

# Conception et sécurisation d'un réseau informatique

Avec pfSense, portail captif et système IDS

Réalisé par:

François-Xavier Leclerc  
Raphaël Beauregard  
Isaac Sondou Gnazou

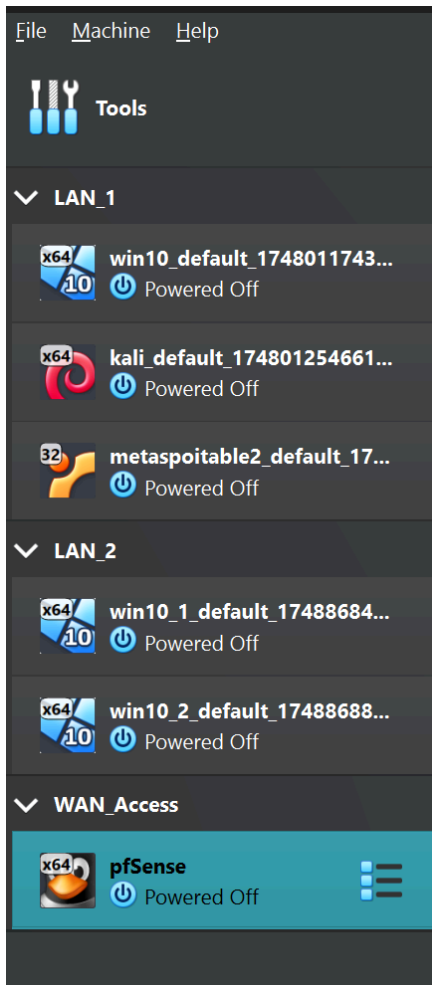
Dans le cadre  
Du cours de Sécurité des Réseaux  
Au collège Cumberland

À noter que les captures d'écran n'auront pas nécessairement les mêmes configurations au fur et à mesure du document. Certaines captures d'écran ont été prises par des membres différents de l'équipe. Il est possible que les adresses IP fluctuent par exemple. Cela ne change aucunement la crédibilité du travail réalisé. À des fins de simplicité, nous allons assumer que le LAN 1 est associé au réseau 193.168.2.0/24 et le LAN 2 172.16.2.0/24 à travers du document.

## Introduction

Dans ce projet, notre but va être de réaliser un réseau informatique virtuel sécurisé qui consistera des trois interfaces suivantes: un WAN géré par pfSense, un LAN1 avec deux machines clients ainsi que Metasploitable 2, et un LAN2 avec deux autres machines clients. PfSense servira de pare-feu, et Snort d'IDS/IPS. Dans pfSense, nous allons configurer un portail captif ainsi que des règles de filtrage personnalisées. Nous allons également réaliser plusieurs tests afin de mettre à l'épreuve notre configuration réseau. Cela nous permettra de mettre en pratique les notions apprises pendant la session et de mieux comprendre comment protéger un réseau contre les menaces.

## Environnement virtuel:



Voici notre configuration VirtualBox:

Nous avons **6 VMs**, répartis sur **3 interfaces**.

### LAN 1:

2 machines clients **Windows** et **Kali**.

Une machine vulnérable **Metasploitable 2**.

### LAN 2:

2 machines clients **Windows**.

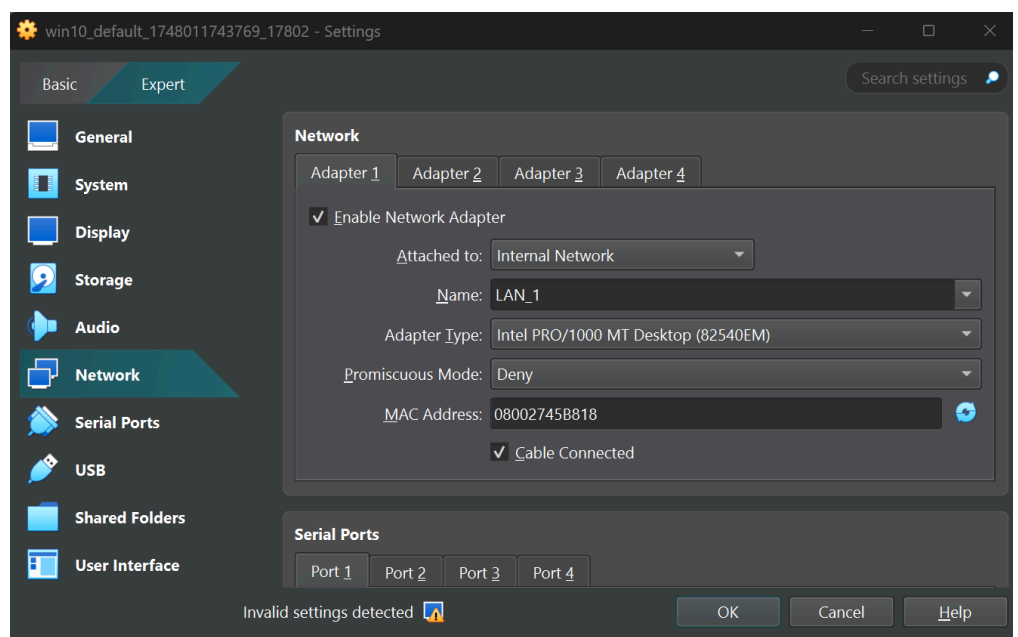
### WAN:

Pare-feu **pfSense** (sert également de IDS avec Snort).

## Architecture réseau:

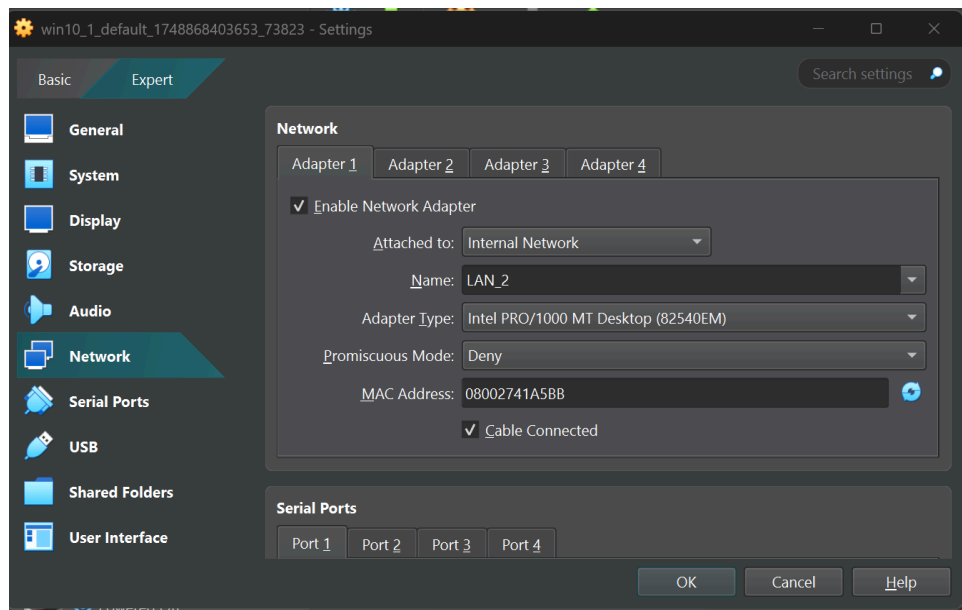
**LAN 1 machines clients:**

*Réseau Interne LAN 1* seulement.



## LAN 2 machines clients:

*Réseau interne LAN 2*  
seulement.

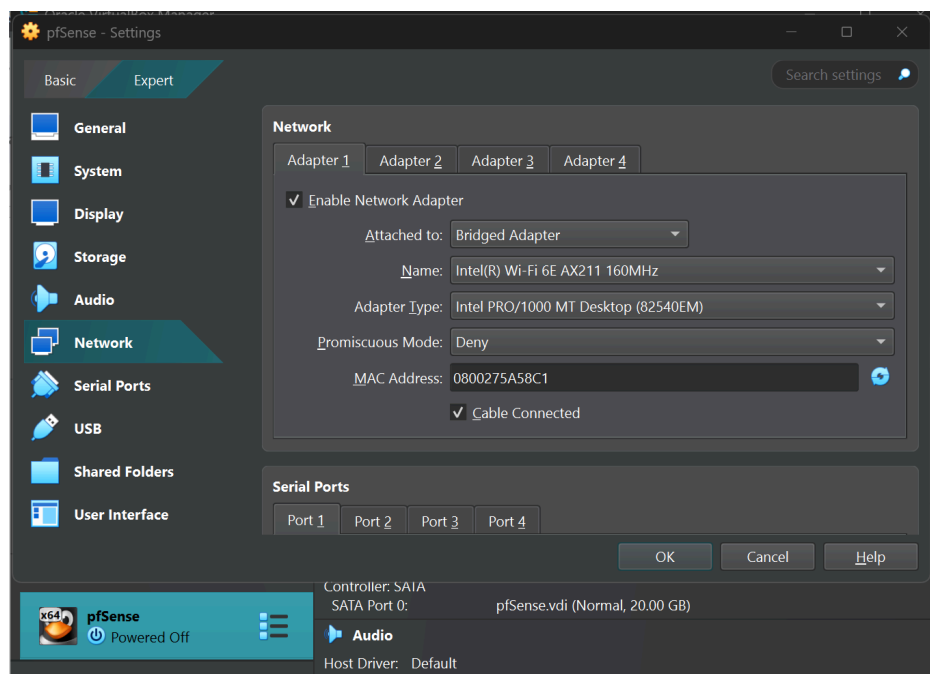


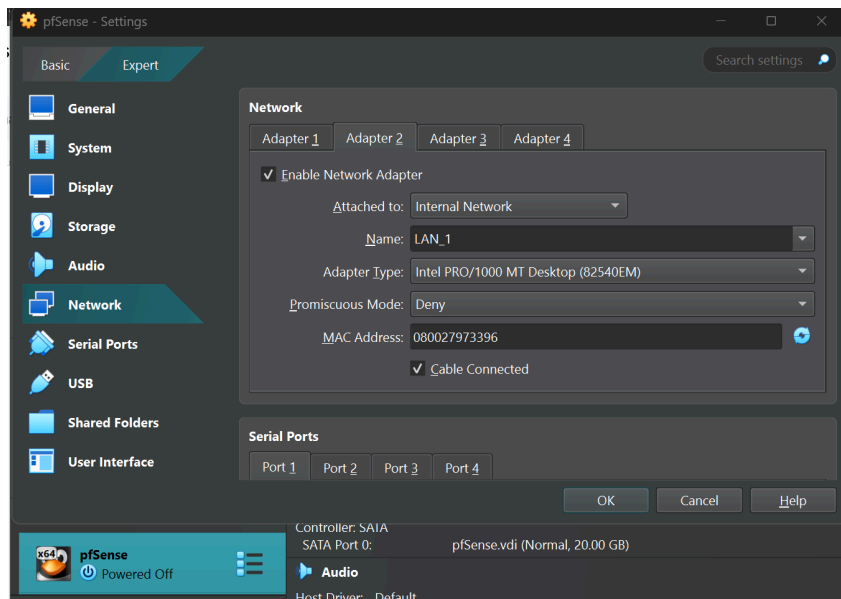
**IMPORTANT: NE PAS ACCORDER L'ACCÈS WAN DIRECTEMENT AUX MACHINES CLIENTS. LE PARE-FEU PFSENSE VA INTERCEPTER LES PAQUETS ET SERVIR DE GATEWAY.**

## WAN Pare-feu pfSense:

### Adaptateur 1:

*Bridged adapter* pour accès Internet.





## Adaptateur 2:

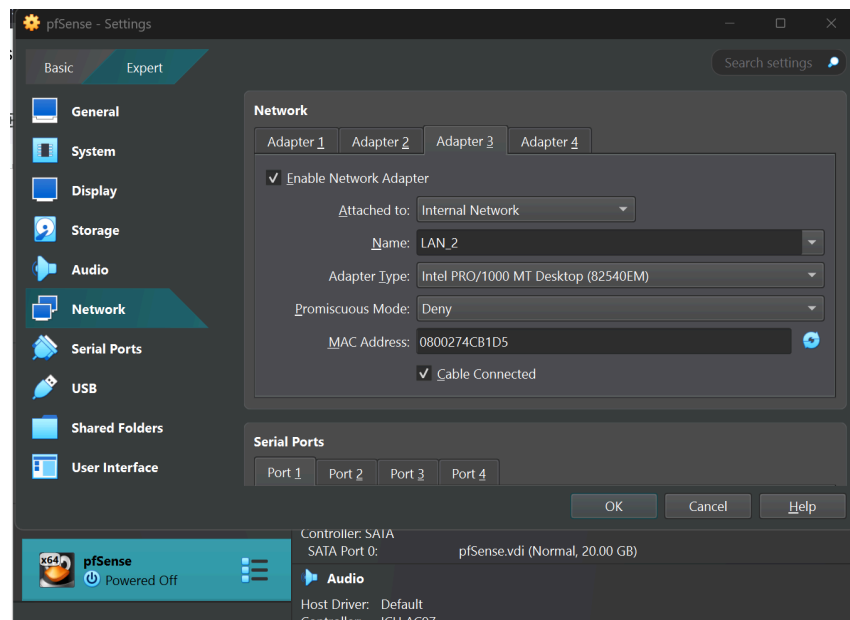
### Réseau interne LAN 1.

Permet de faire le lien avec les machines du LAN 1.

## Adaptateur 3:

### Réseau interne LAN 2.

Lien LAN 2.



## Configuration DHCP sur pfSense

Sur la console de pfSense, utiliser les commandes suivantes pour configurer les interfaces et le serveur DHCP:

```
File Machine View Input Devices Help

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) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 1

Valid interfaces are:

em0      08:00:27:5a:58:c1 (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:97:33:96 (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:4c:b1:d5 (down) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y/n]? █
```

1) Assigner les interfaces (si elles ne sont pas bien assignées par défaut).

En0 = WAN

En1 = LAN1

En2 = LAN2

(LAN2 peut-être appelé OPT1, mais c'est la même chose dans les deux cas).

Dans notre cas, nous allons configurer le LAN 2 sur l'interface web de pfSense afin de démontrer ce qui est possible, mais il est entièrement possible de configurer les 3 interfaces sur cette console.

2) Configurer les adresses IP des interfaces.

Pour LAN 1: **193.168.2.254**  
**24 bits**

Pour LAN 2: **172.16.2.254**  
**24 bits**

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1 - dhcp)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 172.16.2.254

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 OPT1 IPv4 subnet bit count (1 to 32):
> 24
```

**IMPORTANT:** Pour le LAN 1, l'adresse 193.[...] a été choisie afin d'éviter un conflit avec l'adresse WAN.

```

Configure IPv4 address OPT1 interface via DHCP? (y/n) n
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 172.16.2.254

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 OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) y
Enter the start address of the IPv4 client address range: 172.16.2.10
Enter the end address of the IPv4 client address range: 172.16.2.100

```

→ DHCP de .10 à .100 pour les 2 LAN.

## Configuration IP complétée.

```

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

Please wait while the changes are saved to OPT1...[fib_algo] inet.0 (bsearch4#5)
) rebuild_fd_flm: switching algo to radix4_lockless

Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 172.16.2.254/24
You can now access the webConfigurator by opening the following URL in your web browser:
      https://172.16.2.254/

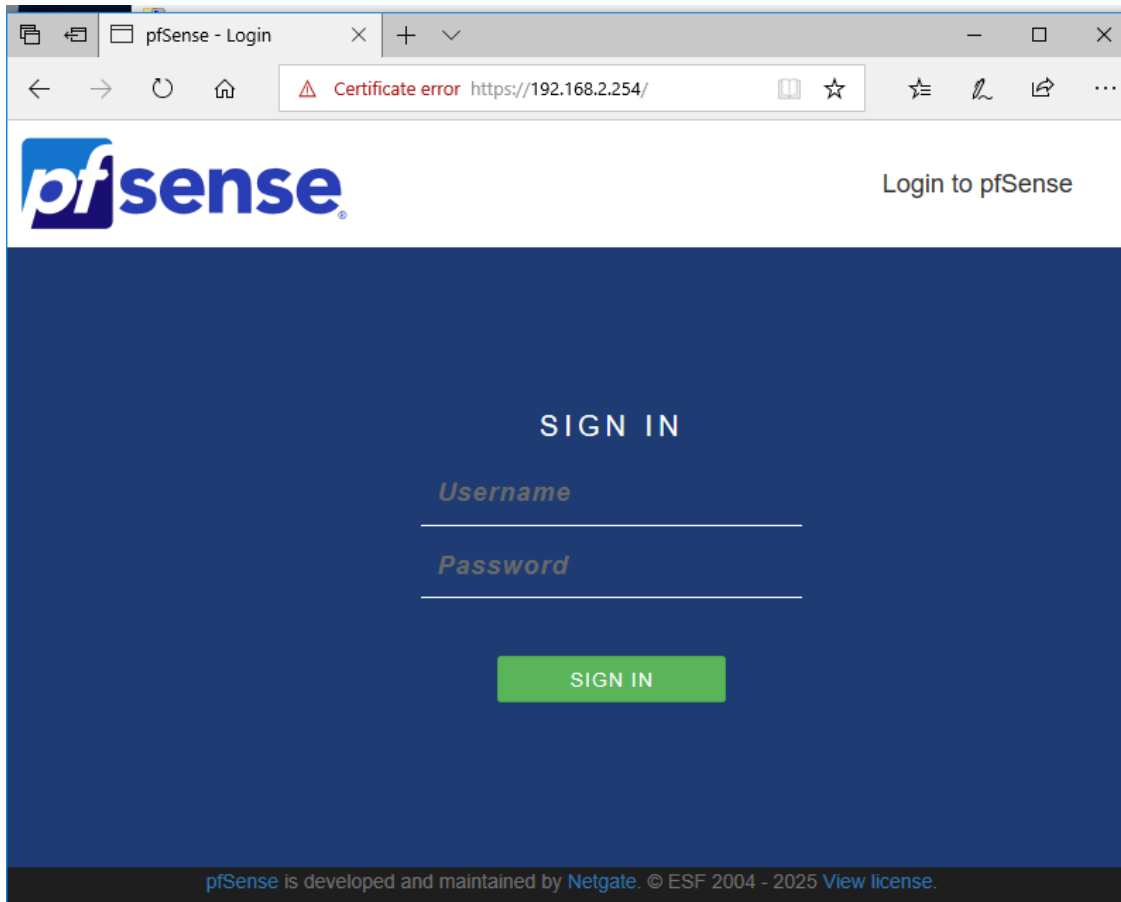
Press <ENTER> to continue.

```

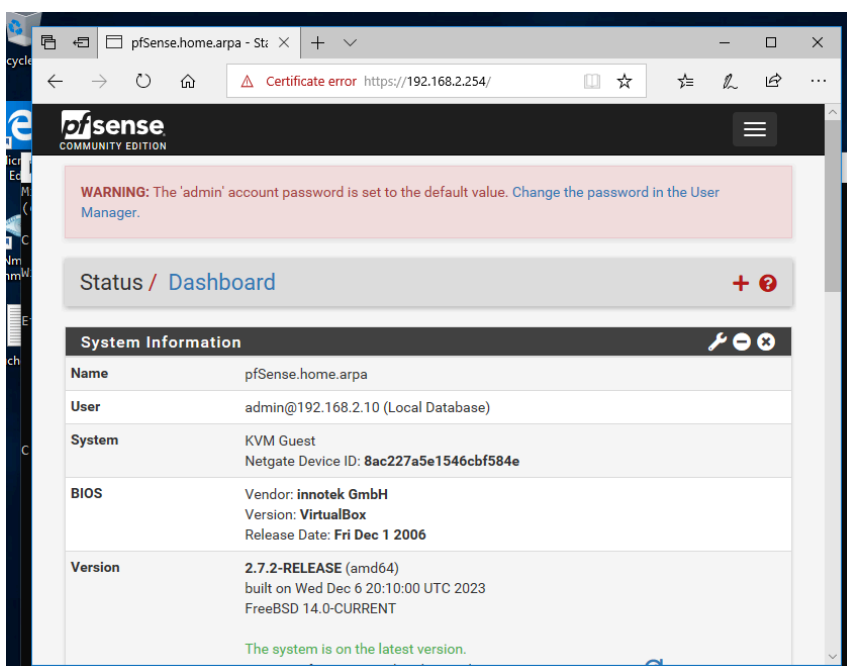
Avec cette configuration, le serveur DHCP va attribuer automatiquement des adresses IP de **193.168.2.10 à .100** pour le **LAN 1** et de **172.16.2.10 à .100** pour le **LAN 2**.

## Configuration web de pfSense

Nous allons accéder au site web de pfSense en utilisant l'IP configurée à l'étape précédente. Dans notre cas: **193.168.2.254** pour le LAN 1 et **172.16.2.254** pour le LAN 2.



Utilisateur par défaut pour se connecter: **Admin/pfsense**.



→ Interface de bienvenue

Dans Services > DHCP Server:

Configurer le serveur DHCP LAN 1 et LAN 2.

Enable

☒ Enable interface

Description

LAN2

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

Static IPv4 Configuration

IPv4 Address

172.16.2.254

/

24

IPv4 Upstream gateway

None

+ Add a new gateway

The LAN2 configuration has been changed.  
The changes must be applied to take effect.  
Don't forget to adjust the DHCP Server range if needed after applying.

✓ Apply Changes



ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

LAN LAN2

## General DHCP Options

DHCP Backend

ISC DHCP

Enable

☒ Enable DHCP server on LAN2 interface

BOOTP

☐ Ignore BOOTP queries

Deny Unknown Clients

Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

192.168.2.254/services\_dhcp.php?if=lan

## Configuration de la plage IP.

## Primary Address Pool

Subnet 172.16.2.0/24

Subnet Range 172.16.2.1 - 172.16.2.254

Address Pool Range

172.16.2.10

From

172.16.2.100

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools

[+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

## Server Options

Tester le DHCP en utilisant ipconfig sur Windows ou ifconfig sur Linux. L'adresse IP devrait être dans le plage IP du serveur DHCP (en commençant à .10):

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vagrant>ipconfig





Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : home.arpa
    IPv4 Address. . . . . : 172.16.2.12
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.2.254

C:\Users\vagrant>
```

Création et configuration du portail captif dans Services > Captive Portal.

Services / Captive Portal / Add Zone    

Add Captive Portal Zone

Zone name


LAN1-PORTAL

Zone name. Can only contain letters, digits, and underscores (\_) and may not start with a digit.

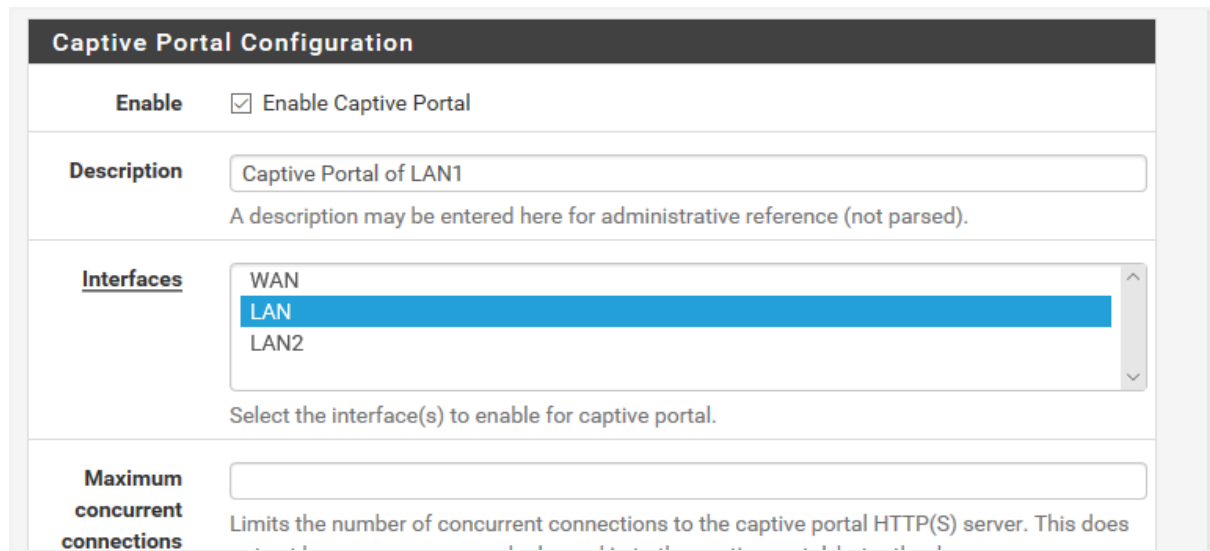
Zone description

Captive Portal of LAN1

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

 Save & Continue

Cocher enable et sélectionner LAN 1.



**Captive Portal Configuration**

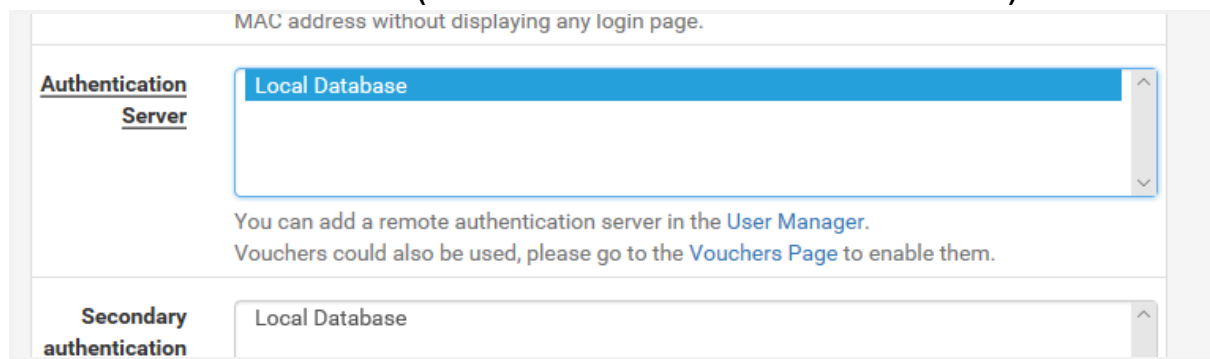
**Enable** ☒ Enable Captive Portal

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

**Interfaces**   
  
  
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

Sélectionner Local Database (authentification via les utilisateurs locaux).



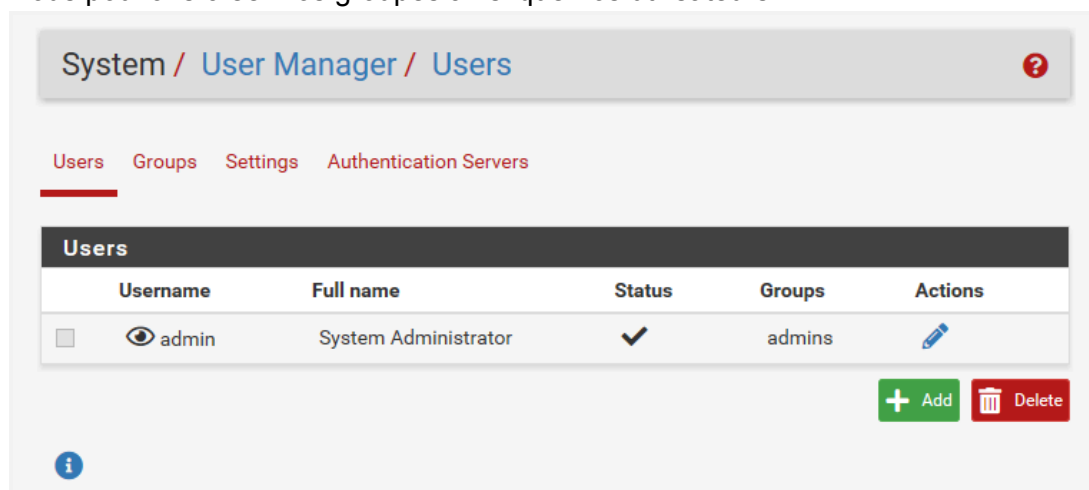
MAC address without displaying any login page.

**Authentication Server**   
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**

Dans System > User Manager:

Nous pouvons créer nos groupes ainsi que nos utilisateurs.



System / [User Manager](#) / [Users](#)

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

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

[+ Add](#) [Delete](#)

[i](#)

Si l'option **Allow only users/groups with "Captive Portal Login" privilege set** est cochée dans la configuration du portail captif, nous devons ajouter la permission **User - Services: Captive Portal Login** aux utilisateurs qui ont le droit de se connecter via le portail captif. Cette permission peut être ajoutée à un groupe pour simplifier la gestion, ou aux utilisateurs individuels pour plus de contrôle.

Nos utilisateurs:

System / User Manager / Users












Users

Groups

Settings

Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	 admin	System Administrator	✓	admins	
<input type="checkbox"/>	 eshvets	Emma Shvets	✓	admins	 
<input type="checkbox"/>	 mlockwood	Mei Lockwood	✓	admins	 
<input type="checkbox"/>	 ywow	Yuri Wow	✓	admins	 

+

 Add

Delete


À NOTER: NORMALEMENT, LES UTILISATEURS N’AURAIENT PAS TOUS ACCÈS AUX PERMISSIONS ADMINISTRATEURS ET NOUS AURIONS CRÉÉ UN GROUPE SÉPARÉ POUR CEUX-CI, MAIS DANS LE CAS DE NOTRE PROJET CETTE CONFIGURATION EST ACCEPTABLE.

Maintenant, nous pouvons tester la connection des utilisateurs au portail captif:

pfSense.home.arpa - Interfa


Captive Portal Login Pa

193.16.2.254:8002/index.php?zone=lan1portal&redin



eshvets

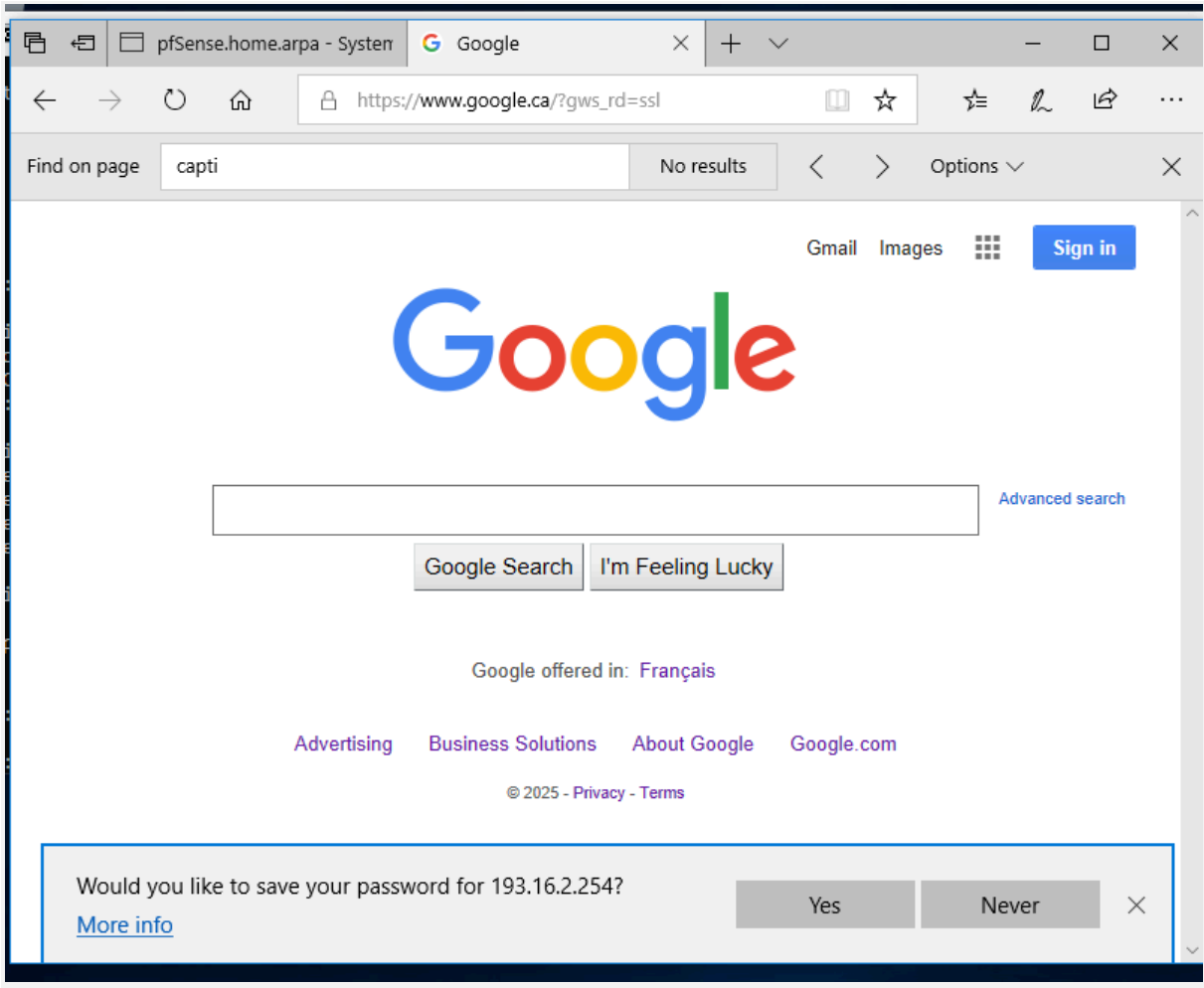
.....



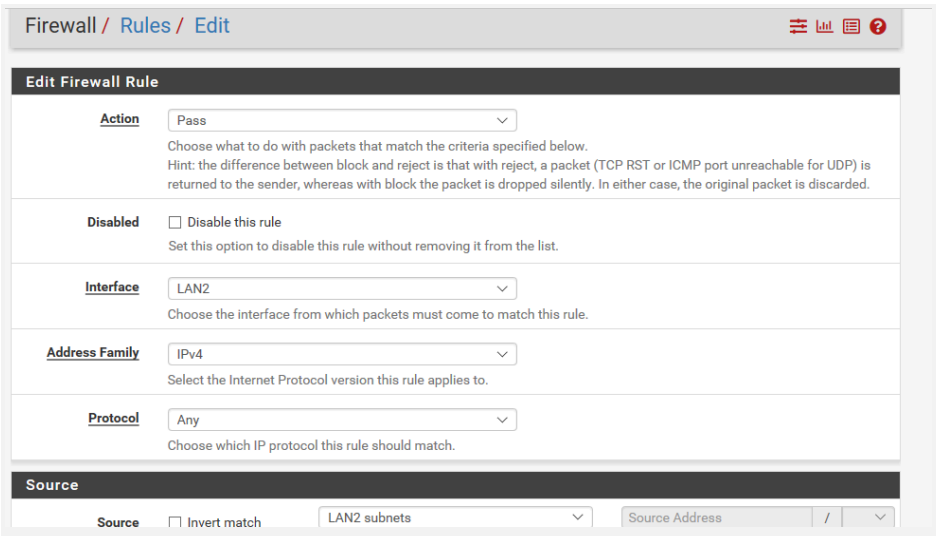
Login

Made with ♥ by Netgate

Après s’être connecté, vérifier l’accès à l’Internet:



Configuration des règles de filtrages du pare-feu dans Firewall > Rules



Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN2 subnets

Source Address

/

Destination

Destination

☐ Invert match

Any

Destination Address

/

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

Internet From LAN2

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

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#).

Sauvegarder la configuration.

Voici les nouvelles règles que nous avons créées pour le LAN 1:

Firewall / Rules / LAN

Floating WAN LAN LAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3/56 KIB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	10/2 KIB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	193.16.2.0/24	*	172.16.2.0/24	*	*	none		auth ping between LANS	
<input type="checkbox"/>	0/0 B	IPv4 *	193.16.2.0/24	*	172.16.2.0/24	*	*	none		Block comms from LAN1 to LAN2	

↑ Add

↓ Add

Delete

Toggle

Copy

Save

+ Separator





























1: Ping de LAN 1 à LAN 2 autorisé.

2: Toute autre communication du LAN 1 au LAN 2 est bloquée.

Pour le LAN 2:

FloatingWANLANLAN2

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 *	172.16.2.0/24	*	*	*	*	none	🌙 Nighttime	night_blockage	   
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	172.16.2.12	*	193.16.2.5	80 (HTTP)	*	none		Authorize HTTP from Win1_LAN1	    
<input type="checkbox"/>	✗ 0/11 KiB	IPv4 *	172.16.2.0/24	*	193.16.2.5	*	*	none		Block Metasploitable access	   
<input type="checkbox"/>	✓ 5/1.96 MiB	IPv4 TCP	172.16.2.0/24	*	193.16.2.0/24	*	*	none		auth ping between LANS	    
<input type="checkbox"/>	✓ 0/1008 B	IPv4 *	172.16.2.0/24	*	193.16.2.0/24	*	*	none		Authorize LAN2 to connect to LAN1	    
<input type="checkbox"/>	✓ 112/14.61 MiB	IPv4 *	172.16.2.0/24	*	*	*	*	none		Internet From LAN2	    

↑ Add

↓ Add

🗑 Delete

🔍 Toggle

📄 Copy

💾 Save

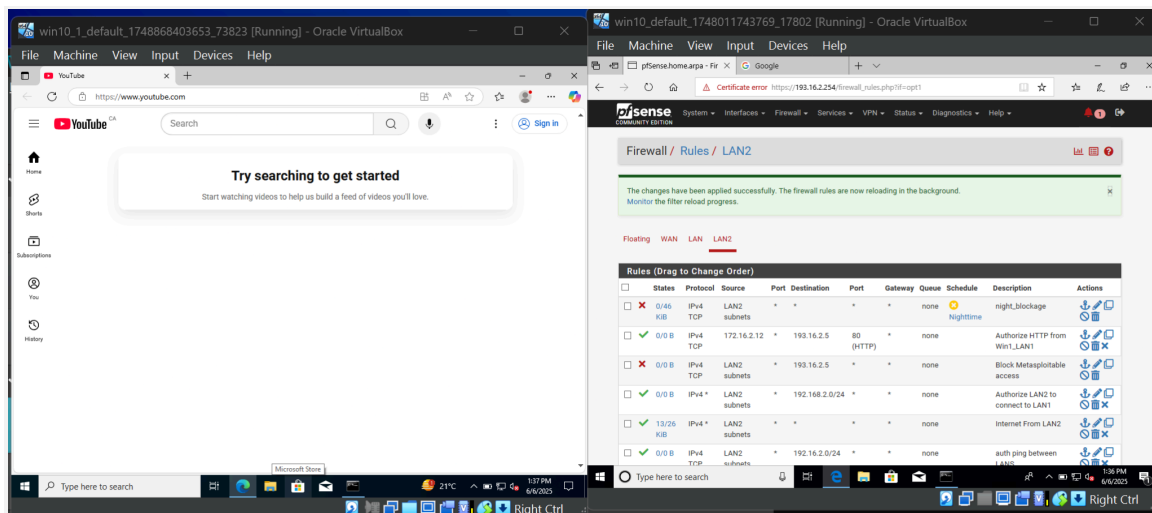
+ Separator

- 1: Blocage d'accès Internet de nuit.
- 2: Autorisation du HTTP d'une machine client à Metasploitable.
- 3: Blocage de toute autre communication avec Metasploitable.
- 4: Ping de LAN 2 à LAN 1 autorisé.
- 5: Toute autre communication du LAN 2 au LAN 1 est autorisée.
- 6: Accès Internet autorisé pour le LAN 2 (règle #1 a la priorité).

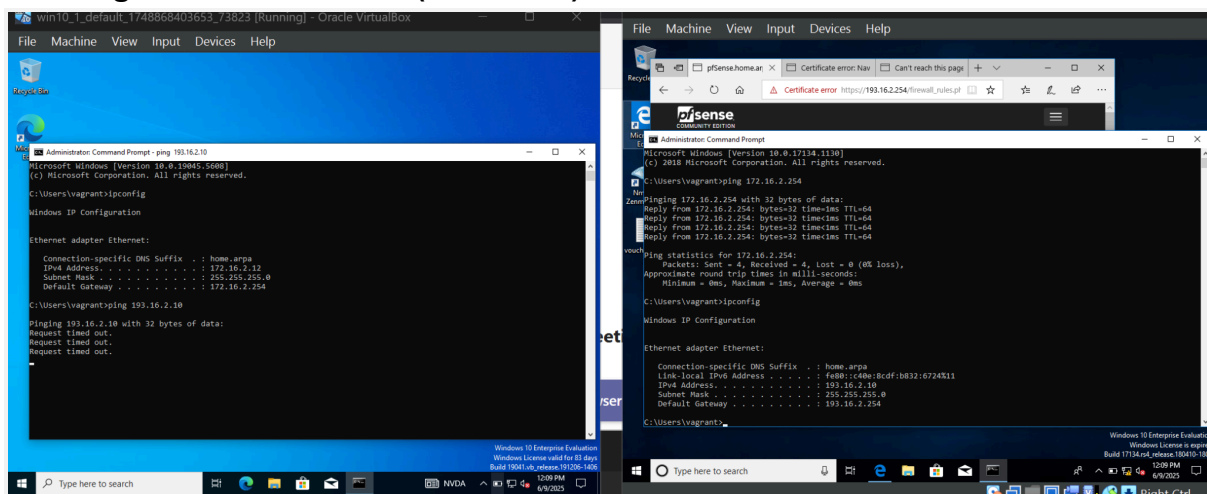
Effectuons les tests suivants afin d'évaluer la configuration des règles:

Test	Attendu
Accès Internet depuis LAN2	✓ Fonctionne (Règle 1)
Ping LAN2 → LAN1	✓ Fonctionne (Règle 2)
Ping LAN1 → LAN2	✗ Bloqué (Règle 3)
Accéder au site de Metasploitable avec 192.168.2.5 sur un navigateur client du LAN 2	✓ Fonctionne (Règle 4)
Autre trafic LAN2 → Metasploitable	✗ Bloqué (Règle 5)
Ping inter-LAN uniquement	✓ ICMP autorisé, autres services bloqués (Règle 6)
Navigation Internet depuis LAN2 la nuit	✗ Bloquée (Règle 7)

## ☑ Accès Internet.

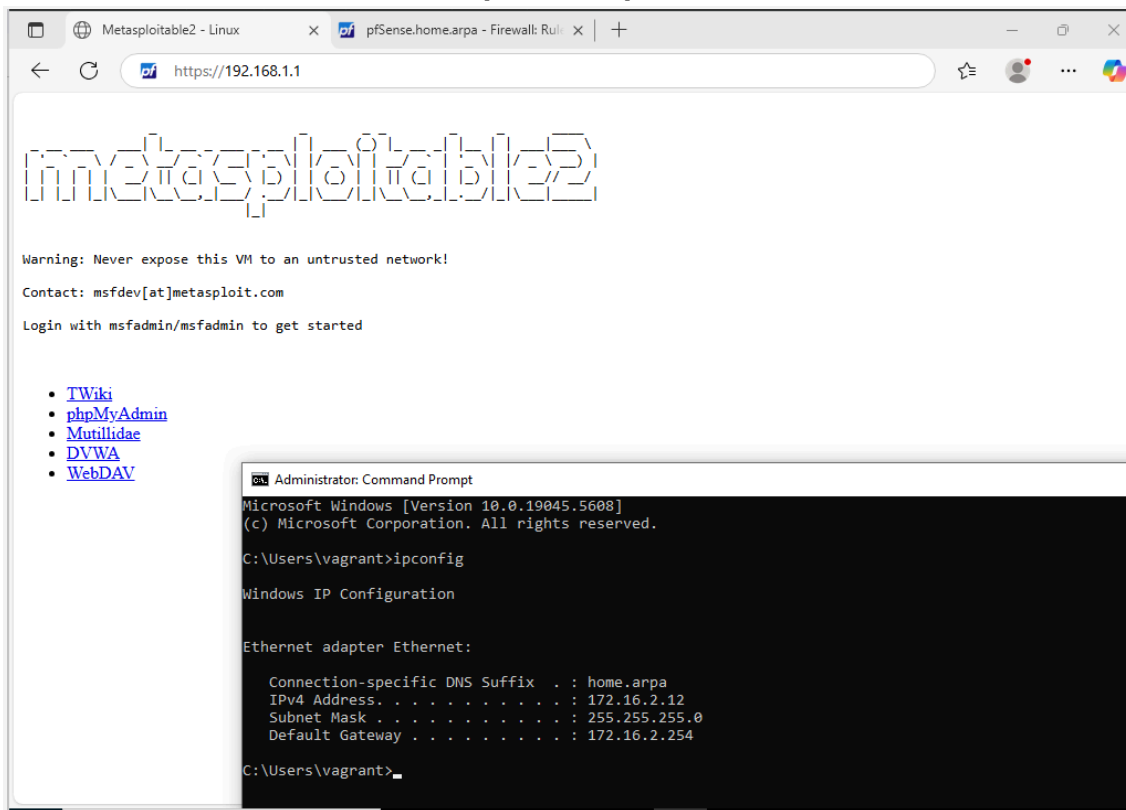


## ☑ Ping LAN 1 <—> LAN 2 (inter-LAN).





☒ **Accès au site web de Metasploitable pour l'adresse IP autorisée.**



The screenshot shows a web browser window with the address bar displaying `https://192.168.1.1`. The page content includes the Metasploitable2 logo, a warning message: "Warning: Never expose this VM to an untrusted network!", contact information: "Contact: msfdev[at]metasploit.com", and login instructions: "Login with msfadmin/msfadmin to get started". Below this, there is a list of links: [TWiki](#), [phpMyAdmin](#), [Mutillidae](#), [DVWA](#), and [WebDAV](#). Overlaid on the bottom right of the browser window is a Windows Command Prompt window titled "Administrator: Command Prompt". The command prompt shows the output of the `ipconfig` command, indicating the IP configuration for the Ethernet adapter.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vagrant>ipconfig

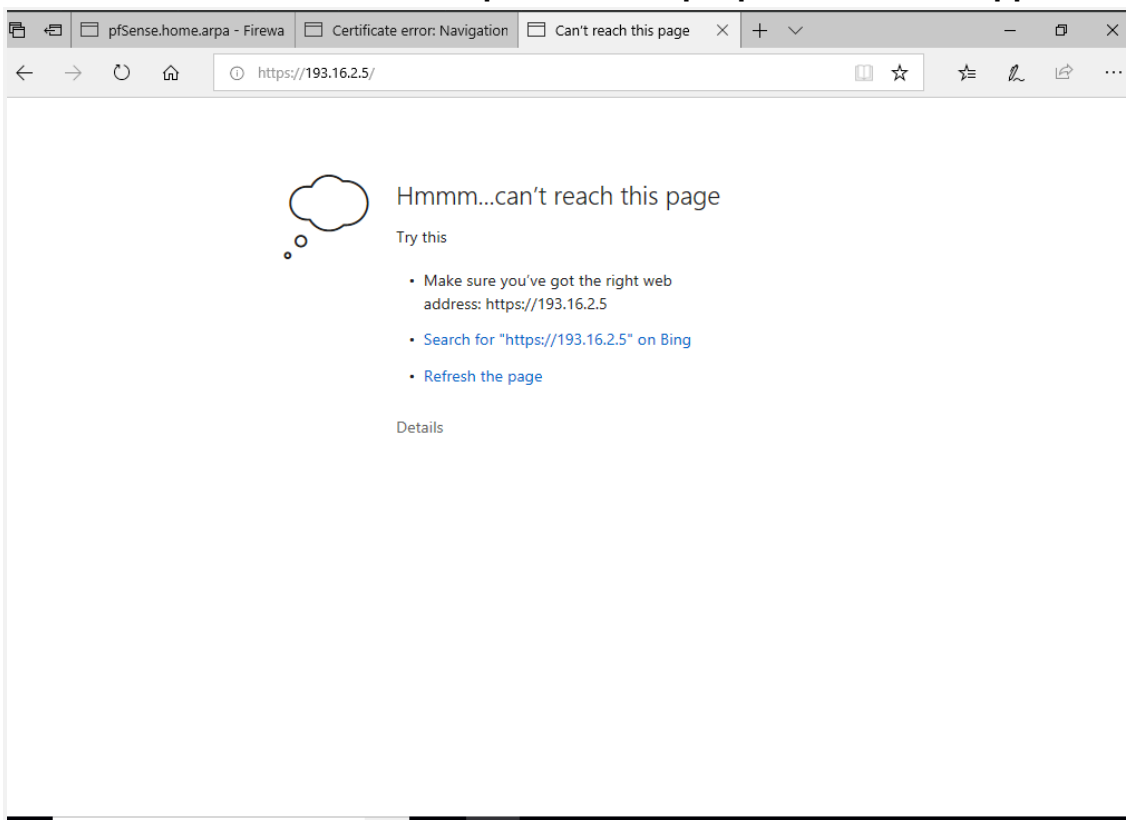
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : home.arpa
    IPv4 Address. . . . . : 172.16.2.12
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.2.254

C:\Users\vagrant>
```

☒ **Accès au site web de Metasploitable bloqué pour les autres appareils.**



The screenshot shows a web browser window with the address bar displaying `https://193.16.2.5/`. The page content displays a "Can't reach this page" error message. The error message includes a cloud icon and the text "Hmmm...can't reach this page". Below this, there is a "Try this" section with three suggestions: "Make sure you've got the right web address: https://193.16.2.5", "Search for 'https://193.16.2.5' on Bing", and "Refresh the page". At the bottom, there is a "Details" link.

Hmmm...can't reach this page

Try this

- Make sure you've got the right web address: <https://193.16.2.5>
- [Search for "https://193.16.2.5" on Bing](#)
- [Refresh the page](#)

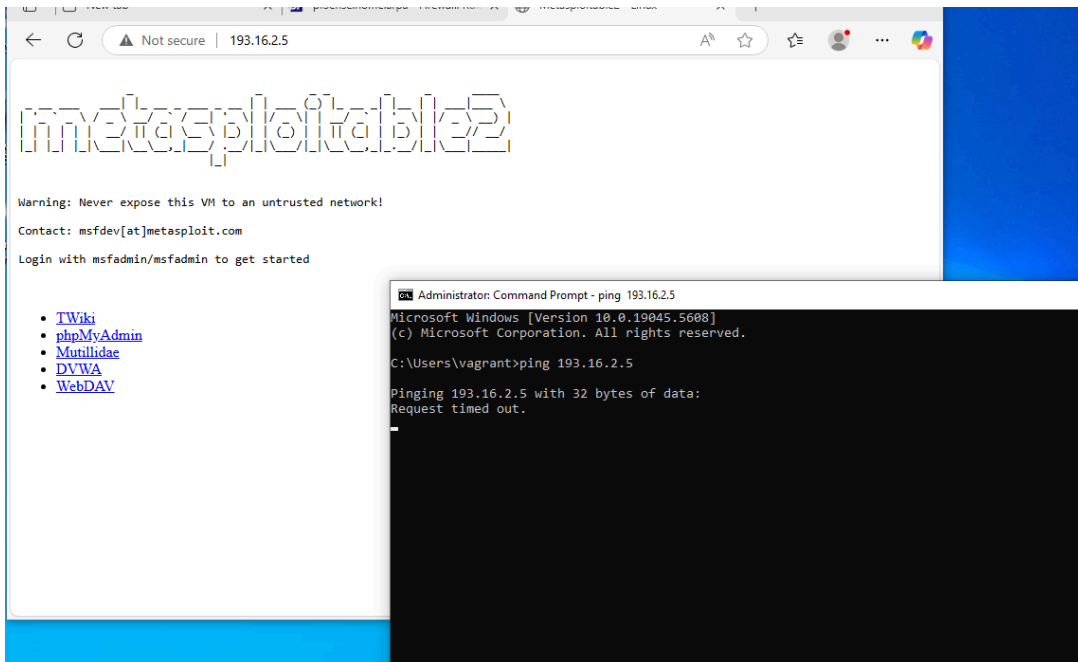
[Details](#)

☒ Ping de LAN 1 à Metasploitable autorisé.

```
C:\Users\vagrant>ping 193.16.2.5

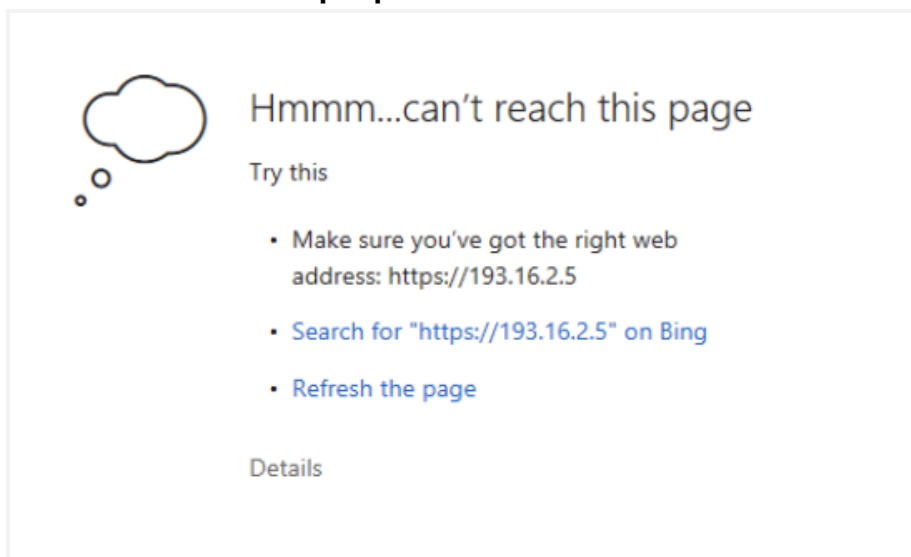
Pinging 193.16.2.5 with 32 bytes of data:
Reply from 193.16.2.5: bytes=32 time<1ms TTL=64
Reply from 193.16.2.5: bytes=32 time<1ms TTL=64
Reply from 193.16.2.5: bytes=32 time<1ms TTL=64
```

☒ Ping de LAN 2 à Metasploitable non autorisé.



The image shows the Metasploitable VM interface in a web browser. The address bar shows '193.16.2.5'. The page displays the 'metasploitable2' logo, a warning message, contact information, and a list of links: TWiki, phpMyAdmin, Metasploit, DVWA, and WebDAV. An 'Administrator: Command Prompt' window is overlaid on the bottom right, showing a failed ping command: 'C:\Users\vagrant>ping 193.16.2.5' resulting in 'Request timed out.'.

☒ Trafic LAN 2 bloqué pendant la nuit.

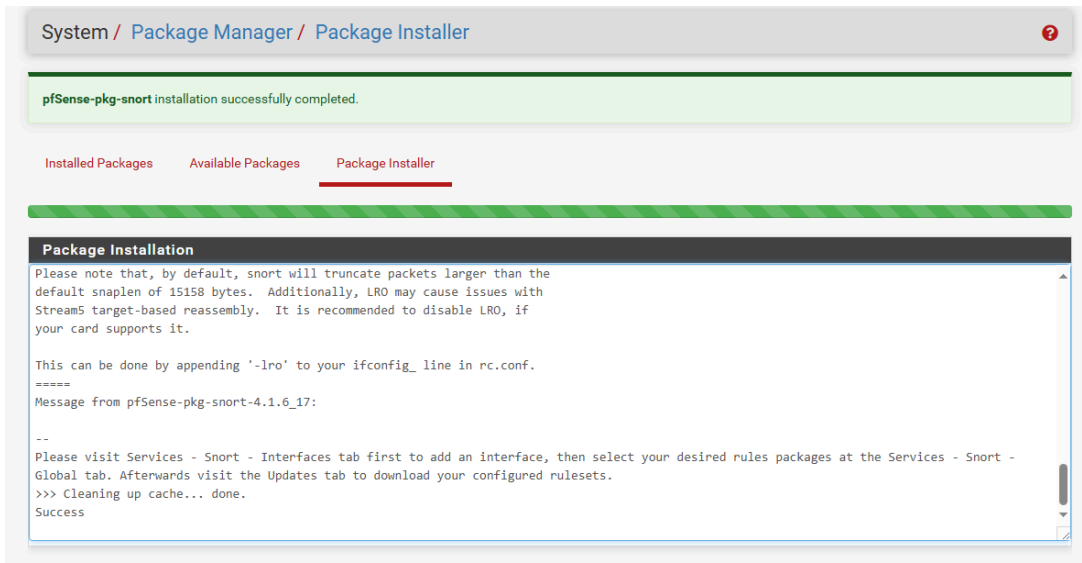


The image shows a 'can't reach this page' error message. It includes a thought bubble icon and the text 'Hmmm...can't reach this page'. Below this, it says 'Try this' and lists three suggestions: 'Make sure you've got the right web address: https://193.16.2.5', 'Search for "https://193.16.2.5" on Bing', and 'Refresh the page'. At the bottom, there is a 'Details' link.

Tous les tests ont été réussis.

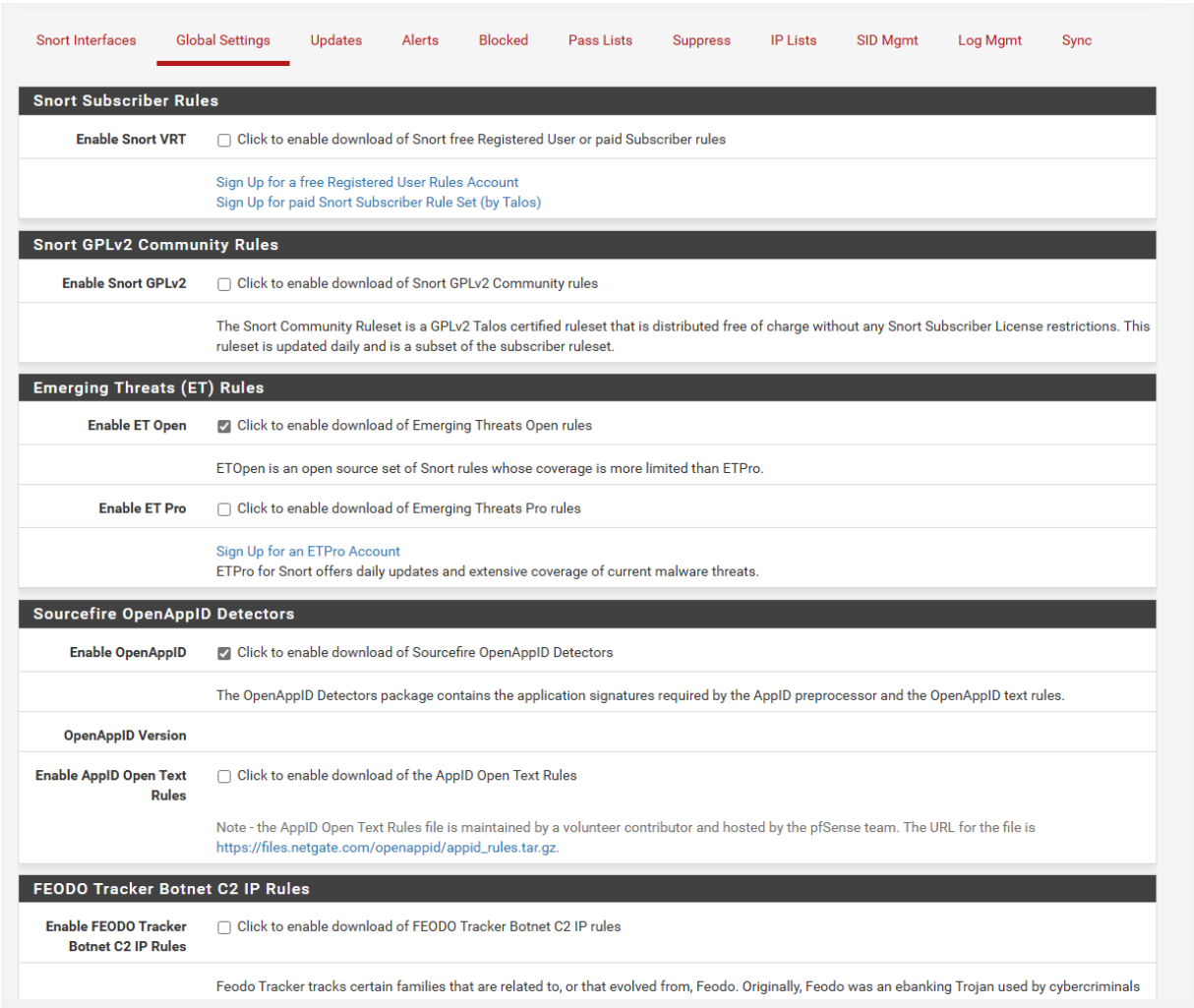
# Installation et configuration d’une solution IDS/IPS avec Snort.

Dans System > Package Manager > Package Installer: Installer Snort.



## Configuration des paramètres de base de Snort:

Dans Services > Snort > Global Settings, cocher “*Enable ET Open*” (ou *enable Snort VRT*) et “*Enable OpenAppID*”.



Création d’une interface dans “Snort Interfaces”.

Interface Settings Overview						
Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions	
<input type="checkbox"/> LAN2 (em2)		AC-BNFA	DISABLED	LAN2		

Add Delete

Mise à jour des règles dans “Updates”.

Cliquer sur “Update Rules”.

Services / Snort / Updates

Snort InterfacesGlobal SettingsUpdatesAlerts

IP ListsSID MgmtLog MgmtSync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	d41ca644ad4466a4d4fee88aaf1b50e	Monday, 09-Jun-25 12:43:11 UTC
Snort GPLv2 Community Rules	0bb396be56a308c00c366db7e3185d78	Monday, 09-Jun-25 12:43:11 UTC
Emerging Threats Open Rules	5b9a66d5d85356ca8b950503b8542fd8	Monday, 09-Jun-25 12:43:12 UTC
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Monday, 09-Jun-25 12:43:11 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Monday, 09-Jun-25 12:43:11 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Rules Update Task

Updating rule sets may take a while ... please wait for the process to complete.

This dialog will auto-close when the update is finished.

Close

Installed Rule Set MD5 Signature		
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	d41ca644ad4466a4d4fee88aaf1b50e	Monday, 09-Jun-25 12:43:11 UTC
Snort GPLv2 Community Rules	0bb396be56a308c00c366db7e3185d78	Monday, 09-Jun-25 12:43:11 UTC
Emerging Threats Open Rules	5b9a66d5d85356ca8b950503b8542fd8	Monday, 09-Jun-25 12:43:12 UTC
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Monday, 09-Jun-25 12:43:11 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Monday, 09-Jun-25 12:43:11 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

# Activation des règles désirées dans “LAN2 Categories”.

Dans notre cas, nous allons tout activer pour s’assurer qu’une alerte est générée.

Services / Snort / Interface Settings / LAN2 - Categories

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

LAN2 Settings

LAN2 Categories

LAN2 Rules

LAN2 Variables

LAN2 Preprocs

LAN2 IP Rep

LAN2 Logs

Automatic Flowbit Resolution

Resolve Flowbits

☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.  
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Snort Subscriber IPS Policy Selection

Use IPS Policy

☐ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.  
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

Select the rulesets (Categories) Snort will load at startup

- Category is auto-enabled by SID Mgmt conf files

- Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

Save

Add all categories to enforcing rules

Enable	Ruleset: Snort GPLv2 Community Rules						
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos certified)						
Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Enable	Ruleset: Snort OPENAPPID Rules
<input checked="" type="checkbox"/>	emerging-activex.rules	<input checked="" type="checkbox"/>	snort_app-detect.rules	<input checked="" type="checkbox"/>	snort_browser-chrome.so.rules	<input checked="" type="checkbox"/>	openappid-ads.rules
<input checked="" type="checkbox"/>	emerging-attack_response.rules	<input checked="" type="checkbox"/>	snort_attack-responses.rules	<input checked="" type="checkbox"/>	snort_browser-ie.so.rules	<input checked="" type="checkbox"/>	openappid-browser_plugin.rules
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	<input checked="" type="checkbox"/>	snort_backdoor.rules	<input checked="" type="checkbox"/>	snort_browser-other.so.rules	<input checked="" type="checkbox"/>	openappid-bussiness_applications.rules
<input checked="" type="checkbox"/>	emerging-botcc.rules	<input checked="" type="checkbox"/>	snort_bad-traffic.rules	<input checked="" type="checkbox"/>	snort_browser-webkit.so.rules	<input checked="" type="checkbox"/>	openappid-collaboration.rules
<input checked="" type="checkbox"/>	emerging-chat.rules	<input checked="" type="checkbox"/>	snort_blacklist.rules	<input checked="" type="checkbox"/>	snort_exploit-kit.so.rules	<input checked="" type="checkbox"/>	openappid-database.rules
<input checked="" type="checkbox"/>	emerging-ciarmy.rules	<input checked="" type="checkbox"/>	snort_botnet-cnc.rules	<input checked="" type="checkbox"/>	snort_file-executable.so.rules	<input checked="" type="checkbox"/>	openappid-file_storage.rules
<input checked="" type="checkbox"/>	emerging-compromised.rules	<input checked="" type="checkbox"/>	snort_browser-chrome.rules	<input checked="" type="checkbox"/>	snort_file-flash.so.rules	<input checked="" type="checkbox"/>	openappid-file_transfer.rules
<input checked="" type="checkbox"/>	emerging-current_events.rules	<input checked="" type="checkbox"/>	snort_browser-firefox.rules	<input checked="" type="checkbox"/>	snort_file-image.so.rules	<input checked="" type="checkbox"/>	openappid-games.rules
<input checked="" type="checkbox"/>	emerging-deleted.rules	<input checked="" type="checkbox"/>	snort_browser-ie.rules	<input checked="" type="checkbox"/>	snort_file-java.so.rules	<input checked="" type="checkbox"/>	openappid-hacktools.rules

# Activation de l’IPS pour bloquer le trafic suspect (si désiré).

Cocher “Block Offenders”.

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.  
  
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

Detection Performance Settings

Résultat d’une alerte dans “Snort > Alerts”.

Un scan nmap du LAN1 au LAN2 est détecté par Snort. On peut voir l’IP source (193.168.2.10) et l’IP de destination (172.16.2.10).

Services / Snort / Alerts

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Alert Log View Settings

Interface to Inspect

LAN (em1)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

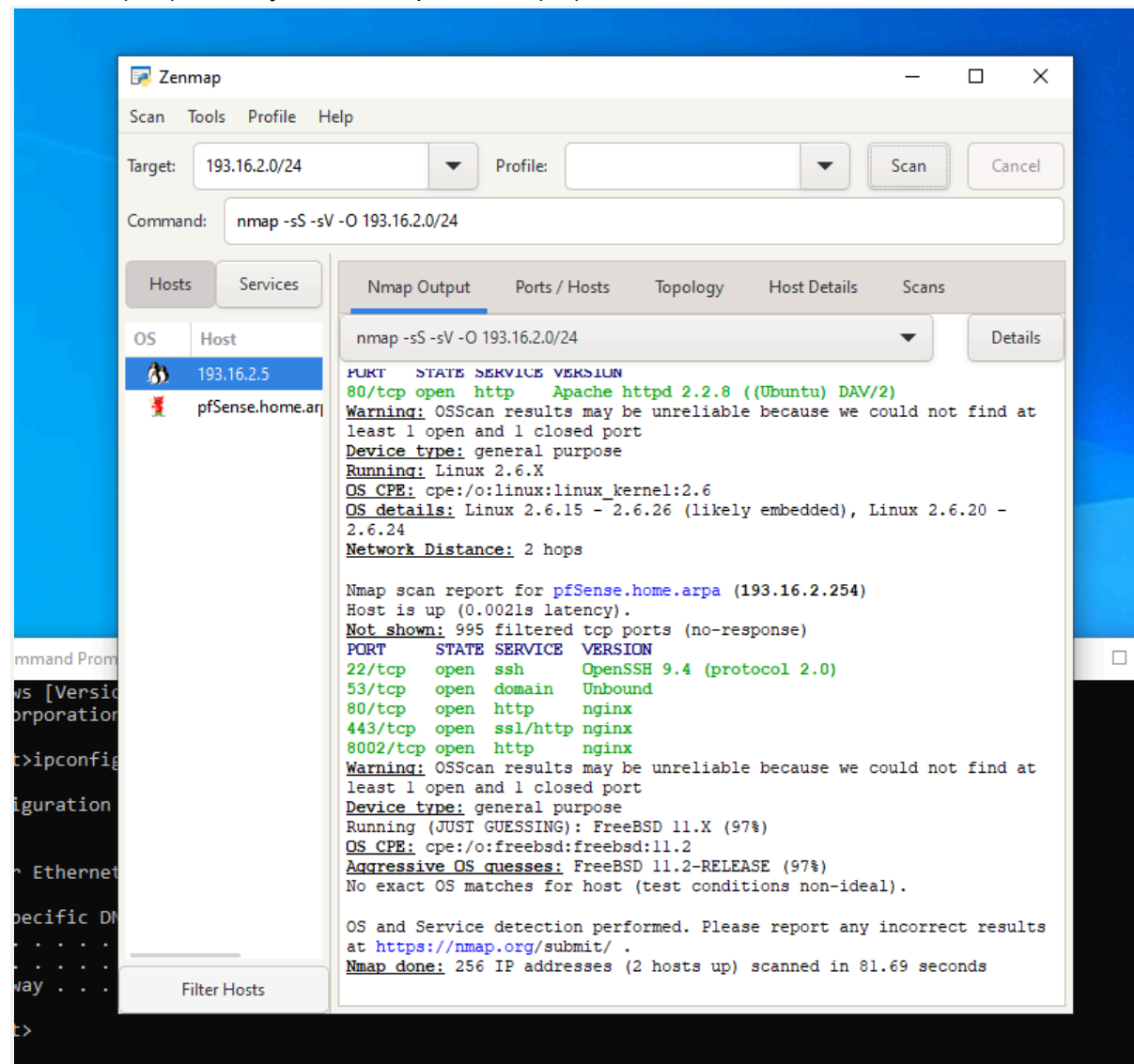
1 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-06-11 06:44:32		3	TCP	Unknown Traffic	193.168.1.10	42544	172.16.1.10	80	119:31	(http_inspect) UNKNOWN METHOD

Nous pouvons conclure que la configuration Snort a bien été réalisée.

## Analyse du réseau LAN 1 (193.168.2.0/24) à partir de Zenmap.

Nmap -sS -sV -O 193.168.2.0/24 → réalisation d'un scan SYN furtif (-sS) avec détection de version des services (-sV) et de système d'exploitation (-O) sur le réseau.



Cela nous permet d'en apprendre plus sur l'état du réseau, plus particulièrement Metasploitable 2 qui est extrêmement vulnérable et qui montre plusieurs ports ouverts.

## Résultats du scan Zenmap:

Starting Nmap 7.97 ( <https://nmap.org> ) at 2025-06-09 13:01 +0000

Nmap scan report for 193.16.2.5

Host is up (0.0033s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24

Network Distance: 2 hops

Nmap scan report for pfSense.home.arpa (193.16.2.254)

Host is up (0.0021s latency).

Not shown: 995 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.4 (protocol 2.0)

53/tcp open domain Unbound

80/tcp open http nginx

443/tcp open ssl/http nginx

8002/tcp open http nginx

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): FreeBSD 11.X (97%)

OS CPE: cpe:/o:freebsd:freebsd:11.2

Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)

No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

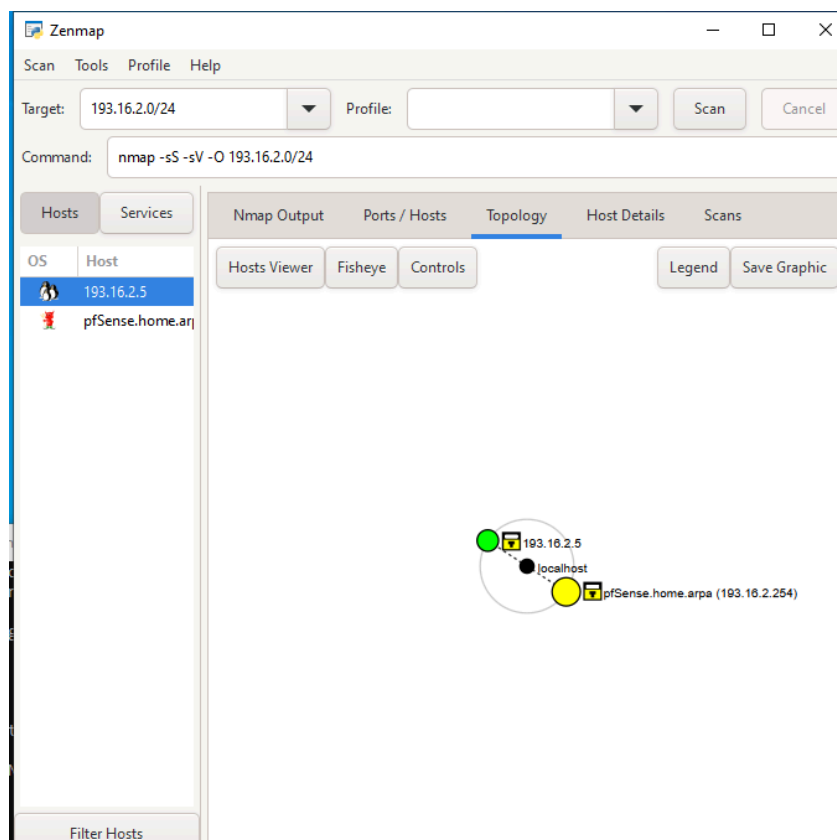
Nmap done: 256 IP addresses (2 hosts up) scanned in 81.69 seconds

## Voici la topologie de notre réseau:

Localhost représentant la machine responsable du scan.

193.168.2.5 représentant la machine Metasploitable 2.

[pfSense.home.arpa](#) (193.168.2.254) représentant la machine pfSense.





## **Conclusion**

Ce projet nous a permis d'en apprendre plus sur la sécurité des réseaux en nous offrant une approche pratique sur un réseau virtuel sécurisé. Nous sommes parvenus à installer et configurer pfSense avec un portail captif ainsi que des règles de filtrages, ainsi que Snort afin de détecter les anomalies. Nous avons ainsi pu renforcer nos compétences en configuration réseau et en sécurité informatique.