

16/10/2023

TP PFSense : COMPTE RENDU

Contenu de la procédure

1. Introduction.....	1
1. Définition du sujet.....	1
2. Problématique.....	1
3. La méthode utiliser.....	1
2. Création de la machine virtuelle	2
1. Création de la vm.....	2
2. Installation de la vm pf sense	2
3. Configuration de base en CLI.....	4
3. Configuration sur l'interface web.....	5
1. Setup de base	5
2. Configuration des interfaces DMZ et WIFI	7

1. Introduction

1. Définition du sujet

Un pare-feu, en informatique, est un peu comme un gardien de sécurité numérique pour votre réseau. Son rôle principal est de protéger un réseau informatique en contrôlant le trafic entrant et sortant. Imagine-le comme une barrière qui filtre tout ce qui tente d'entrer ou de sortir de votre réseau.

*openai.com

2. Problématique

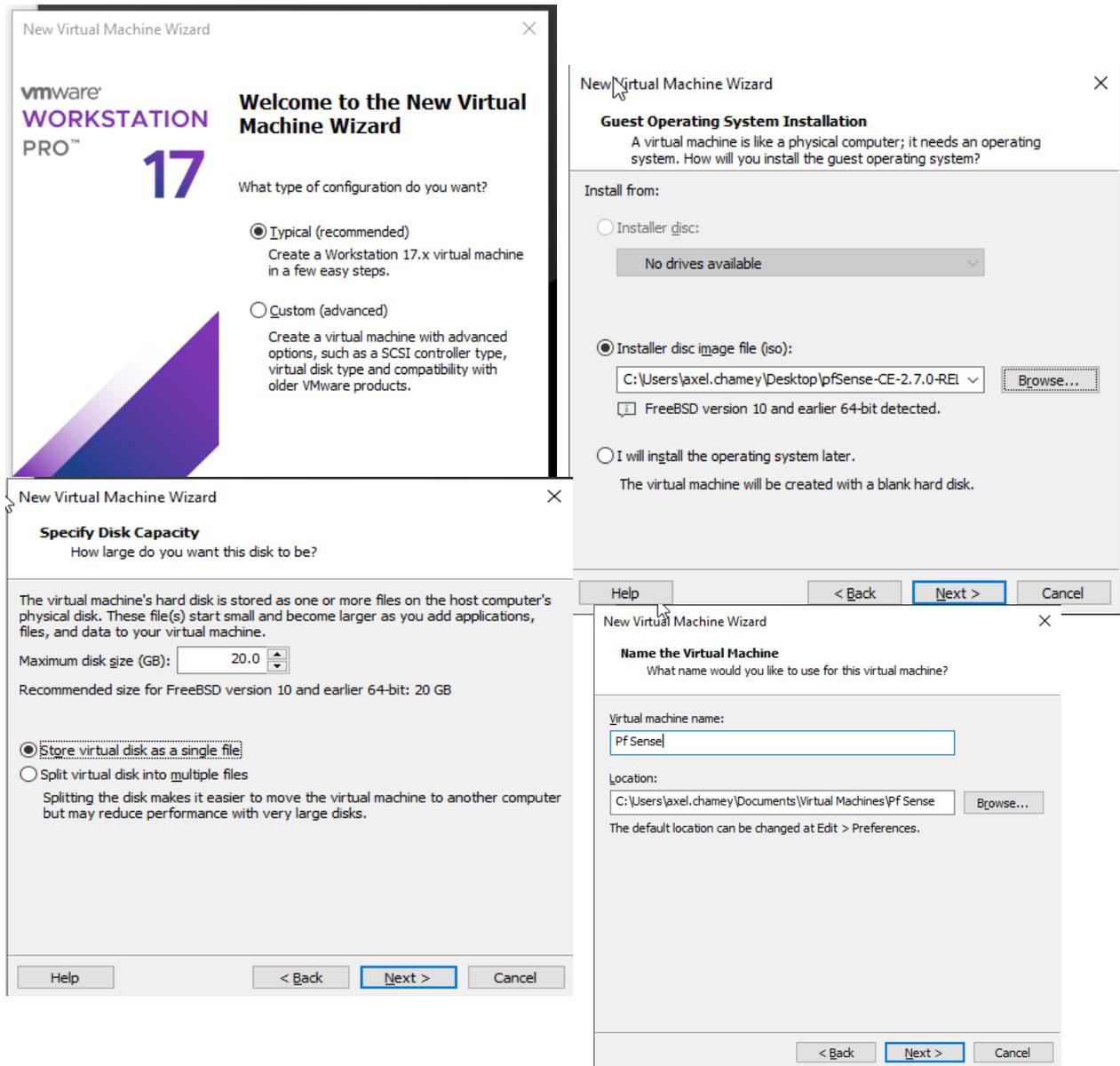
Mise en place d'un pare-feu sur notre plateforme entre le réseau wan et nos réseaux avec des règles de filtrages, un réseau DMZ et un réseau wifi avec un portail captif

3. La méthode utiliser

Création d'une vm pfsense, création d'un réseau lan réserver pour l'interconnexion entre le pare-feu et le routeur principale, ajout des rôles et des règles

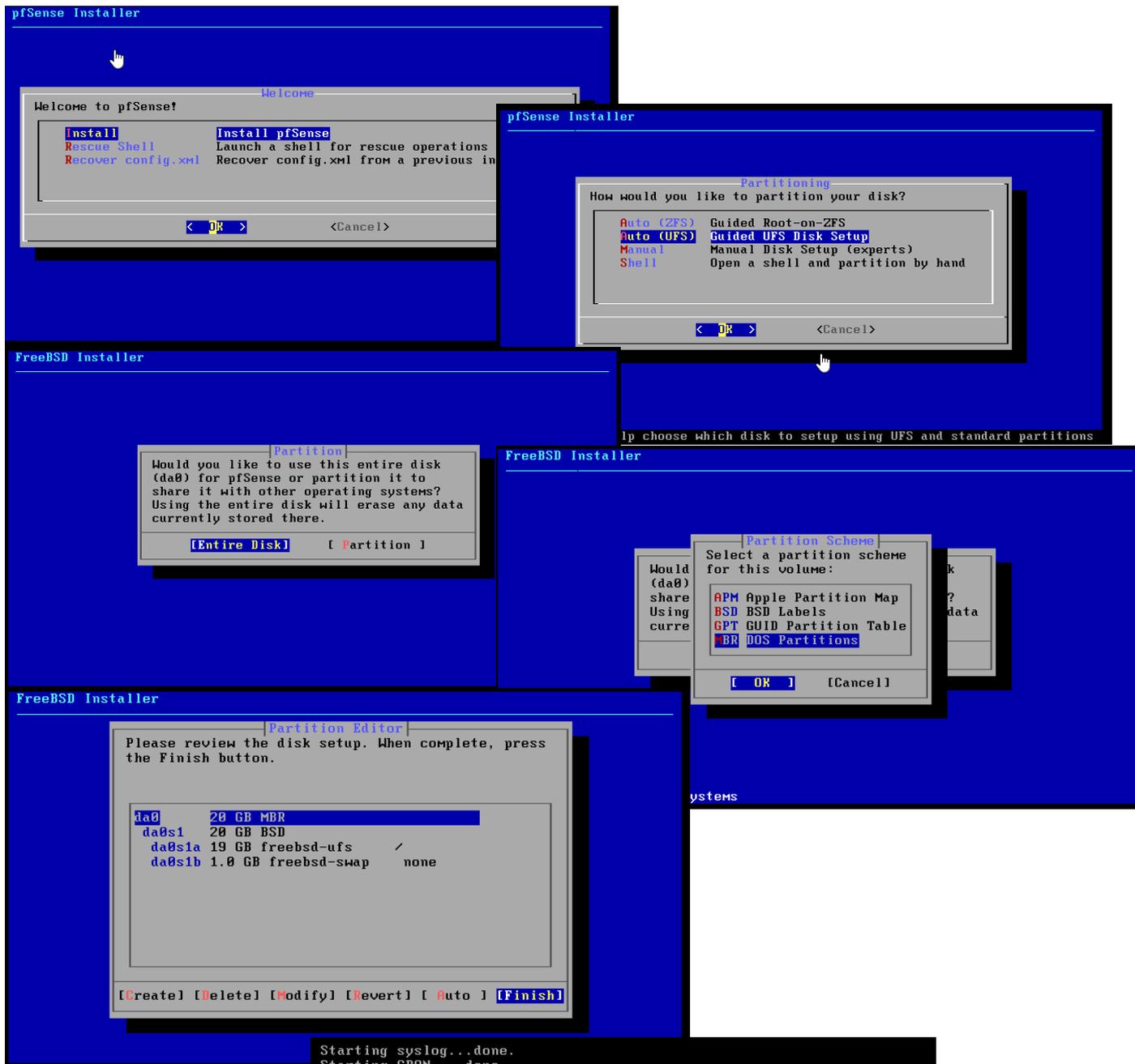
2. Création de la machine virtuelle

1. Création de la vm



ICI J'utilise VMWARE workstation 17 mais un hyperV windows fera aussi bien l'affaire

2. Installation de la vm pf sense



Nous voila sur le pfsense :

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: b5cfd7a08df693e5e2f9

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.113.137/24
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: 1
```

3. Configuration de base en CLI

```
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

Dans un premier temps on selectionne l'option 2 pour fixer l'adresses ip de interface LAN

On sélectionne l'interface LAN (option 2)

```
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 number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.30
```

On rentre notre adresse ip

En général on configure une ip manuellement mais si vous voulez le faire via DHCP rentrez « y »

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

```
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 27
```

La c'est le masque de votre réseau

Faite ENTRE

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

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

Faite NON

Faite ENTRE

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

```
Do you want to enable the DHCP server on LAN? (y/n) n
```

Faite NON

Faite NON

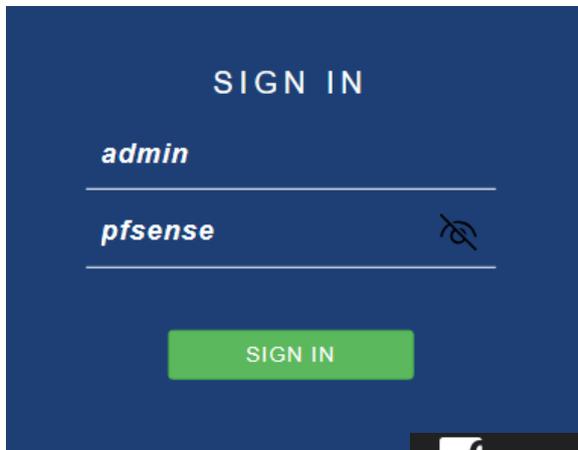
```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.113.137/24
LAN (lan)      -> em1      -> v4: 192.168.10.30/27
```

Et voila, vous avez bien configurer votre interface lan
Vous pouvez désormais acceder à l'interface web

3. Configuration sur l'interface web

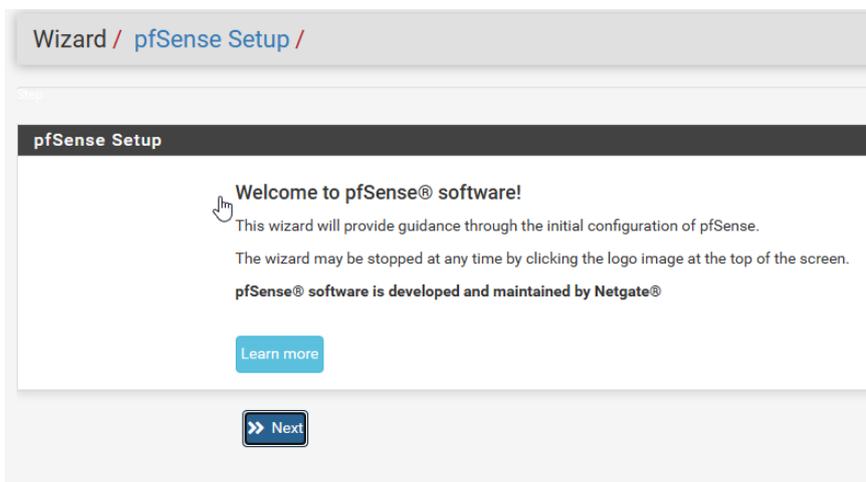
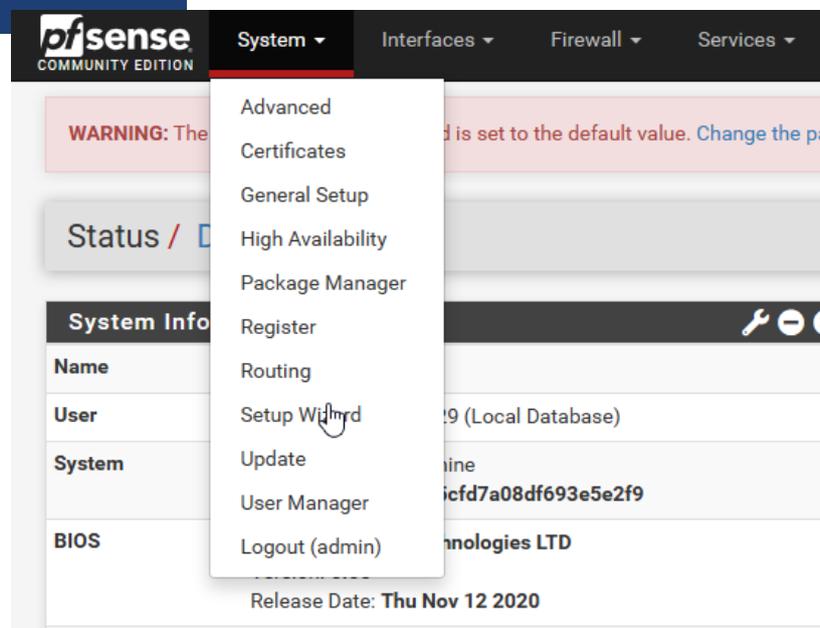
1. Setup de base



Connectez vous sur l'interface web du routeur depuis un poste qui est connecter sur le même réseau

Les identifiants par default sont admin : pfsense

Cliquez sur le menu déroulant « System » puis « Setup Wizard »



Cliquez sur >> NEXT

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TL Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not work. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries, visit Services > DNS Resolver and enable manually configured DNS servers below for client queries.

Primary DNS Server

Secondary DNS Server

Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

Rentrez un nom pour votre PF, le nom de domaine et les ip des serveurs dns (EXTERNES)

Cliquez sur next

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

[» Next](#)

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

[» Next](#)

ICI on configure l'IP et le masque de notre pare-feu

Et enfin cliquez sur reload

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

[» Reload](#)

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates or things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

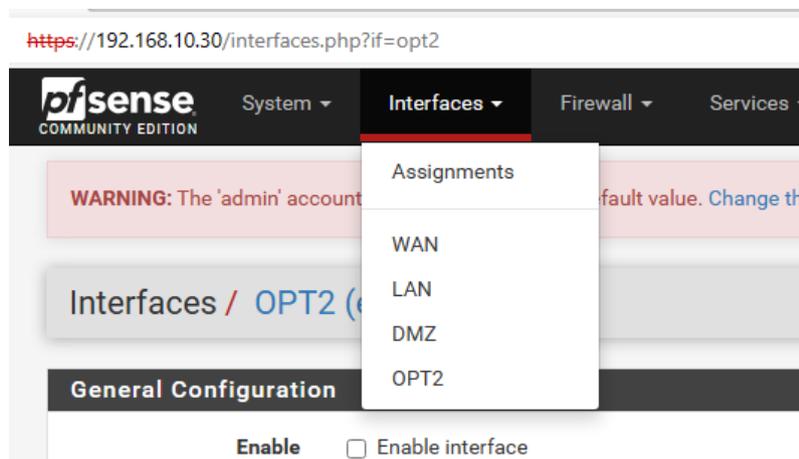
User survey

Please help all the people involved in improving and expanding pfSense (anonymous)

[Anonymous User Survey](#)

2. Configuration des interfaces DMZ et WIFI

Rendez-vous dans le menu interface de votre routeur



Interface	Network port	
WAN	em0 (00:0c:29:f2:71:be)	
LAN	em1 (00:0c:29:f2:71:c8)	Delete
OPT1	em2 (00:0c:29:f2:71:d2)	Delete
Available network ports:	em3 (00:0c:29:f2:71:dc)	+ Add

Ajouter une première interface en cliquant sur le bouton « +ADD », ici ce sera l'interface DMZ

Interfaces / OPT1 (em2)

General Configuration

Enable Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in a private address space, too.

Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

Configurez les paramètres de la nouvelle carte réseau

Vous pouvez ainsi paramétrer au temps de carte réseau que vous en avez sur votre routeur