

## Accès NAT d'un VLAN sur Internet

Sommaire :

- 1. Configuration du LAN 1 ----- 2
- 2. Paramétrage des règles de pare-feu ----- 3

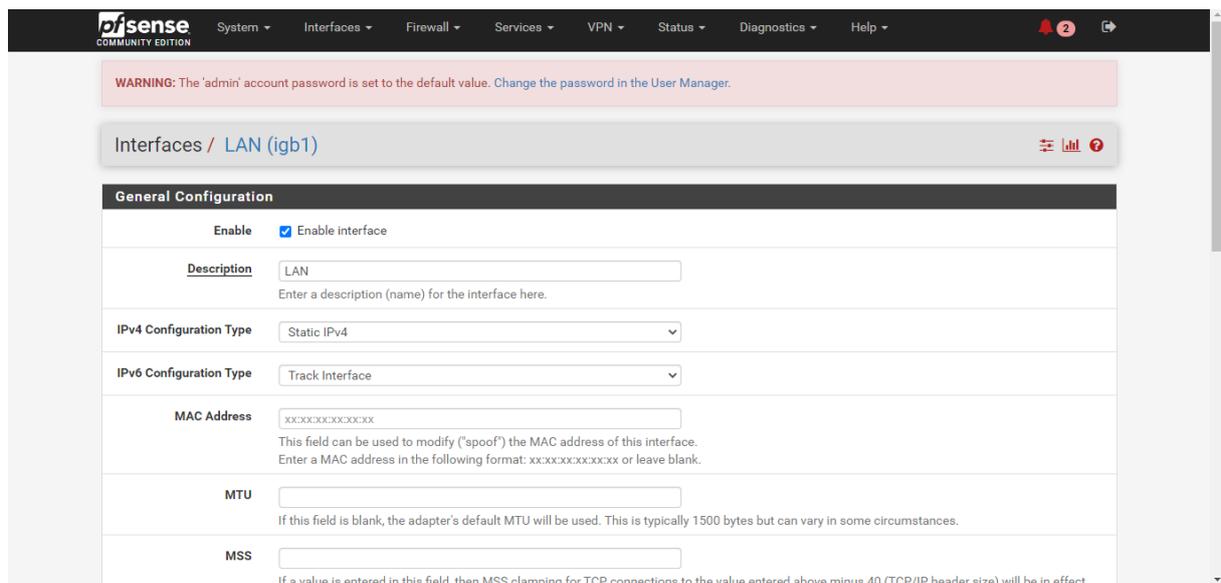
Maintenant que l'on sait comment aller administrer le routeur, nous allons essayer d'obtenir une connexion Internet sur le premier VLAN de celui-ci. Cela nous sera utile pour la communication entre les différents VLAN.

# 1. Configuration du LAN 1

Premièrement, nous devons ajouter un autre câble RJ-45 sur le port 4 du routeur, que l'on relie à la goulotte de l'îlot.



Avant d'essayer d'obtenir une connexion Internet, il faut que le réseau dans lequel on se trouve soit correctement paramétré. Pour cela, on clique en haut sur l'onglet « Interface », puis sur « LAN ». Si tout est bon, la page suivante devrait s'afficher.



Ensuite, cocher la case « Enable Interface » si elle n'est pas déjà cochée, descendre en bas de la page et cliquer sur « Save ». Remonter et Appliquer les changements. Il n'y a pas à modifier l'adresse par défaut de ce premier réseau, donc la configuration de celui-ci était assez courte.

## 2. Paramétrages des règles de Pare-feu

Maintenant que le réseau est bien délimité, il est important d'établir des règles de pare-feu pour établir une connexion Internet. Pour accéder à la page de celles-ci, il faut cliquer sur l'onglet « Firewall », puis « Rules ». On peut ensuite établir des règles pour chaque réseau.

Ici, nous allons nous concentrer sur le WAN et le LAN 1.

Règles à introduire pour le WAN :

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0 / 22 KiB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	⚙️
✗ 0 / 8 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️
✓ 0 / 0 B	IPv4 *	*	*	*	*	*	*	none		📌 🖋️ 🗑️
✓ 0 / 0 B	IPv4 *	*	*	*	*	*	*	none		📌 🖋️ 🗑️

Règles à introduire pour le LAN 1 :

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 3 / 16.34 MiB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	⚙️
✓ 10 / 902 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	📌 🖋️ 🗑️
✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 🖋️ 🗑️

Ces règles sont essentielles pour autoriser le poste à se connecter à Internet.

Si tout cela est bien fait, on devrait obtenir l'accès à Internet. On vérifie cela à l'aide d'une commande Ping (taper « CMD » dans la barre de recherche Windows) suivie d'une adresse internet :

```

C:\Users\SISR>ping www.google.com

Envoi d'une requête 'ping' sur www.google.com [216.58.214.164] avec 32 octets de données :
Réponse de 216.58.214.164 : octets=32 temps=12 ms TTL=113

Statistiques Ping pour 216.58.214.164:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 12ms, Maximum = 12ms, Moyenne = 12ms

C:\Users\SISR>arp -a

Interface : 192.168.1.8 --- 0x6
Adresse Internet  Adresse physique  Type
192.168.1.1       40-62-31-07-bc-c7  dynamique
192.168.1.255    ff-ff-ff-ff-ff-ff  statique
224.0.0.22      01-00-5e-00-00-1b  statique
224.0.0.251     01-00-5e-00-00-fb  statique
224.0.0.252     01-00-5e-00-00-fc  statique
239.255.102.18  01-00-5e-7f-66-12  statique
239.255.255.250 01-00-5e-7f-ff-fa  statique

C:\Users\SISR>

```

Adresse de passerelle LAN 1  
Adresse de diffusion

Comme nous recevons une réponse de l'adresse internet de Google, on en conclut que nous avons bien réussi à établir une connexion Internet sur le LAN 1.

La requête arp -a permet de savoir quelles sont les machines connectées au réseau et quelles sont leurs adresses mac.

```

C:\Users\SISR>ping www.google.com

Envoi d'une requête 'ping' sur www.google.com [216.58.214.164] avec 32 octets de données :
Réponse de 216.58.214.164 : octets=32 temps=12 ms TTL=113

Statistiques Ping pour 216.58.214.164:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 12ms, Maximum = 12ms, Moyenne = 12ms

C:\Users\SISR>tracert www.google.com

Détermination de l'itinéraire vers www.google.com [216.58.214.164]
avec un maximum de 30 sauts :

 1  <1 ms  <1 ms  <1 ms  192.168.1.1
 2  <1 ms  <1 ms  <1 ms  172.16.21.1
 3  1 ms   1 ms   <1 ms  5.50.84.62
 4  2 ms   1 ms   1 ms   31.33.19.2
 5  *      *      *      Délai d'attente de la demande dépassé.
 6  *      *      *      Délai d'attente de la demande dépassé.
 7  *      *      11 ms  62.34.2.187
 8  12 ms  12 ms  12 ms  be15.cbr01-ntr.net.bbox.fr [212.194.171.96]
 9  *      *      12 ms  62.34.2.58
10  12 ms  12 ms  12 ms  72.14.204.68
11  13 ms  13 ms  13 ms  216.239.40.75
12  12 ms  12 ms  11 ms  216.239.48.43
13  12 ms  12 ms  12 ms  par10s42-in-f4.1e100.net [216.58.214.164]

```

Adresse de passerelle LAN 1  
Adresse de la goulotte

La commande tracert permet de voir le chemin que prennent es paquets lors du ping. Ici, on voit qu'ils passent bien par l'adresse de passerelle du LAN 1.



## Routage et Filtrage entre les LAN 2 et 3

### Sommaire :

1 – Création et configuration des LAN 2 et 3 -----	02
2 – Mise en place des règles de parefeu -----	06
3 – Test de connectivité entre les LANs 2 et 3 -----	07

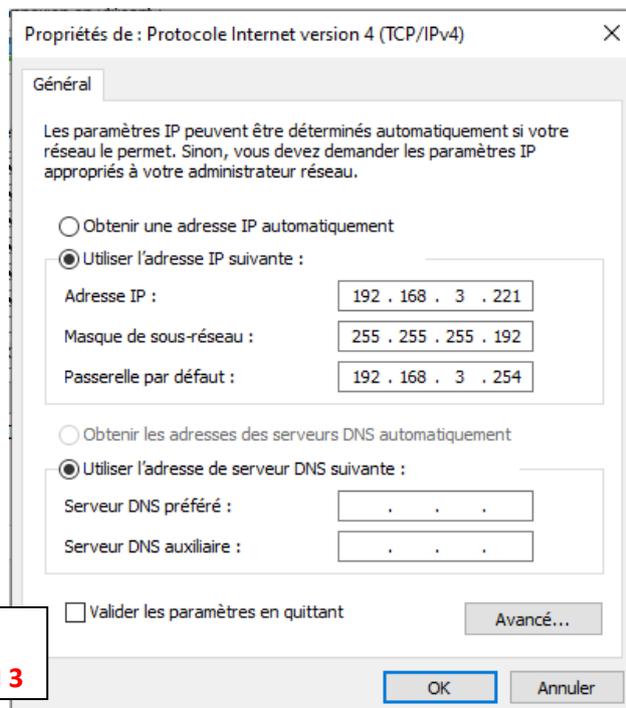
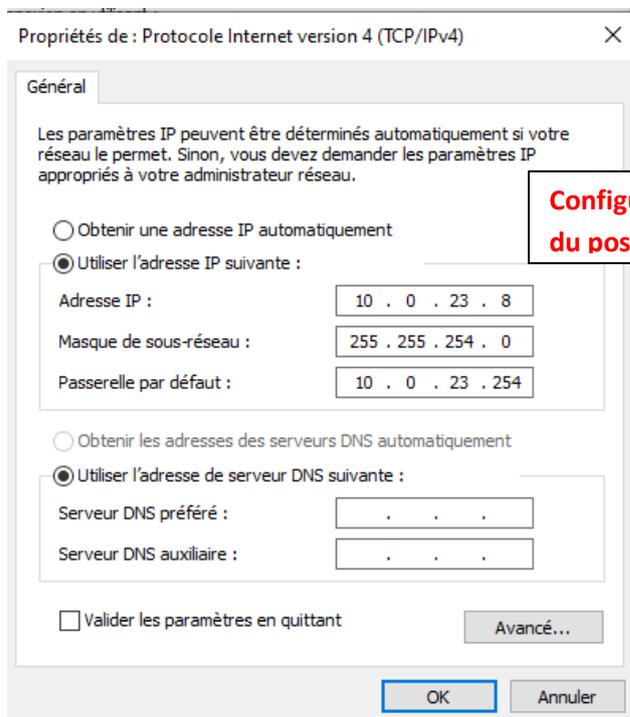
# 1- Création et configuration des LAN

Il faut avant tout brancher les câbles sur les ports suivants :



Notre première étape va être de créer et configurer les deux LAN dans l'interface.

On prend d'abord sur les ordinateurs une configuration réseau conforme en allant dans **Paramètres → Centre réseau et Partage → Ethernet 2 → Propriétés → Protocole Internet version 4.**



Pour cela, il faut cliquer sur les onglets « Interfaces » → « Assignments », puis en bas à droite dans le tableau des interfaces, cliquer sur « + Add », puis sauvegarder les modifications en appuyant sur « Save ».

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port	
WAN	igb0 (40:62:31:07:bc:c6)	
LAN	igb1 (40:62:31:07:bc:c7)	Delete
LAN2	igb2 (40:62:31:07:bc:c8)	Delete
LAN3	igb3 (40:62:31:07:bc:c9)	Delete
Available network ports:	igb4 (40:62:31:07:bc:ca)	+ Add

Save

Ensuite, on clique sur le nom de la nouvelle interface, puis on la renomme en fonction du LAN correspondant.

A présent, on configure les LAN correctement. Pour le LAN 2, je donne l'adresse IP **10.0.23.254 /23**. Le LAN 3 quant à lui est assigné en **192.168.3.254 /26**.

LAN 2 :

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces / LAN2 (igb2)

**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". 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 RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface 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 any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

LAN 3 :

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager](#)

## Interfaces / LAN3 (igb3)

### 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". 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 RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface 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 any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

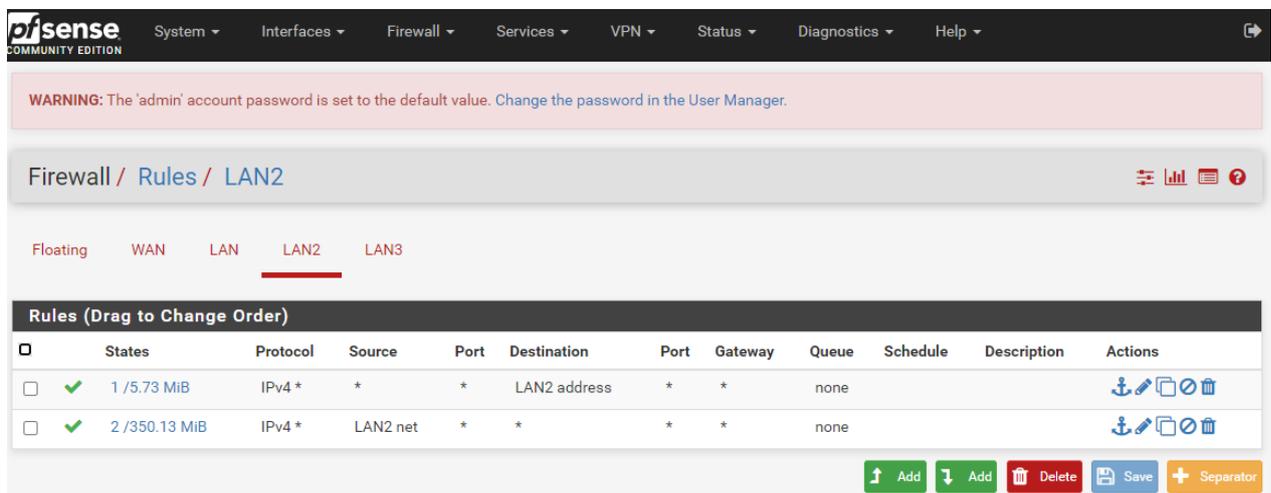
Quand notre configuration est terminée, on appuie sur le bouton bleu « Save » en fin de page.

## 2- Mise en place des règles de pare-feu

Une fois les LAN créés, il est important de contrôler les échanges entre les différents réseaux. Pour cela, nous allons créer des règles de pare-feu sur le routeur. Dans l'interface, cliquer sur l'onglet « **Firewall** » → « **Rules** ».

Par défaut, deux règles sont créées automatiquement lors de la création d'une nouvelle interface.

LAN 2 :



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / LAN2

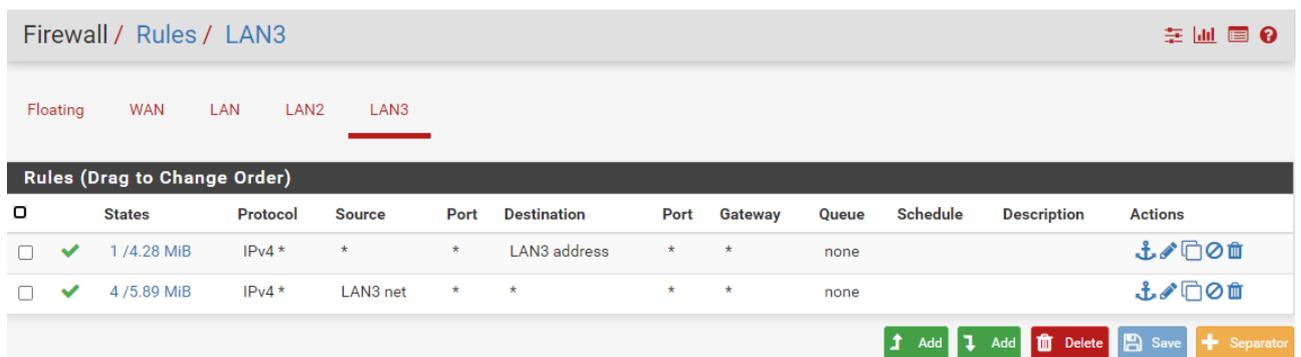
Floating WAN LAN LAN2 LAN3

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 5.73 MiB	IPv4 *	*	*	LAN2 address	*	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	✓ 2 / 350.13 MiB	IPv4 *	LAN2 net	*	*	*	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>

[↑ Add](#) [↓ Add](#) [Delete](#) [Save](#) [+ Separator](#)

LAN 3 :



Firewall / Rules / LAN3

Floating WAN LAN LAN2 LAN3

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 4.28 MiB	IPv4 *	*	*	LAN3 address	*	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	✓ 4 / 5.89 MiB	IPv4 *	LAN3 net	*	*	*	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>

[↑ Add](#) [↓ Add](#) [Delete](#) [Save](#) [+ Separator](#)

Pour l'instant, cela est suffisant pour notre environnement de travail.

### 3- Test de connectivité entre les LAN 2 et 3

Maintenant que tout est correctement paramétré sur l'interface, nous devons nous assurer que les deux réseaux peuvent effectivement communiquer entre eux, et qu'ils passent par le bon chemin.

Pour cela, nous allons faire deux types de test différents :

- Un ping suivi d'un tracert pour vérifier que l'on passé bien par le bon chemin, dans un sens puis dans l'autre
- Un ping suivi d'un arp -a pour vérifier que l'ordinateur retiens bien les bonnes adresses, dans un sens puis dans l'autre

LAN 2 vers LAN 3 :

```
C:\Windows\system32\cmd.exe
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.1:
  Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
  Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\SISR>ping 192.168.3.221

Envoi d'une requête 'Ping' 192.168.3.221 avec 32 octets de données :
Réponse de 192.168.3.221 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 192.168.3.221:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
  Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\SISR>tracert 192.168.3.221

Détermination de l'itinéraire vers 192.168.3.221 avec un maximum de 30 sauts.

  1  <1 ms  <1 ms  <1 ms  10.0.23.254
  2  <1 ms  <1 ms  <1 ms  192.168.3.221

Itinéraire déterminé.
```

Le ping a fonctionné : les deux machines communiquent entre elles

La commande montre que les requêtes passent d'abord par le routeur sur le port LAN 2, puis arrivent à destination

```

C:\Users\SISR>ping 192.168.3.221

Envoi d'une requête 'Ping' 192.168.3.221 avec 32 octets de données :
Réponse de 192.168.3.221 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 192.168.3.221:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\SISR>apr -a
'apr' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\SISR>arp -a

Interface : 169.254.217.22 --- 0x4
    Adresse Internet    Adresse physique      Type
    169.254.255.255     ff-ff-ff-ff-ff-ff    statique
    224.0.0.22          01-00-5e-00-00-16    statique
    224.0.0.251         01-00-5e-00-00-fb    statique
    224.0.0.252         01-00-5e-00-00-fc    statique
    239.255.255.250     01-00-5e-7f-ff-fa    statique

Interface : 10.0.23.8 --- 0x6
    Adresse Internet    Adresse physique      Type
    10.0.23.254         40-62-31-07-bc-c8    dynamique
    10.0.23.255         ff-ff-ff-ff-ff-ff    statique
    224.0.0.22          01-00-5e-00-00-16    statique
    224.0.0.251         01-00-5e-00-00-fb    statique
    224.0.0.252         01-00-5e-00-00-fc    statique
    239.255.102.18     01-00-5e-7f-66-12    statique
    239.255.255.250     01-00-5e-7f-ff-fa    statique

```

Le ping a fonctionné : les deux machines communiquent entre elles

La commande montre que l'ordinateur a enregistré la bonne adresse de passerelle pour les requêtes du LAN 2 vers le LAN 3

### LAN 3 vers LAN 2 :

```

C:\Users\SISR>ping 10.0.23.8

Envoi d'une requête 'Ping' 10.0.23.8 avec 32 octets de données :
Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 10.0.23.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\SISR>tracert 10.0.23.8

Détermination de l'itinéraire vers 10.0.23.8 avec un maximum de 30 sauts.

  1  <1 ms  <1 ms  <1 ms  192.168.3.254
  2  <1 ms  <1 ms  <1 ms  10.0.23.8

Itinéraire déterminé.

```

Le ping a fonctionné : les deux machines communiquent entre elles

La commande montre que les requêtes passent d'abord par le routeur sur le port LAN 3, puis arrivent à destination

```

C:\Users\SISR>ping 10.0.23.8

Envoi d'une requête 'Ping' 10.0.23.8 avec 32 octets de données :
Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 10.0.23.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\SISR>arp -a

Interface : 192.168.3.221 --- 0x5
  Adresse Internet    Adresse physique    Type
  192.168.3.254      40-62-31-07-bc-c9  dynamique
  192.168.3.255      ff-ff-ff-ff-ff-ff  statique
  224.0.0.22         01-00-5e-00-00-16  statique
  224.0.0.251        01-00-5e-00-00-fb  statique
  224.0.0.252        01-00-5e-00-00-fc  statique
  239.255.102.18     01-00-5e-7f-66-12  statique
  239.255.255.250    01-00-5e-7f-ff-fa  statique
  255.255.255.255    ff-ff-ff-ff-ff-ff  statique

```

Le ping a fonctionné : les deux machines communiquent entre elles

La commande montre que l'ordinateur a enregistré la bonne adresse de passerelle pour les requêtes du LAN 3 vers le LAN 2

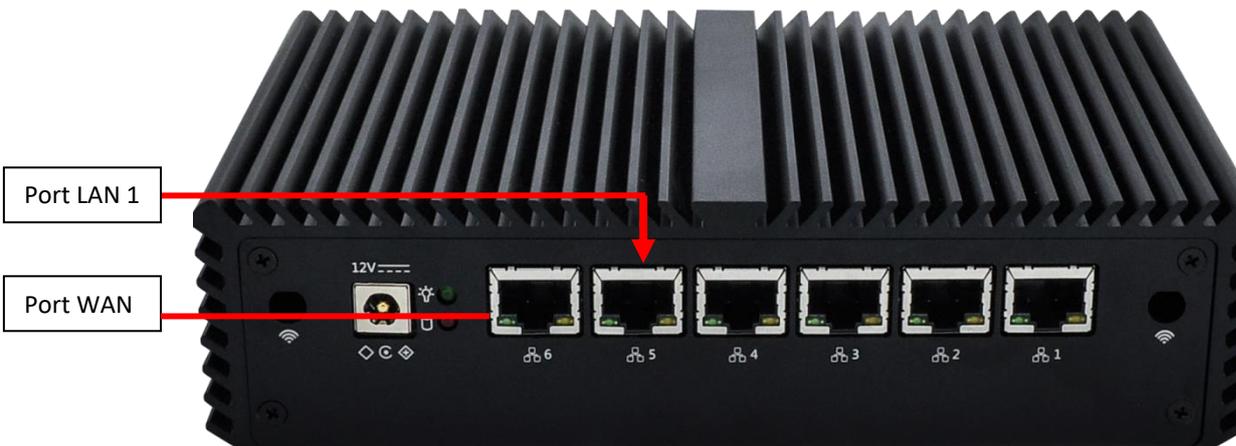
## Prise en main administrative du PFSense



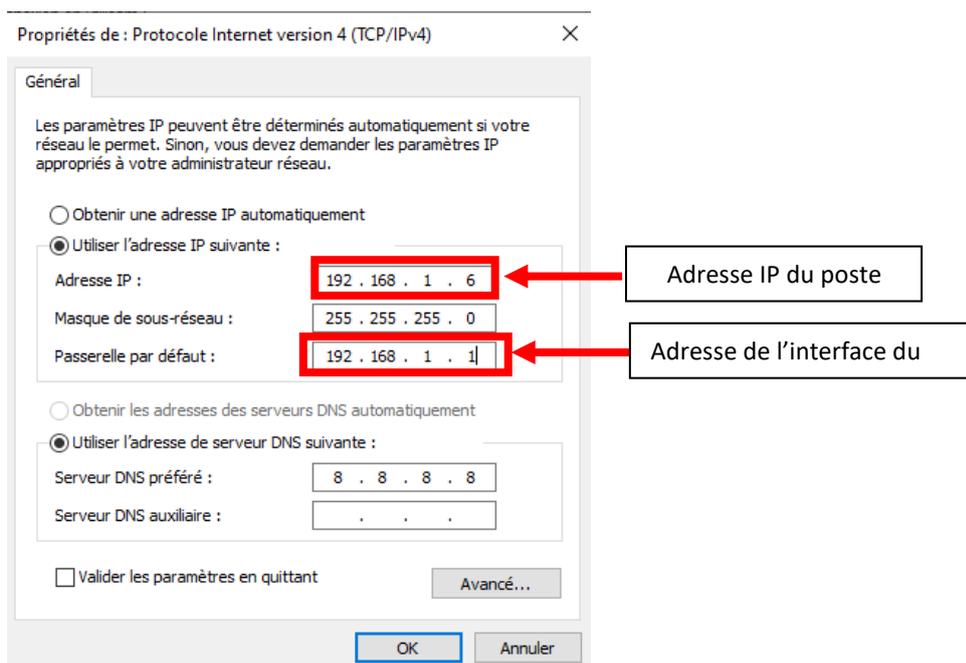
Dans ce document, nous allons voir comment se connecter pour la première fois à l'interface d'un un routeur PFSense.

# 1. Initialisation du routeur

Avant de commencer à utiliser le routeur, il faut correctement le brancher et le relier à l'environnement. Nous allons donc brancher un câble RJ-45 sur le port 5 (le port 6 est réservé pour le WAN).



Ensuite, nous allons installer une configuration réseau (adresse IP, masque, interface dans le même réseau que le routeur) compatible avec l'adresse par défaut du PfSense (192.168.1.1). Pour aller modifier cela, il faut se rendre dans les Paramètres -> Réseau et Internet -> Centre Réseau et Partage -> Ethernet 2 -> Propriétés -> Protocole Internet version 4. On rentre ensuite les informations, et quelque on doit obtenir quelque chose de ce style :



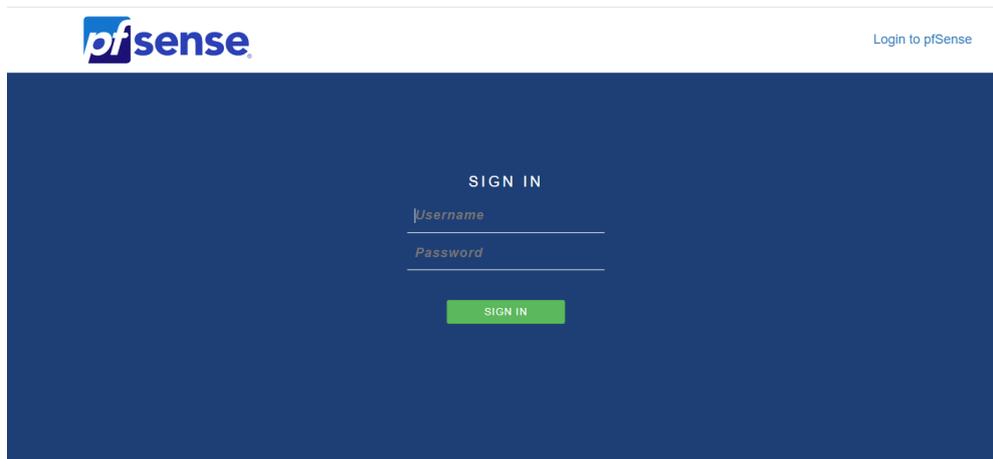
Pour vérifier que la configuration est bonne, on peut, avant de se connecter au routeur, tenter une commande Ping dans l'invite de commande (taper « CMD » dans la barre de recherche Windows) vers son adresse. On devrait avoir une réponse du routeur :

```
Microsoft Windows [version 10.0.19044.2604]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\SISR>ping 192.168.1.1 ← Adresse de l'interface du routeur

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
```

Puis, on va maintenant sur un navigateur et on rentre l'adresse du routeur.



Des identifiants vous sont demandés. Par défaut, ce sont :

User = admin

Password = pfsense

Une fois cela fait, vous devriez accéder à l'interface du PfSense :

The screenshot displays the pfSense Community Edition dashboard. At the top, a navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning banner at the top left states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Status / Dashboard" section is active. The dashboard is divided into two main columns. The left column, titled "System Information", contains a table with the following data:

<b>Name</b>	pfSense.localdomain
<b>User</b>	admin@192.168.1.6 (Local Database)
<b>System</b>	pfSense Netgate Device ID: 561af036cc7b58747e
<b>BIOS</b>	Vendor: American Megatrends Inc. Version: 5.12 Release Date: Fri Nov 23 2018
<b>Version</b>	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE  Obtaining update status
<b>CPU Type</b>	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz Current: 2200 MHz, Max: 2301 MHz 4 CPUs: 1 package(s) x 2 core(s) x 2 hardware threads AES-NI CPU Crypto: Yes (inactive)
<b>Kernel PTI</b>	Enabled

The right column, titled "Netgate Services And Support", shows the contract type as "Community Support" and "Community Support Only". Below this, a section titled "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" provides information about support options. It states: "If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**." It also mentions the option to upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. A list of links is provided at the bottom:

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com