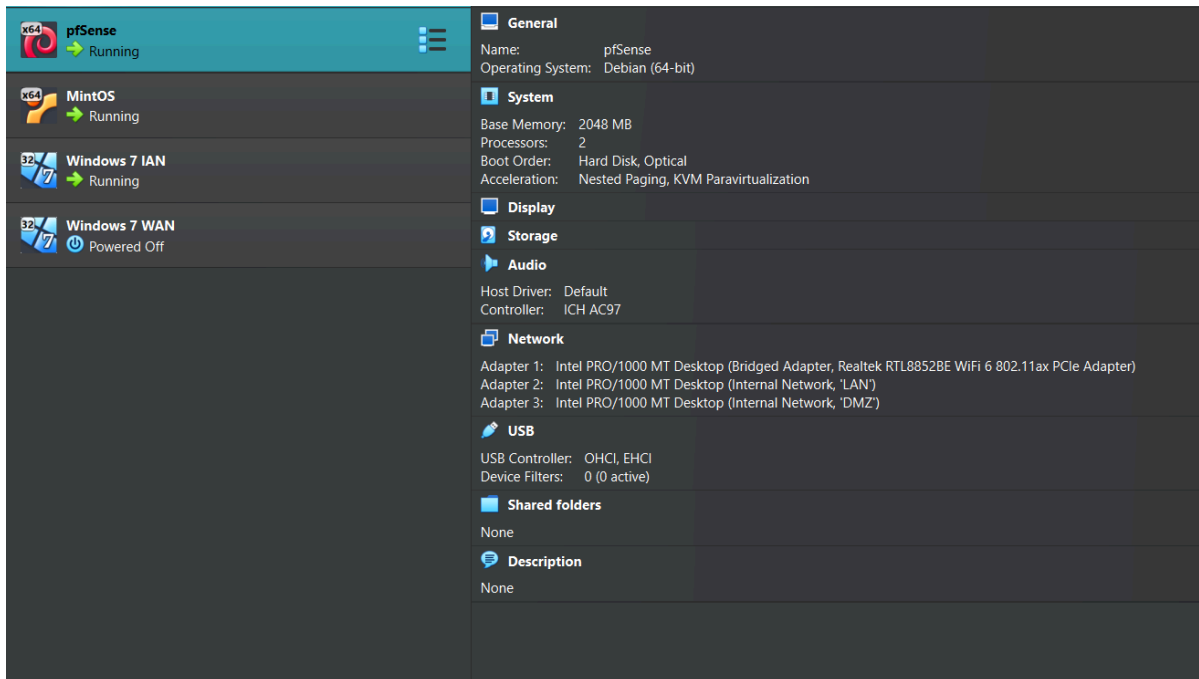


**Module : Sécurité Informatique**  
**Workshop - Fascicule 4**  
**Installation et Configuration de pfSense**

Voici notre architecture:



Voici notre architecture a niveau de VirtualBox:



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

```
aymen@aymen-VirtualBox: ~  
File Edit View Search Terminal Help  
aymen@aymen-VirtualBox:~$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 08:00:27:11:7b:cc brd ff:ff:ff:ff:ff:ff  
    inet 192.168.109.20/24 brd 192.168.109.255 scope global dynamic noprefixroute  
        valid_lft 18/34sec preferred_lft 18/34sec  
    inet6 fe80::a490:db81:5f23:115b/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
aymen@aymen-VirtualBox:~$
```

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 . . . . . : fe80::d37c:d113:32c0:d4cc%11
    IPv4 Address. . . . . : 192.168.108.21
    Subnet Mask . . . . . : 255.255.255.0
    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\uboxuser>
```

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

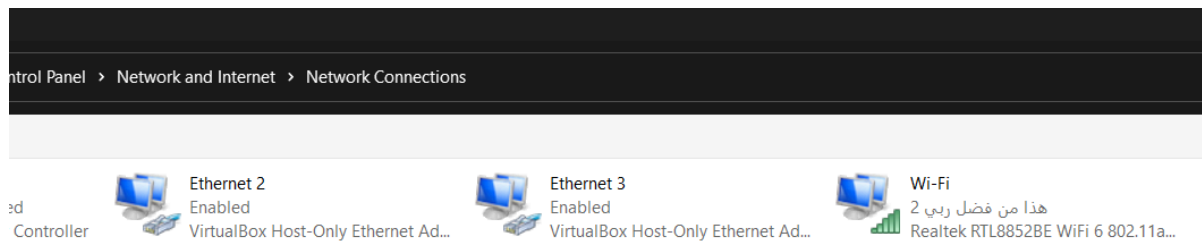
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

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

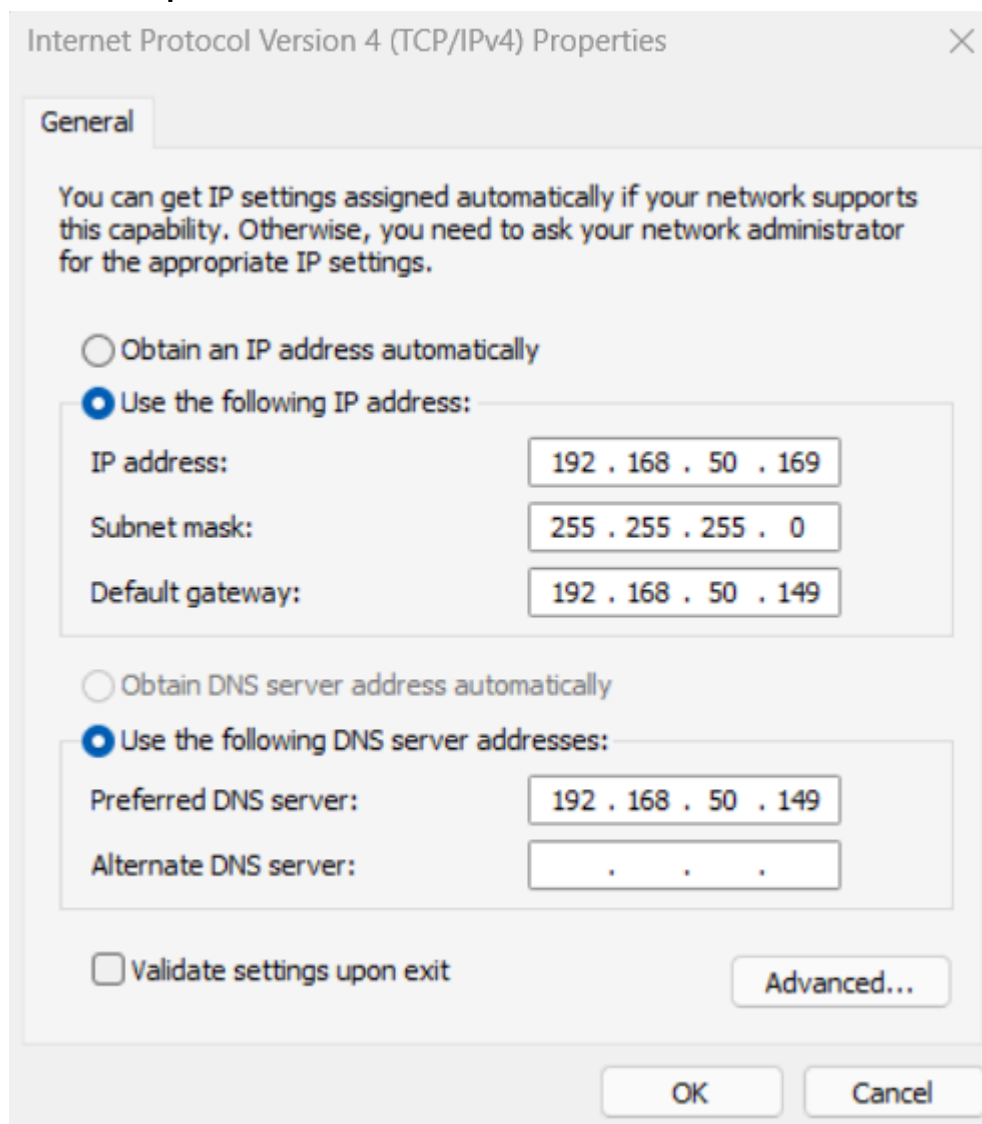
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable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

Enter an option: █
```

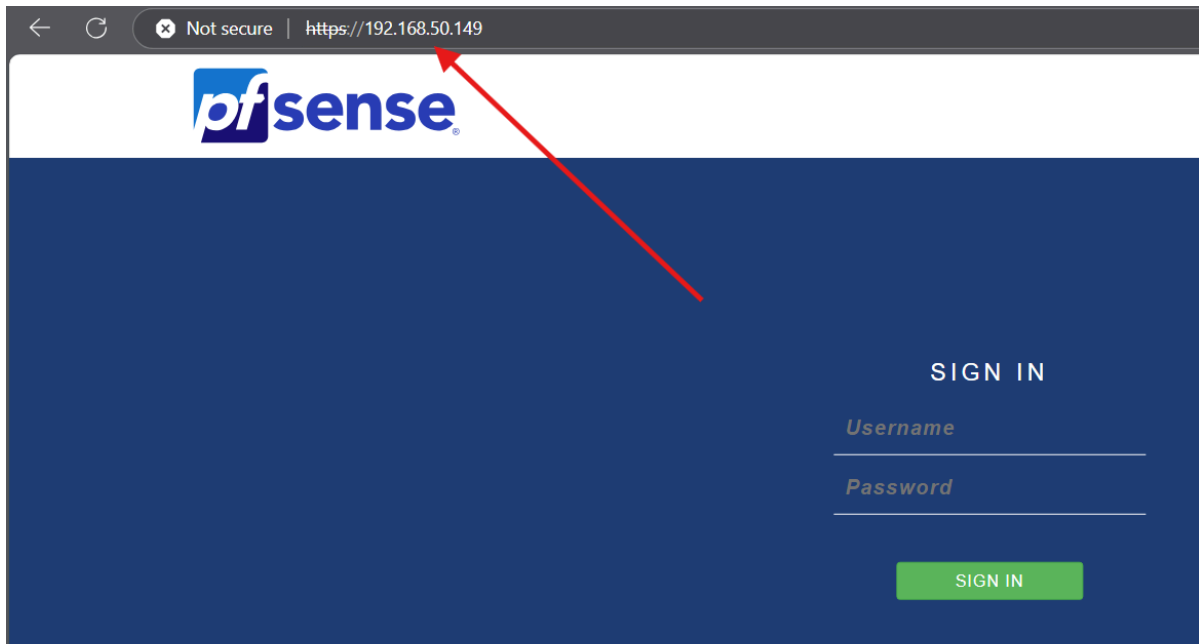
Voici notre liste des connection réseaux au niveau de panneau de configuration:



**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:

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / WAN

Floating **WAN** LAN OPT1 OpenVPN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 18/2.67 MIB	IPv4 *	*	*	*	*	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Refresh</a> <a href="#">Close</a>
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	LAN address	*	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Refresh</a> <a href="#">Close</a>
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none		Fascicule4-Rule2	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Refresh</a> <a href="#">Close</a>
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN OpenVPN_Client-to-Site wizard	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Refresh</a> <a href="#">Close</a>

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

[i](#)

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

pfSense  
COMMUNITY EDITION

System ▾  
Interfaces ▾  
Firewall ▾  
Services ▾  
VPN ▾  
Status ▾  
Diagnostics ▾  
Help ▾

Firewall / Rules / LAN

Floating   WAN   **LAN**   OPT1   OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	Blocked_Entertainment	*	*	none	Work_Hours	Fascicule4-Rule9	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	21 (FTP)	*	none		Fascicule4-Rule8-FTP	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	23 (Telnet)	*	none		Fascicule4-Rule8-TELENT	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Fascicule4-Rule8-HTTP	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN subnets	*	Teams_Domains	3478 - 3481	*	none		Fascicule4-Rule7	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	Blocked_Social_Media	*	*	none		Fascicule4-Rule6	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.109.20	22 (SSH)	*	none		Fascicule4-Rule4	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Fascicule4-Rule1	

Add   Add   Delete   Toggle   Copy   Save   Separator

Activate

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

pfSense  
COMMUNITY EDITION

System ▾  
Interfaces ▾  
Firewall ▾  
Services ▾  
VPN ▾  
Status ▾  
Diagnostics ▾  
Help ▾

Firewall / Rules / OPT1

Floating   WAN   LAN   **OPT1**   OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	OPT1 subnets	*	*	none		Fascicule4-Rule11	
<input type="checkbox"/>	0/0 B	IPv4 *	OPT1 subnets	*	LAN subnets	*	*	none		Fascicule4-Rule10	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	OPT1 address	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	OPT1 address	80 (HTTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	*	*	none			

Add   Add   Delete   Toggle   Copy   Save   Separator

Voici la liste de schedules du notre firewall:

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾

Firewall / Schedules

**Schedules**

	Name	Range: Date / Times / Name	Description
🕒	Work_Hours	Mon - Fri / 8:00-12:00 / Mon - Fri / 13:00-17:30 /	Planification des heures de travail

🕒 Indicates that the schedule is currently active.

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

Firewall / Aliases / IP

IP Ports URLs All

**Firewall Aliases IP**

Name	Type	Values
Blocked_Entertainment	Host(s)	www.youtube.com, www.netflix.com
Blocked_Social_Media	Host(s)	facebook.com, instagram.com
Teams_Domains	Host(s)	teams.microsoft.com

## Workshop - Fascicule 5

### Sécurité Informatique

### Mettre en place une solution IDS et Mettre en place une solution VPN

Voici la liste packages installé au niveau de pfSense:

System / Package Manager / Installed Packages

Installed PackagesAvailable 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 InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppress

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode
<input type="checkbox"/> LAN (em1)	✓	AC-BNFA	DISABLED

Voici la liste des alerts après le test:



Alert Log View Settings

Interface to Inspect

LAN (em1)

Auto-refresh view

250

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

9 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-12-18 03:19:11	⚠	0	ICMP		192.168.109.20		192.168.108.21		1:1000001	2024-2025-G5
2024-12-18 03:19:10	⚠	0	ICMP		192.168.109.20		192.168.108.21		1:1000001	2024-2025-G5
2024-12-18 03:19:09	⚠	0	ICMP		192.168.109.20		192.168.108.21		1:1000001	2024-2025-G5
2024-12-18 03:19:04	⚠	0	ICMP		192.168.109.20		192.168.108.21		1:1000001	2024-2025-G5
2024-12-17 22:00:00	⚠	0	TCP	Unknown Traffic	192.168.109.21	40702	192.168.109.1	80	110-21	(/bin/unknown) UNKNOWN METHOD

Voici notre Authoritiy pour la certification:

Authorities

Certificates

Revocation

Search

Search term





Both

Search

Clear

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPN_Root_CA	✓	self-signed	2	ST=Tunis, OU=IT, O=esprit, L=Ariana, CN=esprit.local, C=TN Valid From: Tue, 17 Dec 2024 21:07:51 +0100 Valid Until: Fri, 15 Dec 2024 21:07:51 +0100	OpenVPN Client	   

Add

Voici notre certification server et user pour OpenVPN:

System

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

System / Certificates / Certificates

Authorities

Certificates

Certificate Revocation

Search

Search term









Both

Search

Clear

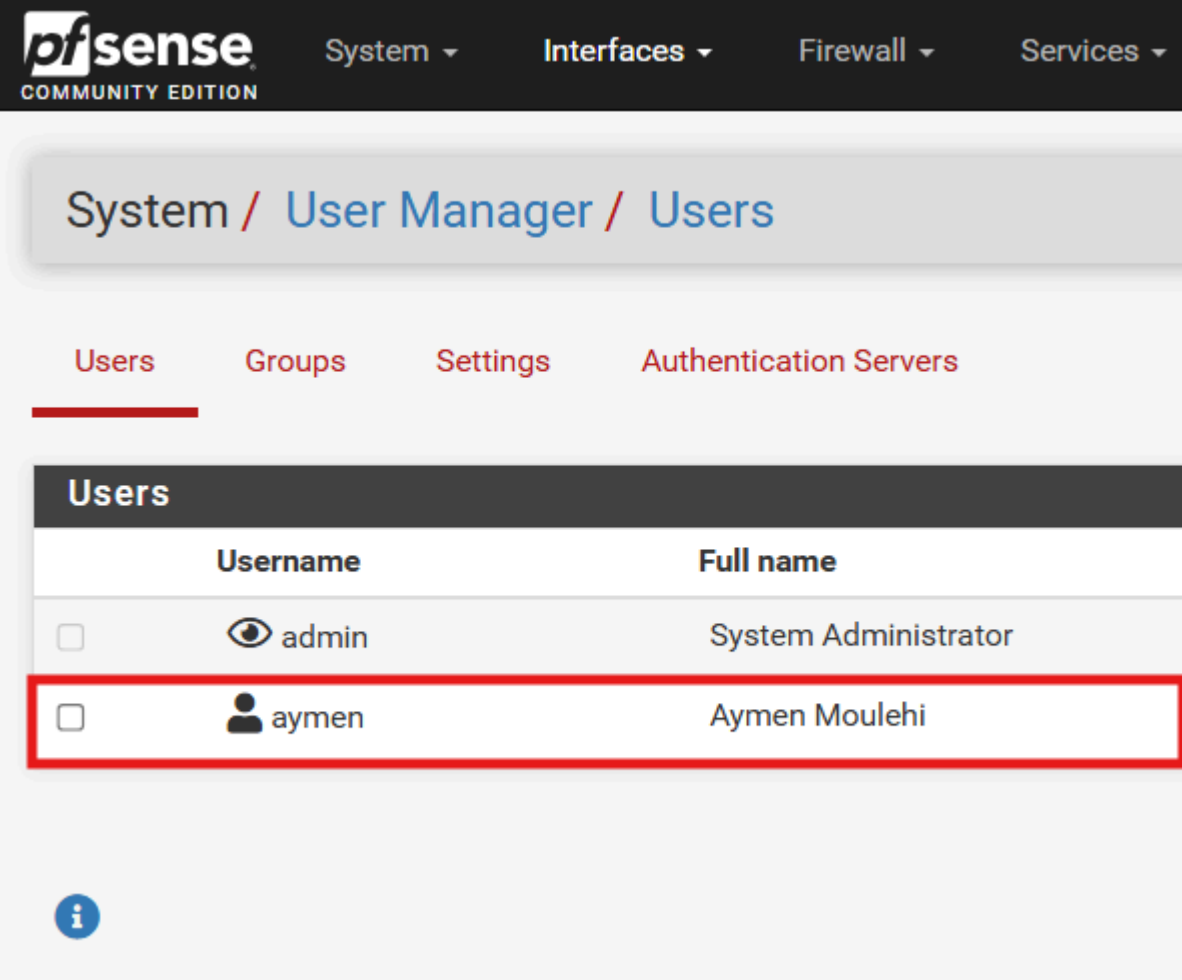
Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
VPN_Root_CA_Certificate Server Certificate CA: No Server: Yes	VPN_Root_CA	ST=Tunis, OU=IT, O=esprit, L=Ariana, CN=esprit.local, C=TN Valid From: Tue, 17 Dec 2024 21:14:49 +0100 Valid Until: Fri, 15 Dec 2024 21:14:49 +0100	webConfigurator OpenVPN Server	   
VPN-User_CA User Certificate CA: No Server: No	VPN_Root_CA	ST=Tunis, OU=IT, O=esprit, L=Ariana, CN=aymen, C=TN Valid From: Tue, 17 Dec 2024 21:34:41 +0100 Valid Until: Fri, 15 Dec 2024 21:34:41 +0100	User Cert	   

Add/Sign

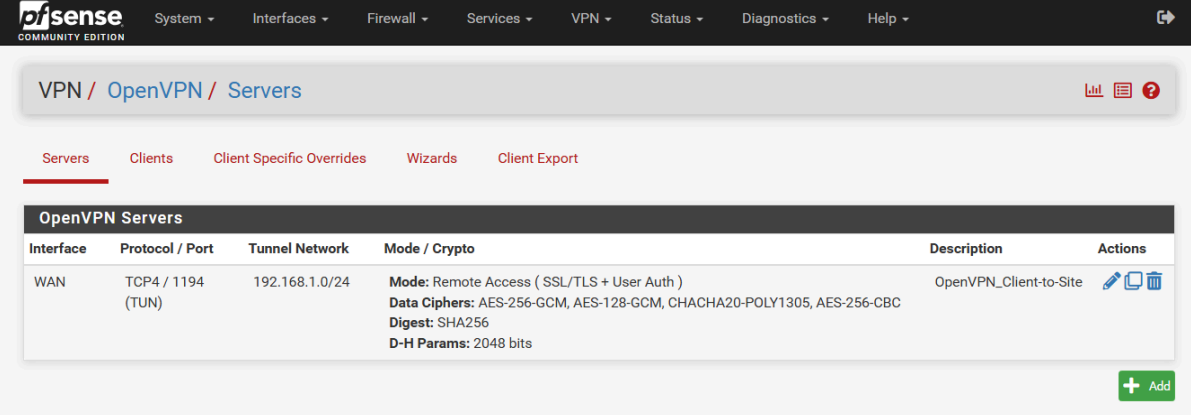
Voici notre user pour OpenVPN:



The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', and 'Services'. The breadcrumb trail is 'System / User Manager / Users'. Below this, there are tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers'. The 'Users' tab is active. The main content area is titled 'Users' and contains a table with two columns: 'Username' and 'Full name'. The table lists two users: 'admin' (System Administrator) and 'aymen' (Aymen Moulehi). The row for 'aymen' is highlighted with a red border. An information icon is visible at the bottom left of the table area.

	Username	Full name
<input type="checkbox"/>	admin	System Administrator
<input type="checkbox"/>	aymen	Aymen Moulehi

Voici la configuration server pour OpenVPN:



The screenshot shows the pfSense web interface for OpenVPN server configuration. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The breadcrumb trail is 'VPN / OpenVPN / Servers'. Below this, there are tabs for 'Servers', 'Clients', 'Client Specific Overrides', 'Wizards', and 'Client Export'. The 'Servers' tab is active. The main content area is titled 'OpenVPN Servers' and contains a table with columns: 'Interface', 'Protocol / Port', 'Tunnel Network', 'Mode / Crypto', 'Description', and 'Actions'. The table lists one server configuration for the 'WAN' interface. The 'Mode / Crypto' column contains detailed configuration information. An 'Add' button is visible at the bottom right of the table area.

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	TCP4 / 1194 (TUN)	192.168.1.0/24	Mode: Remote Access ( SSL/TLS + User Auth ) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN_Client-to-Site	

Voici la configuration client pour OpenVPN:

VPN / OpenVPN / Clients

Servers Clients Client Specific Overrides Wizards Client Export

OpenVPN Clients					
Interface	Protocol	Server	Mode / Crypto	Description	Actions
WAN	TCP4 (TUN)	192.168.1.60:1194	<b>Mode:</b> Peer to Peer ( SSL/TLS ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256	OpenVPN-User-1	

+ Add

Voici la page du export dans pfSense:

Save as default

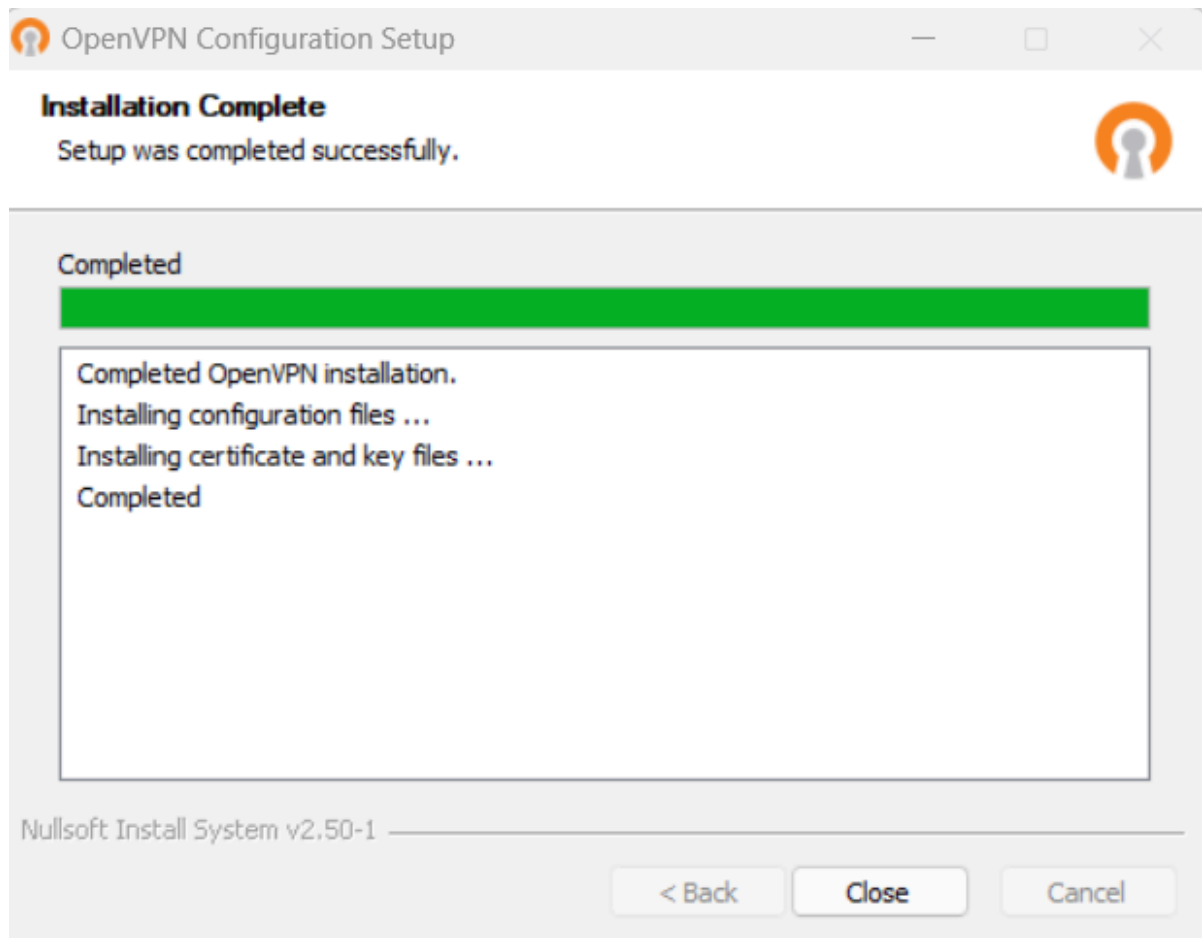
Search Clear

Enter a search string or \*nix regular expression to search.

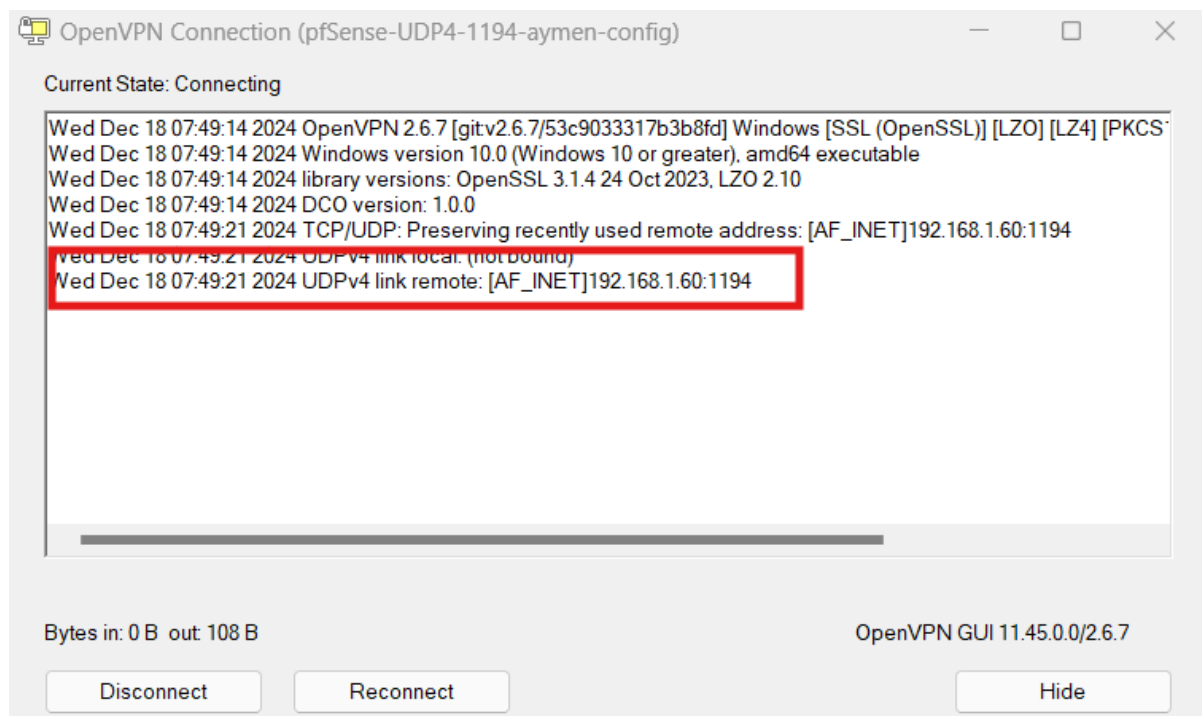
Certificate Name	Export
VPN-User_CA	- Inline Configurations: Most Clients  Android  OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive  Config File Only - Current Windows Installers (2.6.7-lx001): 64-bit  32-bit - Previous Windows Installers (2.5.9-lx601): 64-bit  32-bit - Legacy Windows Installers (2.4.12-lx601): 10/2016/2019  7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle  Viscosity Inline Config

certificates are shown

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):**



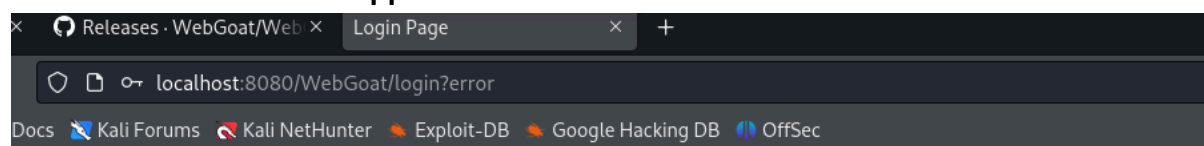
```
(moataz@kali)-[~]
$ sudo docker run -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 -e TZ=Europe/Amsterdam webgoat/goatandwolf

[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: --webgoat.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/webgoat/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
2024-12-15 16:28:17.970 INFO 23 — [main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.
2024-12-15 16:28:17.970 INFO 23 — [main] .s.d.r.c.RepositoryConfigurationDelegate : 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 queries. A database is a collection of data. The data is organized into rows, columns and tables, and indexed to make finding relevant information more efficient. 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, department, salary, and authentication token.

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

## 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 privileges.

✓

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 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

#### 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 Tiling 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!