

CCI Campus

TP Pfsense

Cybersécurité

GEBUS Louis
15/06/2022

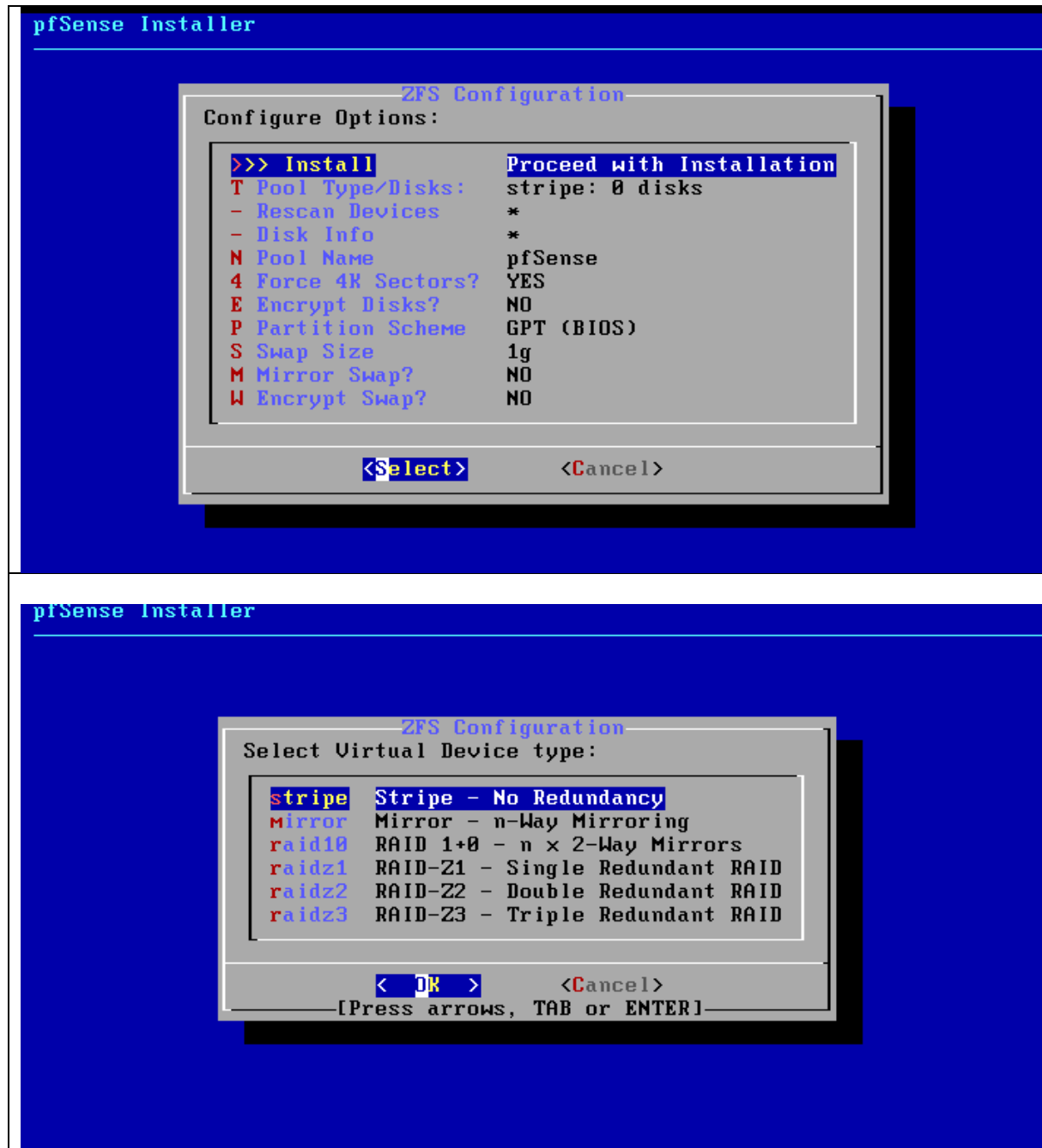
TP Pfsense

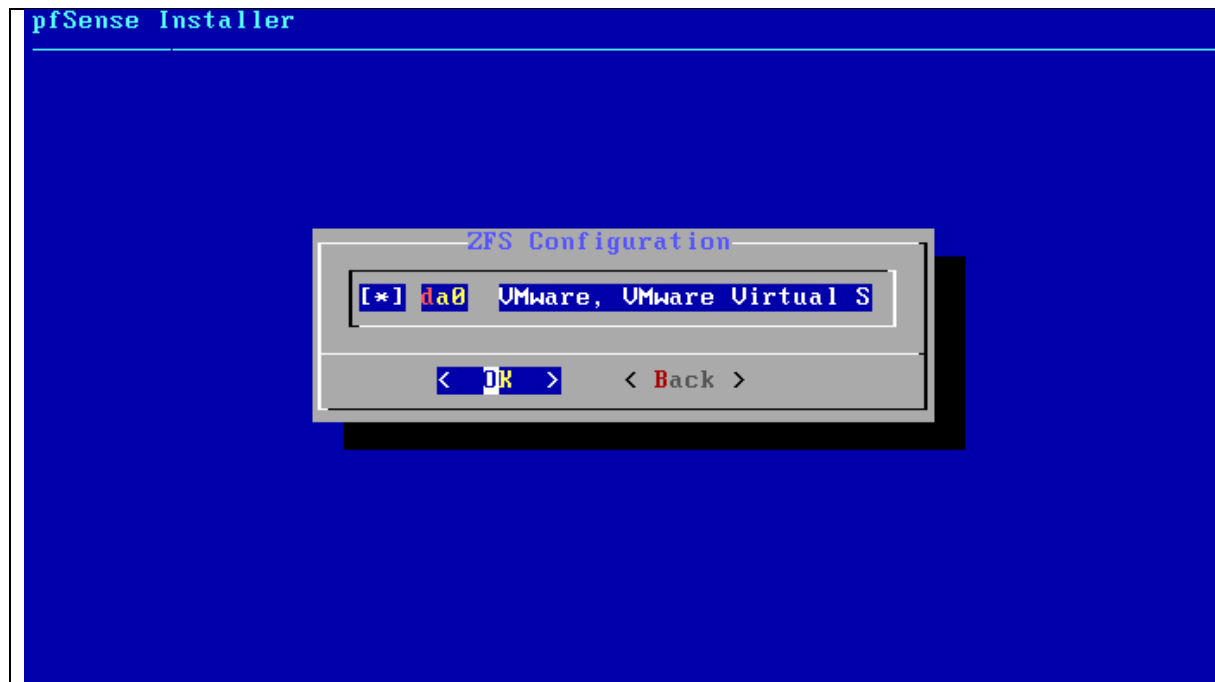
Table des matières

TP Pfsense.....	1
Installation/ configuration et paramétrage de Pfsense	1
Montage vm windows 10 pro	7
Filtrage : « deny all »	17
Filtrage : internet.....	19
Portail Captif.....	23

Installation/ configuration et paramétrage de Pfsense







pfSense Installer

Manual Configuration

The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?

< Yes >

< No >

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete
```

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
```

```
VMware Virtual Machine - Netgate Device ID: 2843bd92632052643419
```

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.135.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
```

- | | |
|-----------------------------------|----------------------------------|
| 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: █
```

VMware Virtual Machine - Netgate Device ID: 2843bd92632052643419

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 192.168.135.128/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24

- | | |
|-----------------------------------|----------------------------------|
| 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: 2

Available interfaces:

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

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

WAN (wan) -> em0 -> v4/DHCP4: 192.168.135.128/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24

- | | |
|-----------------------------------|----------------------------------|
| 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: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.254█

```

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: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.254

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

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.254

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

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

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

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

```

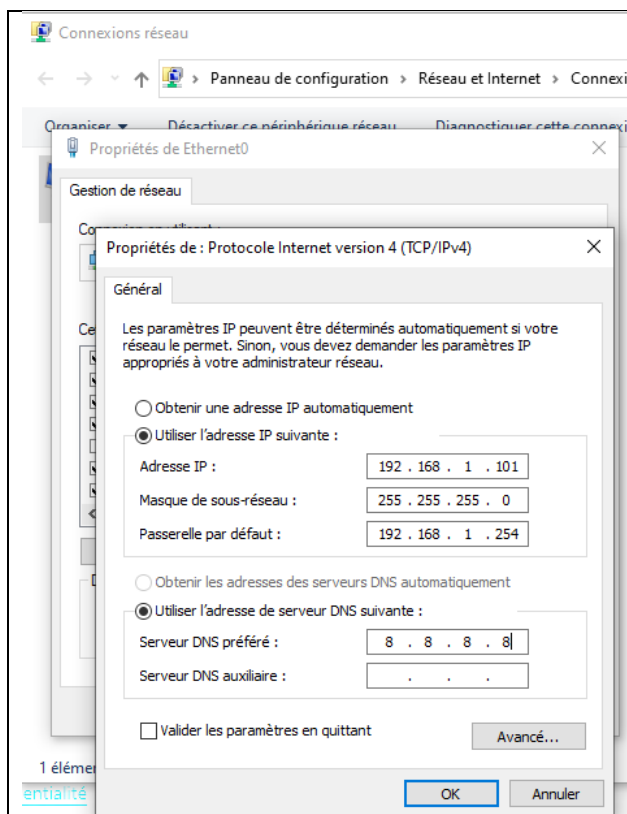
```
For a WAN, enter the new LAN IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>  
  
Enter the new LAN IPv6 address. Press <ENTER> for none:  
>  
  
Do you want to enable the DHCP server on LAN? (y/n) n  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...  
  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y  
  
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
Restarting webConfigurator...  
  
The IPv4 LAN address has been set to 192.168.1.254/24  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
http://192.168.1.254/  
  
Press <ENTER> to continue.█
```

La configuration de pfsense en ligne de commande est terminée

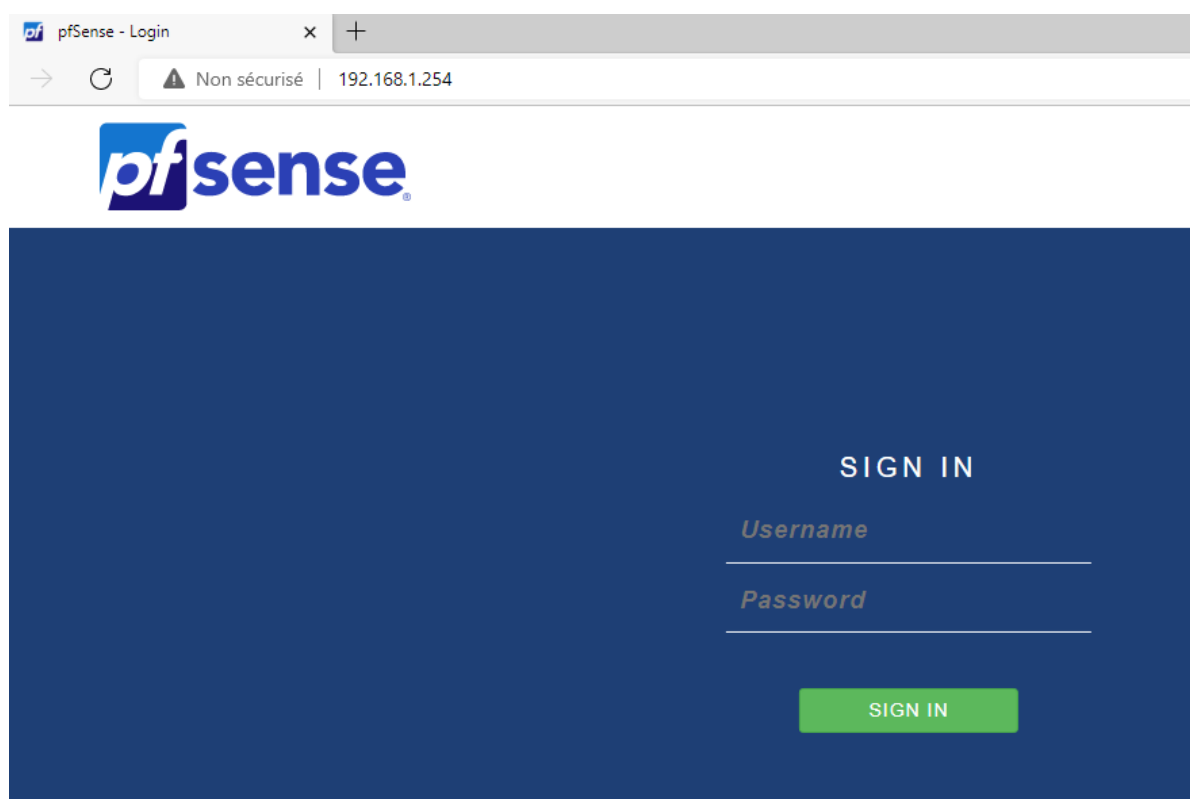
Nous pouvons passer au montage du windows 10 client

Montage vm windows 10 pro

Passage en static et en passerelle par defaults mettre l'adresse de Pfsense soit 192.168.1.101 :



Passage sur l'interface web : Depuis la vm en réseau local, il suffit d'ouvrir un navigateur web et d'y taper l'ip de Pfsense. C'est-à-dire la 192.168.1.254 pour le coup



Username : admin

Password : pfsense

Configuration du DNS de google à faire (8.8.8.8)

Suite à la connexion le msg suivant apparaît :

```
Message from syslogd@pfSense at Jun  1 13:41:25 ...
php-fpm[230041]: /index.php: Successful login for user 'admin' from: 192.168.1.101 (Local Database)
```

Nous arrivons sur le tableau de bord de pfsense

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.1.101 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 2843bd92632052643419
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE The system is on the latest version. Version information updated at Wed Jun 1 13:48:55 UTC 2022
CPU Type	Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	02 Hours 10 Minutes 27 Seconds
Current date/time	Wed Jun 1 13:51:31 UTC 2022
DNS server(s)	<ul style="list-style-type: none"> 127.0.0.1 192.168.135.2 8.8.8.8
Last config change	Wed Jun 1 13:48:03 UTC 2022

Configuration, dns de google de google à renseigner 8.8.8.8

Services / DHCP Server / LAN

The changes have been applied successfully.

LAN

General Options

Enable

☒ Enable DHCP server on LAN 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 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 below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers

☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

192.168.1.0

Subnet mask

255.255.255.0

Available range

192.168.1.1 - 192.168.1.254

Range

192.168.1.10

192.168.1.245

From

To

Servers

WINS servers

WINS Server 1

WINS Server 2

DNS servers

8.8.8.8

DNS Server 2

DNS Server 3

DNS Server 4

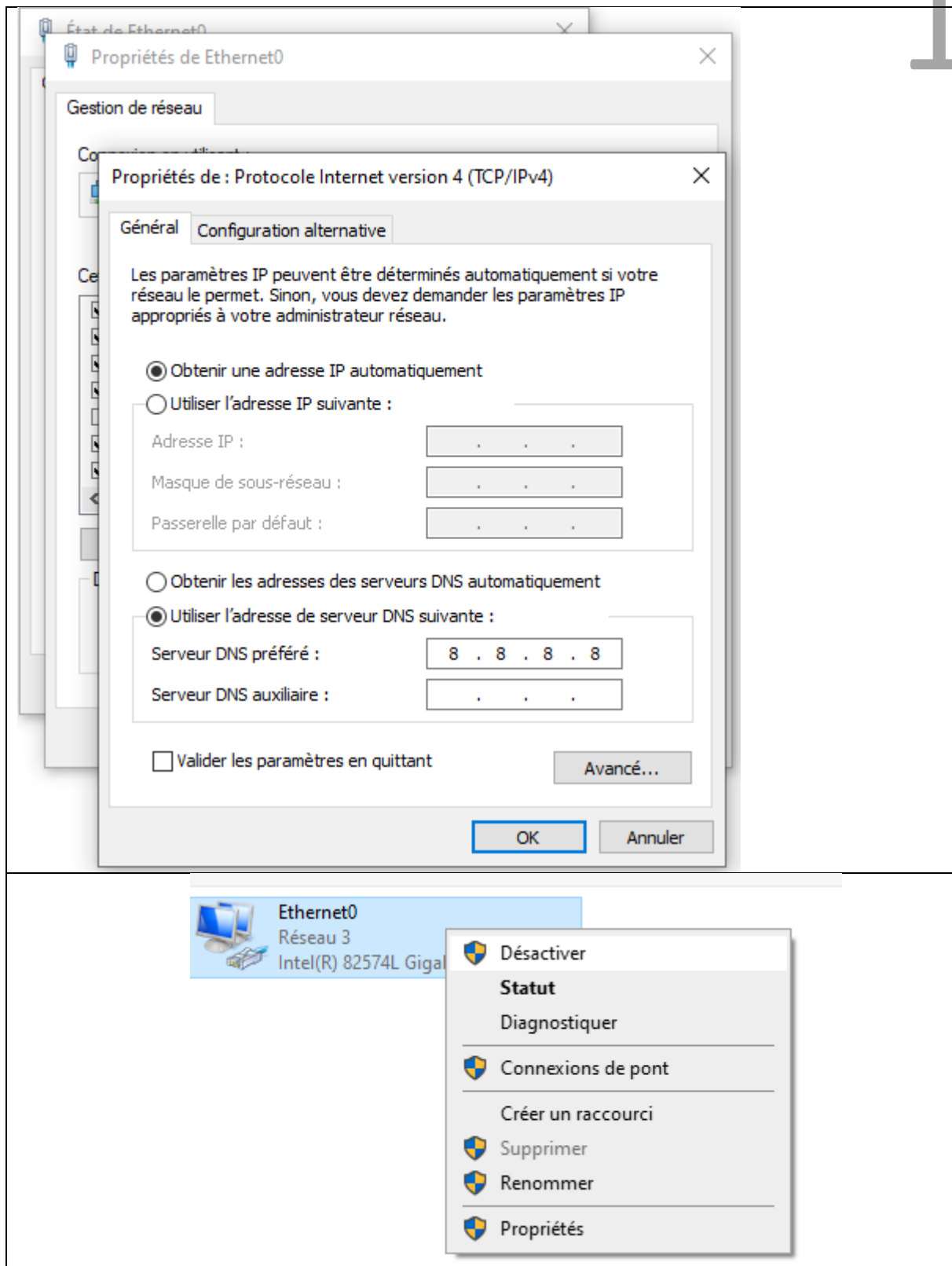
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

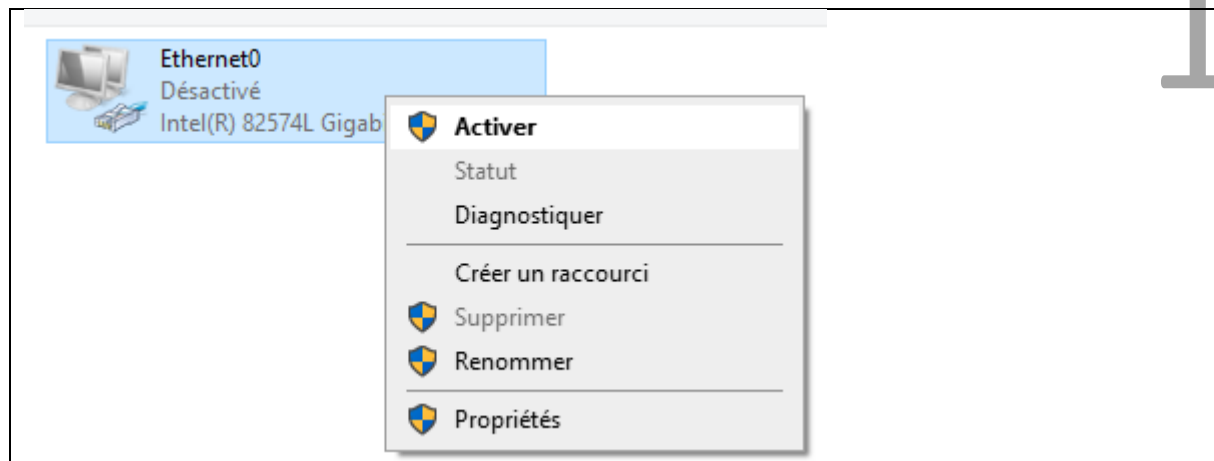
Ne pas oublier de cliquer sur save

Puis passage en automatique (DHCP) dans paramètre de carte réseau

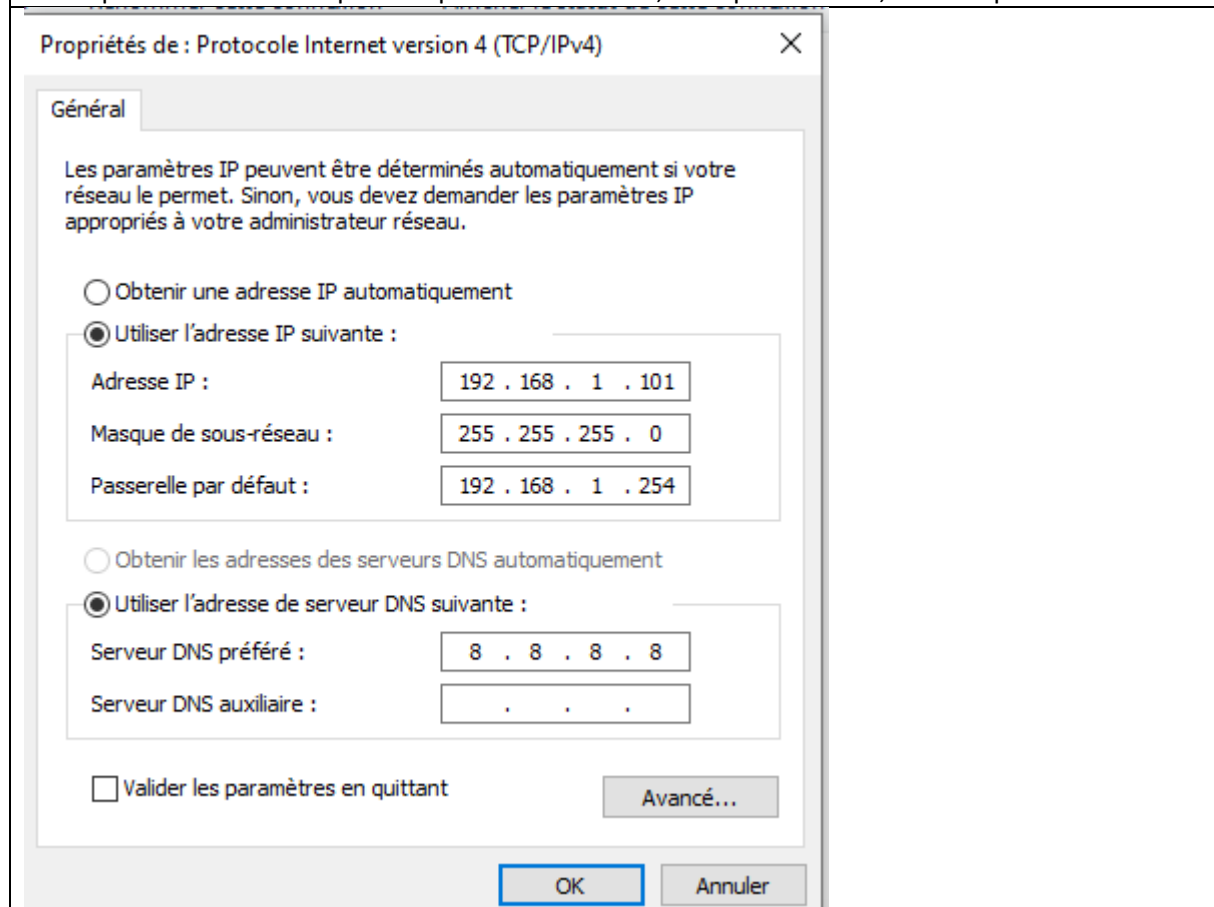
TP PFSense

GEBUS LOUIS





Le dhcp devait être activé pour le tp du dernier cours, mais pour celui là, il faut repasser en static :



Suite à des problèmes de dns j'ai tout reconfigurer, voici les nouvelles configurations :

WAN (wan)	-> em0	-> v4/DHCP4: 10.77.43.21/24
LAN (lan)	-> em1	-> v4: 192.168.50.254/24

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	-	Enabled	192.168.135.0
VMnet1	Custom	-	-	-	192.168.75.0
VMnet2	Bridged	Intel(R) Ethernet Connection (...)	-	-	-

< >

Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to: Automatic Settings...

☒ NAT (shared host's IP address with VMs) NAT Settings...

☐ Host-only (connect VMs internally in a private network)

☐ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet0

☒ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: Subnet mask:

Restore Defaults Import... Export... OK Cancel Apply Help

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	-	Enabled	192.168.135.0
VMnet1	Custom	-	-	-	192.168.75.0
VMnet2	Bridged	Intel(R) Ethernet Connection (...)	-	-	-

< >

Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to: Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

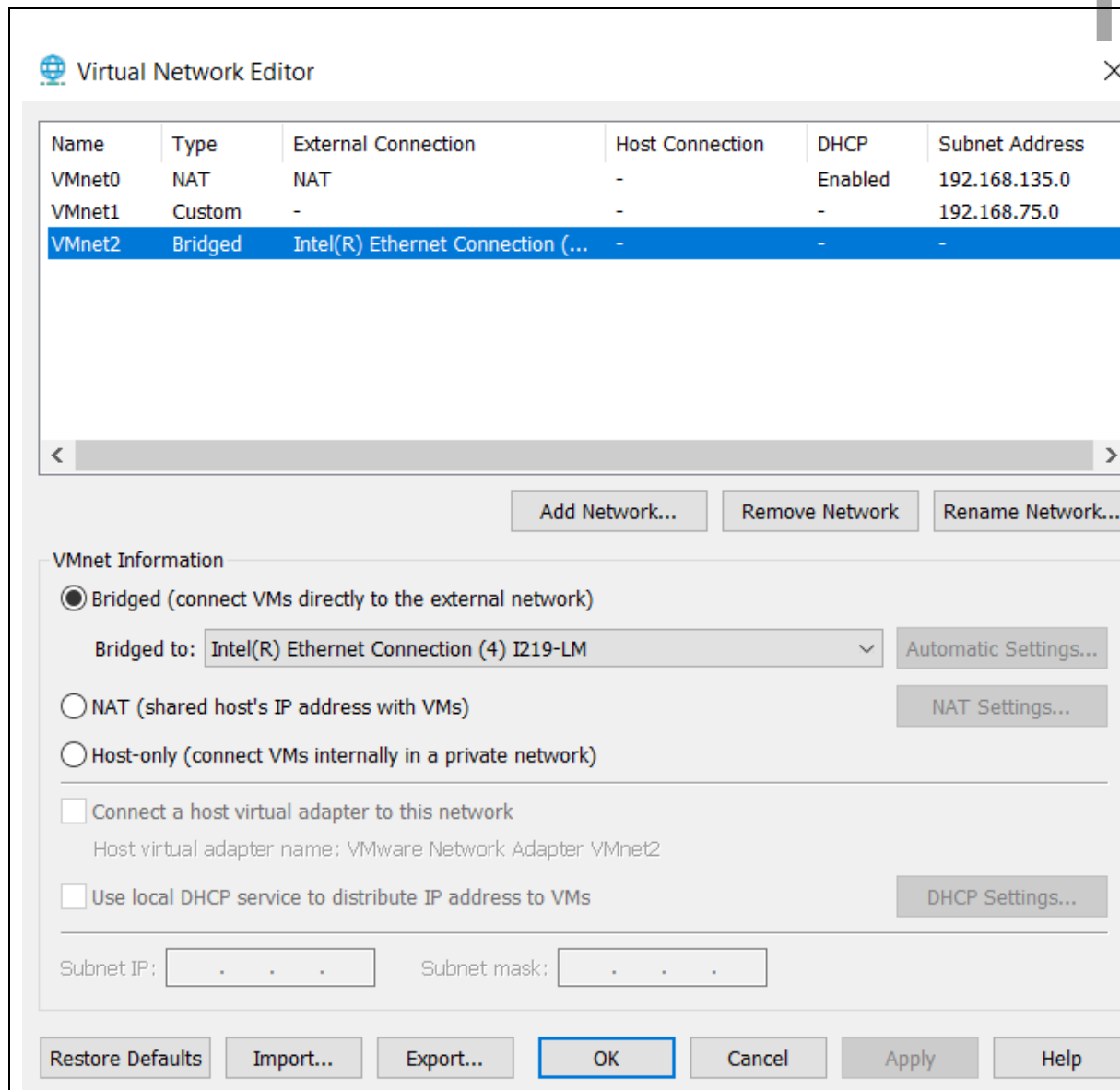
☐ Connect a host virtual adapter to this network

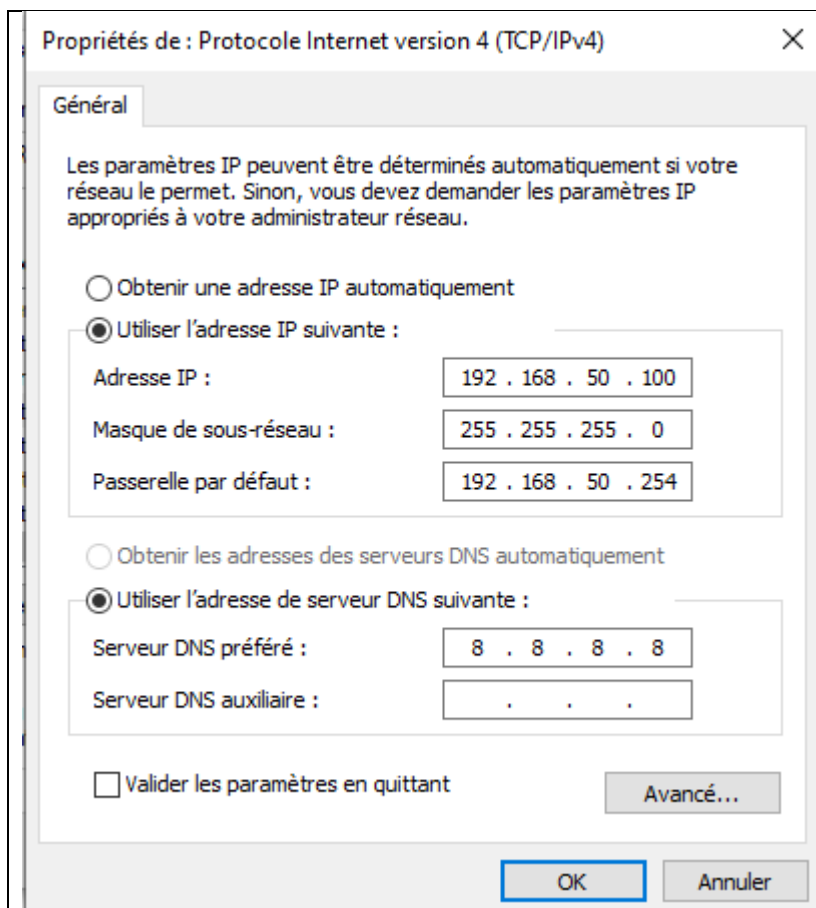
Host virtual adapter name: VMware Network Adapter VMnet1

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

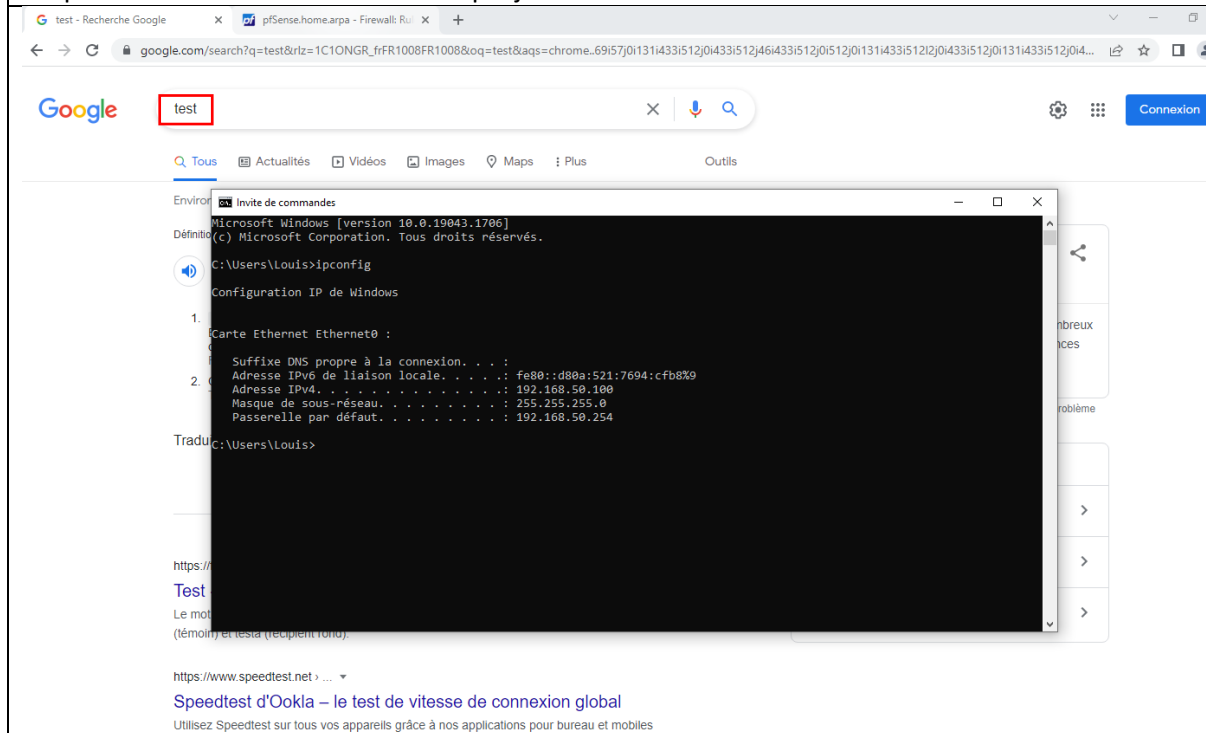
Subnet IP: Subnet mask:

Restore Defaults Import... Export... OK Cancel Apply Help





On peut voir sur le screen ci dessous que j'ai bien maintenant de nouveaux accès à internet :



Filtrage : « deny all »

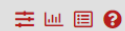
Je vais maintenant passer au filtrage « deny all »

Création d'une nouvelle règle :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 / 101 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 39 KiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	0 / 0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Configuration de la règle : Je bloque tout comme demander

Firewall / Rules / Edit



Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

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

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

Rule Information

Tracking ID

1655284513

Created

6/15/22 09:15:13 by admin@192.168.50.100 (Local Database)

Updated

6/15/22 09:22:33 by admin@192.168.50.100 (Local Database)

Save

Application des changements :

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

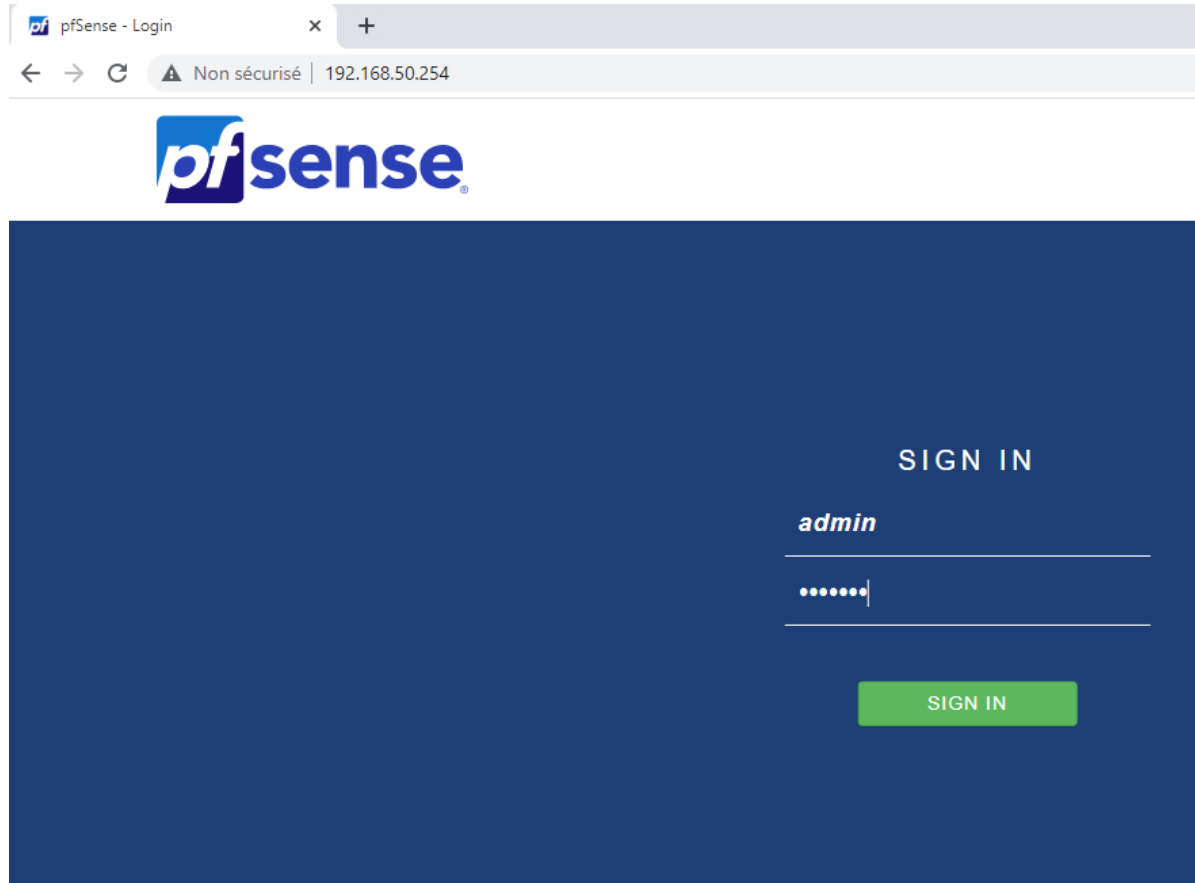
Je reboot ma vm pfsense en appuyant sur 5 puis y :

```
pfSense will reboot. This may take a few minutes, depending on your hardware.  
Do you want to proceed?
```

```
Y/y: Reboot normally  
R/r: Reroot (Stop processes, remount disks, re-run startup sequence)  
S: Reboot into Single User Mode (requires console access!)  
Enter an option: y
```

```
pfSense is rebooting now.
```

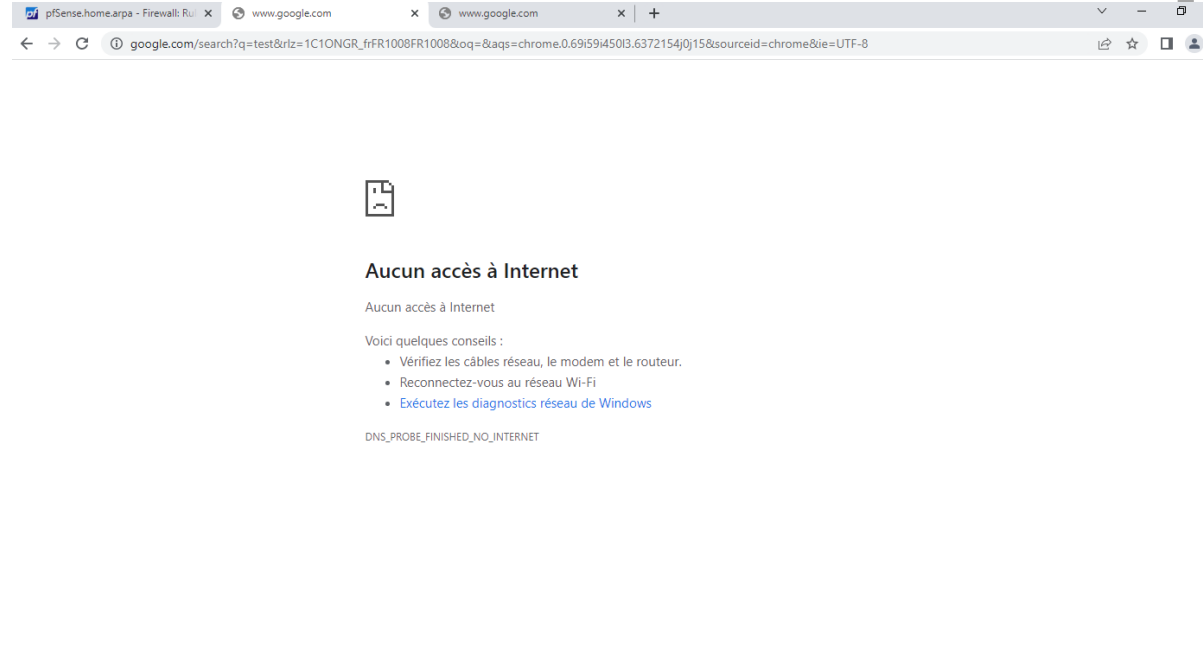
Je me reconnecte sur l'interface web :



Le message suivant apparaît :

```
Message from syslogd@pfSense at Jun 15 09:33:07 ...  
php-fpm[24491]: /index.php: Successful login for user 'admin' from: 192.168.50.10  
0 (Local Database)
```

Test : Je n'ai bien plus accès à internet



Filtrage : internet

Nous allons maintenant procéder au filtrage internet :

Création d'un alias :

Firewall / Aliases / Ports

IP Ports URLs All

Name	Values	Description	Actions
Alias1	80, 443, 53		

[+ Add](#) [Import](#)

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

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

Type

Port(s)

Hint Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	Entry added	Actions
80	Wed, 15 Jun 2022 09:10:57 +0000	
443	Wed, 15 Jun 2022 09:10:57 +0000	
53	Wed, 15 Jun 2022 11:36:57 +0000	


[Save](#) [Export to file](#) [+ Add Port](#)

Mise en place de la règle TCP/UDP et du lien avec l'alias :

☐ ☒ 16 / 2.07 MiB IPv4 TCP/UDP LAN net * * Alias1 * none Port 80 + 443 + 53

Configuration de cette règle :

Firewall / Rules / Edit





Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

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

LAN 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

(other)

Alias1

(other)

Alias1

From

Custom

To

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

Port 80 + 443 + 53

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

Rule Information

Tracking ID

1655292157

Created

6/15/22 11:22:37 by admin@192.168.50.100 (Local Database)

Updated

6/15/22 11:37:45 by admin@192.168.50.100 (Local Database)

Save

Mise en place de la règle ICMP :

☐ ☒ 0/0 B IPv4 ICMP * * * * * none

Configuration de cette règle :

Firewall / Rules / Edit

?

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

any

Alternate Host

Datagram conversion error

Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source

☐ Invert match

any

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

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

Rule Information

Tracking ID

1655292178

Created

6/15/22 11:22:58 by admin@192.168.50.100 (Local Database)

Updated

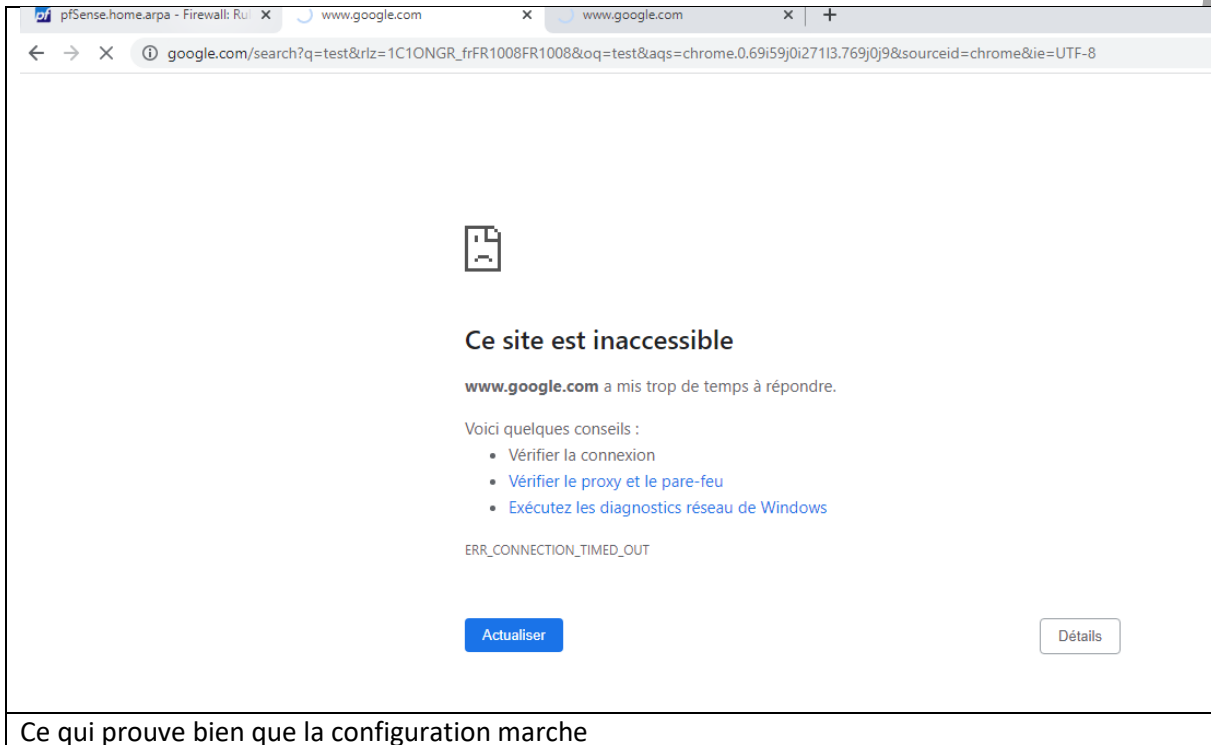
6/15/22 11:38:20 by admin@192.168.50.100 (Local Database)

Save

Suite à la mise en place de l'alias et l'application de ces 2 règles, nous allons faire le test :

Test 1 : J'ai bien de nouveau accès à internet

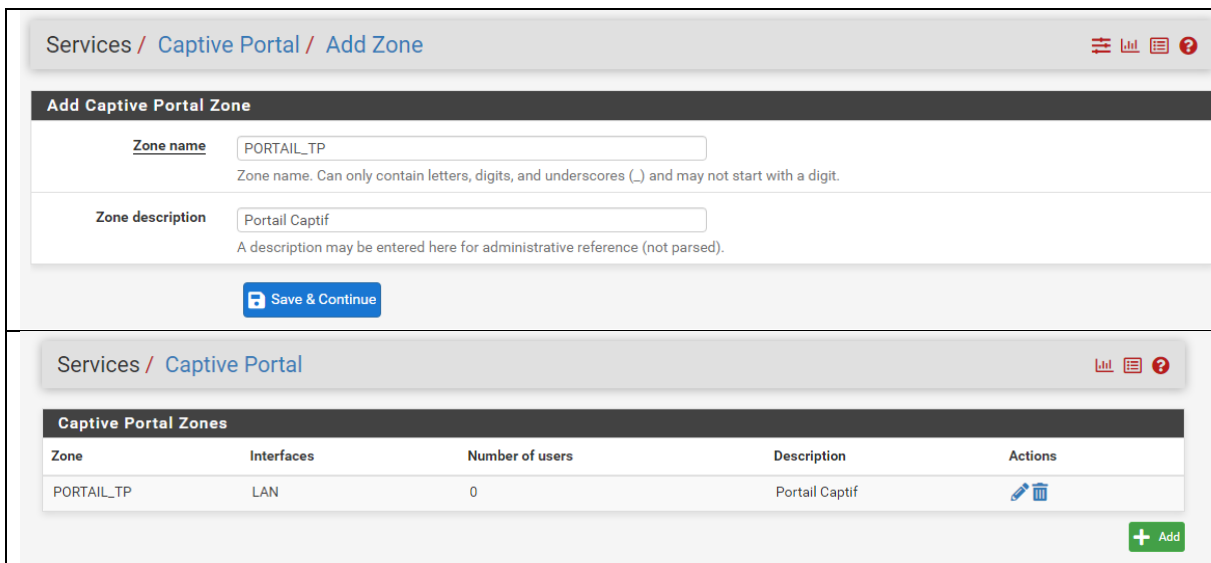






The screenshot shows a web browser window with multiple tabs. The active tab is a Google search page for the query "test". The page displays a large error message: "Ce site est inaccessible" (This site is inaccessible). Below this, it states "www.google.com a mis trop de temps à répondre." (www.google.com took too long to respond). It then provides some advice: "Voici quelques conseils : Vérifier la connexion, Vérifier le proxy et le pare-feu, Exécutez les diagnostics réseau de Windows". The error code "ERR_CONNECTION_TIMED_OUT" is visible. At the bottom, there are two buttons: "Actualiser" (Refresh) and "Détails" (Details).

Ce qui prouve bien que la configuration marche

Portail Captif



The screenshot shows the pfSense web interface for configuring a Captive Portal. The top navigation bar shows "Services / Captive Portal / Add Zone". The main content area is titled "Add Captive Portal Zone" and contains two input fields: "Zone name" (set to "PORTAIL_TP") and "Zone description" (set to "Portail Captif"). Below these fields is a "Save & Continue" button. The bottom section of the interface shows a table titled "Captive Portal Zones" with the following data:

Zone	Interfaces	Number of users	Description	Actions
PORTAIL_TP	LAN	0	Portail Captif	 

At the bottom right of the table, there is a green "Add" button.

System / User Manager / Groups / Edit

Users
Groups
Settings
Authentication Servers

Group Properties

Group name
Portail

Scope
Local

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description
Utilisateurs du Portail

Group description, for administrative information only

Group membership

admin
agent

Not members
Members

Move to "Members"
Move to "Not members"

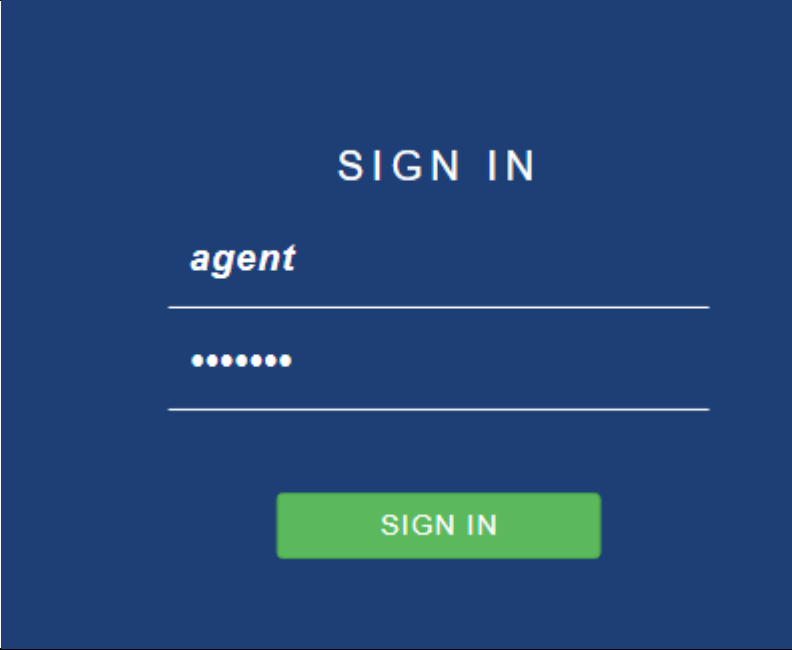
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges

Name	Description	Action
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	

Add

PS : Je ne montre pas toutes les étapes, car il y aurait beaucoup trop de screens



pfSense

COMMUNITY EDITION

System ▾Status ▾Help ▾

System / User Manager / Users

Users

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	agent	Agent 007	✓	Agent	
<input type="checkbox"/>	test	Un utilisateur du Portail	✓	Portail	

Add

Delete

Je me suis donc connecté avec le « compte » agent

Merci d’avoir pris le temps de lire mes 26 pages de tp ^^