

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

Belerge Jérémy

BTS SIO 2

Schéma réseaux

Le PFsense c'est quoi ?

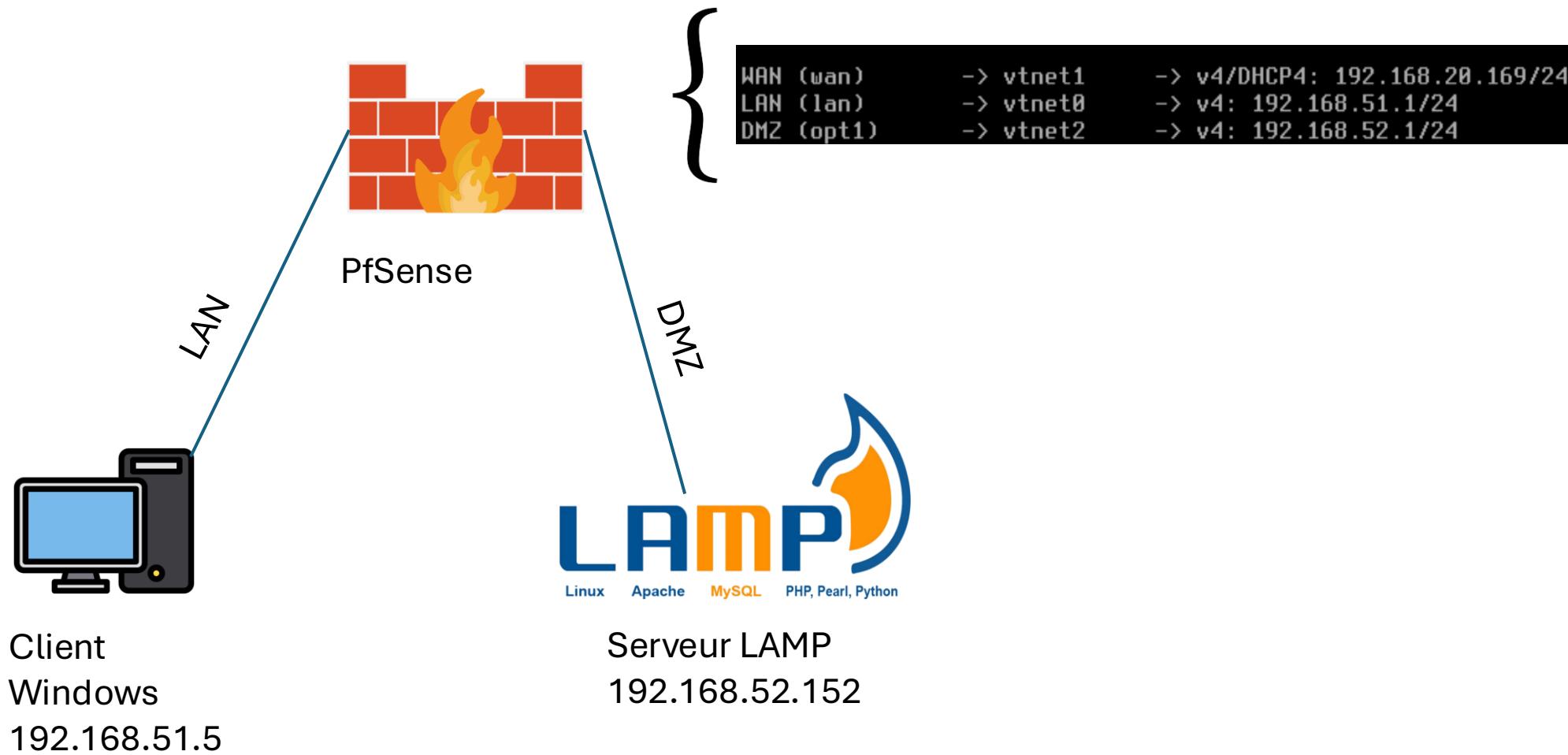
Le PfSense comment on y accède

La règle WAN vers DMZ

La règle pour un accès RDP

Monitoring

Schéma réseaux





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

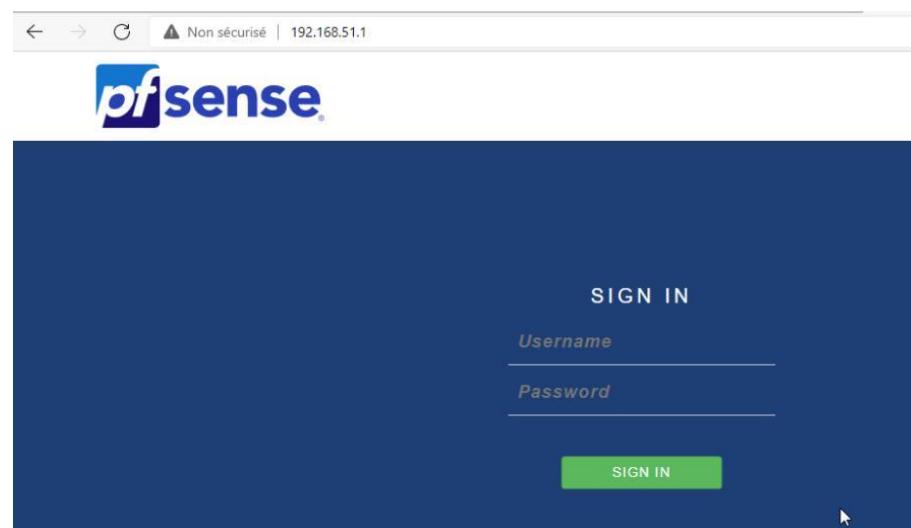
Pour résumer: pfSense est une solution logicielle libre qui transforme un matériel courant en un routeur/pare-feu professionnel et évolutif, idéale pour sécuriser, surveiller et contrôler l'ensemble des échanges d'un réseau informatique.



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 entrer dans notre PFsense
(192.168.51.1)

Utilisateur: admin
Password : pfsense



Consignes:

- WAN -> DMZ

Depuis Firewall -> NAT

The screenshot shows a configuration page for a NAT rule. At the top, there are several status indicators and action buttons. Below this, the rule settings are detailed:

- Disabled:** **WAN** **TCP** * * **WAN address** **80 (HTTP)** **192.168.52.152** **80 (HTTP)** **Edit** **Delete**
- No RDR (NOT):** **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:** **Invert match.** **WAN address** **Type** **Address/mask**
- Destination port range:** **HTTP** **From port** **Custom** **HTTP** **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** **Type** **192.168.52.152** **Address**
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)
- Redirect target port:** **HTTP** **Port** **Custom**
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.

Cette règle va nous permettre d'avoir accès à 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 :

A screenshot of a web browser displaying the 'Apache2 Debian Default Page'. The page features the red Debian logo and the text 'Apache2 Debian Default Page'. A prominent red bar contains the text 'It works!'. Below this, there is explanatory text about the purpose of the page and instructions for replacing the default file. At the bottom, a grey bar reads 'Configuration Overview'.



Consignes:

-RDP

Depuis Firewall -> NAT

The screenshot shows a configuration page for a 'Edit Redirect Entry' rule. At the top, there are several status indicators: a checkmark, a blue checkmark, a crossed-out gear icon, 'WAN', 'TCP', and two asterisks. To the right of these are fields for 'WAN address' (5500), '192.168.51.5', and '3389 (MS RDP)'. Below this, the rule details are listed:

- Disabled:** Disable this rule
- No RDR (NOT):** Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.
- Interface:** WAN (dropdown)
Choose which interface this rule applies to. In most cases "WAN" is specified.
- Address Family:** IPv4 (dropdown)
Select the Internet Protocol version this rule applies to.
- Protocol:** TCP (dropdown)
Choose which protocol this rule should match. In most cases "TCP" is specified.
- Source:**
- Destination:** Invert match. Type: Address/mask /
- Destination port range:** From port: Other (dropdown) 5500 To port: Other (dropdown) 5500
Custom 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:** Type: Address 192.168.51.5

Cette règle va nous permettre de pouvoir autorisé le bureau à distance

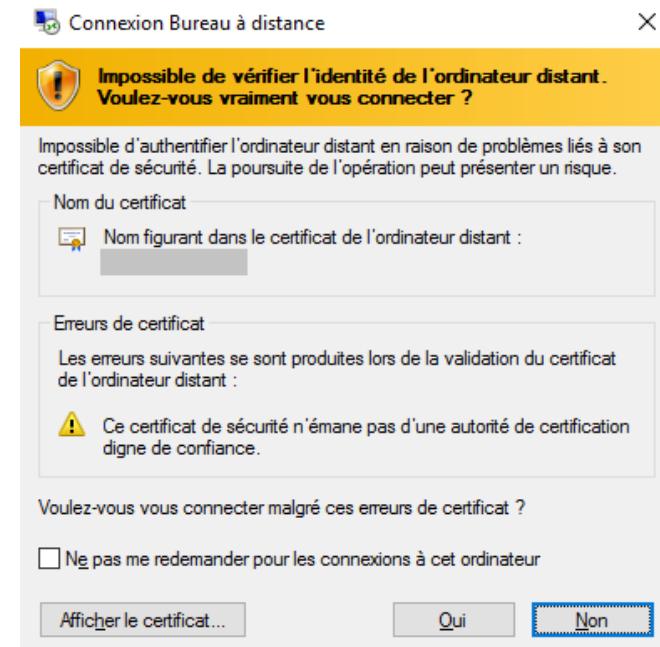
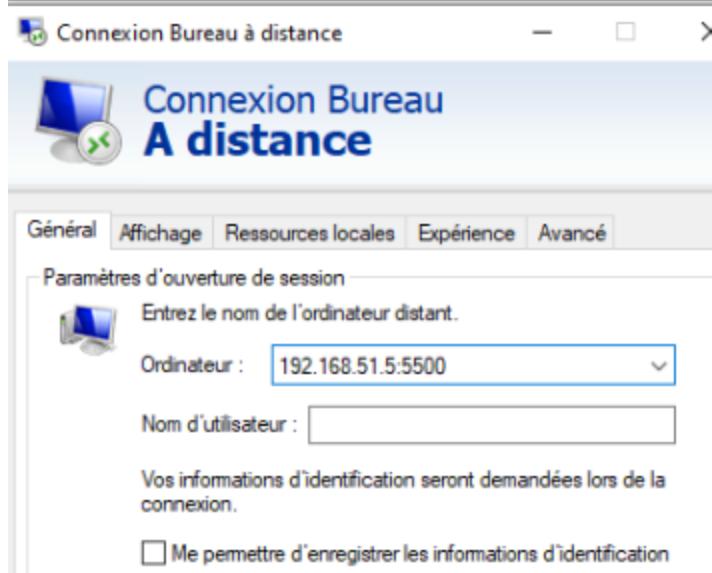
(Attention il ne faut pas oublier d'activer le bureau à distance sur vos machines windows)
Pour cela il faut suivre ce chemin : Paramètre -> Système -> Bureau à distance



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)

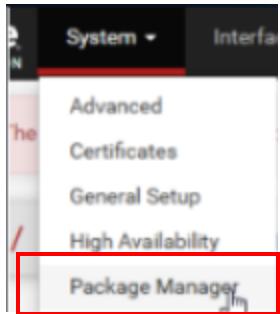
Si le message apparait c'est normal , c'est car le certificat n'est pas officiel



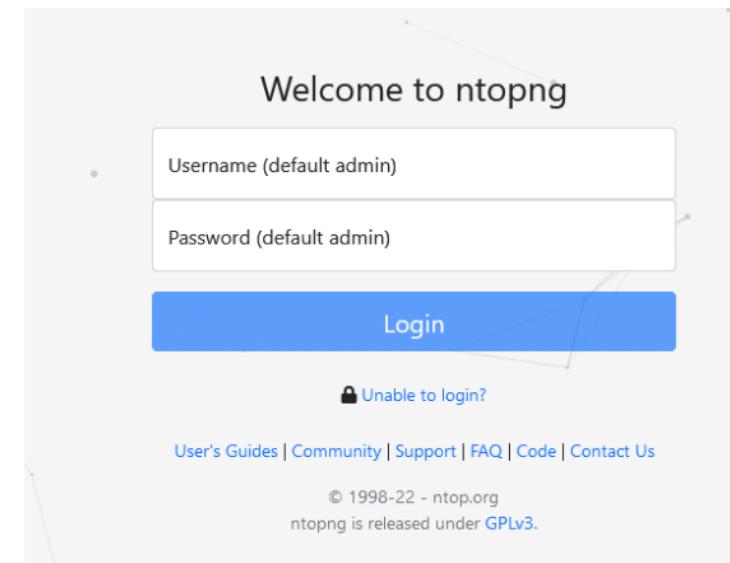
Consignes:

-Monitoring | NtopNG

Pour installer le package, connectez-vous à l'interface web, ouvrez l'onglet **System**, puis sélectionnez **Package Manager**. Recherchez le package **n topng** 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 a 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.

