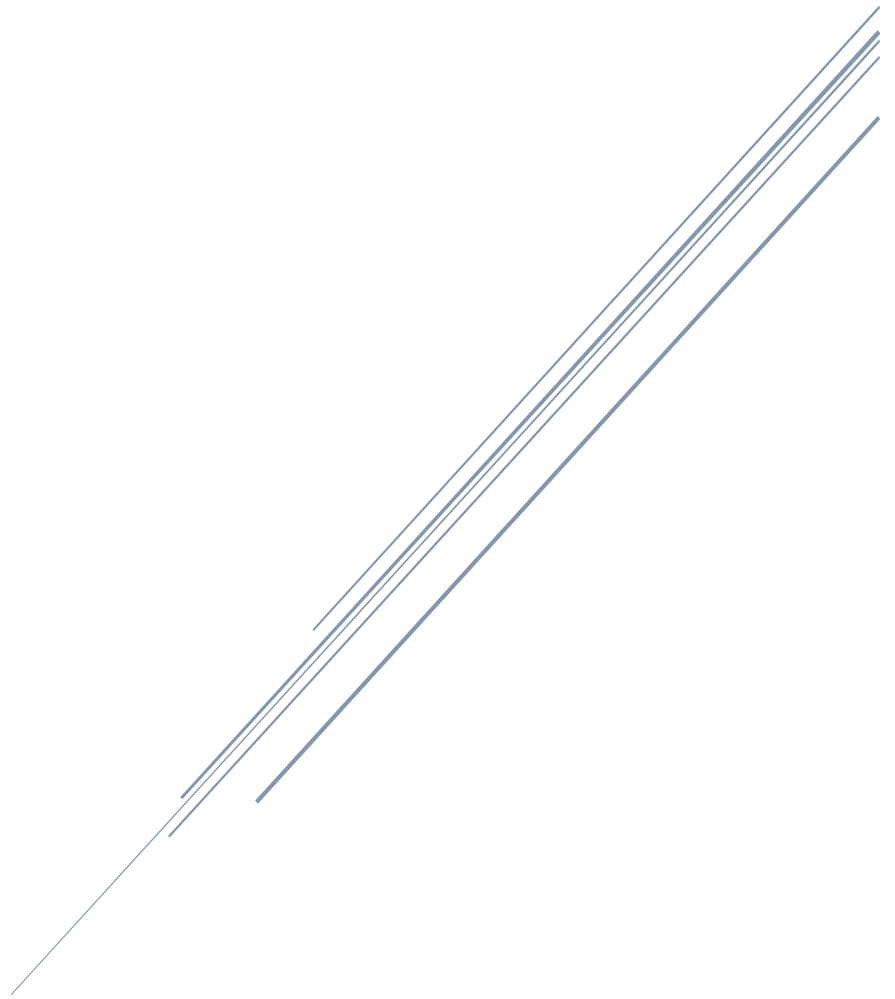


DESCRIPTION D'UNE MISSION

BTS SIO SISR



Sommaire:

Le cahier des charges3-4

Contexte	3
Expressions des besoins	3
Outils disponibles	3
Description de l'existant.....	4
Délais	4

Pfsense..... 5-10

Installation	5-6
Configuration du NAT	7
Configuration DHCP & DNS	8-9
Règles de pare-feu.....	10

Test 12-16

Test du DHCP	12-13
Test du réseau NAT.....	14
Test du DNS	15
Test des règles de pare-feu	16

Bilan.17

Le cahier des charges

Contexte :

L'entreprise Madnot vient de faire l'acquisition de nouveau bureau pour son activité, elle souhaite donc qu'un accès internet soit mis en place.

En tant qu'administrateur systèmes et réseau, nous avons reçu comme missions de mettre en place l'infrastructure permettant l'accès à internet pour les futurs salariés. L'entreprise dispose de deux ordinateurs sous Windows 10 pour les 2 salariés et d'un serveur sous Debian 11.

Expression des besoins :

Mise en place d'un routeur

- Configuration d'un réseau local avec accès internet
- Configuration DHCP
- Configuration DNS
- Mise en place de règles de pare-feu pour qu'un serveur local soit accessible en SSH via le réseau public

Outils disponibles :

Un serveur nous a été mis à disposition, il s'agit d'un HP BL460C G8 (Blade) dans un HP C7000. Nous disposons d'un accès IPMI (ILO) à ce serveur. Un hyperviseur ESXI est installé sur celui-ci.



Ci-dessus à gauche le serveur HP BL460C G8 mis à disposition, il s'agit d'une lame qui s'insère dans un châssis ici un HP C7000 (à droite) qui comporte 16 lames.

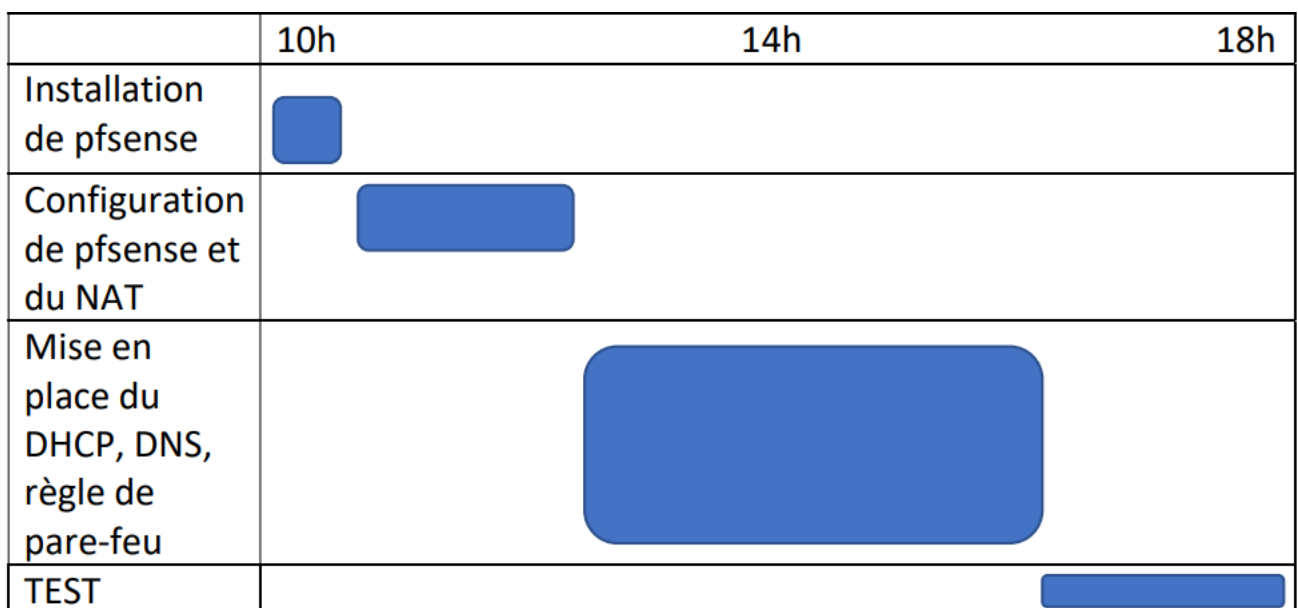
Description de l'existant :

Une FTO Orange est présente sur le site, la box orange (avec IP publique) a été installée et configurée. Un HP C7000 est présent dans la baie réseau de l'entreprise, une lame HP BL460C G8 installer sous ESXI nous ai mis à disposition pour nos besoins.

Délais :

Nous devons intervenir le 16/01/2022 pour la mise en place du réseau, nous disposons de la journée entière pour cette mission, notre journée commence à 10h et finis à 18h.

Voici ci-dessous un diagramme de Gantt qui représente l'avancement de la mission :

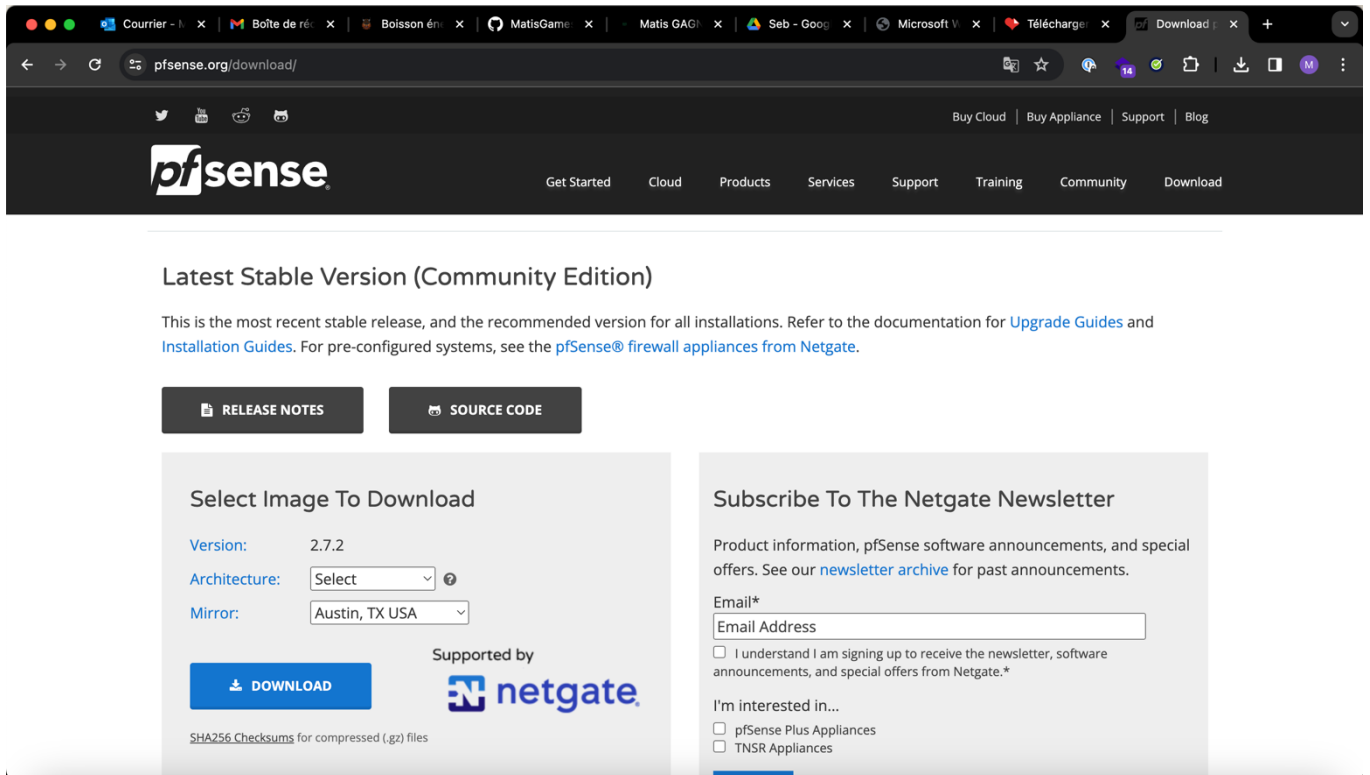


Pfsense :

Installation :

PfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.

Pour son installation nous allons télécharger l'ISO de pfsense sur leur site officiel dans l'onglet download :

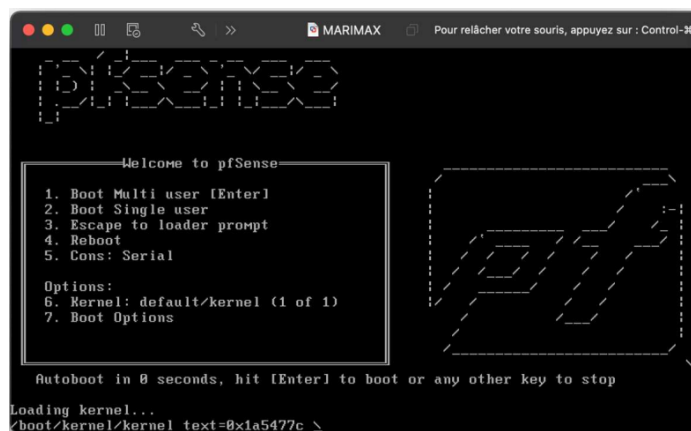


The screenshot shows the pfSense website's download page. The browser's address bar displays 'pfsense.org/download/'. The website header includes the pfSense logo and navigation links: 'Get Started', 'Cloud', 'Products', 'Services', 'Support', 'Training', 'Community', and 'Download'. Below the header, the page title is 'Latest Stable Version (Community Edition)'. A sub-header states: 'This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#).' Two buttons are visible: 'RELEASE NOTES' and 'SOURCE CODE'. The main content area is divided into two columns. The left column, titled 'Select Image To Download', shows 'Version: 2.7.2', 'Architecture: Select', and 'Mirror: Austin, TX USA'. A blue 'DOWNLOAD' button is present, along with the 'Supported by netgate' logo and a note: 'SHA256 Checksums for compressed (.gz) files'. The right column, titled 'Subscribe To The Netgate Newsletter', contains a text box for 'Email Address', a checkbox for 'I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate.*', and a section 'I'm interested in...' with checkboxes for 'pfSense Plus Appliances' and 'TNSR Appliances'.

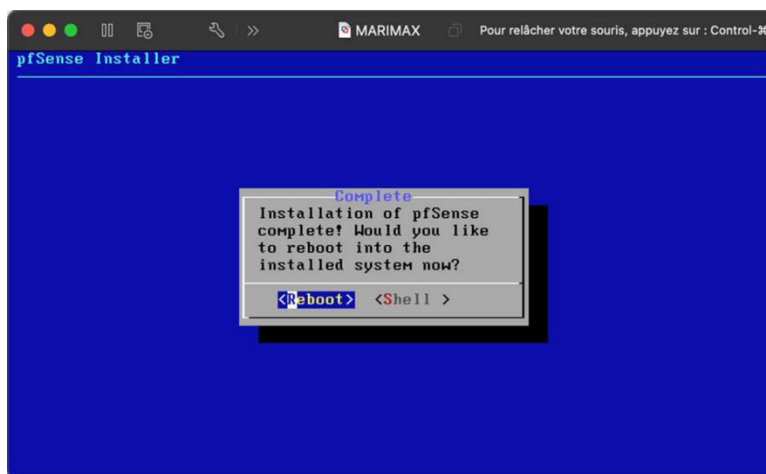
Pour notre routeur pfsense nous avons besoin de 2 cartes réseau sur notre machine virtuelle, une pour le WAN (réseau privé) et une deuxième pour le LAN (réseau local) nous allons mettre en place un NAT entre ces deux réseaux.

Nous devons donc installer une carte réseau qui sera utilisée pour le réseau WAN et une seconde carte réseau qui sera elle utilisée pour le réseau LAN. Le WAN est le réseau public ici 192.168.1.0, il s'agit du réseau LAN de notre routeur orange.

Le LAN est le réseau local ici 192.168.10.0 Une fois nos deux cartes réseau installées, nous pouvons démarrer l'installation de PfSense.



Nous complétons l'installation en entrant différents paramètres.



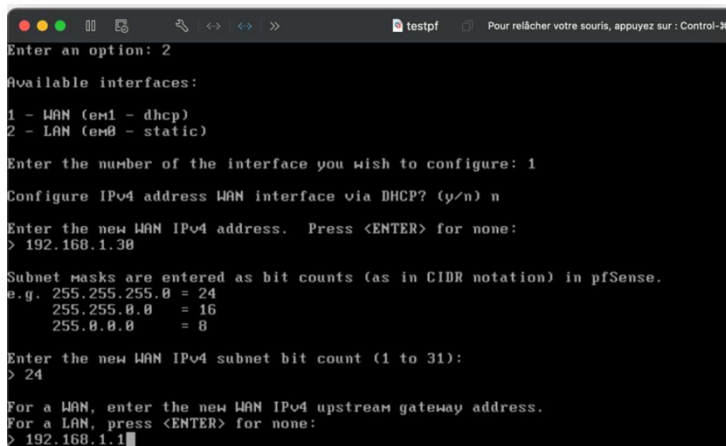
Configuration du NAT :

NAT (Network Address Translation) est un processus de modification des adresses IP et des ports source et de destination. La traduction d'adresses réduit le besoin d'adresses publiques IPv4 et masque les plages d'adresses réseau privées.

Le processus est généralement effectué par des routeurs ou des pare-feux.

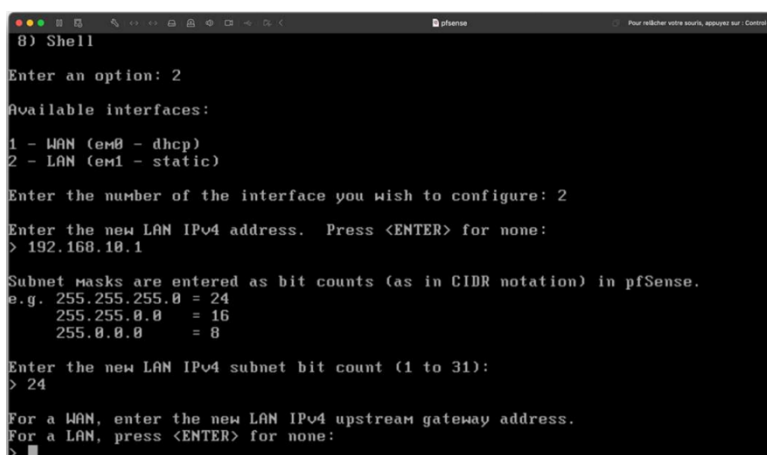
Pour cela nous allons premièrement référencer l'interface LAN et WAN, dans notre cas l'interface em0 correspond à l'interface LAN (192.168.10.0) et l'interface em1 correspond à l'interface WAN (192.168.1.30).

Nous devons ensuite assigner les IP aux interfaces. Nous commençons avec l'interface WAN, nous lui attribuons une IP du réseau LAN de la box orange, nous renseignons l'IP locale de la box orange en tant que IPV4 upstream gateway :



```
Enter an option: 2
Available interfaces:
1 - WAN (em1 - dhcp)
2 - LAN (em0 - static)
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.30
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 WAN IPv4 subnet bit count (1 to 31):
> 24
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1
```

Nous configurons ensuite l'interface du LAN avec l'IP 192.168.10.1 :



```
8) Shell
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp)
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:
> 192.168.10.1
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 31):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

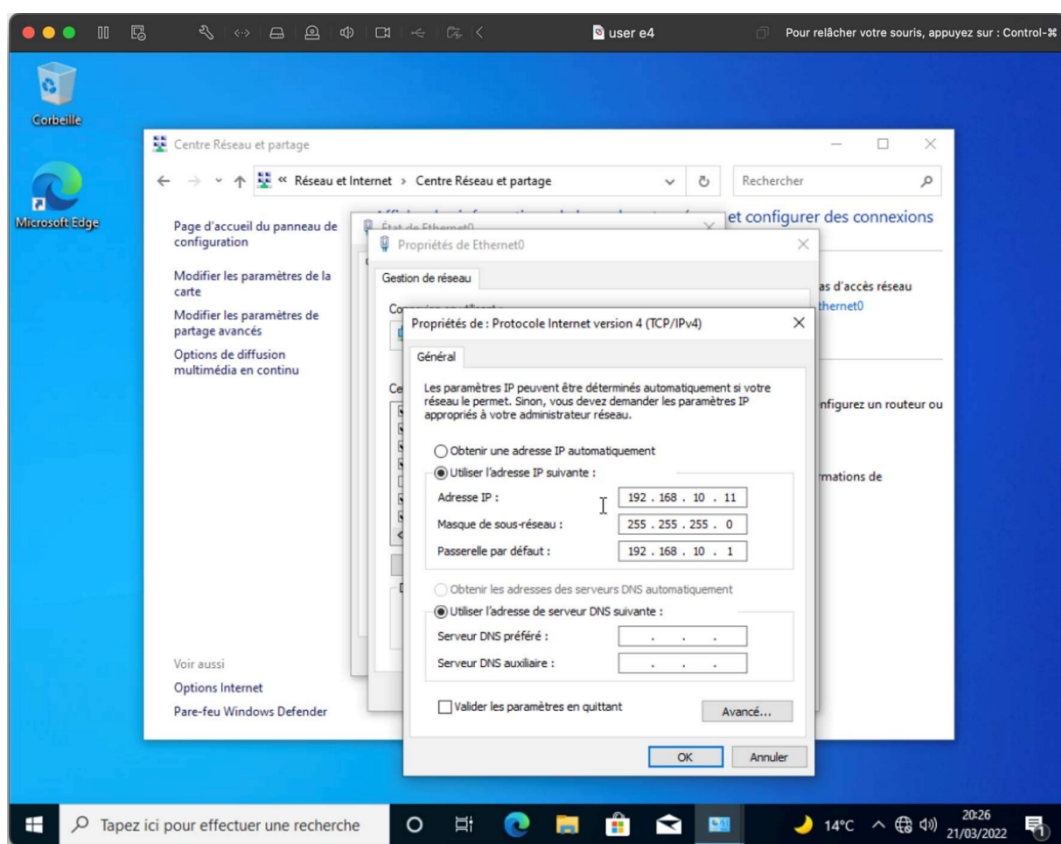
Notre NAT est maintenant configuré et nous pouvons depuis le réseau local accéder au réseau public.

Configuration DHCP & DNS :

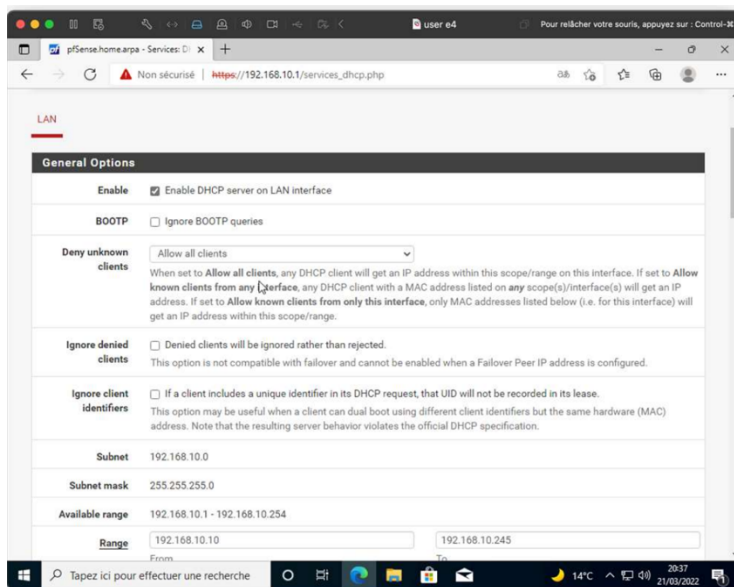
Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.

Le Domain Name System ou DNS est un service informatique distribué utilisé qui traduit les noms de domaine Internet en adresse IP ou autres enregistrements.

Pour la configuration du DHCP et du DNS nous avons besoin d'accéder à l'interface WEB de pfSense qui est accessible depuis le réseau local, pour cela nous allons donc utiliser un des ordinateurs présents dans ce réseau et via un navigateur accédez à 192.168.10.1. Il n'y a pas encore de DHCP nous devons donc paramétrer les réglages réseau de l'ordinateur utilisé à la main.

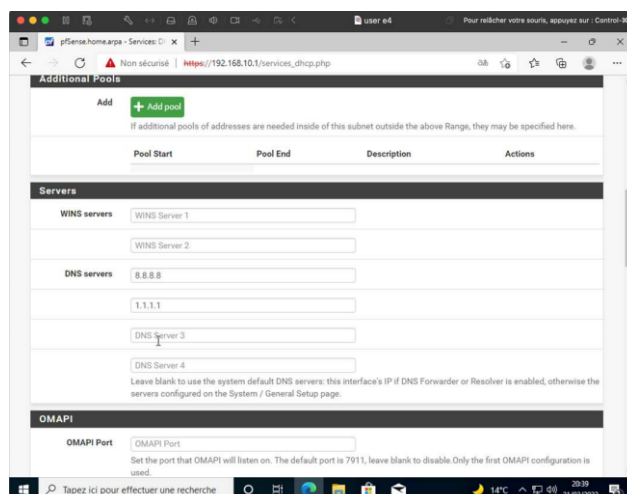


Sur l'interface web de pfSense nous rendons dans « services » puis dans « DHCP server » nous y entrons différents paramètres et notamment la plage d'adresses IP que nous souhaitons attribuer en DHCP.



Nous configurons ensuite le serveur DNS qui sera attribué, ici nous utiliserons les serveurs DNS de Google (8.8.8.8) en serveur numéro 1 et ceux de clouflare (1.1.1.1) en 2ème serveur DNS.

Le DNS Google permet de minimiser les latences entre la demande de résolution d'un domaine et l'envoi de son IP au client. La couverture des serveurs DNS Google est presque globale afin de placer physiquement un serveur de noms le plus près possible de l'utilisateur qui en fait la demande.



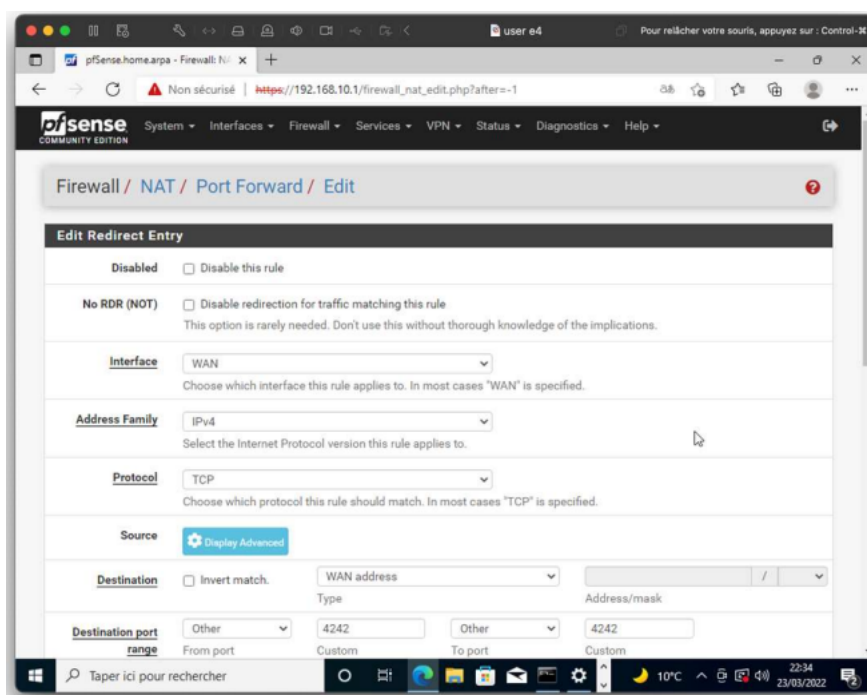
Règles de pare-feu :

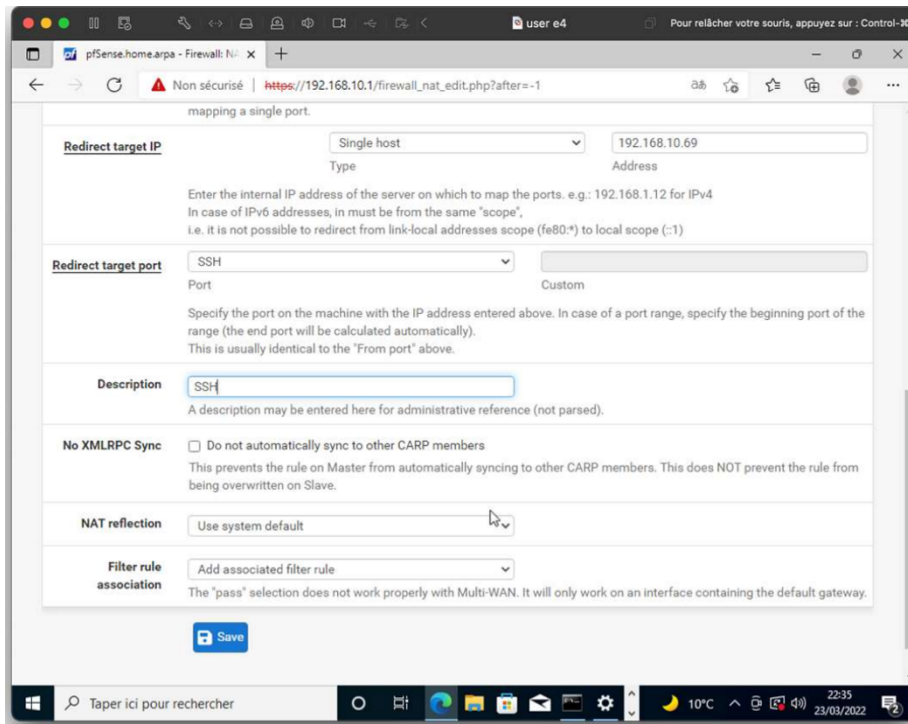
Nous allons tout d'abord déplacer notre pfsense dans la DMZ (Zone démilitarisée) du routeur orange pour qu'il soit accessible depuis l'extérieur.

Madnot souhaite pouvoir accéder en SSH à son serveur debian à distance depuis le réseau public, ne disposant pas d'adresses IP publiques supplémentaires, nous allons créer une règle qui redirigera les requêtes sur l'IP WAN vers l'IP local du serveur, nous allons aussi créer une redirection de port pour ajouter une couche de sécurité.

La connexion SSH se fera sur le port 4242 de l'IP 192.168.1.30 qui sera redirigé sur le port 22 de l'IP 192.168.10.69 (serveur debian).

Pour effectuer cette redirection, nous devons créer une règle dans le NAT, la voici ci dessous :

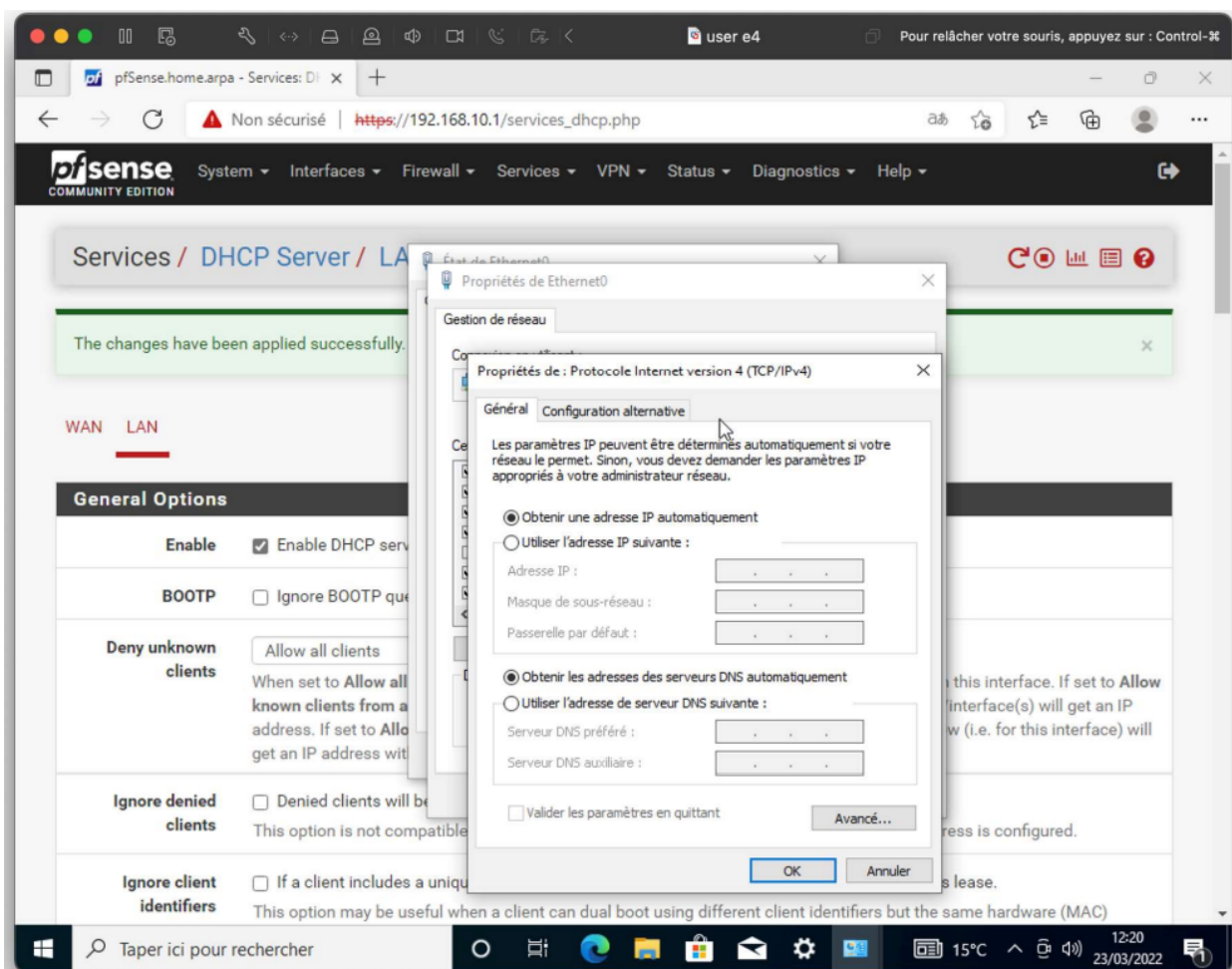




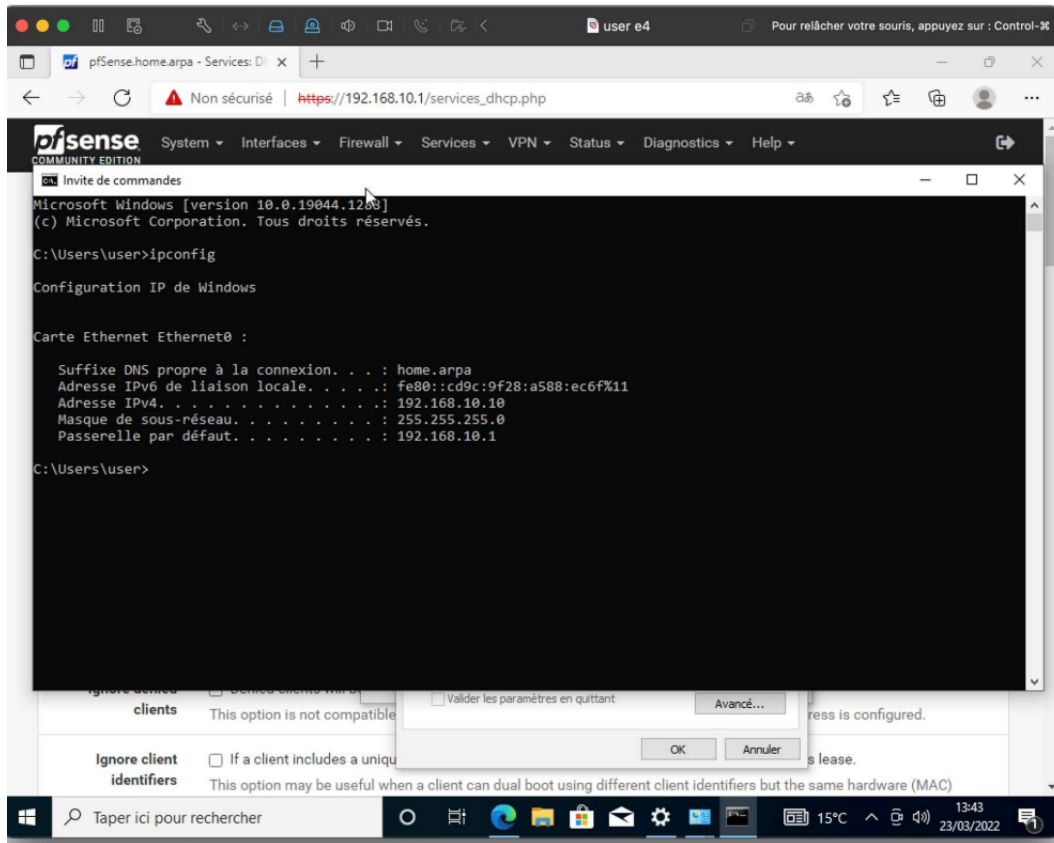
Règles de pare-feu :

Test DHCP & DNS :

Pour tester le fonctionnement du DHCP nous nous rendons sur un des ordinateurs présents dans le réseau local, nous nous rendons ensuite dans les paramètres de la carte réseau de celui-ci nous sélectionnons DHCP. L'ordinateur devrait donc recevoir de la part de notre routeur une adresse IP, le masque de sous réseau ainsi que la passerelle. Il devrait aussi recevoir les 2 serveurs DNS que nous avons précédemment sélectionnés.



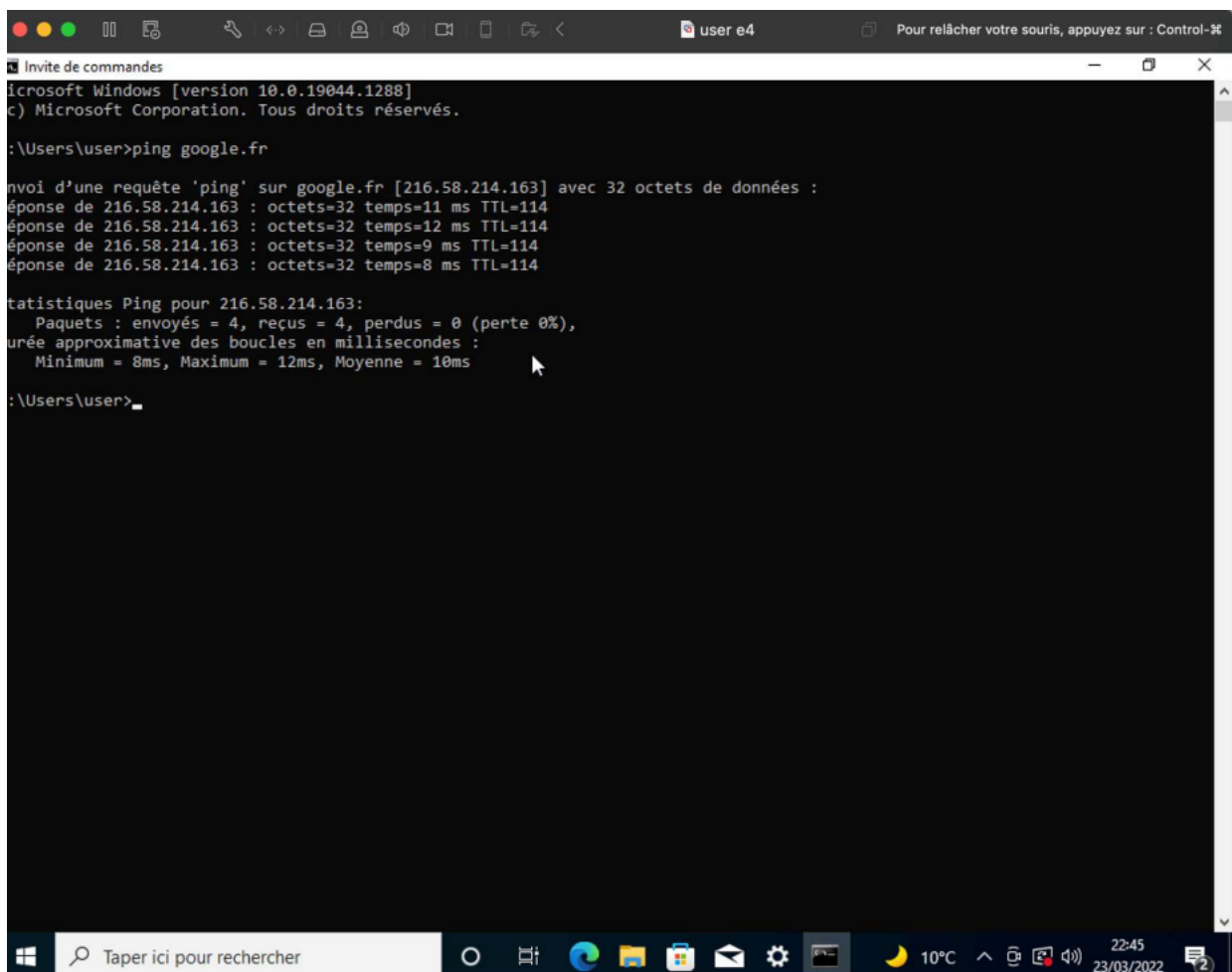
Pour vérifier qu'une configuration réseau a bien été attribuée à notre ordinateur, il nous suffit de nous rendre dans l'invite de commande et d'écrire « ipconfig » cette commande permet d'afficher la configuration réseau.



Nous pouvons voir ici que le DHCP a bien fonctionné, notre ordinateur a récupéré une configuration réseau.

Test du NAT :

Pour vérifier le bon fonctionnement du DNS que nous avons paramétré nous pouvons via un ping vers un nom de domaine depuis un ordinateur présent dans le réseau local vérifié si le nom de domaine est bien traduit en adresse IP, ici nous allons effectuer un ping vers google.fr.



```
Microsoft Windows [version 10.0.19044.1288]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\user>ping google.fr

Envoyé d'une requête 'ping' sur google.fr [216.58.214.163] avec 32 octets de données :
Réponse de 216.58.214.163 : octets=32 temps=11 ms TTL=114
Réponse de 216.58.214.163 : octets=32 temps=12 ms TTL=114
Réponse de 216.58.214.163 : octets=32 temps=9 ms TTL=114
Réponse de 216.58.214.163 : octets=32 temps=8 ms TTL=114

Statistiques Ping pour 216.58.214.163:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 8ms, Maximum = 12ms, Moyenne = 10ms

C:\Users\user>
```

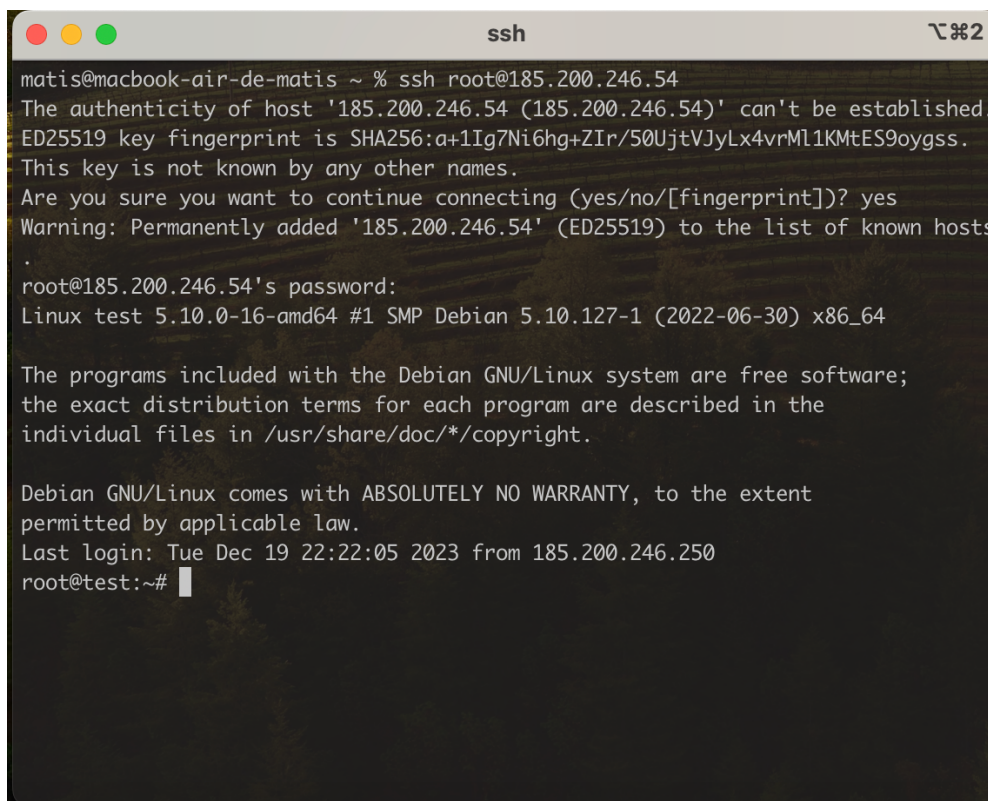
Nous pouvons voir ci-dessus que le nom de domaine a bien été traduit en adresse IP et que nous obtenons une réponse à notre ping, le DHCP a donc bien fourni le serveur DNS souhaité et celui-ci est fonctionnel.

Test de la règle de pare-feu :

Pour permettre à Madnot d'accéder à son serveur à distance, nous avons mis en place une règle NAT qui redirige les requêtes sur l'IP WAN sur le port 4242 vers le port 22 sur l'IP locale de leur serveur. Pour tester le fonctionnement de la règle, il nous suffit d'essayer de nous connecter en SSH sur l'IP WAN et sur le port 4242 via un ordinateur extérieur au réseau.

De plus le serveur pfsense est en DMZ nous pouvons donc directement envoyer une requête SSH a notre IP publique (104.28.54.13) qui sera redirigée vers le pfsense qui lui-même redirigera la requête vers notre serveur.

```
ssh user@104.28.54.13 -p 4242
```

A screenshot of a terminal window titled 'ssh' with a window control bar (red, yellow, green buttons) and a system tray icon (⌘#2). The terminal shows a user at 'matis@macbook-air-de-matis' running 'ssh root@185.200.246.54'. The output includes a warning about the host's authenticity, a confirmation to continue, a warning about adding the host to the known hosts list, the password prompt, and the Debian system's boot information and license notice. The prompt 'root@test:~#' is visible at the bottom.

```
matis@macbook-air-de-matis ~ % ssh root@185.200.246.54
The authenticity of host '185.200.246.54 (185.200.246.54)' can't be established.
ED25519 key fingerprint is SHA256:a+1Ig7Ni6hg+ZIr/50UjtVJyLx4vrML1KMtES9oygss.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '185.200.246.54' (ED25519) to the list of known hosts
.
root@185.200.246.54's password:
Linux test 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Dec 19 22:22:05 2023 from 185.200.246.250
root@test:~#
```

Nous pouvons voir que depuis un ordinateur sur un réseau extérieur à celui de l'entreprise nous accédons bien en SSH au serveur de l'entreprise. Notre règle ainsi que notre redirection de port sont fonctionnelles.

Bilan

Cette mission m'a permis d'appliquer mes connaissances en termes de conception ainsi que de mise en place d'une infrastructure, en effet la création de cette infrastructure a nécessité des connaissances dans plusieurs domaines, notamment en systèmes et en réseau.

Cela m'a aussi permis de découvrir pfsense qui est un routeur virtuel et qui dans notre cas répondait parfaitement à notre besoin. Mes recherches autour de celui-ci m'ont énormément apporté en termes de connaissance réseau.

Cette mission m'a aussi permis d'apprendre à solutionner un besoin en apportant une solution, ici la problématique d'accéder au serveur à distance m'a amené à faire des recherches qui m'ont amené jusqu'à la solution que nous avons mise en place.