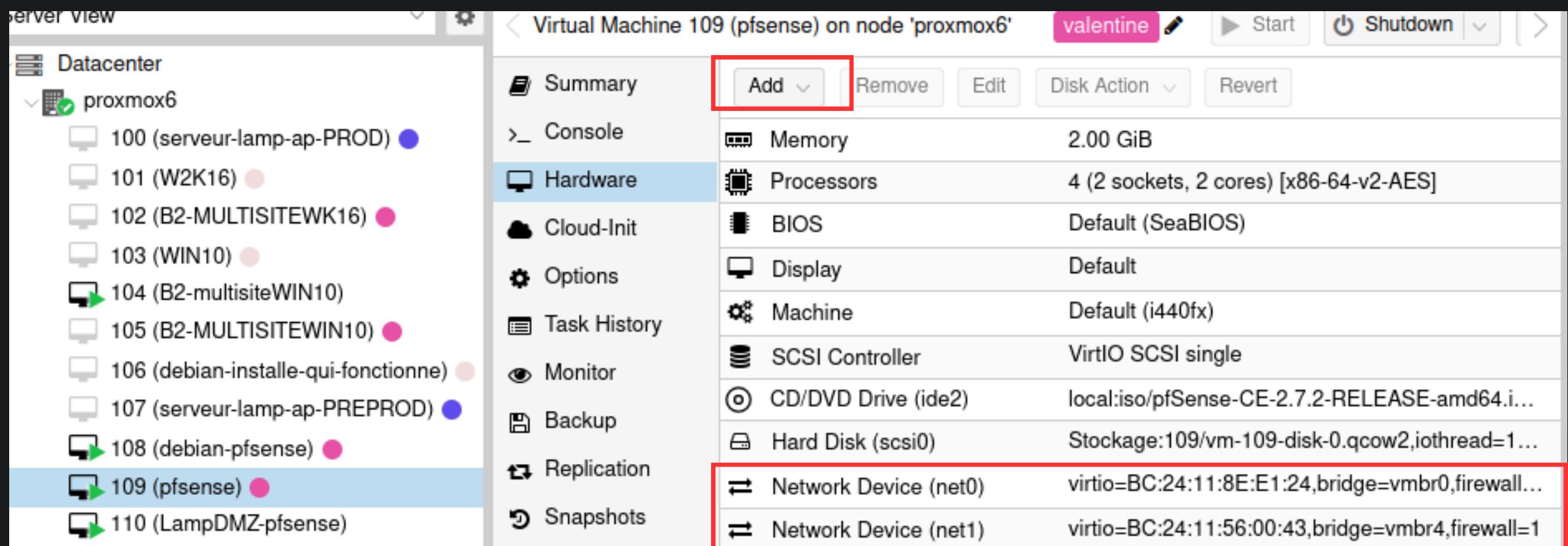


TP – PFSENSE



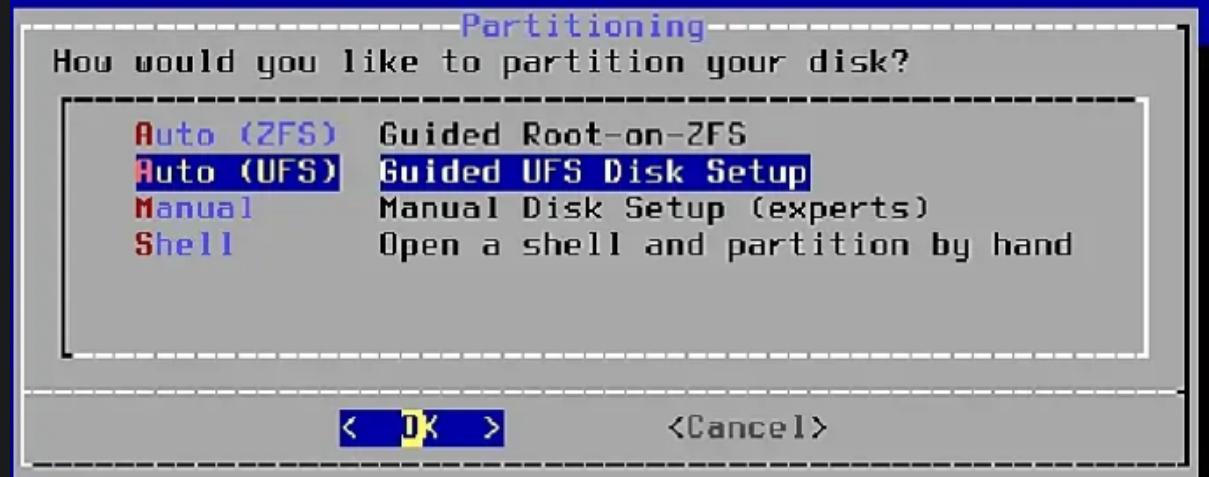
INSTALLATION PFSENSE

Lorsque vous installez sur proxmox, mettez 2 cartes réseaux pour votre pfSense (une pour le LAN, une pour le WAN) Pour cela, cliquez sur "Add" puis sur "Network Device"

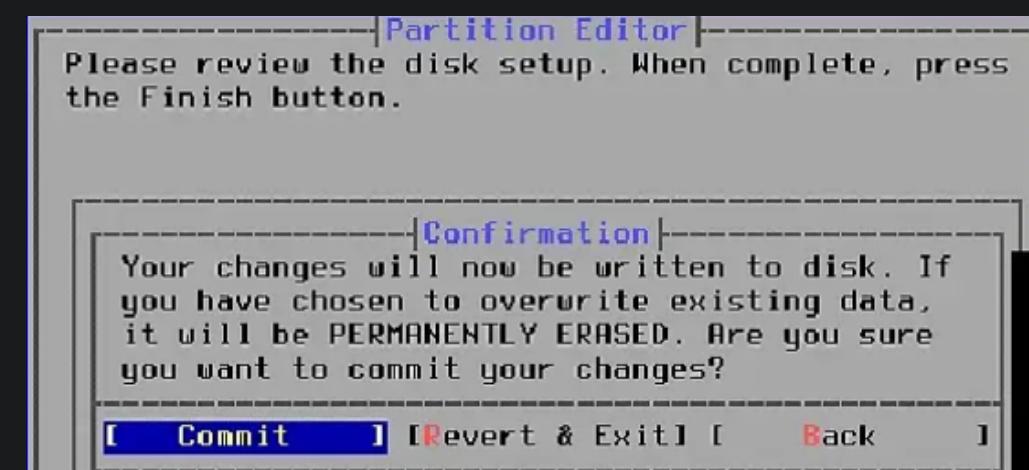


INSTALLATION PFSENSE

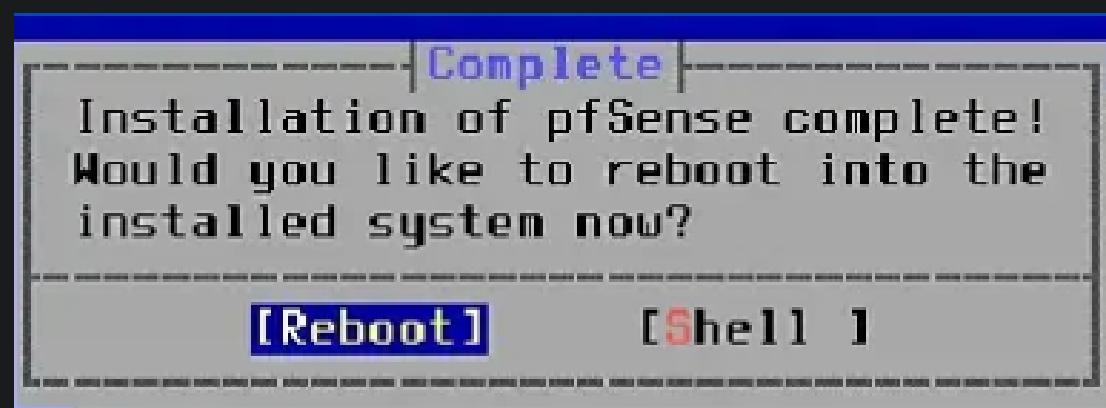
Procémons à l'installation, suivez ces étapes:



INSTALLATION PFSENSE



INSTALLATION PFSENSE



```
Network interface mismatch -- Running interface assignment
vtnet0: link state changed to UP
vtnet1: link state changed to UP

Valid interfaces are:

vtnet0 52:54:00:01:05:af (down) VirtIO Network Adapter
vtnet1 bc:24:11:76:60:68 (down) VirtIO Network Adapter
```

Les 2 cartes réseau de notre machine pfSENSE ont été détectées et sont passées au statut "UP".

INSTALLATION PFSENSE

Assignons les cartes réseaux détectées aux interfaces WAN et LAN

Indiquez "vtnet0" et faites "Entrée" pour assigner cette carte en tant qu'interface WAN

Indiquez "vtnet1" pour l'autre carte pour l'assigner en tant qu'interface LAN

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 a or nothing if finished): vtnet1
```

Saisissez "y" pour valider et patientez pendant que pfsense assigne les interfaces aux cartes réseaux

```
The interfaces will be assigned as follows:
WAN -> vtnet0
LAN -> vtnet1

Do you want to proceed [y/n]? y
```



INSTALLATION PFSENSE

Nous allons maintenant changer l'adresse IP du LAN, pour cela, dans le menu, je choisis "2"

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

Enter an option: ■
```

Je presse "2" pour sélectionner le LAN, je presse "n", je saisis mon adresse IP qui est ici "192.168.40.33", je saisis "24", je presse "entrée" car je ne dois pas modifier ceci, je presse "n" à la question, je presse "entrée", je presse "n". Votre adresse IP est modifiée.

```
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:
> 192.168.40.33
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:
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n
```

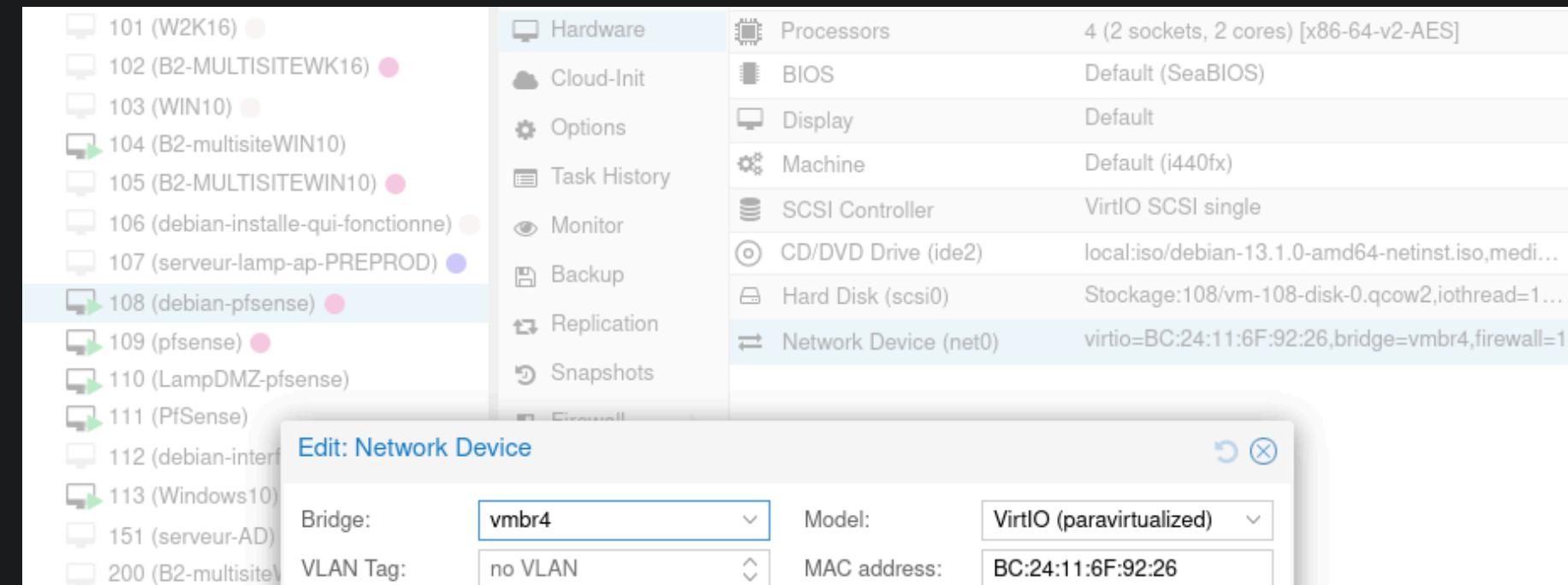
```
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.40.33/24
You can now access the webConfigurator by opening the following URL in your browser:
http://192.168.40.33/
```

ACCES À L'INTERFACE GRAPHIQUE

J'installe une seconde VM dotée d'une interface graphique (debian, windows...)

Il faudra attribué à cette VM la même carte réseau que le LAN (l'adresse IP de mon LAN est 192.168.40.33 et l'IP de ma carte réseau pour le LAN est 192.168.40.32)

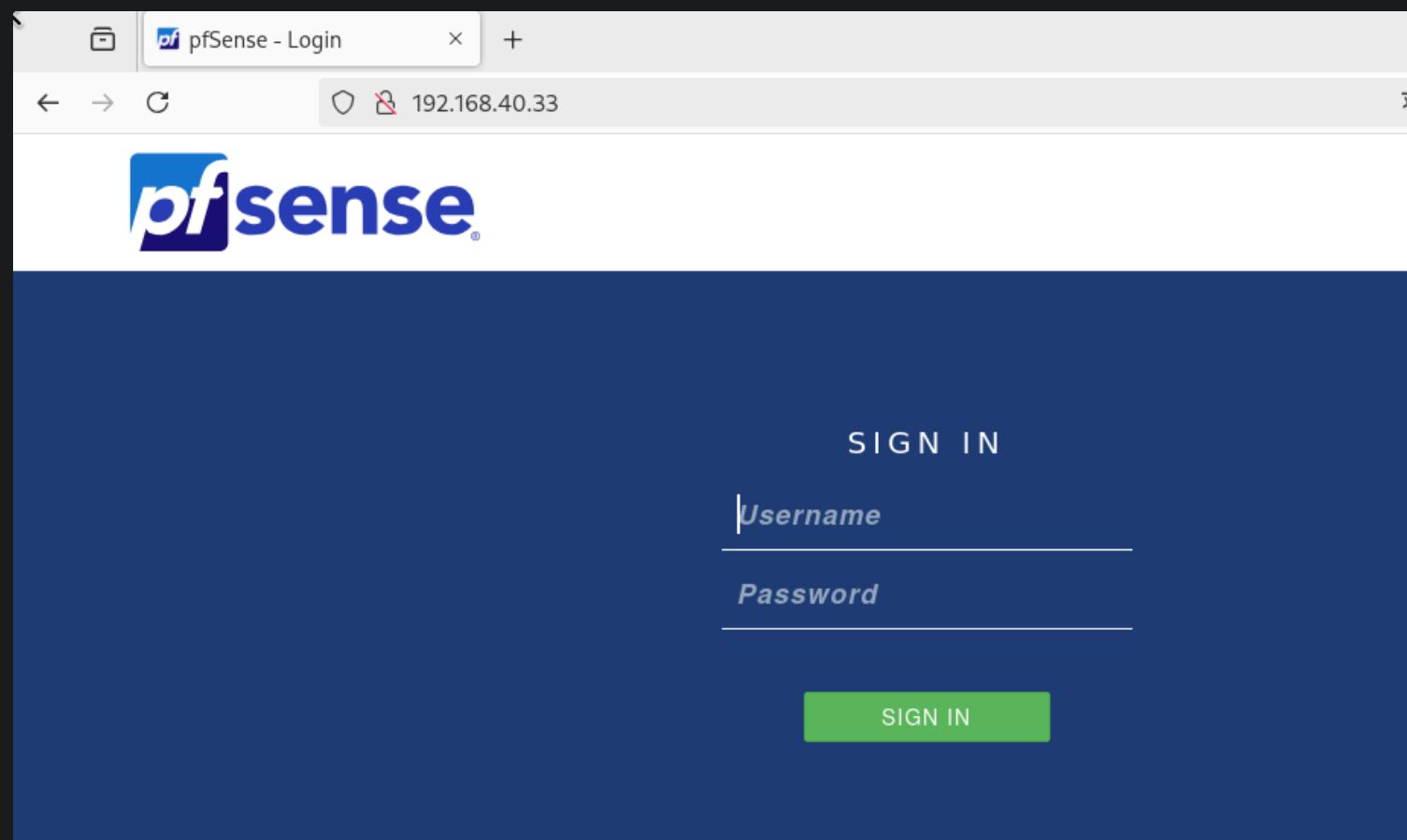


Il faudra attribué à cette VM une adresse IP en 192.168.40.x (j'ai choisi 192.168.40.34) afin qu'elle puisse afficher l'interface graphique de pfsense

```
user@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    link/ether bc:24:11:6f:92:26 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    altname enx0c24116f9226
    inet 192.168.40.34/24 brd 192.168.40.255 scope global noprefixroute ens18
        valid_lft forever preferred_lft forever
```

ACCES À L'INTERFACE GRAPHIQUE

En allant sur le moteur de recherche et en tapant l'adresse IP du LAN, je tombe sur l'interface graphique:



Les login sont admin en username et pfsense en password

CONNECTER UN SERVEUR LAMP

Ajoutez une nouvelle carte réseau à votre PFSense (comme vu au début du TP), ce sera la carte réseau pour votre DMZ.

Installez un serveur LAMP, une fois dessus, vous allez devoir changer l'adresse IP de votre serveur et ajouter la gateway, faites nano /etc/network/interfaces:

```
GNU nano 7.2
/etc
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens18
iface ens18 inet static
    address 192.168.31.27
    netmask 255.255.255.0
    gateway 192.168.31.28
```

Pour la gateway, vous mettrez l'adresse IP de la carte réseau que vous venez d'ajouter "192.168.31.28", c'est la carte réseau dédié à votre DMZ

Vous devrez forcément mettre une adresse ip similaire à 192.168.31.x (ici on mettra 192.168.31.27)

```
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:22:a6:c2 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.31.27/24 brd 192.168.31.255 scope global ens18
        valid_lft forever preferred_lft forever
        inet6 fe80::be24:11ff:fe22:a6c2/64 scope link
            valid_lft forever preferred_lft forever
root@debian:~# ip route
default via 192.168.31.28 dev ens18 onlink
192.168.31.0/24 dev ens18 proto kernel scope link src 192.168.31.27
```

CONNECTER UN SERVEUR LAMP

Pour la gateway, vous mettrez l'adresse IP de la carte réseau que vous venez d'ajouter "192.168.31.28", c'est la carte réseau dédié à votre DMZ

Vous devrez forcément mettre une adresse ip similaire à 192.168.31.x (ici on mettra 192.168.31.27)

```
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:22:a6:c2 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.31.27/24 brd 192.168.31.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe22:a6c2/64 scope link
        valid_lft forever preferred_lft forever
root@debian:~# ip route
default via 192.168.31.28 dev ens18 onlink
192.168.31.0/24 dev ens18 proto kernel scope link src 192.168.31.27
```

ACCÈS DU LAN VERS LA DMZ

Pour le NAT cela permet d'envoyer la page WEB vers le LAN en faisant une redirection de ce port :

The screenshot shows a 'Port Forward' configuration screen. It lists a single rule: WAN interface, TCP protocol, source port 80 (HTTP), destination port 80 (HTTP), and destination address 192.168.31.27.

This is a detailed configuration for the port forward rule. It includes fields for Action (Disabled), Interface (WAN), Address Family (IPv4), Protocol (TCP), Source (WAN address 192.168.31.27), Destination (HTTP port 80), Destination Port Range (HTTP port 80), Redirect target IP (192.168.31.27), and Redirect target port (HTTP port 80).

Pour le LAN nous autorisons l'accès au site web à partir du LAN

The screenshot shows a 'Rules' table under the 'LAN' tab. It contains two rules: one for port 1/1.92 MiB (disabled) and another for port 0/0 B (enabled) which allows LAN subnets to access port 80 (HTTP).

This is a detailed configuration for the LAN access rule. It includes fields for Action (Pass), Interface (LAN), Address Family (IPv4), Protocol (TCP), Source (LAN subnets), Destination (WAN address 192.168.31.27), Destination Port Range (HTTP port 80), and Extra Options (Log, Description: autorisation d'accès au site web a partir du lan).

ACCÈS DU WAN VERS LA DMZ

Il va falloir retirer les deux premières règles car elles sont gênantes, pour cela, allez dans “Firewall” → “WAN”, allez tout en bas et décochez les deux cases, enregistrez les changements

Floating	WAN	LAN	DMZ					
Rules (Drag to Change Order)								
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
<input type="checkbox"/>	0/1.04 MiB	*	RFC 1918 networks	*	*	*	*	*
<input type="checkbox"/>	0/12 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.31.27	80 (HTTP)	*	none

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 per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such 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.

ACCÈS DU WAN VERS LA DMZ

Pour le WAN direction vers le site web sur le port 80

Firewall / Rules / WAN

Floating WAN LAN DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/12 KiB	IPv4 TCP	*	*	192.168.31.27	80 (HTTP)	*	none	NAT	

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.

Associated filter rule: This is associated with a NAT rule.
Editing the interface, protocol, source, or destination of associated filter rules is not permitted.
[View the NAT rule](#)

Interface: WAN
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
Choose which IP protocol this rule should match.

Source

Source: Invert match Any Source Address /

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

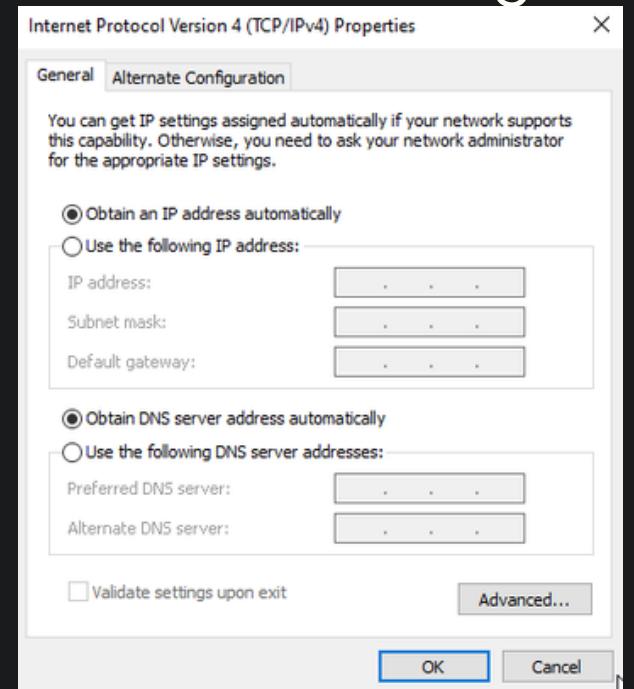
Destination: Invert match Address or Alias 192.168.31.27 /

Destination Port Range: HTTP (80) 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.

ACCES AU WEB VIA LE WAN

Sur une machine virtuelle Windows 10, sur proxmox, dans Network, je mets la carte réseau de mon WAN.
Dans mes configurations d'adresse ip:

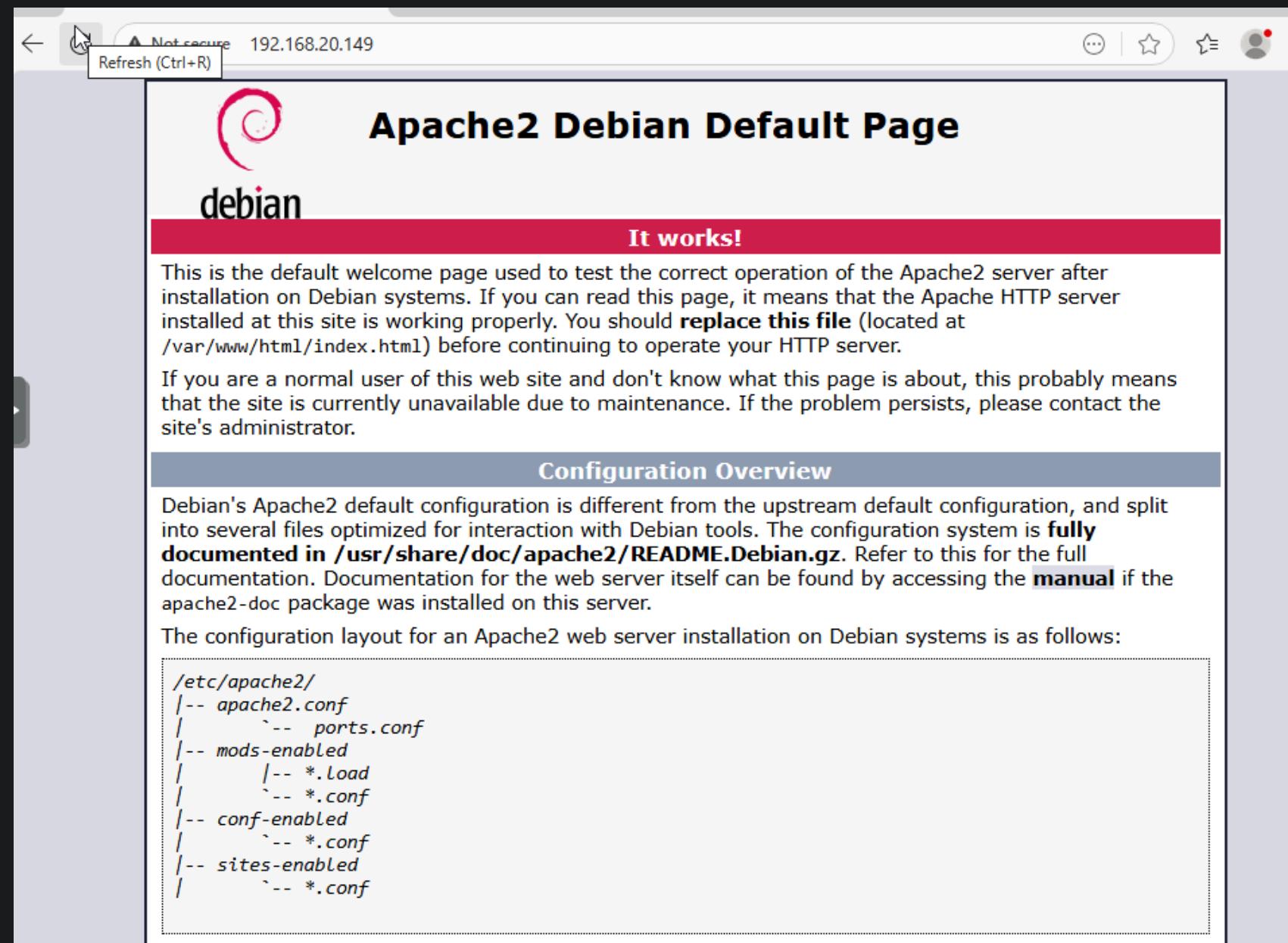


Les données vont être récupérées automatiquement grâce à la carte réseau et ainsi, vous aurez internet:



ACCES AU WEB VIA LE WAN

Je me rends sur Edge, je rentre l'adresse ip de mon WAN et je peux bien accéder à l'interface Apache: tout fonctionne bien.



ACCES AU WEB VIA LE LAN

Je me rends dans Firewall → Rules → LAN,
j'ajoute une règle:

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

Choose which IP protocol this rule should match.

Source

Source: Invert match LAN subnets 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 Address or Alias: 192.168.31.27 /

Destination Port Range: HTTP (80) 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

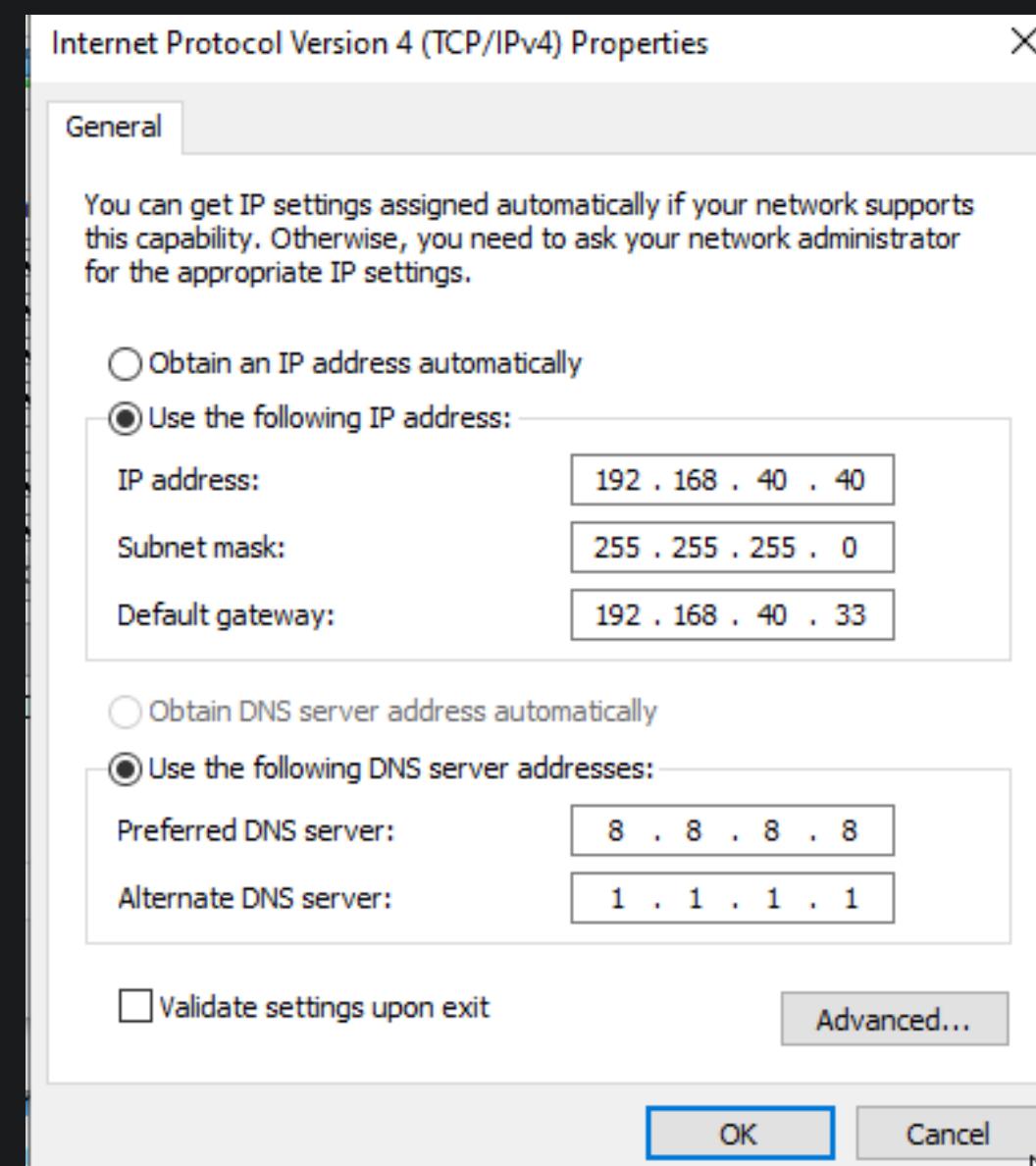
Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description:

ACCES AU WEB VIA LE LAN

Sur une machine cliente avec la carte réseau du LAN:

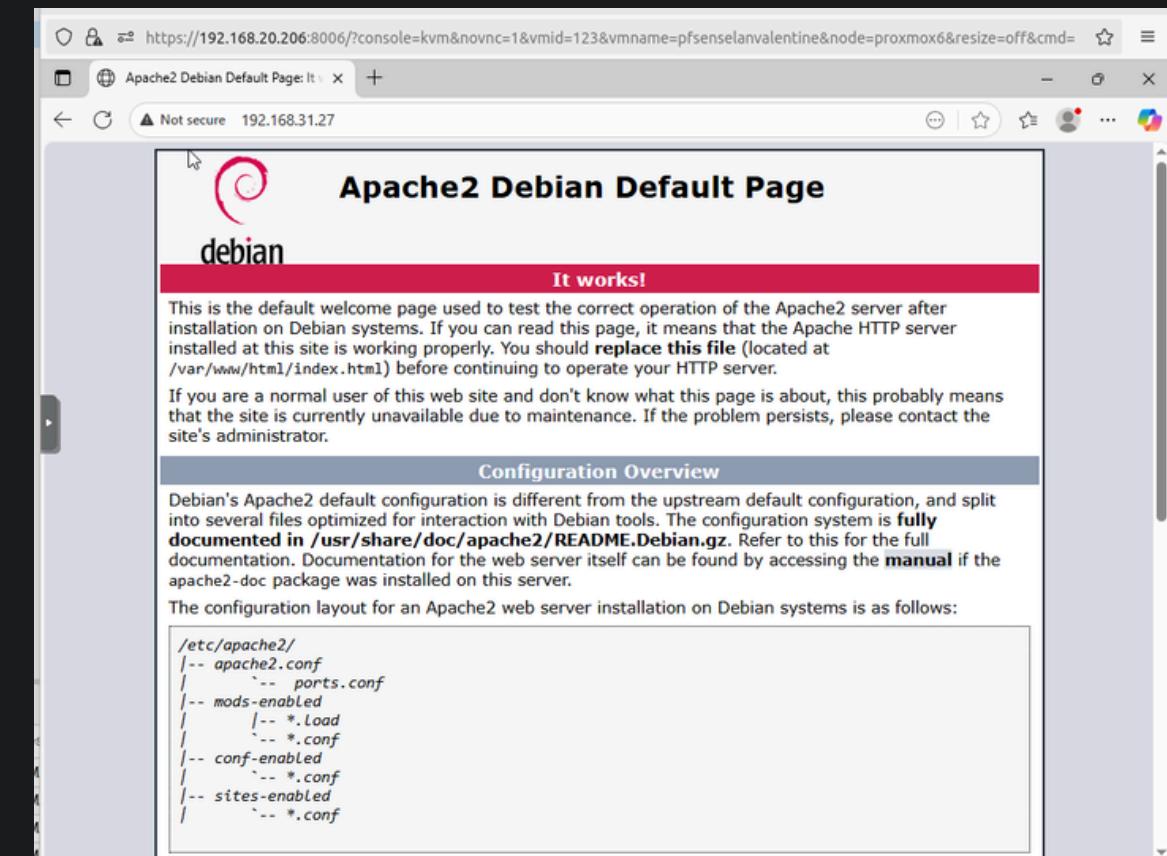
J'accède aux paramètres IP:



IP sur la même plage
que mon LAN

Gateway = IP du LAN

Je peux accéder au site:
le LAN redirige le client vers la DMZ

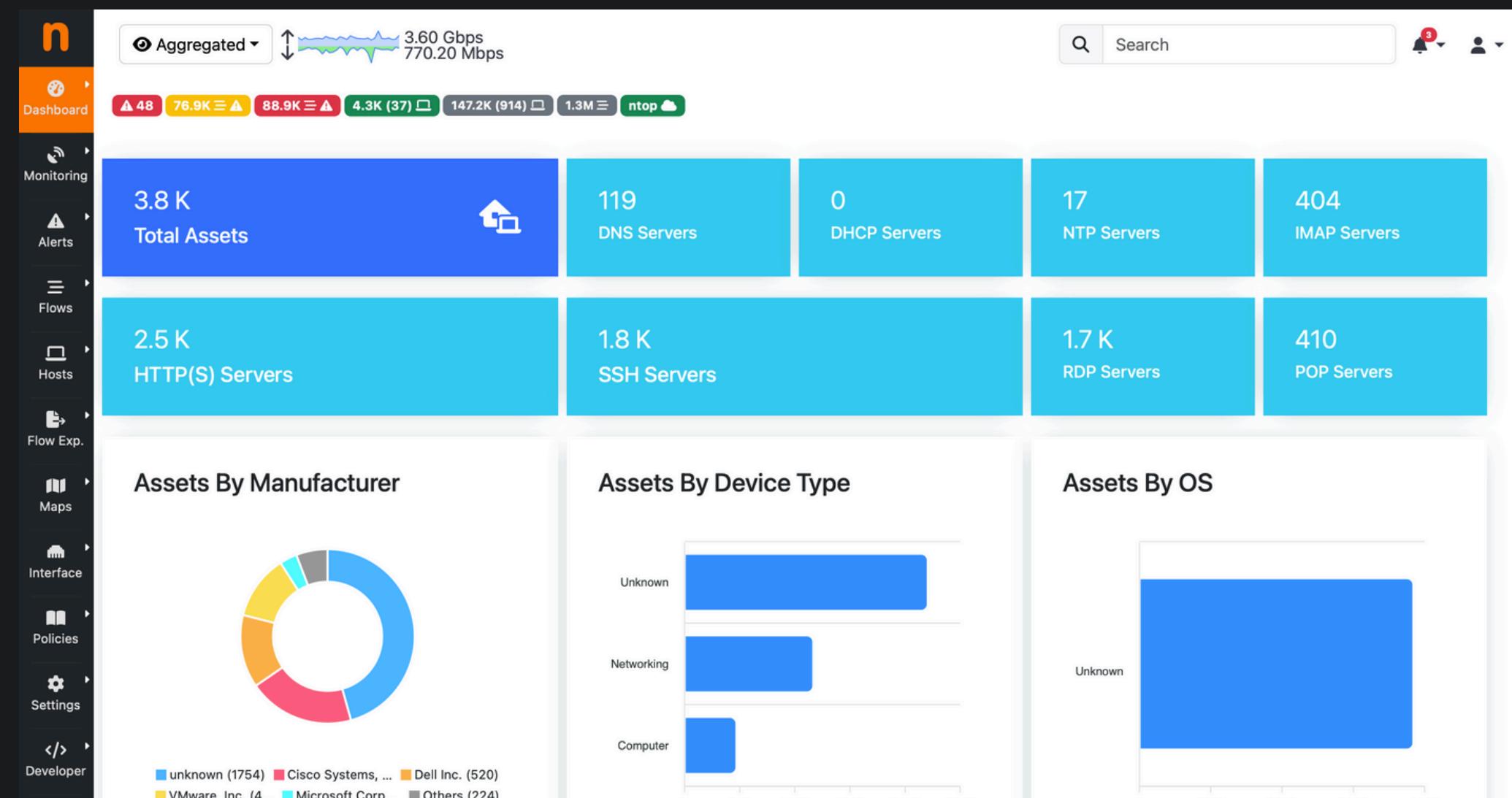


DMZ ADDON



NTOP

- Il analyse le trafic réseau en temps réel.
- Il détaille les protocoles et adresses IP.
- Son interface web est simple et intuitive.
- Il s'intègre facilement avec pfSense.
- Il aide à détecter rapidement les anomalies.



INSTALLATION DE NTOP

Allez sur votre interface graphique pfSense

Déroulez System → Package Manager → Available Packages

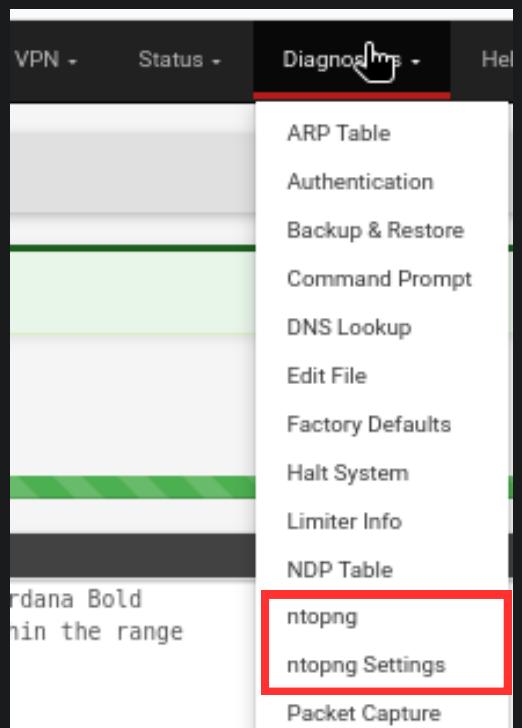
Recherchez ntop et installez le

The screenshot shows the pfSense Package Manager interface. The top navigation bar includes links for pfSense COMMUNITY EDITION, System (highlighted with a red box), Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is "System / Package Manager / Available Packages". Below this, there are tabs for "Installed Packages" and "Available Packages" (which is selected and highlighted with a red box). A search bar at the top has a red box around it, containing the search term "ntop" and a "Search" button. A message below the search bar says "Enter a search string or *nix regular expression to search package names and descriptions." The results table has columns for Name, Version, and Description. One result, "ntopng 0.8.13_10", is shown with a detailed description: "ntopng (replaces ntop) is a network probe that shows network usage in a way similar to what top does for processes. In interactive mode, it displays the network status on the user's terminal. In Web mode it acts as a Web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics." Below the description is a green "Install" button with a white plus sign, also highlighted with a red box. At the bottom, it lists "Package Dependencies" including webfonts-0.30_14, ntopng-5.6.d20230920.1, libmaxminddb-1.7.1_1, graphviz-8.1.0_1, redis-7.2.1, and gdbm-1.23.

The screenshot shows the pfSense Package Manager interface during a package installation. The top navigation bar includes links for pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is "System / Package Manager / Available Packages". Below this, there are tabs for "Installed Packages", "Available Packages" (selected and highlighted with a red box), and "Package Installer" (disabled). A message at the top says "Please wait while the installation of pfSense-pkg-ntopng completes. This may take several minutes. Do not leave or refresh the page!". The "Package Installation" section lists the packages being installed: openpgm: 5.2.122_6 [pfSense], pfSense-pkg-ntopng: 0.8.13_10 [pfSense], png: 1.6.40 [pfSense], psutils: 1.17_5 [pfSense], redis: 7.2.1 [pfSense], tiff: 4.4.0_2 [pfSense], uchardet: 0.0.8 [pfSense], webfonts: 0.30_14 [pfSense], wepb: 1.3.2 [pfSense]. It indicates that 38 packages are to be installed, requiring 212 MiB more space, with 26 MiB to be downloaded. The progress bar shows "[1/38] Fetching ntopng-5.6.d20230920.1.pkg: ..".

INSTALLATION DE NTOP

L'installation a fait apparaître deux nouvelles options dans "Diagnostics":

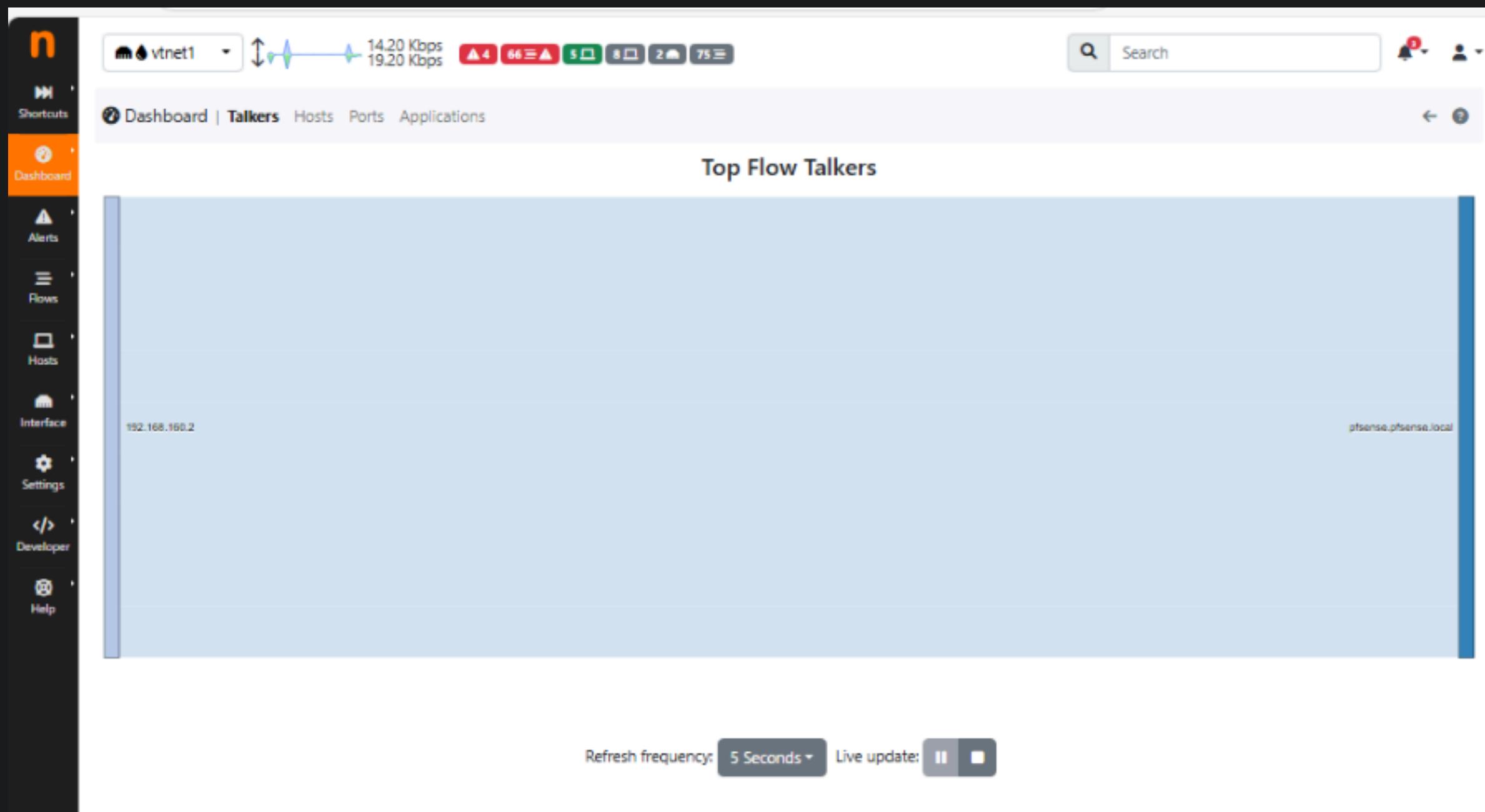


Cliquez sur "ntopng settings", cochez "Enable ntopng" puis configurez un mot de passe et choisissez l'interface LAN. Sauvegardez vos changements

The screenshot shows the 'ntopng Settings' configuration page. At the top, there are two tabs: 'ntopng Settings' (selected) and 'Access ntopng'. Below the tabs is a section titled 'General Options'. Under 'General Options', there is a checkbox labeled 'Enable ntopng' which is checked. Next to it is a note: 'Check this to enable ntopng.' Below this is another checkbox labeled 'Keep Data/Settings' which is also checked. To its right is a note: 'Keep ntopng settings, graphs and traffic data. Note: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade!' Below these checkboxes is a field for 'ntopng Admin Password' containing a series of dots (*****). Below that is a note: 'Enter the password for the ntopng GUI. Minimum 5 characters.' Below the password field is a field for 'Confirm ntopng Admin Password' containing a series of dots (*****). At the bottom of the page is a 'Interface' dropdown menu with three options: 'LAN' (selected and highlighted in blue), 'DMZ', and 'WAN'.

INSTALLATION DE NTOP

Une fois ceci fait, allez sur Access ntopng et cliquez sur le lien
Avec l'adresse IP de votre machine LAN, vous pourrez accéder à l'interface ntop
Ainsi, vous pourrez monitorer votre réseau



ACCÈS BUREAU À DISTANCE

Ajoutez une machine Windows Server et modifiez sa carte réseau pour y mettre la carte réseau de notre DMZ

Sur cette machine: une adresse IP 192.168.x.2, L'adresse IP DMZ du pare-feu, DNS préféré 8.8.8.8, DNS secondaire 1.1.1.1

Ajoutons une redirection de port:

Pour cela, allons sur Firewall → NAT → Port Forward → Edit

Ajoutez une règle:

On va faire en sorte que l'interface WAN en Protocol TCP à destination de l'adresse WAN sur le port 5500 (redirection de port pour des raisons de sécurité) redirige vers notre Windows Serveur.

The screenshot shows a configuration page for a port forwarding rule. The fields are as follows:

- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Display Advanced
- Destination:** WAN address (Type: Address/mask)
- Destination port range:** From port: Other, To port: 5500
- Redirect target IP:** 192.168.31.24 (Type: Address)
- Redirect target port:** MS RDP (Port: Custom)

Below the form, there is a note: "Enter the internal IP address of the server on which to map the ports, e.g.: 192.168.1.12 for IPv4".

ACCÈS BUREAU À DISTANCE

Vérifions dans les règles du WAN si nous avons une règle qui confirme bien la redirection RDP vers Windows serveur:

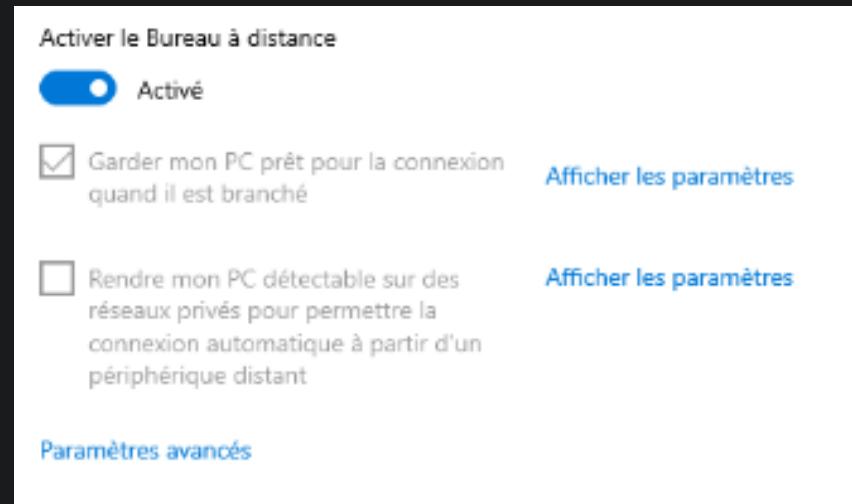


This is a detailed view of the "NAT Redirection RDP vers Windows Serveur" rule configuration. It includes the following sections:

- Action:** Pass (selected)
- Associated filter rule:** This is associated with a NAT rule. (disabled)
- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Any (Source Address: 192.168.170.2)
- Destination:** MS RDP (3389) (From: Custom, To: Custom)

ACCÈS BUREAU À DISTANCE

Il faut maintenant sur votre Windows Serveur autoriser le bureau à distance



On va ensuite dans la gestion de l'ordinateur et on y ajoute un user s'il n'y a pas de Active Directory (Utilisation de l'administrateur perso)

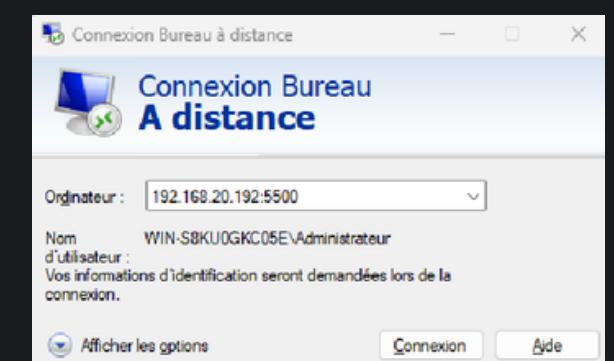
Nous allons ensuite dans "groupes", on clique sur « Serveurs Accès Distant RDS » et on ajoute notre user.

Ensuite on va dans le panneau de configuration de l'ordinateur-> Système et sécurité -> Système

-> Paramètres d'utilisation à distance et on choisit notre utilisateur:

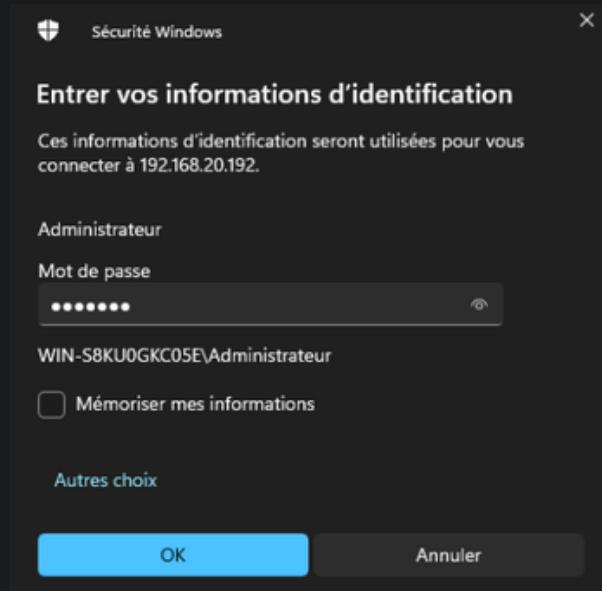


Sur notre machine connectée au réseau WAN, allez dans le bureau à distance et connectez vous à votre Windows Server avec l'IP Windows server et son port:



ACCÈS BUREAU À DISTANCE

Entrez les logs:



Vous avez maintenant accès au serveur:

