**Configuration du "Bureau à distance"**

**Étape 1 - Mise en place**

Sur le SERVEUR2, vous avez besoin de trois utilisateurs RD1, RD2 et RD3 qui ont le même mot de passe.

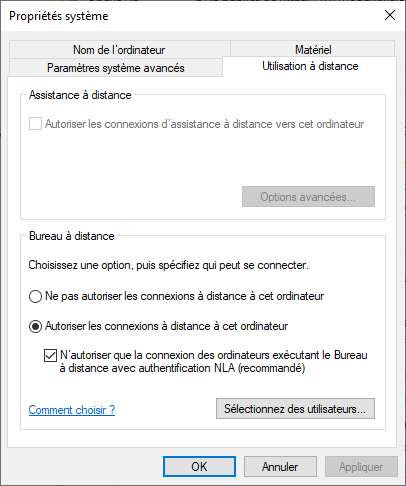
Les utilisateurs RD1, RD2 et RD3 sont dans le groupe Administrateurs.

**Étape 2a - Activation du "Bureau à distance" sur le SERVEUR2**

Ouvrir une session avec "Administrateur" sur le SERVEUR2.

+Pause

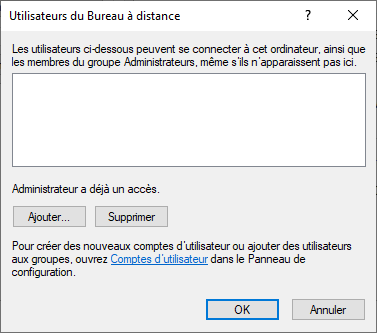
"Paramètres d'utilisation à distance" onglet "**Utilisation à distance**"



Dans la section "**Bureau à distance**"

* activer "Autoriser les connexions à distance à cet ordinateur"
* cocher "N’autoriser que la connexion des ordinateurs … NLA (recommandé)"

Cliquer sur le bouton "**Sélectionnez des utilisateurs...**" et lire les informations



Par défaut, seul les membres du groupe Administrateurs ont accès au "Bureau à distance".

Le bouton "**Ajouter…**" permet d’ajouter des **utilisateurs** et des "**Principaux de sécurité intégrés**".

**note: il n’est pas possible d’ajouter des groupes**

**Étape 2b - Activation du "Bureau à distance" sur le SERVEUR1**

Ouvrir une session avec "Administrateur" sur le SERVEUR1.

Vous devez effectuer la même configuration qu'à l'étape 2a sur le SERVEUR1.

**Configuration du pare-feu dans pfSense**

**Objectifs**

Vous devez configurer le pare-feu du routeur pfSense afin de pouvoir ouvrir une session MSTSC vers vos serveurs virtuels à partir de votre serveur réel.

**Étape 1a - Planification de la configuration du routeur pfSense**

**Voici un résumé de la configuration pour le groupe INTENSIF**

**Voici la configuration du routeur si vous pouvez configurer plusieurs adresses IP du côté WAN.**

**NOTE: c'est le cas du routeur pfSense du cours C43**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Adresse IP**  **WAN** | **Protocole** | **Port local** | **Adresse IP**  **LAN** | **Port distant** |
| **MSTSC1** | 10.57.**yy**.**xx + 100** | TCP | 3389 | 192.168.1.10 | 3389 |
| **MSTSC2** | 10.57.**yy**.**xx + 200** | TCP | 3389 | 192.168.1.20 | 3389 |

* Pour le groupe intensif, la valeur de **yy** est **43**
* Exemple pour l’ordinateur 5 du local C4.08 la valeur de **xx** est **5**
* Exemple pour l’ordinateur 24 du local C4.08 la valeur de **xx** est **24**

**Voici un résumé de la configuration pour le groupe RÉGULIER**

**Voici la configuration du routeur si vous pouvez configurer plusieurs adresses IP du côté WAN.**

**NOTE: c'est le cas du routeur pfSense du cours C43**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Adresse IP**  **WAN** | **Protocole** | **Port local** | **Adresse IP**  **LAN** | **Port distant** |
| **MSTSC1** | 10.57.**yy**.**xx + 100** | TCP | 3389 | 192.168.1.10 | 3389 |
| **MSTSC2** | 10.57.**yy**.**xx + 200** | TCP | 3389 | 192.168.1.20 | 3389 |

* Pour le groupe régulier, la valeur de **yy** est **143**
* Exemple pour l’ordinateur 5 du local A5.37 la valeur de **xx** est **5**
* Exemple pour l’ordinateur 24 du local A5.37 la valeur de **xx** est **24**

**Étape 1b - Informations supplémentaires**

Le site <http://ip4.me> permet d’afficher l’adresse IP du côté WAN de votre routeur.

**Planification de la configuration d’un routeur avec une seule adresse IP du côté WAN**

**Le routeur permet de configurer un port distant et un port local**

**Voici la configuration d’un routeur si vous n'avez qu'une seule adresse IP du côté WAN.**

**C'est le cas de votre routeur à la maison s'il est possible de configurer un port distant et un port local.**

**C'est le cas pour les routeurs de certains fournisseurs internet.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Adresse IP**  **WAN** | **Protocole** | **Port local** | **Adresse IP**  **LAN** | **Port distant** |
| **ORDI1** | Adresse IP de votre fournisseur internet | TCP | 3389 | 192.168.1.10 | 3389 |
| **ORDI2** | Adresse IP de votre fournisseur internet | TCP | 3389 | 192.168.1.20 | 3390 |
| **ORDI3** | Adresse IP de votre fournisseur internet | TCP | 3389 | 192.168.1.30 | 3391 |

**Planification de la configuration d’un routeur avec une seule adresse IP du côté WAN**

**Le routeur permet de configurer un port distant mais pas le port local.**

**Voici la configuration d’un routeur si vous n'avez qu'une seule adresse IP du côté WAN.**

**C'est le cas de votre routeur à la maison s'il n'est pas possible de configurer un port local.**

**C'est le cas pour les routeurs de certains fournisseurs internet.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Adresse IP**  **WAN** | **Protocole** | **Port local** | **Adresse IP**  **LAN** | **Port distant** |
| **ORDI1** | Adresse IP de votre fournisseur internet | TCP | 3389 | 192.168.1.10 | 3389 |
| **ORDI2** | Adresse IP de votre fournisseur internet | TCP | **3390** | 192.168.1.20 | 3390 |
| **ORDI3** | Adresse IP de votre fournisseur internet | TCP | **3391** | 192.168.1.30 | 3391 |

Le port local n'est pas configurable au niveau du routeur, ce qui veut dire qu'il faut modifier le numéro du port dans le registre Windows de chaque ordinateur qui n'utilise pas le port 3389.

**La clé de registre qui modifie le port du protocole RDP pour 3390, 00000d3e est la valeur hexadécimale de 3390.**

Le contenu d'un fichier REG qui modifie le port d'écoute du "Bureau à distance" pour 3390.

**Windows Registry Editor Version 5.00**

**[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]**

**"PortNumber"=dword:00000d3e**

**La clé de registre qui modifie le port du protocole RDP pour 3391, 00000d3f est la valeur hexadécimale de 3391.**

Le contenu d'un fichier REG qui modifie le port d'écoute du "Bureau à distance" pour 3391.

**Windows Registry Editor Version 5.00**

**[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]**

**"PortNumber"=dword:00000d3f**

**Étape 1c - Informations sur le pare-feu Windows**

**Par défaut, le port 3389 est ouvert pour les protocoles TCP et UDP.**



**Étape 1d - PowerShell et le pare-feu Windows**

**$nomTCP = "Bureau à distance — Mode utilisateur (TCP-Entrant)"**

**Get-NetFirewallRule -DisplayName $nomTCP | `**

**Get-NetFirewallPortFilter | Select-Object Protocol,LocalPort**

**Protocol LocalPort**

**-------- ---------**

**TCP 3389**

**$nomUDP = "Bureau à distance — Mode utilisateur (UDP-Entrant)"**

**Get-NetFirewallRule -DisplayName $nomUDP | `**

**Get-NetFirewallPortFilter | Select-Object Protocol,LocalPort**

**Protocol LocalPort**

**-------- ---------**

**UDP 3389**

**Si vous modifiez le numéro du port pour le protocole RDP dans le registre, vous devez ajouter des règles de trafic entrant pour autoriser ce port en TCP et UDP.**

**Voici la commande qui permet de créer une règle de trafic entrant qui ouvre le port 3390 en TCP.**

**New-NetFirewallRule -DisplayName "\_RDP\_TCP\_3390" `**

**-Profile "Private,Public" `**

**-Direction Inbound `**

**-Action Allow `**

**-Protocol TCP `**

**-LocalPort 3390**

**Voici la commande qui permet de créer une règle de trafic entrant qui ouvre le port 3390 en UDP.**

**New-NetFirewallRule -DisplayName "\_RDP\_UDP\_3390" `**

**-Profile "Private,Public" `**

**-Direction Inbound `**

**-Action Allow `**

**-Protocol UDP `**

**-LocalPort 3390**



**$nomTCP = "\_RDP\_TCP\_3390"**

**Get-NetFirewallRule -DisplayName $nomTCP | `**

**Get-NetFirewallPortFilter | Select-Object Protocol,LocalPort**

**Protocol LocalPort**

**-------- ---------**

**TCP 3390**

**$nomUDP = "\_RDP\_UDP\_3390"**

**Get-NetFirewallRule -DisplayName $nomUDP | `**

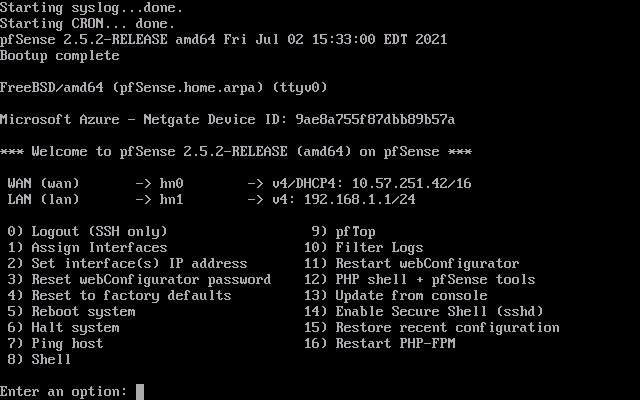
**Get-NetFirewallPortFilter | Select-Object Protocol,LocalPort**

**Protocol LocalPort**

**-------- ---------**

**UDP 3390**

**Étape 2 - Accès à la page web du routeur pfSense**



L'adresse IP du réseau WAN est 10.57.**x**.**y** et permet de configurer le routeur à partir du serveur réel.

L’adresse IP du réseau LAN est 192.168.1.1 et permet de configurer le routeur à partir de vos serveurs virtuels.

Pour accéder à la page de configuration du routeur à partir de votre serveur réel: https://10.57.**x**.**y**

Pour accéder à la page de configuration du routeur à partir de vos serveurs virtuels: https://192.168.1.1

nom d'utilisateur = admin

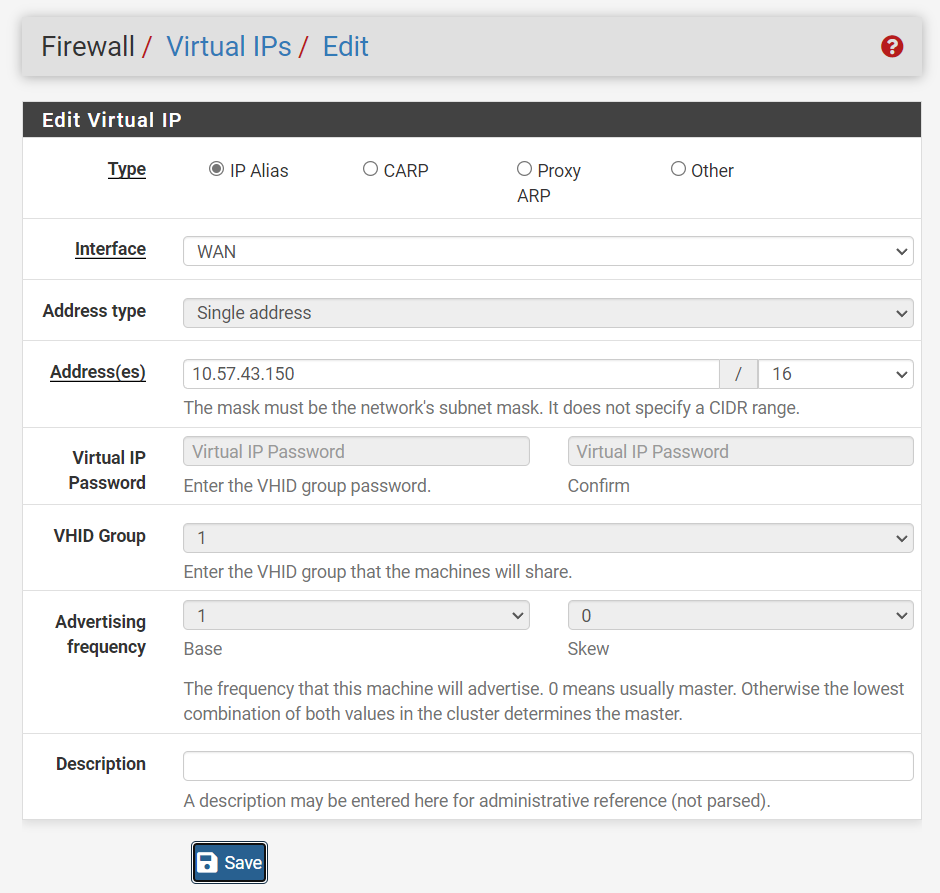
mot de passe = pfsense

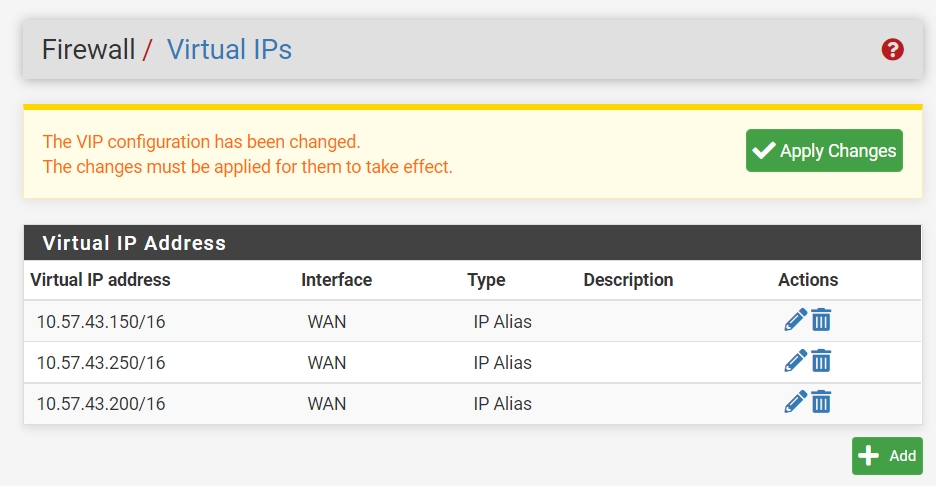
**Étape 3 - Ajout des adresses IP virtuels sur le routeur pfSense**

10.57.**yy**.**xx + 100**

10.57.**yy**.**xx + 200**

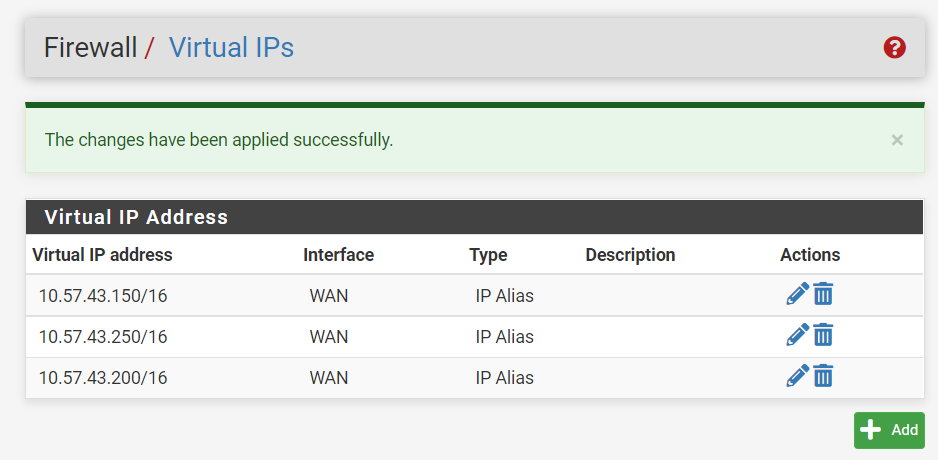
10.57.**yy**.**xx + 150**





Cliquer sur le bouton "**Apply Changes**"

**Voici la configuration finale**



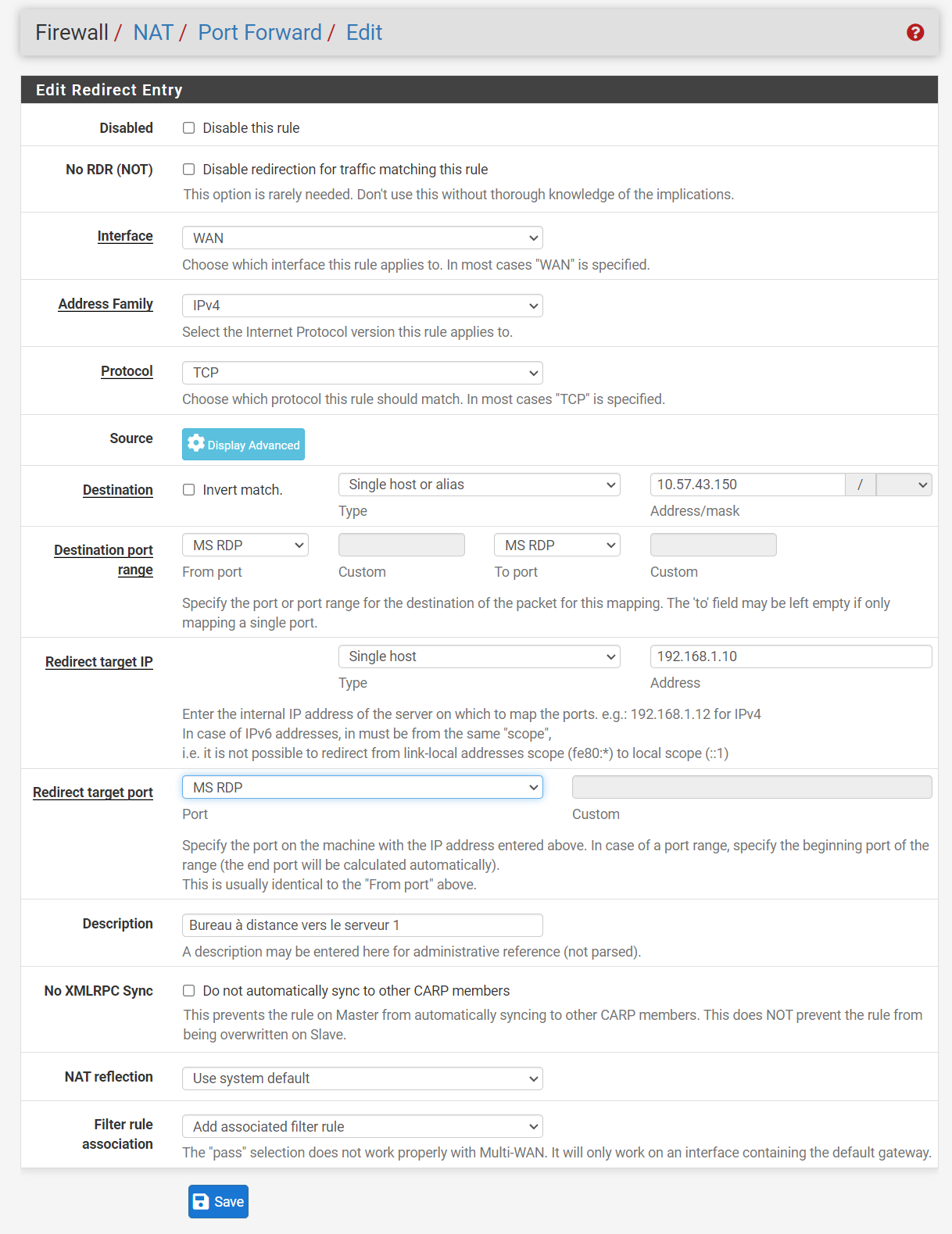
**Étape 4 - Configuration de la redirection des ports sur le routeur pfSense**

**Il faut configurer deux redirections de ports.**

Il faut rediriger le port 3389 de l'adresse IP 10.57.**yy**.**xx + 100** vers le port 3389 de l'adresse IP 192.168.1.10.

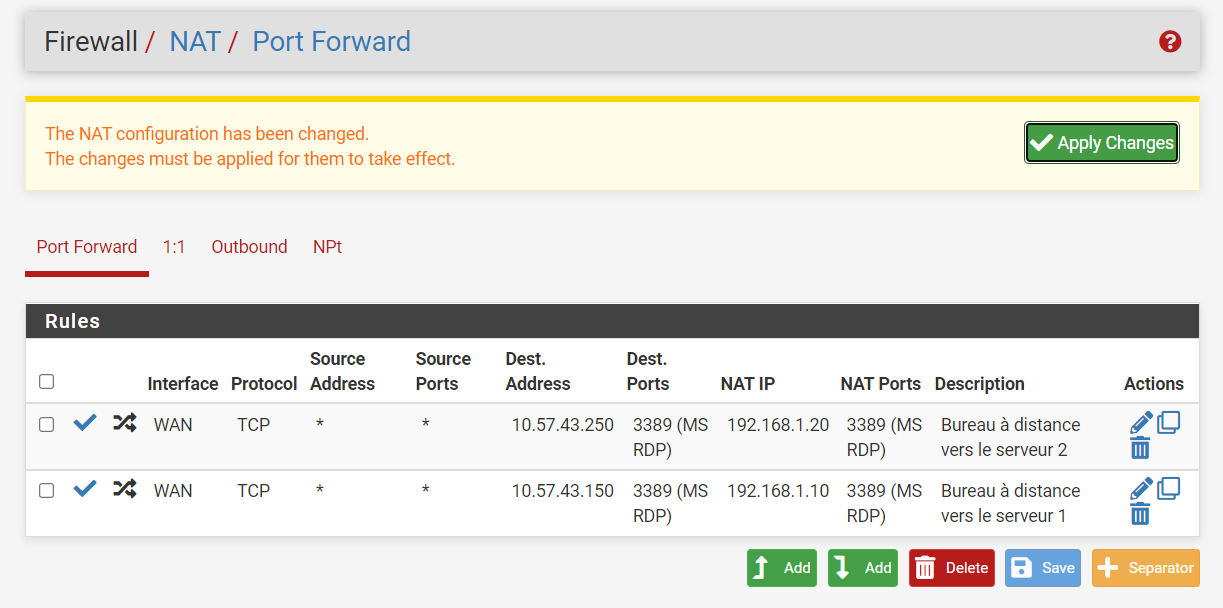
Il faut rediriger le port 3389 de l'adresse IP 10.57.**yy**.**xx + 200** vers le port 3389 de l'adresse IP 192.168.1.20.

**Voici la configuration d'une redirection de port qui utilise "MS RDP".**



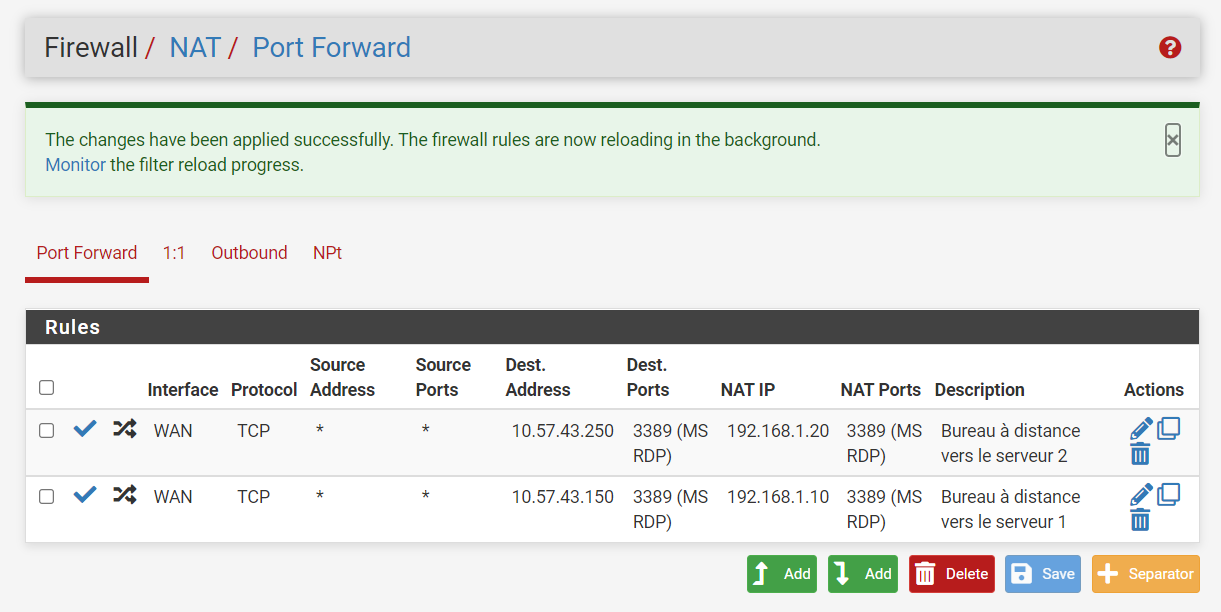
**La capture d’écran affiche seulement la redirection de port pour le protocole "MS RDP".**

**Vous devez conserver les redirections de port pour vos sites Web.**



Cliquer sur le bouton "**Apply Changes**"

**Voici la configuration finale**



**Étape 5 - À partir du serveur réel, tester l'accès aux ports avec PowerShell**

**Test-NetConnection -ComputerName 10.57.yy.xx + 100 -Port 3389**

**Test-NetConnection -ComputerName 10.57.yy.xx + 200 -Port 3389**

**Étape 6 - À partir du serveur réel, tester les accès à distance aux serveurs**

Tester l'accès au "**Bureau à distance**" vers vos serveurs virtuels à partir de votre serveur réel.

10.57.**yy**.**xx + 100** 🡺 SERVEUR1 10.57.**yy**.**xx + 200** 🡺 SERVEUR2

Pour s'authentifier correctement au SERVEUR1. Pour s'authentifier correctement au SERVEUR2.

