TUTOS-INFO
L'informatique par l'exemple

TUTORIEL

Configurer l'accès à DynFi depuis l'extérieur

MODULE 2

DynFi
DYNAMIC FIREWALLS

SOMMAIRE

EXPERT

DIFFICULTE

Note importante :

Nous supposons, ici, que vous avez un serveur Proxmox fonctionnel connecté à Internet avec DynFi 3.0 installé et une machine Debian, avec interface graphique, connectée au réseau "LAN" (voir tutoriel DynFi – Module 1 sur notre site).

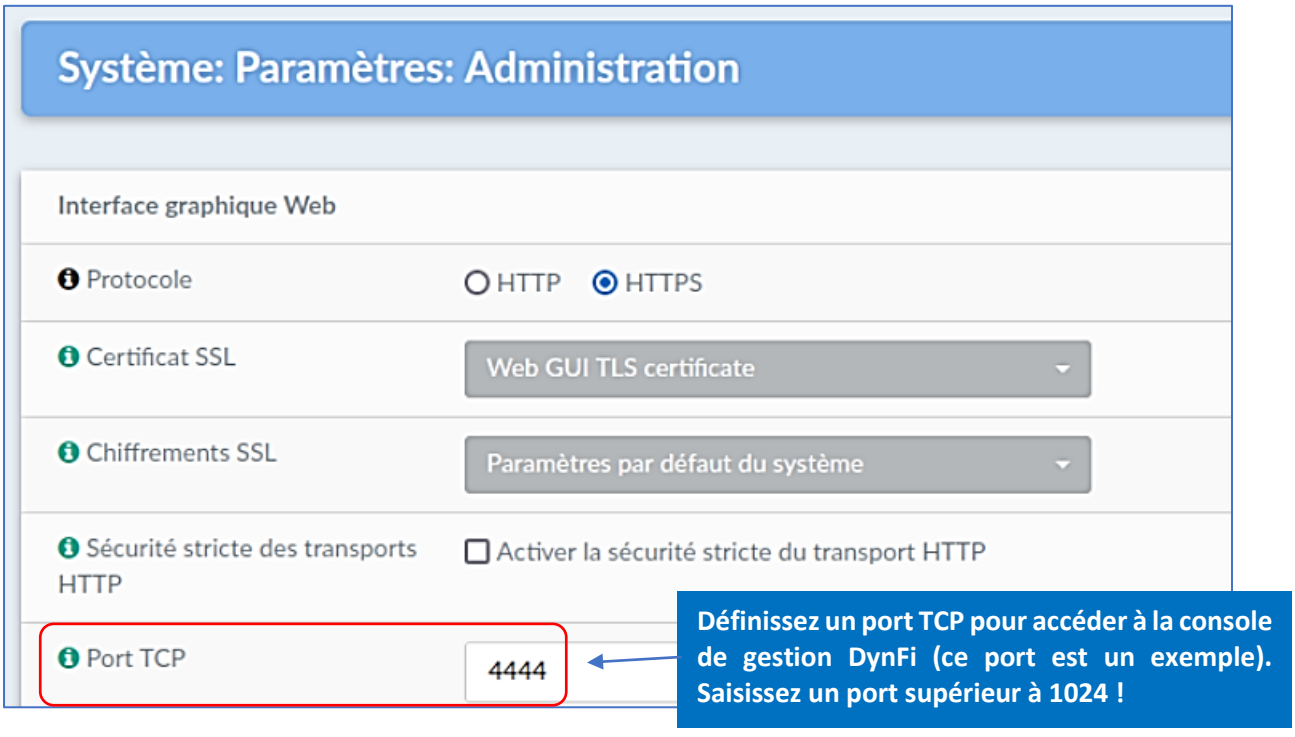
1 – MODIFIER L'URL DE CONNEXION A LA CONSOLE DE GESTION DE DYNFI 3.0

Dans cette partie, nous allons modifier le port TCP de l'adresse URL de DynFi. Par défaut, la console de gestion de DynFi est accessible, depuis l'interface "LAN", via une adresse de type https://ipdynfi (le port TCP "443" est configuré de base).

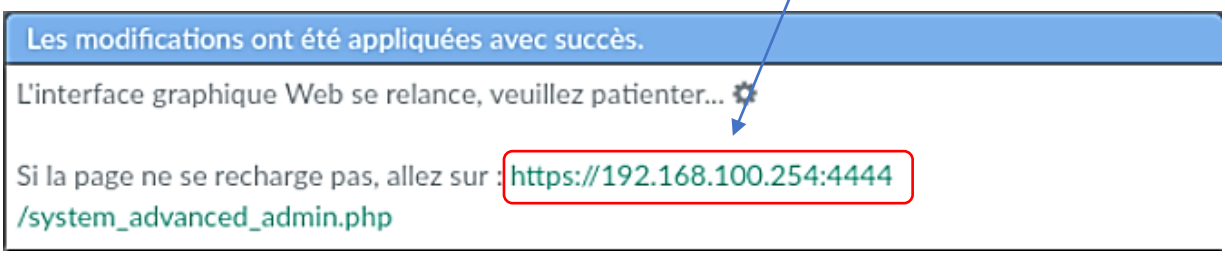
Nous allons utiliser, ici, un **port TCP supérieur à 1024** et qui est un port "libre" sur notre réseau, c'est-à-dire non encore utilisé par un service. En modifiant le port TCP on augmente à minima la sécurité d'accès à la console :

- **Depuis votre machine Debian qui est connectée à votre réseau local** (interface "**LAN**"), connectez-vous à la console de gestion de DynFi 3.0 (voir tutoriel 1). Dans notre cas, nous saisissons l'URL suivante : https://192.168.100.254

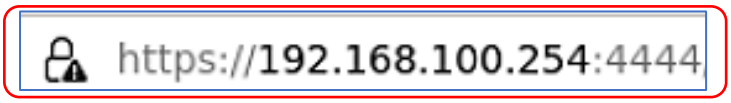
- Une fois sur le tableau de bord DynFi, cliquez "**Système**" – "**Paramètres**" – "**Administration**" ; une fenêtre s'affiche. Ajoutez un port "TCP" (supérieur à 1024 et non utilisé dans votre infra) et cliquez le bouton "**Sauvegarder**" :



- Une fenêtre s'affiche et vous indique que l'adresse URL d'accès à DynFi a été modifiée :



- Reconnectez-vous à la console de gestion de DynFi en saisissant la nouvelle adresse suivie du port TCP configuré (ici "4444") pour vérifier le bon fonctionnement de l'accès sécurisé.



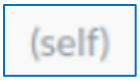
Comme nous pouvons le constater, le changement de port TCP n'a pas affecté l'accès à la console DynFi depuis le réseau local « **LAN** ». Cela est normal car la politique de sécurité de **Dynfi autorise par défaut les flux à l'intérieur du réseau local. Une "règle" de pare-feu a automatiquement été créée qui autorise la connexion.**

Afin de comprendre pourquoi nous pouvons nous connecter à la console DynFi depuis une machine du réseau local, il faut aller dans le menu "**Pare-feu**" – "**Règles**" et cliquer sur l'interface "**LAN**" ; une règle "auto générée" par DynFi est déjà présente. **Cette règle laisse passer les flux "80" (http) et "443" (https) :**

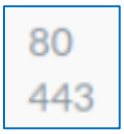
Compréhension de la règle de pare-feu :

 on autorise (flèche verte)

 le trafic entrant sur l'interface (LAN ici)



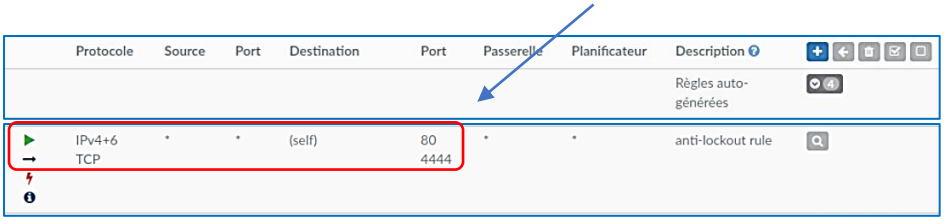
vers nous-mêmes ("self", c'est-à-dire le routeur DynFi)



on "ouvre" les ports autorisés (80/http et 443/https)

Cette règle stipule donc que les flux entrants sur le réseau "**LAN**" de type TCP/80 (http) et TCP/443 (https) sont autorisés à passer vers la machine désignée (ici "self" signifie pare-feu ou machine locale donc DynFi).

La règle a été automatiquement créée par DynFi à l'installation. En changeant le port TCP par le 4444 comme vu précédemment, on peut s'interroger sur le fait que l'accès se fasse toujours depuis le réseau local alors que seuls les ports 80 et 443 ont été ouverts à la base. La raison est qu'en modifiant la configuration d'accès par défaut, DynFi a automatiquement modifié la règle de pare-feu de l'interface "LAN" :



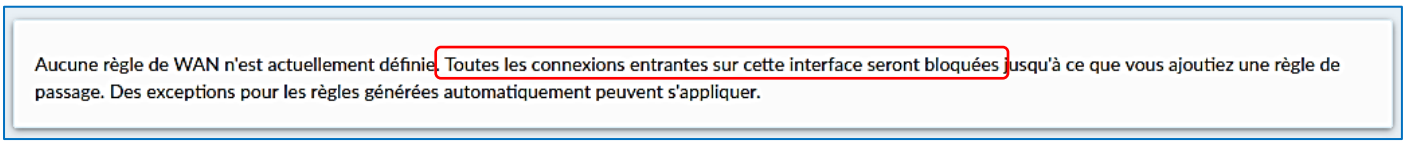
2 – CREATION D'UNE REGLE "DNAT" DANS LE PARE-FEU DYNFI POUR AUTORISER L'ACCES A LA CONSOLE DE GESTION DEPUIS L'INTERFACE "WAN"

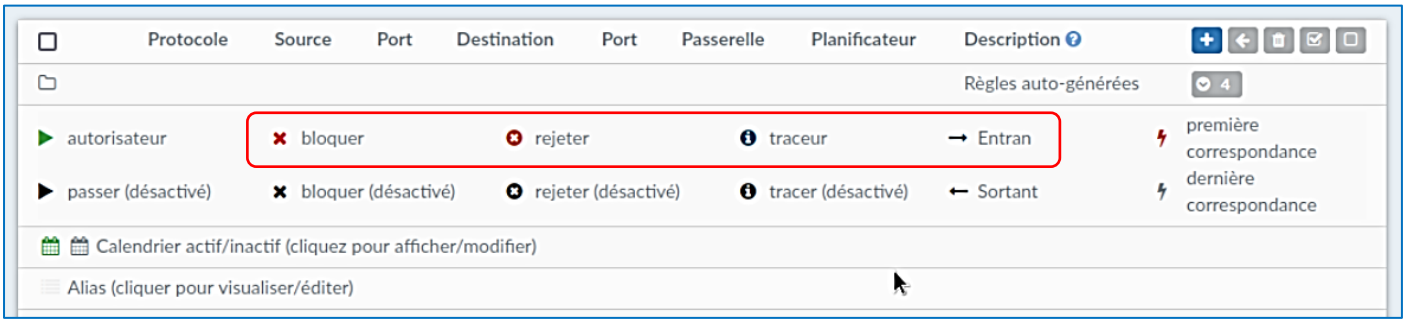
En ce qui concerne les flux entrants depuis l'interface "WAN" la politique de sécurité de DynFi est complètement différente. **En effet, par défaut, tout le trafic entrant par la "WAN" est, par défaut, interdit**.

Cela signifie que si l'on souhaite accéder à la console de gestion de Dynfi depuis l'extérieur il faudra créer une règle spécifique.

Pour comprendre ce blocage des flux entrants sur la WAN, effectuez les manipulations suivantes :

- Cliquez "**Pare-feu**" – "**Règles**" – "**WAN**" ; un écran s'affiche :

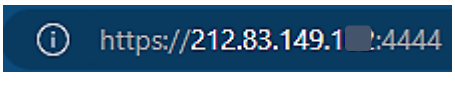




On constate **qu'aucun trafic entrant via l'interface "WAN" n'est autorisé** :

Pour accéder à la console de gestion de DynFi depuis l'extérieur**, il sera donc nécessaire de créer une règle dite "DNAT" dans le pare-feu au niveau du trafic entrant** sur l'interface « **WAN** ». **Cette règle DNAT permettra de rediriger le trafic entrant sur la « WAN » vers une machine spécifique du réseau local** (en l'occurrence notre routeur Dynfi) et on autorisera le port TCP 4444 que l'on vient de modifier).

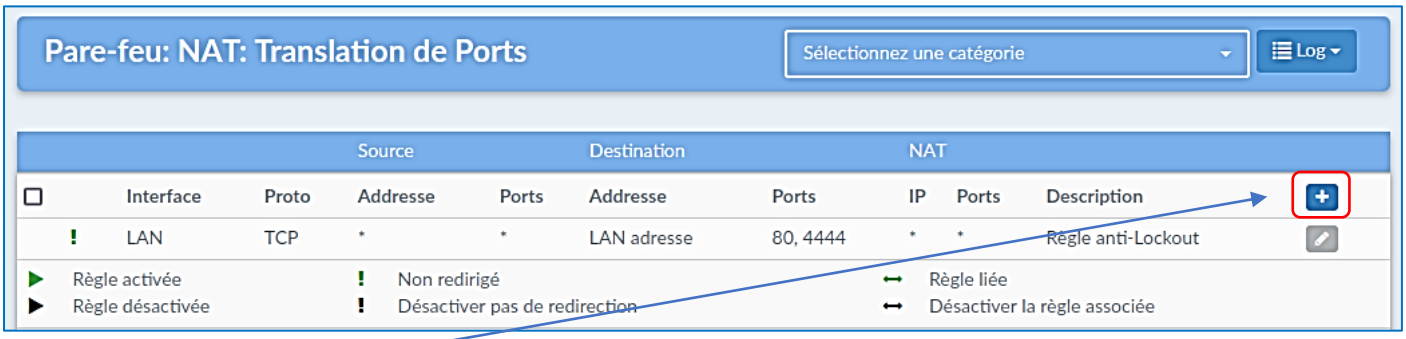
Pour vous rendre compte du blocage, il suffit de saisir, depuis une machine qui n'est pas connectée au réseau "LAN" virtuel, (par exemple votre PC personnel), l'adresse WAN du routeur DynFi suivie du port 4444 ; vous constaterez que l'accès à la console est impossible (le pare-feu bloque les flux entrants par l'interface WAN) :

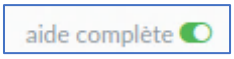


Par défaut, le trafic entrant sur l'interface "WAN" est bloqué. Il n'est pas possible de se connecter à la console de gestion de DynFi depuis l'extérieur tant qu'une règle autorisant le flux n'a pas été configurée sur l'interface WAN du routeur.

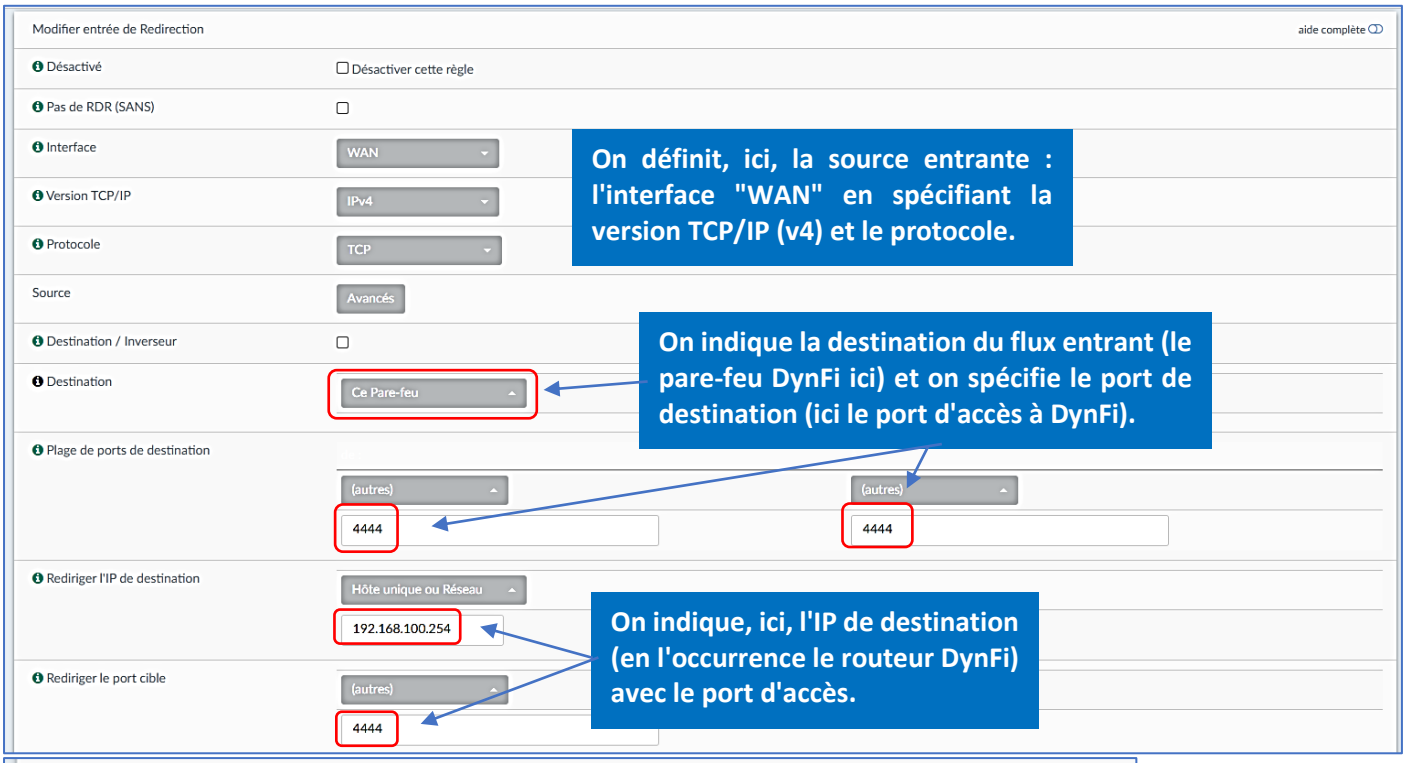
Pour remédier au problème, **il est nécessaire de créer une règle dite "DNAT"** dans le pare-feu. **Une règle "DNAT" (Destination Nat)** est une règle permettant de **rediriger les flux entrants sur une interface (la WAN ici) vers une machine spécifique du réseau local LAN**.
La création de la règle DNAT, permettant d'autoriser l'accès à la console de gestion de DynFi depuis l'interface WAN, s'effectue de la manière suivante :

- Cliquez "**Pare-feu**" – "**Règles**" – "**Translation de ports**" ; une fenêtre s'affiche et on peut comprendre que seuls les flux LAN sont autorisés pour les ports 80 et 4444 :



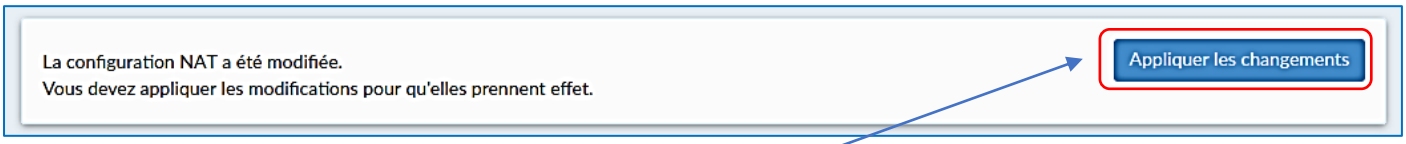
- Cliquez le petit "**+**" sur fond bleu en haut à droite ; une nouvelle fenêtre s'affiche et vous pouvez activer l'aide complète en déplaçant le curseur "aide complète" 

- Le paramétrage de la règle DNAT se présente ainsi :



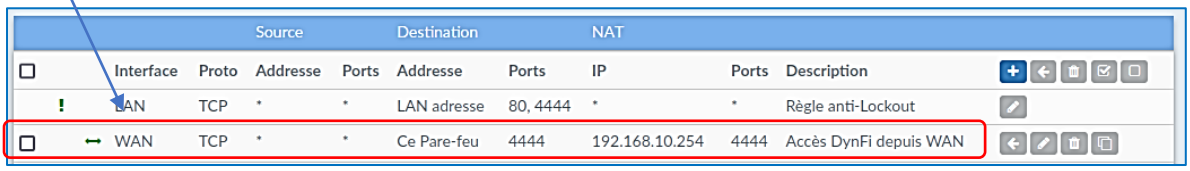
Une fois la règle paramétrée, on la sauvegarde en cliquant le bouton "**Sauvegarde**" :

Une fenêtre affiche le message suivant (modification détectée) :



- Cliquez le bouton "**Appliquer les changements**"

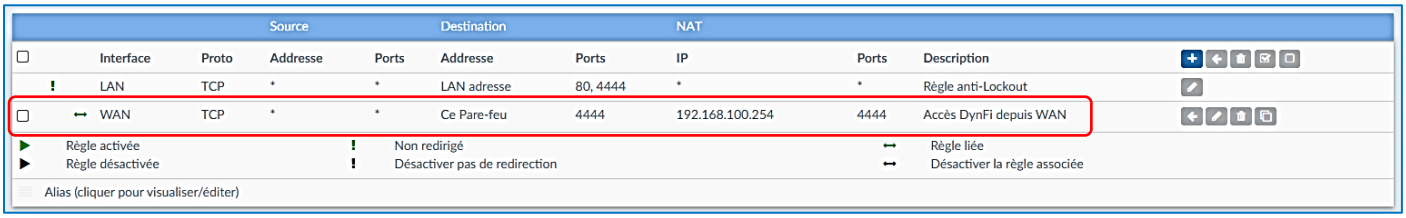
La règle DNAT créée s'affiche :



		Source		Destination		NAT		
Interface	Proto	Addresse	Ports	Addresse	Ports	IP	Ports	Description
LAN	TCP	*	*	LAN adresse	80, 4444	*	*	Règle anti-Lockout
WAN	TCP	*	*	Ce Pare-feu	4444	192.168.10.254	4444	Accès DynFi depuis WAN

La règle DNAT créée peut s'expliquer ainsi :

- Tous les flux TCP avec le port "4444" qui arrivent sur l'interface WAN sont autorisés à destination de la machine locale ayant l'IP 192.168.100.254 (le routeur DynFi) :



		Source		Destination		NAT		
Interface	Proto	Addresse	Ports	Addresse	Ports	IP	Ports	Description
LAN	TCP	*	*	LAN adresse	80, 4444	*	*	Règle anti-Lockout
WAN	TCP	*	*	Ce Pare-feu	4444	192.168.100.254	4444	Accès DynFi depuis WAN

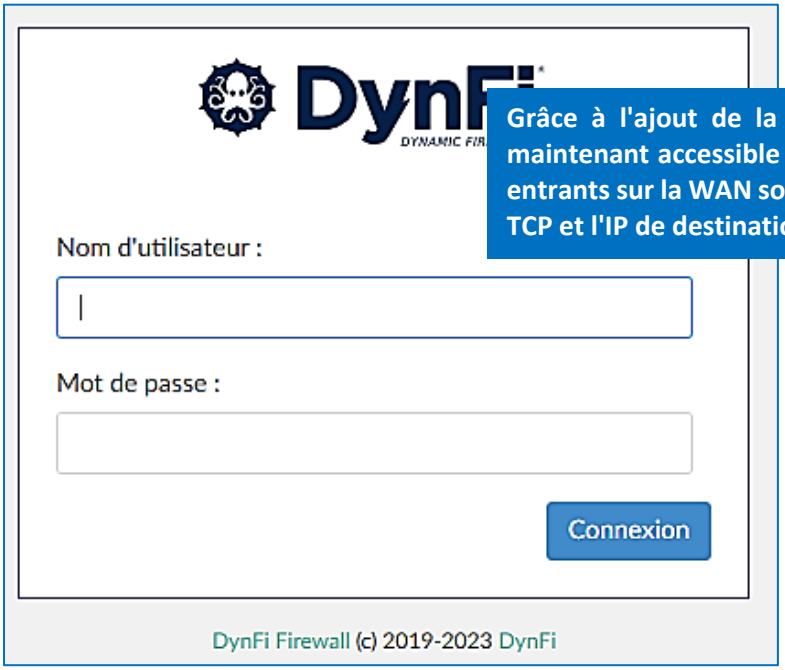
Règle activée — Non redirigé — Règle liée
Règle désactivée — Désactiver pas de redirection — Désactiver la règle associée
Alias (cliquer pour visualiser/éditer)

Attention, si vous travaillez à votre domicile (derrière une box) et que vous souhaitez tester l'accès à DynFi depuis une machine extérieure (c'est-à-dire non connectée à l'interface LAN de DynFi) il faudra ouvrir le port 4444 dans votre box et le faire pointer vers l'IP WAN de votre routeur DynFi (nous ne pouvons pas expliquer cette manipulation car les box sont toutes différentes).

Dans notre cas, notre serveur est externalisé et nous possédons une adresse IP Failover. Pour que l'on puisse se connecter via l'interface WAN à la console de gestion de DynFi, nous procédons ainsi :

- Ouvrez un navigateur web
- Saisissez l'IP WAN de DynFi (ou la Failover si vous avez un serveur externalisé) suivie du port 4444

La fenêtre de connexion à la console de gestion de DynFi s'affiche :



Nous étudierons, dans un autre tutoriel, les notions de règles DNAT (ouverture et redirection de port SSH et http).