TP Pfsense / DMZ

HEGO Maxence

Contexte du TP :

Une société souhaite installer un serveur WEB dans son architecture réseau qui doit être accessible depuis Internet. Afin de sécuriser son réseau, l'entreprise fait le choix d'un Firewall Pfsense.

Au cours de ce TP nous verrons comment installer et configurer Pfsense.

DMZ :

Une DMZ (Zone démilitarisé) est un segment de réseau isolé et sécurisé qui sert de zone tampon entre un réseau interne fiable (comme le réseau d'une entreprise) et un réseau externe non fiable (généralement Internet).

Partie 1 – Installation de Pfsense

Installation de Pfsense sur le Proxmox

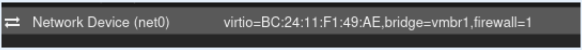
Note :

Pour pouvoir continuer l'installation et la configuration de Pfsense on doit se connecter à l'interface WEB depuis le réseau LAN. Pour ce faire, on va créer une seconde VM que l'on va placer dans le réseau local.

Préparation de la VM :

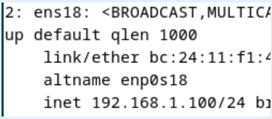
On va utiliser une debian 12 avec interface graphique.

Une fois l'installation terminé on place cette VM dans le réseau local LAN. On choisi donc comme carte réseau dans le proxmox la seconde qui est associé au réseau local.



```
⇄ Network Device (net0)        virtio=BC:24:11:F1:49:AE,bridge=vmbr1,firewall=1
```

La VM obtient une adresse DHCP dans le bon réseau LAN.



```
2: ens18: <BROADCAST,MULTICA
up default qlen 1000
    link/ether bc:24:11:f1:4
    altname enp0s18
    inet 192.168.1.100/24 br
```

Configuration de Pfsense :

Note :

Par défaut :

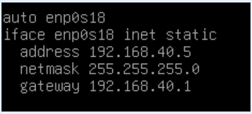
- login : **admin**
- Mdp : **pfsense**

Partie 2 – Serveur LAMP dans la DMZ

Serveur LAMP :

On va maintenant placer un serveur LAMP dans la DMZ. On chosi d'utiliser la troisième interface réseau du proxmox.

On commence par modifier l'addresse IP du serveur LAMP situé dans la DMZ :

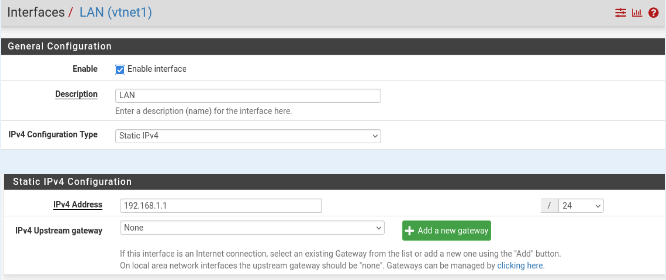


```
auto enp0s18
iface enp0s18 inet static
  address 192.168.40.5
  netmask 255.255.255.0
  gateway 192.168.40.1
```

Configuration des Interfaces :

Configuration des Interfaces : LAN :

On s'assure que l'interface LAN est activé et que l'adresse IP de l'interface LAN du pfsense est bien configuré.



Interfaces / LAN (vtnet1)

General Configuration

Enable: ☑ Enable interface

Description: LAN

Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

Static IPv4 Configuration

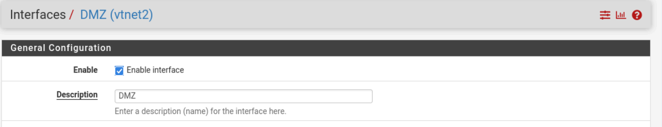
IPv4 Address: 192.168.1.1 / 24

IPv4 Upstream gateway: None

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.

Configuration des Interfaces : DMZ

On configure maintenant l'interface DMZ, pareil que pour l'interface LAN.



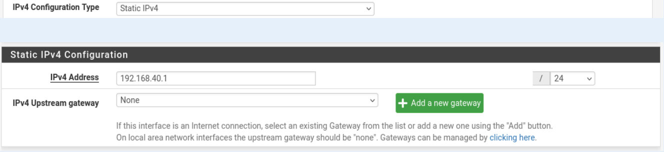
Interfaces / DMZ (vtnet2)

General Configuration

Enable: ☑ Enable interface

Description: DMZ

Enter a description (name) for the interface here.



IPv4 Configuration Type: Static IPv4

Static IPv4 Configuration

IPv4 Address: 192.168.40.1 / 24

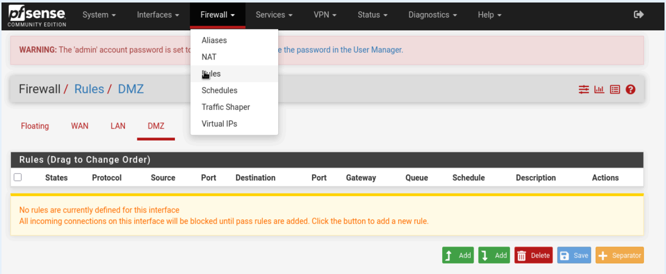
IPv4 Upstream gateway: None

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.

Règles de Pare-Feu :

Firewall DMZ :

Sous Firewall > Rules, on sélectionne DMZ et on ajoute une nouvelle règle :



WARNING: The 'admin' account password is set t… e the password in the User Manager.

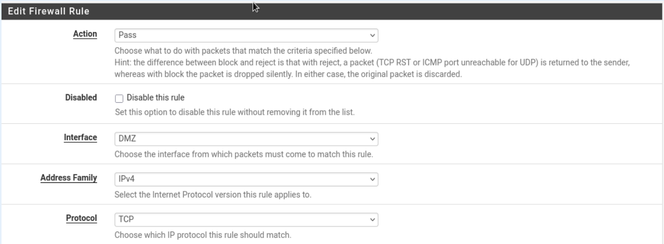
Firewall / Rules / DMZ

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

On configure pour autoriser les connexions http et https vers le serveur LAMP de la DMZ :



Edit Firewall Rule

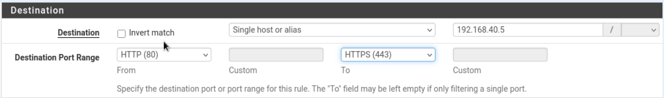
Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: DMZ
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.



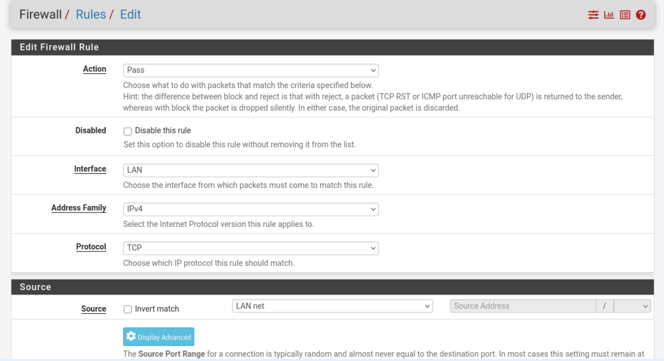
Destination

Destination: ☐ Invert match — Single host or alias — 192.168.40.5 /

Destination Port Range: From: HTTP (80) — Custom: — To: HTTPS (443) — Custom:
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Firewall LAN :

On ajoute également une règle pour le LAN, on autorise les connexions du LAN vers le serveur LAMP de la DMZ.


Firewall / Rules / Edit

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 net | 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


Destination

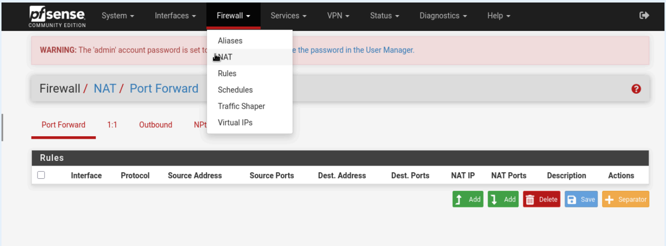
Destination: ☐ Invert match | Single host or alias | 192.168.40.5 /

Destination Port Range: HTTP (80) From | Custom | HTTPS (443) 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.

Port Forwarding :

Port Forward :

Sous firewall > NAT, on ajoute une nouvelle règle.



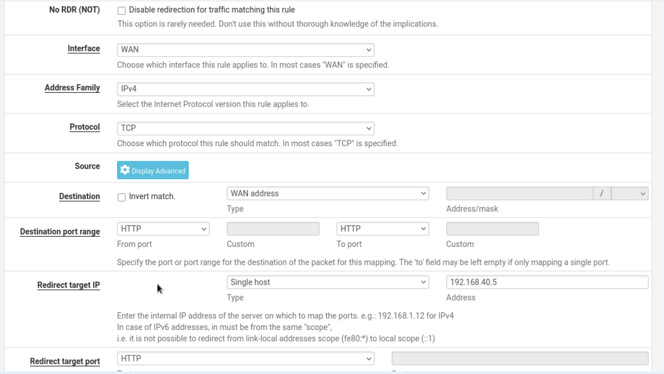
WARNING: The 'admin' account password is set t… e the password in the User Manager.

Firewall / NAT / Port Forward

Rules

☐	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions

On entre comme redirect target IP l'adresse du serveur LAMP :



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

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 Single host (Type) — 192.168.40.5 (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, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

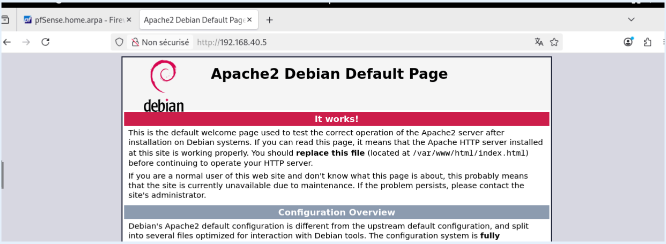
Redirect target port HTTP

♨ **On a terminé les étapes de configurations du pfsense.**

Partie 3 – Tests LAN et WAN

Test LAN :

On essaie de se connecter au serveur LAMP depuis la VM situé dans le réseau LAN. On entre directement l'adresse IP du serveur.



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.

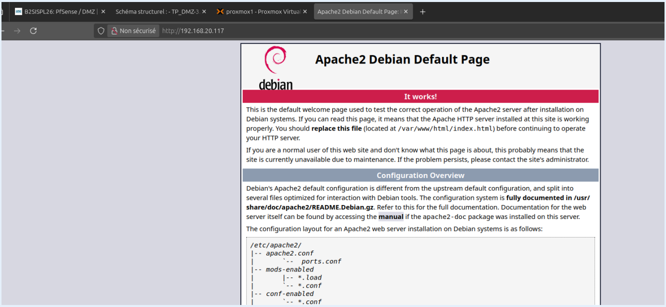
Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully**

On a bien accès depuis le réseau local.

Test WAN :

On veut maintenant vérifier si on a accès au site depuis le réseau WAN. Cette fois çi on entre l'addresse IP public du serveur Pfsense et on vérifie que l'on arrive bien sur la page web du serveur LAMP.



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 into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
```

On est bien redirigé sur le serveur depuis le WAN.

Partie 4 – Monitoring Pfsense

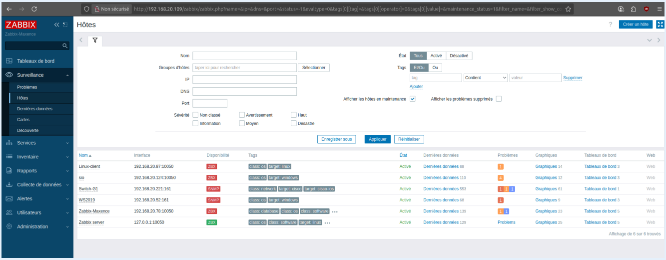
Choix de la solution :

On choisi comme solution Zabbix, en effet Zabbix est une solution gratuite et open source adapté à nos besoins.

Zabbix :

Lors du TP B3 : Supervision Zabbix, j'ai installé un serveur Zabbix qui permet de monitorer les équipements sur un réseau. Pour cela on dispose de deux méthodes, une avec agent Zabbix et une avec le SNMP.

Ci dessous le tableau de supervision de mes différents équipements réseaux :



Afficher les hôtes en maintenance ☑

Afficher les problèmes supprimés ☐

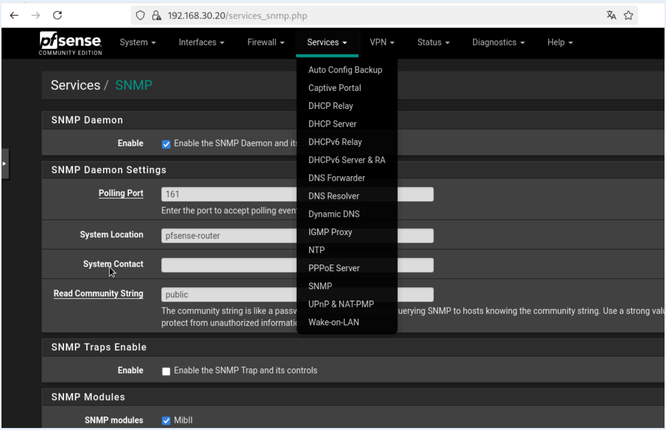
Nom ▲	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
Linux-client	192.168.20.87:10050	ZBX	class: os target: linux	Activé	Dernières données 68	1	Graphiques 14	Tableaux de bord 3	Web
sio	192.168.20.124:10050	ZBX	class: os target: windows	Activé	Dernières données 110	4	Graphiques 12	Tableaux de bord 3	Web
Switch-G1	192.168.20.221:161	SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 553	1 1 1	Graphiques 61	Tableaux de bord 1	Web
WS2019	192.168.20.52:161	SNMP	class: os target: windows	Activé	Dernières données 68	1	Graphiques 9	Tableaux de bord 3	Web
Zabbix-Maxence	192.168.20.78:10050	ZBX	class: database class: os class: software ...	Activé	Dernières données 139	1 1	Graphiques 23	Tableaux de bord 5	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Activé	Dernières données 129	Problems	Graphiques 25	Tableaux de bord 5	Web

Affichage de 6 sur 6 trouvés

SNMP :

On choisi d'utiliser la méthode SNMP.

On va dans services > SNMP et on coche Enable SNMP service.



Services / SNMP

SNMP Daemon

Enable ☑ Enable the SNMP Daemon and its

SNMP Daemon Settings

Polling Port: 161

System Location: pfsense-router

System Contact:

Read Community String: public

SNMP Traps Enable

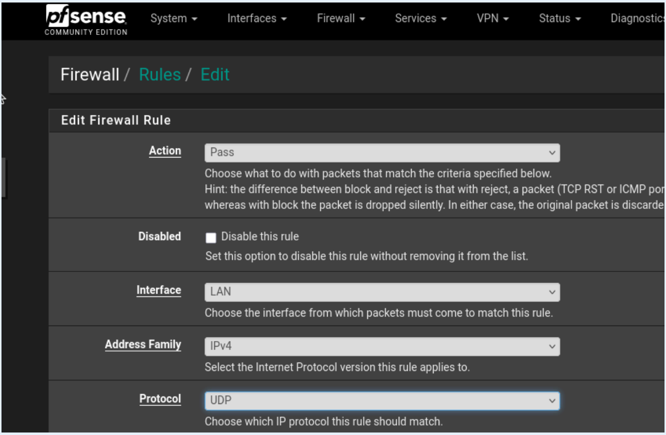
Enable ☐ Enable the SNMP Trap and its controls

SNMP Modules

SNMP modules ☑ MibII

Firewall :

On configure maintenant la règle du pare-feu :



Firewall / Rules / Edit

Edit Firewall Rule

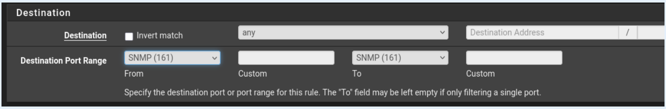
Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP por
whereas with block the packet is dropped silently. In either case, the original packet is discarde

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 UDP
Choose which IP protocol this rule should match.



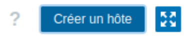
Destination

Destination ☐ Invert match any Destination Address /

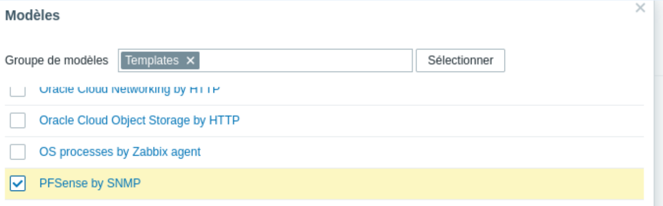
Destination Port Range SNMP (161) From, Custom; SNMP (161) To, Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Configuration dans Zabbix :

On ajoute maintenant le nouvel hôte dans Zabbix :



On sélectionne le template correspondant :



Modèles

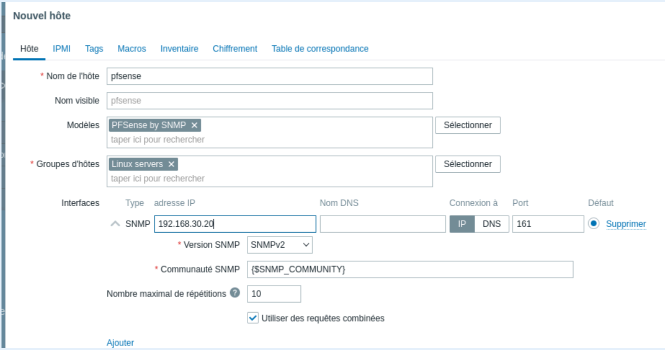
Groupe de modèles Templates ✕ Sélectionner

☐ Oracle Cloud Networking by HTTP
☐ Oracle Cloud Object Storage by HTTP
☐ OS processes by Zabbix agent
☑ PFSense by SNMP

On entre l'IP du pfsense et la communauté défini précédemment :

Hôte

Macro: {$COMMUNITY}
Valeur: public



* Nom de l'hôte: pfsense

Nom visible: pfsense

Modèles: PFSense by SNMP

* Groupes d'hôtes: Linux servers

Interfaces: SNMP — adresse IP: 192.168.30.20 — Connexion à: IP — Port: 161 — Défaut: ●

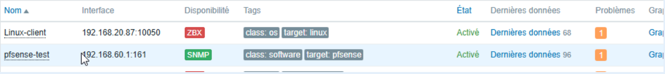
* Version SNMP: SNMPv2

* Communauté SNMP: {$SNMP_COMMUNITY}

Nombre maximal de répétitions: 10

☑ Utiliser des requêtes combinées

Le pfsense est bien monitorer par notre Zabbix :



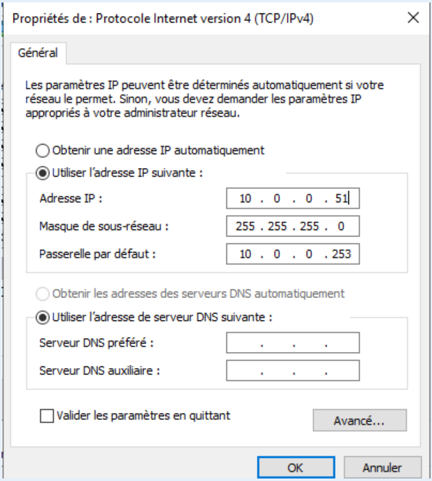
Nom ▲	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Gra
Linux-client	192.168.20.87:10050	ZBX	class: os target: linux	Activé	Dernières données 68	1	Gra
pfsense-test	192.168.60.1:161	SNMP	class: software target: pfsense	Activé	Dernières données 96	1	Gra

---

Partie 5 – Bureau à distance RDP

Configuration Windows server :

On commence par lui donner une adresse IP dans la DMZ. On défini la passerelle comme l'interface DMZ du pfsense :



Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

○ Obtenir une adresse IP automatiquement

● Utiliser l'adresse IP suivante :

Adresse IP : 10 . 0 . 0 . 51

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 10 . 0 . 0 . 253

○ Obtenir les adresses des serveurs DNS automatiquement

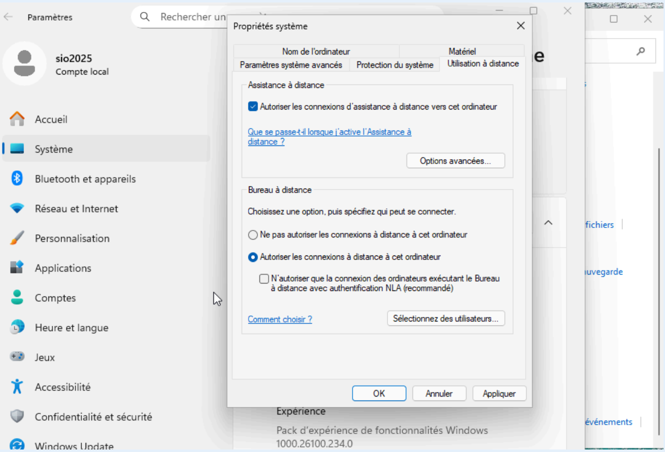
● Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : . . .

Serveur DNS auxiliaire : . . .

☐ Valider les paramètres en quittant

On active ensuite le bureau à distance :



Propriétés système

Nom de l'ordinateur | Matériel | Paramètres système avancés | Protection du système | Utilisation à distance

Assistance à distance

☑ Autoriser les connexions d'assistance à distance vers cet ordinateur

Que se passe-t-il lorsque j'active l'Assistance à distance ?

Bureau à distance

Choisissez une option, puis spécifiez qui peut se connecter.

○ Ne pas autoriser les connexions à distance à cet ordinateur

● Autoriser les connexions à distance à cet ordinateur

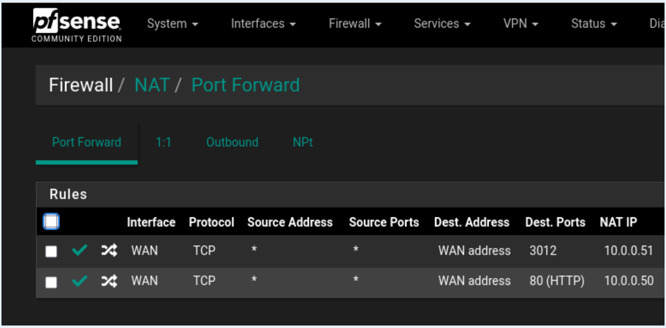
☐ N'autoriser que la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA (recommandé)

Comment choisir ?

🖉 Configuration Pfsense :

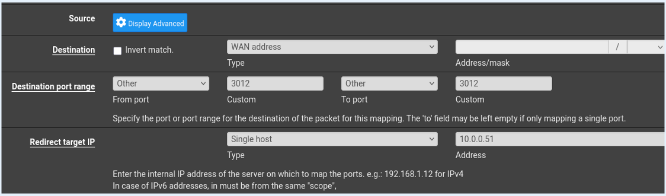
On passe maintenant à la configuration pfsense.

On commence par ajouter une nouvelle règle NAT :



☐			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP
☐	✓	⤮	WAN	TCP	*	*	WAN address	3012	10.0.0.51
☐	✓	⤮	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.50

On défini le port custom pour la connexion puis on renseigne l'IP du Windows server dans redirect target IP :



Source

Destination ☐ Invert match. WAN address (Type) — Address/mask

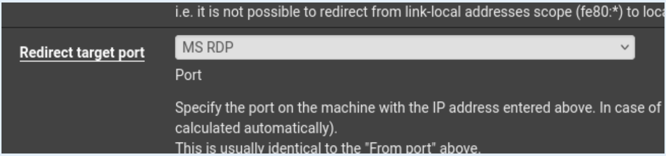
Destination port range Other (From port) — 3012 (Custom) — Other (To port) — 3012 (Custom)

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 Single host (Type) — 10.0.0.51 (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, in must be from the same "scope",

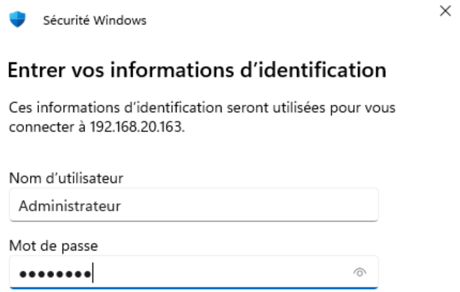
Dans redirect target port on dit que l'on utilise le RDP :


i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to loca

Redirect target port MS RDP (Port)

Specify the port on the machine with the IP address entered above. In case of
calculated automatically).
This is usually identical to the "From port" above.

On peut maintenant essayer de se connecter, cela fonctionne bien, la règle fonctionne :


Sécurité Windows

Entrer vos informations d'identification

Ces informations d'identification seront utilisées pour vous connecter à 192.168.20.163.

Nom d'utilisateur: Administrateur

Mot de passe: ••••••••

☐ Mémoriser mes informations