

Projet E4 : création et configuration d'un PfSense

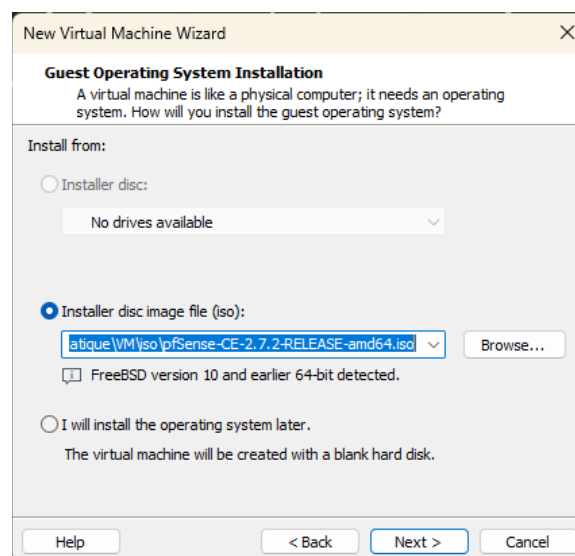
Dans cette présentation nous allons voir comment j'ai créé et configuré un routeur PfSense pour une entreprise fictive se nommant « notatech »

Mise en situation : Nous créons le PfSense dans une infrastructure comportant déjà 2 Windows server en redondance comportant les adresses 192.168.1.10 et 192.168.1.5

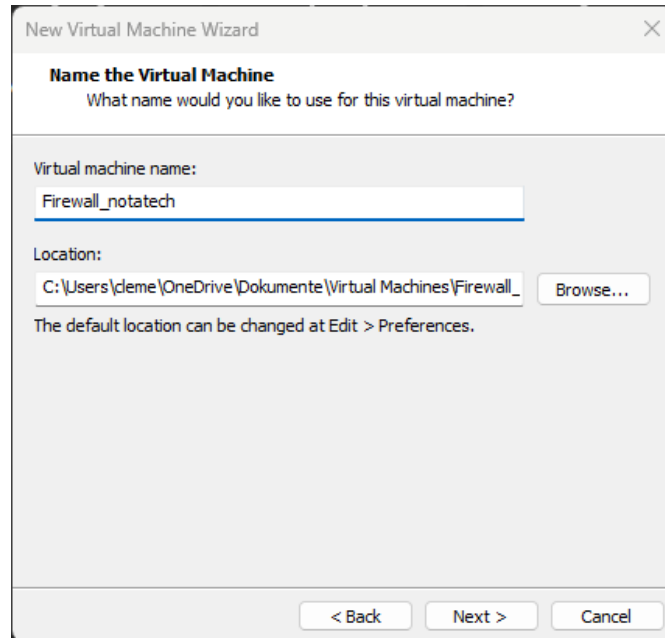
Tout d'abord passons à la **Création de la machine virtuelle**. Pour ce faire sur VMWare je crée une nouvelle machine virtuelle et sélectionne une configuration **Typical**



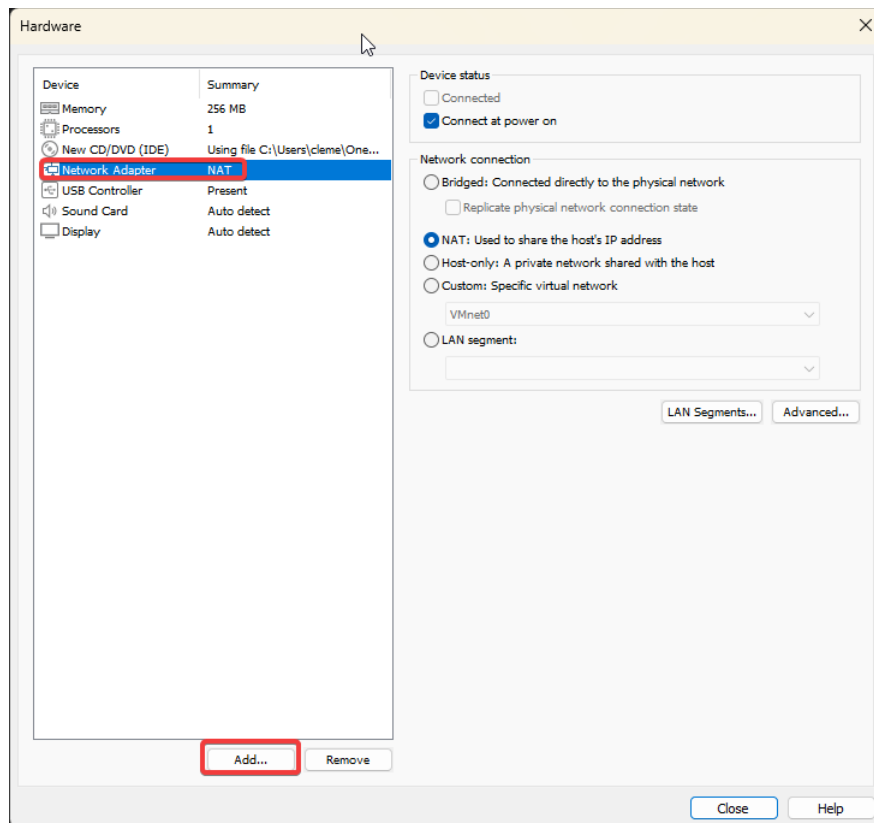
Ensuite ici je rentre le chemin vers l'iso de mon **PfSense**



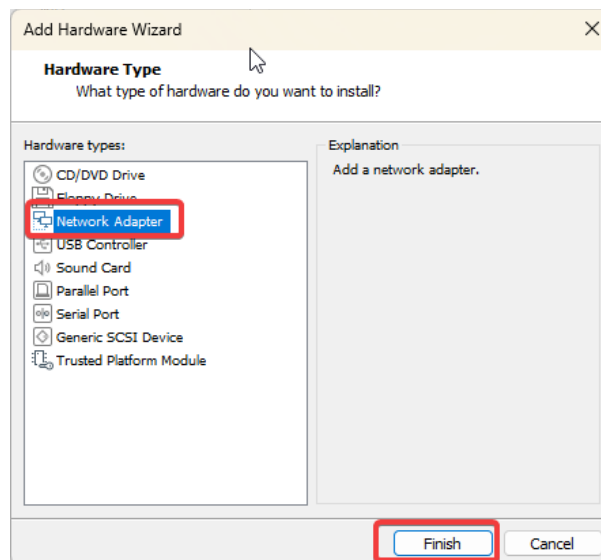
Dans la prochaine fenêtre je nomme ma machine « **firewall_notatech** » étant donné que la machine a pour but d'être un routeur mais peut être configurée aussi comme un pare-feu



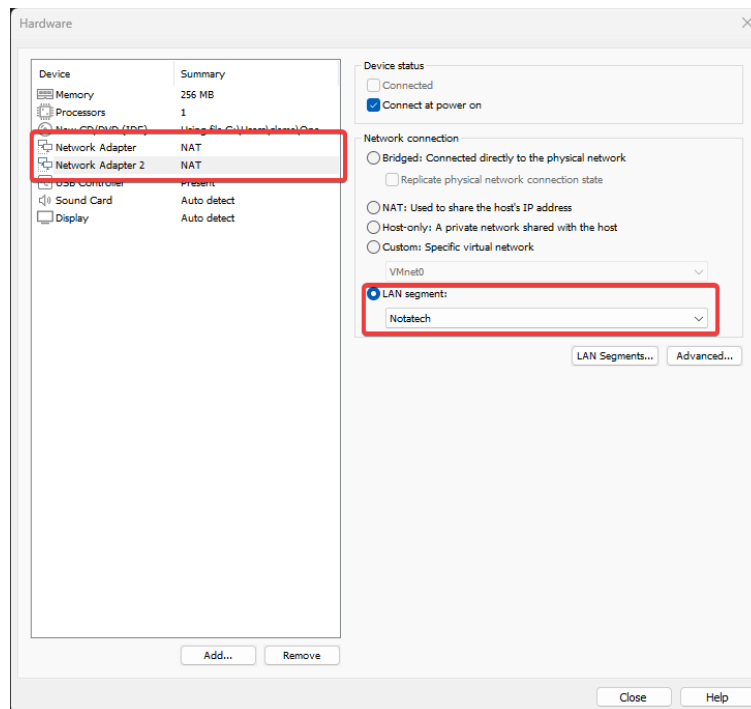
Pour les autres paramètres je les laisse par défaut et arrivé ici je clique sur « **customize hardware** » ici on va ajouter une deuxième carte réseau de manière à en avoir une en NAT et une en LAN segment de manière à transmettre le réseau **WAN** aux machines connectées Ici je clique sur « **Add** » pour ajouter un équipement



Ensuite cette page s'ouvre ou je sélectionne « **network adaptater** » puis **finish**

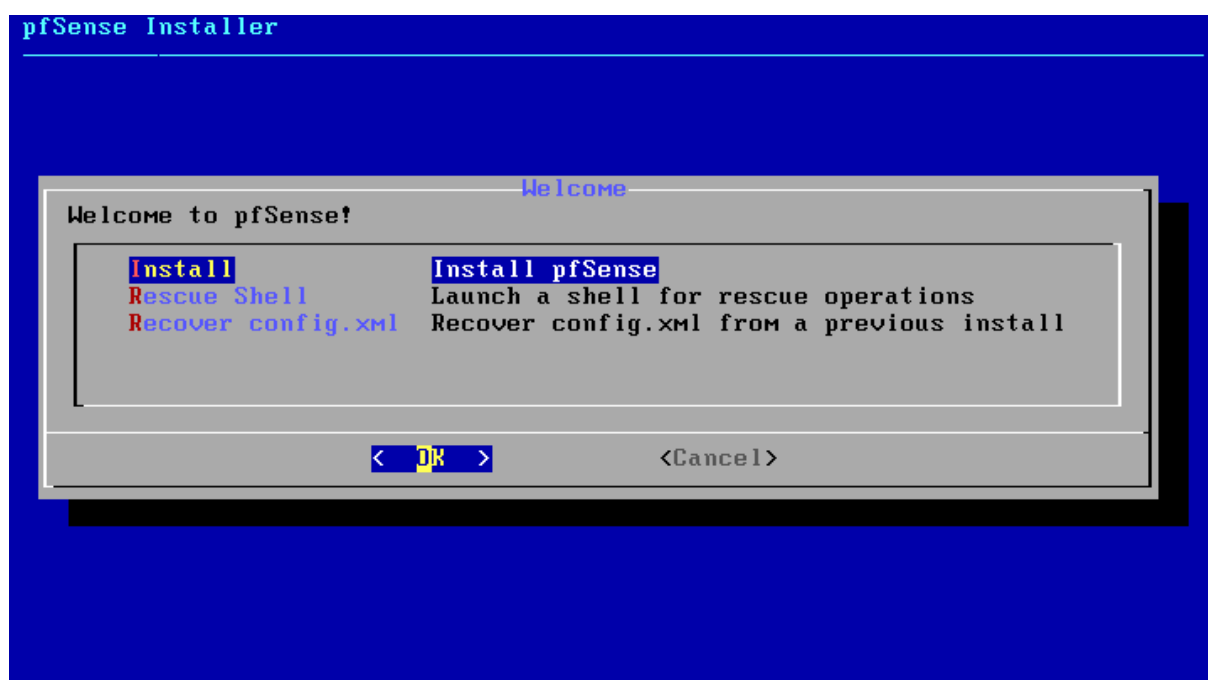


Et finalement je configure cette 2^{ème} carte réseau en LAN segment et la met sur le segment **Notatech**

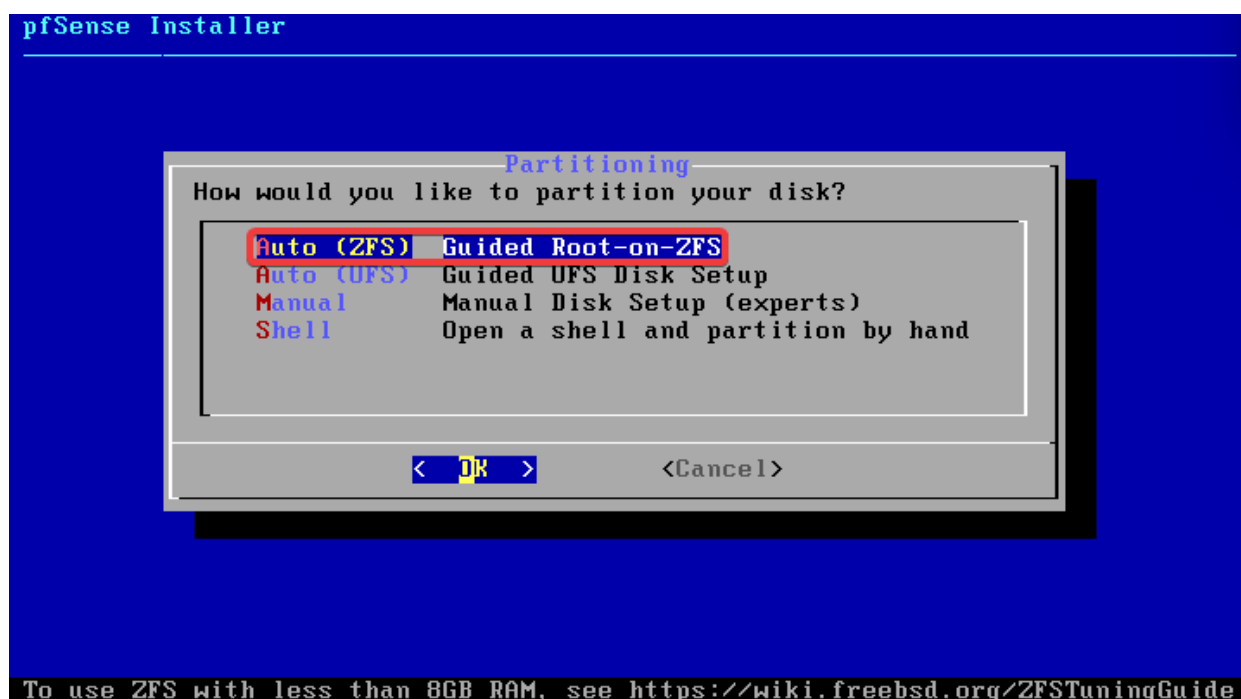


Installation du PfSense :

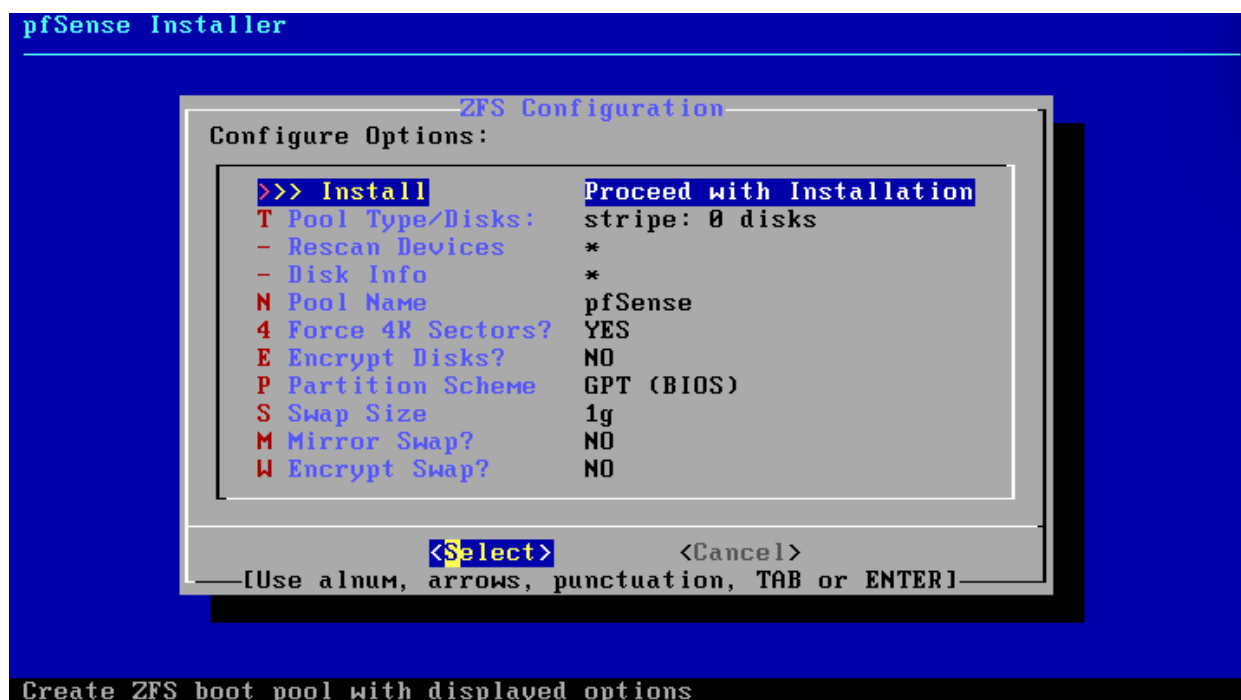
Ici on va passer a la partie installation du système pfsense. Arrivé sur cette première page, je sélectionne « **install PfSense** »



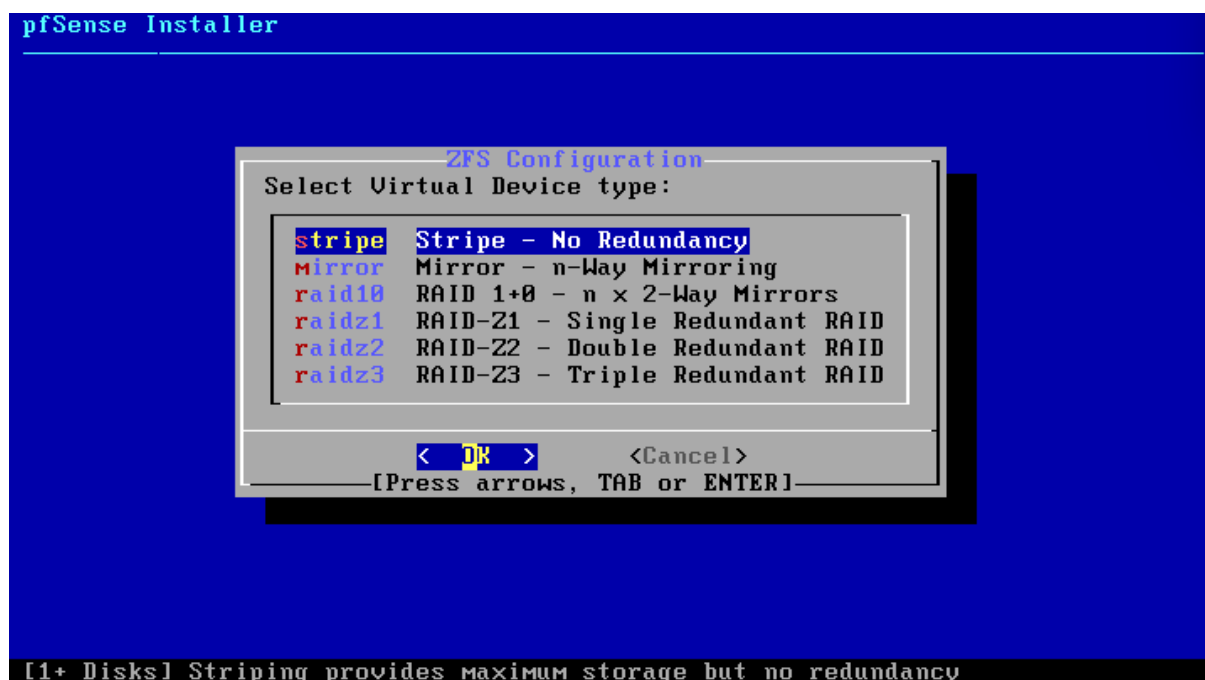
Ici je prends la 1^{ère} option : « **Auto ZFS** »



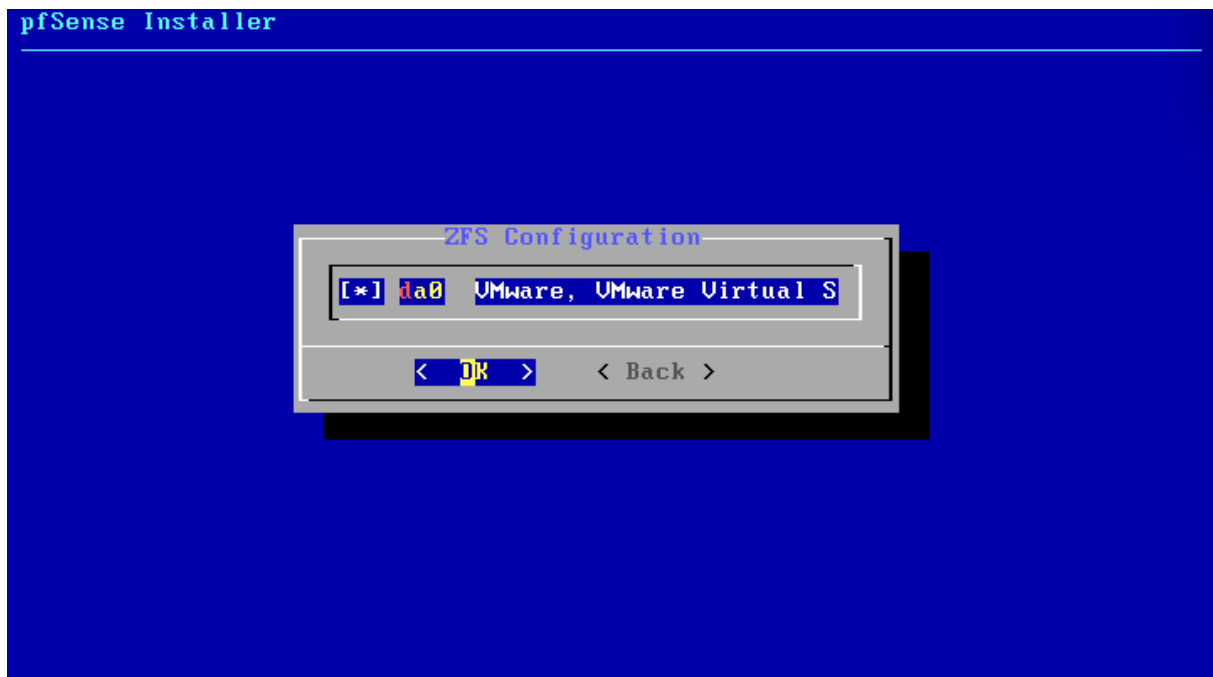
Ici je sélectionne **Install** et fait **Select**



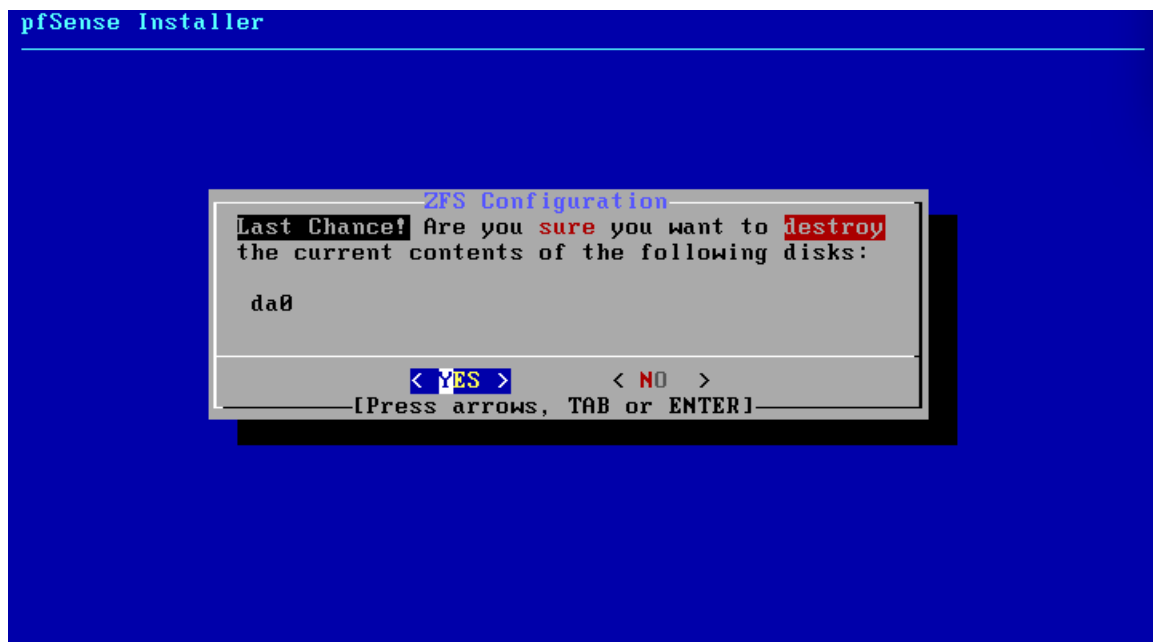
Ici je sélectionne **Stripe** car je ne souhaite pas configurer de redondance pour le moment



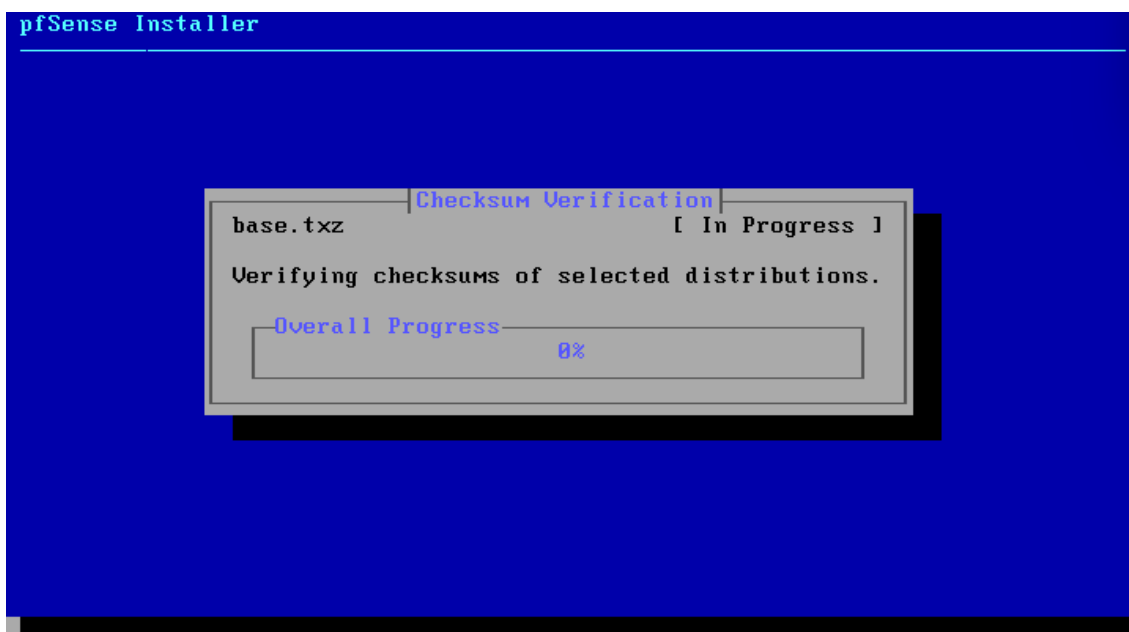
Ensuite je sélectionne mon disque ici et clique sur **OK**



Ce message m'indique que les données sur le disque « da0 » vont être supprimés, je n'y fais pas attention car je n'ai rien sur le disque en question



Et ensuite PfSense va finalement s'installer, il nous faudra juste redémarrer notre machine à la fin de cette progression



Ensuite une fois bien installé et redémarré, le PfSense nous affiche une page comme celle-ci, nous indiquant les IP des différentes interfaces et les options de paramètre

```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 3f64ecda514e62012b8d

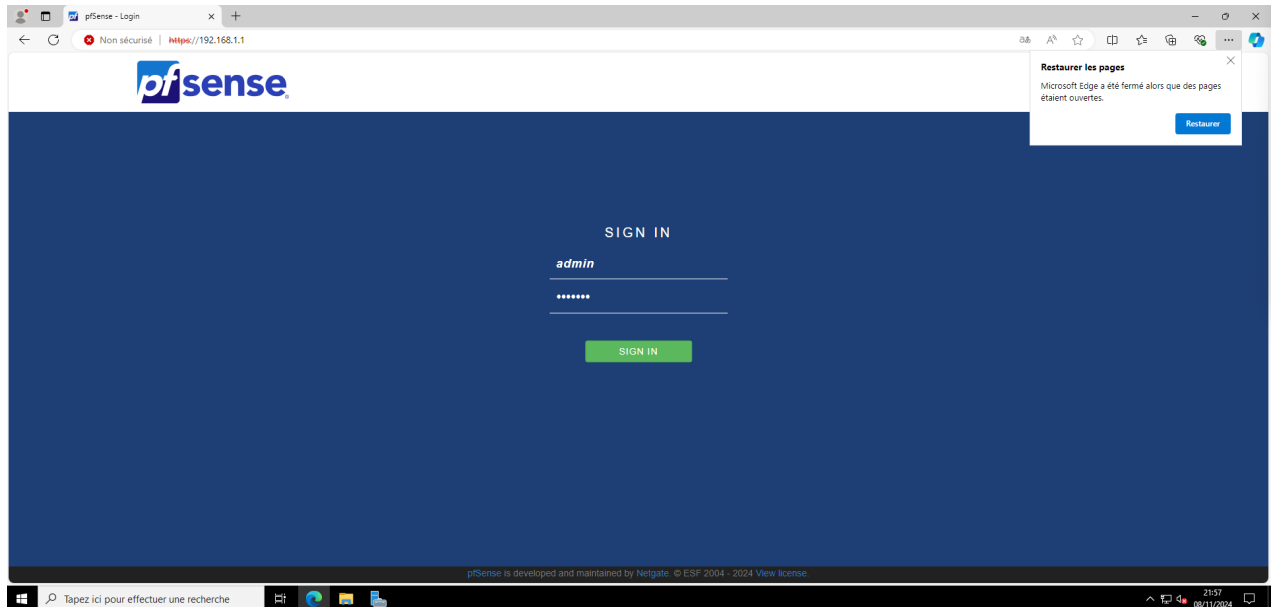
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.73.162/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

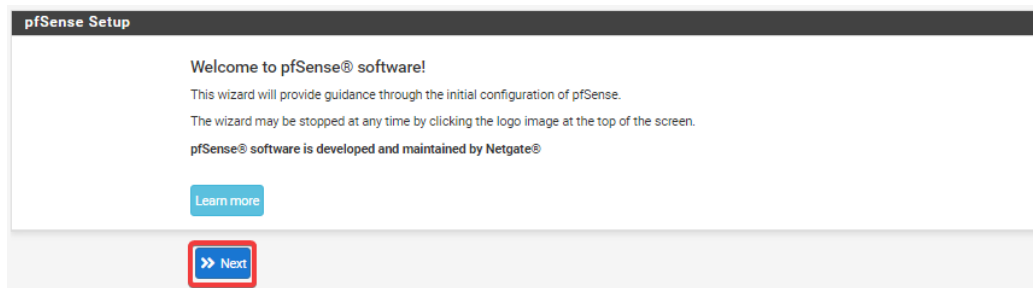
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option: 
```


Nous n'allons pas rester plus sur la machine PfSense, nous allons juste la laisser démarrée et la configurer par l'interface web, en marquant l'IP LAN de notre PfSense dans une barre de recherche sur une machine du réseau. Je me connecte ici avec les identifiants génériques Admin Pfsense



Ensuite nous allons rentrer dans la configuration de notre **PfSense**, je clique donc simplement sur **Next**



Ici pour le **Hostname** je laisse **PfSense**, pour ce qui est du domaine je rentre mon nom de domaine **Notatech.local**, pour le serveur DNS primaire je rentre l'IP de mon serveur AD principal **192.168.1.10** et pour le second je rentre celui de mon serveur en redondance **192.168.1.5**

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' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. 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 and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

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

[Next](#)

Ici on me demande l'adresse IP LAN, je rentre l'adresse de mon PfSense **192.168.1.1**

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 je modifie mes identifiants de connexion a mon interface WEB PfSense

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

[Next](#)

Et la configuration principale de notre PfSense est terminée !

Congratulations! pfSense is now configured.

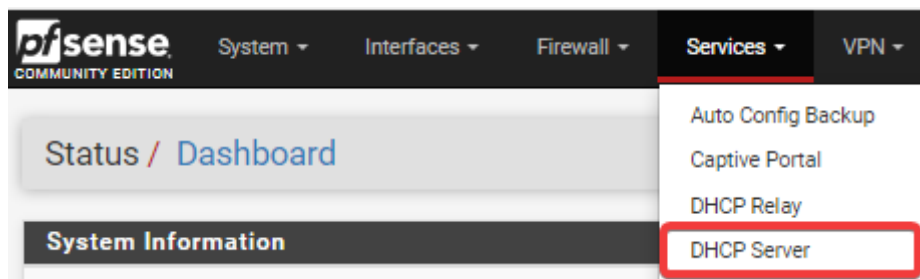
We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Configuration DHCP :

Ici nous allons configurer le DHCP sur le PfSense

Je commence donc tout d'abord par me rendre dans **Services > DHCP Server**



Ici je coche « **Enable DHCP server on LAN interface** », je définis mon **Pool Range** de **192.168.1.100** jusqu'à **192.168.1.200** et finalement je renseigne l'IP de mes 2 serveurs AD dans les **Server Options**

General DHCP Options	
DHCP Backend	ISC DHCP
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 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.
Ignore Denied Clients	☐ Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request 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.
Primary Address Pool	
Subnet	192.168.1.0/24
Subnet Range	192.168.1.1 - 192.168.1.254
Address Pool Range	192.168.1.100 From 192.168.1.200 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	
WINS Servers	WINS Server 1 WINS Server 2
DNS Servers	192.168.1.10 192.168.1.5

Et finalement dans **Other DHCP Options**, je renseigne l'adresse de ma passerelle qui est donc l'adresse de mon PfSense, **192.168.1.1** et je renseigne mon nom de domaine **notatech.local**

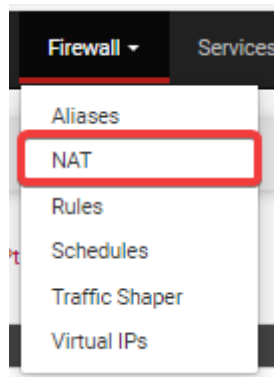
Other DHCP Options	
Gateway	192.168.1.1
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.	
Domain Name	notatech.local
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.	

Je sauvegarde et applique et voilà **la configuration de notre DHCP est terminée**

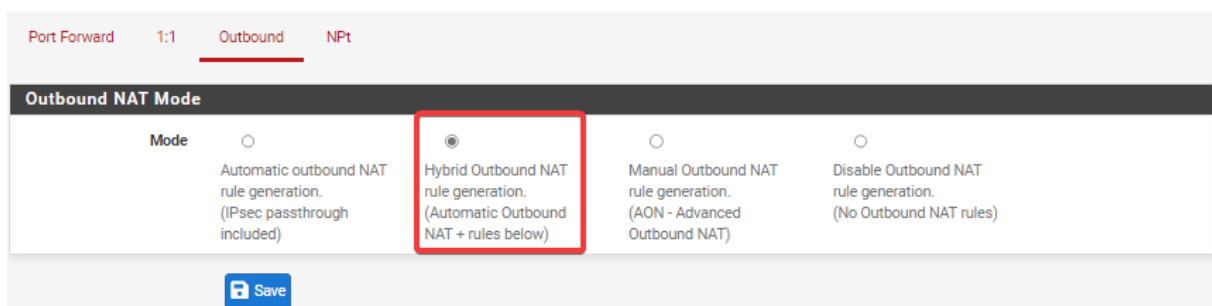
Configuration internet pour les clients :

Dans cette partie nous allons configurer le PfSense pour qu'il diffuse la connexion internet aux utilisateurs dans le réseau

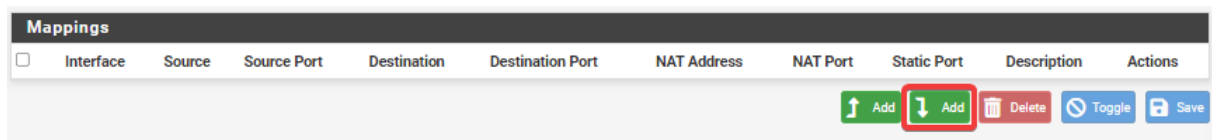
Dans un premier temps, dans l'interface web du PfSense je clique sur **Firewall > NAT**



Ensuite ici je sélectionne **Hybrid Outbound NAT**



Ici je clique sur **Add** pour ajouter une nouvelle règle



Ensuite cette page apparaît, ici pour l'interface je sélectionne **WAN** car c'est l'interface qui peut communiquer avec internet, pour la famille d'adresse je sélectionne **IPv4** car nous n'avons pas besoin de configurer d'IPv6, en source je sélectionne **Network or Alias** et rentre l'adresse **192.168.1.1** car c'est notre adresse **LAN**

Edit Advanced Outbound NAT Entry

Disabled

☐ Disable this rule

Do not NAT

☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface

WAN

The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which protocol this rule should match. In most cases "any" is specified.

Source

Network or Alias

192.168.1.1

Type

Source network for the outbound NAT mapping.

Port or Range

Destination

Any

Type

Destination network for the outbound NAT mapping.

Port or Range

☐ Not

Invert the sense of the destination match.

Translation

Address

WAN address

Type

Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

Port or Range

Enter the external source Port or Range used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by "-".
Leave blank when Static Port is checked.

☐ Static Port

Ensuite je sauvegarde ces paramètres, les applique et les machines pourront se connecter à internet.