



Mise en situation

La société Vikor désire installer un serveur Web au sein de son architecture réseau ,ce serveur doit être accessible depuis le LAN de l'entreprise ainsi que de « l'extérieur » ,à savoir internet.
Afin de sécuriser au maximum son réseau ,le choix de PfSense a été fait en raison de sa flexibilité et du nombre de fonctionnalités disponibles.

Sommaire



Schéma réseaux

Le PFSense c'est quoi ?

Le PfSense comment on y accède

La règle WAN vers DMZ

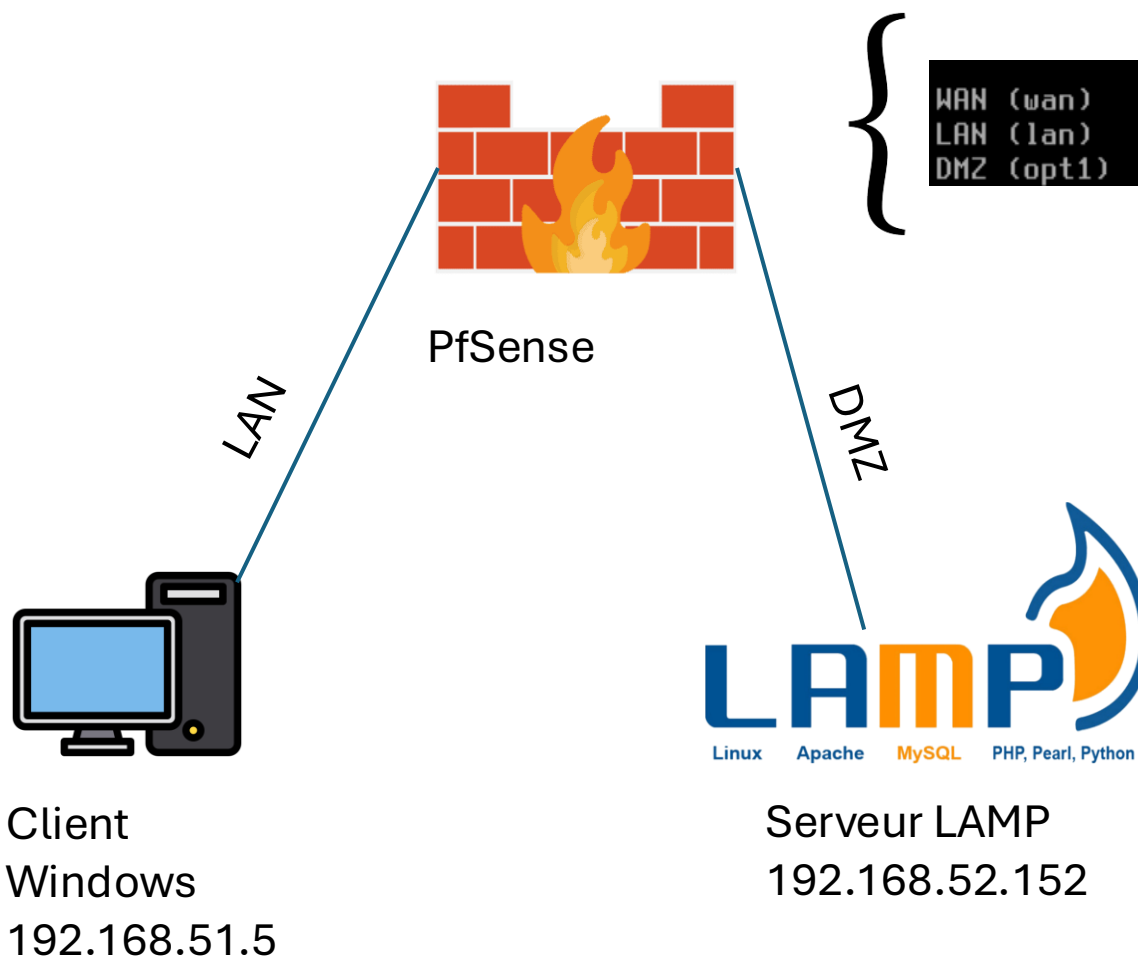
La règle pour un accès RDP

Monitoring

Schéma réseaux

Belerge Jérémie

BTS SIO 2



WAN (wan)	-> vtnet1	-> v4/DHCP4: 192.168.20.169/24
LAN (lan)	-> vtnet0	-> v4: 192.168.51.1/24
DMZ (opt1)	-> vtnet2	-> v4: 192.168.52.1/24



Consignes:

-Le PFsense c'est quoi ?

Pfsense est un OS transformant n'importe quel ordinateur en routeur/pare-feu. Basé sur FreeBSD, connu pour sa fiabilité et surtout sa sécurité, Pfsense est un produit OpenSource adapté à tout type d'entreprise.

Voici ses principales fonctionnalités :

- Gestion complète par interface web
- Pare-feu stateful avec gestion du NAT, NAT-T
- Gestion de multiples WAN
- DHCP server et relay
- Failover (possibilité de monter un cluster de pfsense)
- Load balancing
- VPN Ipsec, OpenVPN, L2TP
- Portail captif

Source: www.it-connect.fr

Pour résumer : pfSense est une solution logicielle libre qui transforme un matériel courant en un routeur/pare-feu professionnel et évolutif, idéale pour sécuriser, surveiller et contrôler l'ensemble des échanges d'un réseau informatique.



Consignes:

-Le PFsense comment on y accède ?

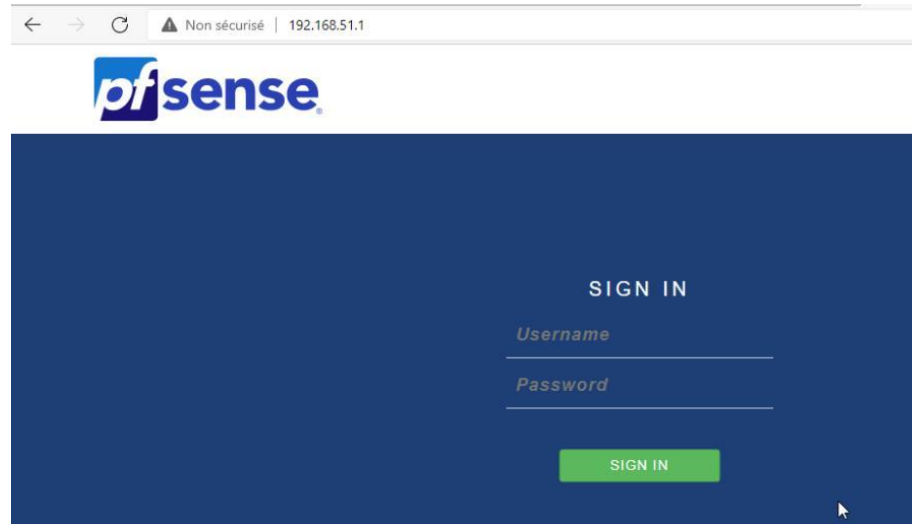
```
WAN (wan)      -> vtnet1      -> v4/DHCP4: 192.168.20.169/24
LAN (lan)      -> vtnet0      -> v4: 192.168.51.1/24
DMZ (opt1)     -> vtnet2      -> v4: 192.168.52.1/24
```

Voici la configuration du
PFsense

Wan -> 192.168.20.169

LAN -> 192.168.51.1

DMZ -> 192.168.52.1



Depuis la machine dans la LAN , il nous
faut rentrer l'ip entré dans notre
PFsense
(192.168.51.1)

Utilisateur: admin
Password : pfsense



Consignes:

- WAN -> DMZ

Depuis Firewall -> NAT

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.52.152	80 (HTTP)			
-------------------------------------	-------------------------------------	-------------------------------------	-----	-----	---	---	-------------	-----------	----------------	-----------	--	--	--

Disabled	<input type="checkbox"/> Disable this rule
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule <small>This option is rarely needed. Don't use this without thorough knowledge of the implications.</small>
Interface	<div>WAN</div> <div>Choose which interface this rule applies to. In most cases "WAN" is specified.</div>
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>TCP</div> <div>Choose which protocol this rule should match. In most cases "TCP" is specified.</div>
Source	<div> Display Advanced</div>
Destination	<div><input type="checkbox"/> Invert match.</div> <div><div>WAN address</div><div>Type</div></div> <div><div></div><div>Address/mask</div></div>
Destination port range	<div><div>HTTP</div><div>From port</div></div> <div><div>Custom</div><div></div></div> <div><div>HTTP</div><div>To port</div></div> <div><div>Custom</div><div></div></div>
<small>Specify the port or port ranges for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.</small>	

Redirect target IP	<div>Address or Alias</div> <div>Type</div>	<div>192.168.52.152</div> <div>Address</div>
<small>Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)</small>		
Redirect target port	<div>HTTP</div> <div>Port</div>	<div>Custom</div> <div></div>
<small>Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.</small>		



Cette règle va nous permettre d'avoir accès a notre page web depuis notre WAN. On rentre l'ip 192.168.52.152 (de notre LAMP) afin de pouvoir y accéder depuis notre WAN.



Consignes:

-Test

Résultat depuis notre WAN :



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split



Consignes:

-RDP

Depuis Firewall -> NAT

✓	✓	✗	WAN	TCP	*	*	WAN address	5500	192.168.51.5	3389 (MS RDP)
Edit Redirect Entry										
Disabled <input type="checkbox"/> Disable this rule										
No RDR (NOT) <input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.										
Interface WAN Choose which interface this rule applies to. In most cases "WAN" is specified.										
Address Family IPv4 Select the Internet Protocol version this rule applies to.										
Protocol TCP Choose which protocol this rule should match. In most cases "TCP" is specified.										
Source ⚙ Display Advanced										
Destination <input type="checkbox"/> Invert match. WAN address Type Address/mask										
Destination port range Other 5500 Other 5500 From port Custom To port Custom Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.										
Redirect target IP Address or Alias 192.168.51.5 Type Address										

Cette regle va nous permettre de pouvoir autorisé le bureau a distance

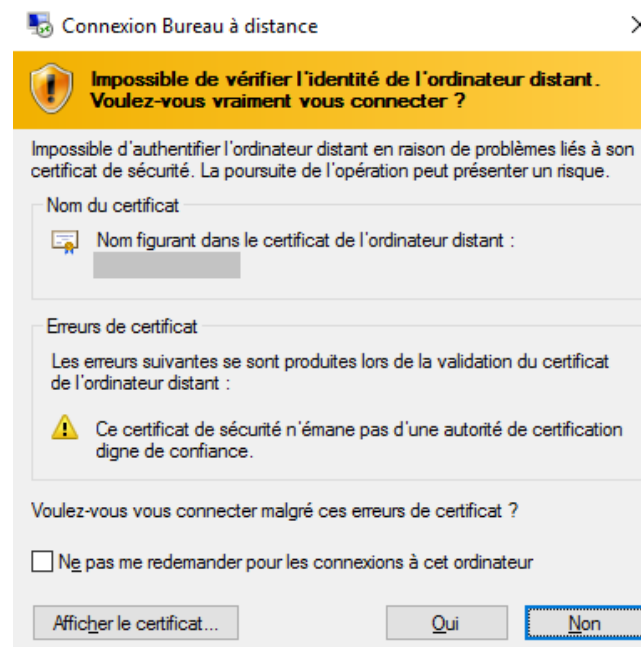
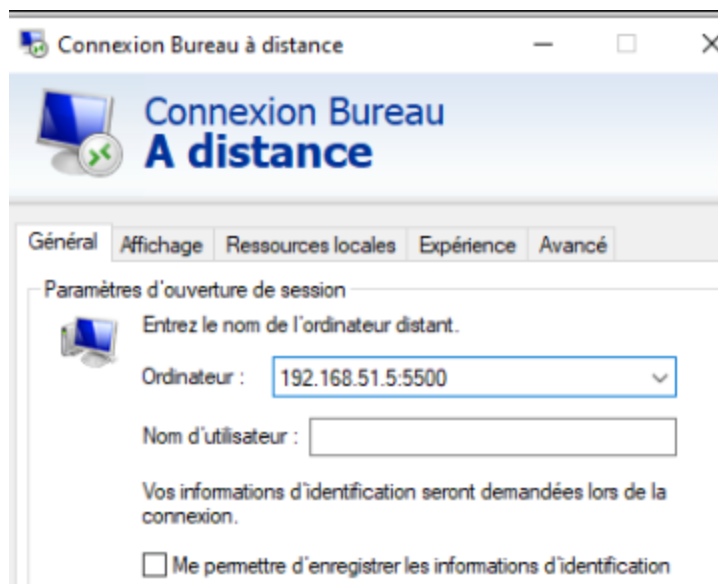
(Attention il ne faut pas oublier d'activé le bureau a distance sur vos machines windows)
Pour cela il faut suivre ce chemin : Parametre -> Système -> Bureau a distance



Consignes:

-Test

Afin de se connecter au Bureau à distance :



Sur la deuxième machine il faudra alors rentrer l'ip de notre machine cible , ainsi que le port qui est renseigné dans notre règle (ici 5500)

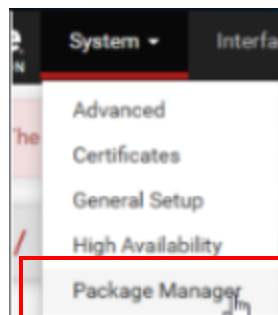
Si le message apparait c'est normal , c'est car le certificat n'est pas officiel



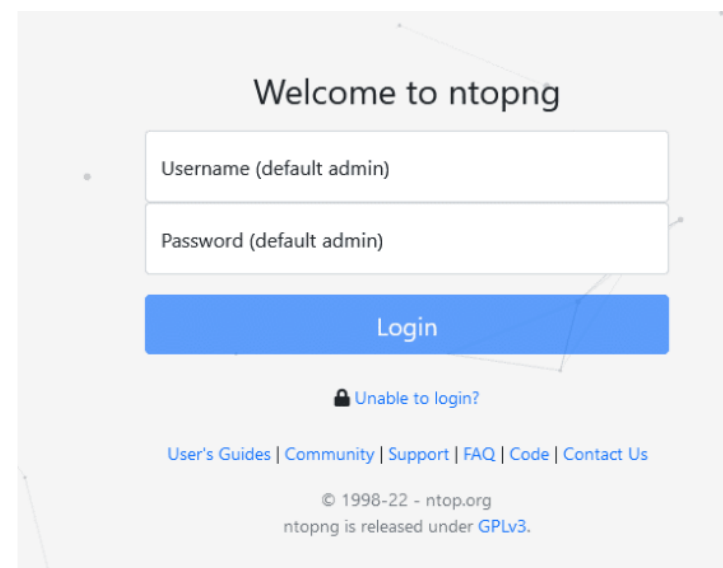
Consignes:

-Monitoring | NtopNG

Pour installer le package, connectez-vous à l'interface web, ouvrez l'onglet **System**, puis sélectionnez **Package Manager**. Recherchez le package **ntopng** et cliquez sur **Installer** pour démarrer l'installation



Une fois l'installation terminée, accédez à **Diagnostic** → **ntopng Settings** pour effectuer la configuration. Activez l'option **Enable ntopng** afin d'activer le service, puis enregistrez les modifications. Puis afin d'accéder à l'interface il faudra noter 192.168.51.1:3000





Consignes:

-Monitoring | NtopNG

L'outil permet une surveillance en temps réel du trafic réseau à travers différents modules. Le **tableau de bord** fournit une vue globale du débit, du volume de paquets échangés et des protocoles utilisés. La section **Hosts** répertorie les appareils connectés ainsi que leur consommation de bande passante, tandis que **Flows** présente les connexions actives entre ces hôtes. Enfin, l'analyse du trafic propose des **graphiques** détaillant l'utilisation des protocoles et l'évolution du trafic au fil du temps.

