



**MODULE 2**

**CONFIGURER L'ACCES  
A LA CONSOLE pfSENSE  
DEPUIS LE WEB**

# SOMMAIRE

1. MODIFIER LE PORT D'ACCES DE LA CONSOLE
2. CREATION D'UNE REGLE DNAT DANS LE PARE-FEU DE PFSENSE (redirection de port)

© [tutos-info.fr](https://tutos-info.fr) - 02/2024



DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

# 1 – MODIFIER LE PORT D'ACCES DE LA CONSOLE

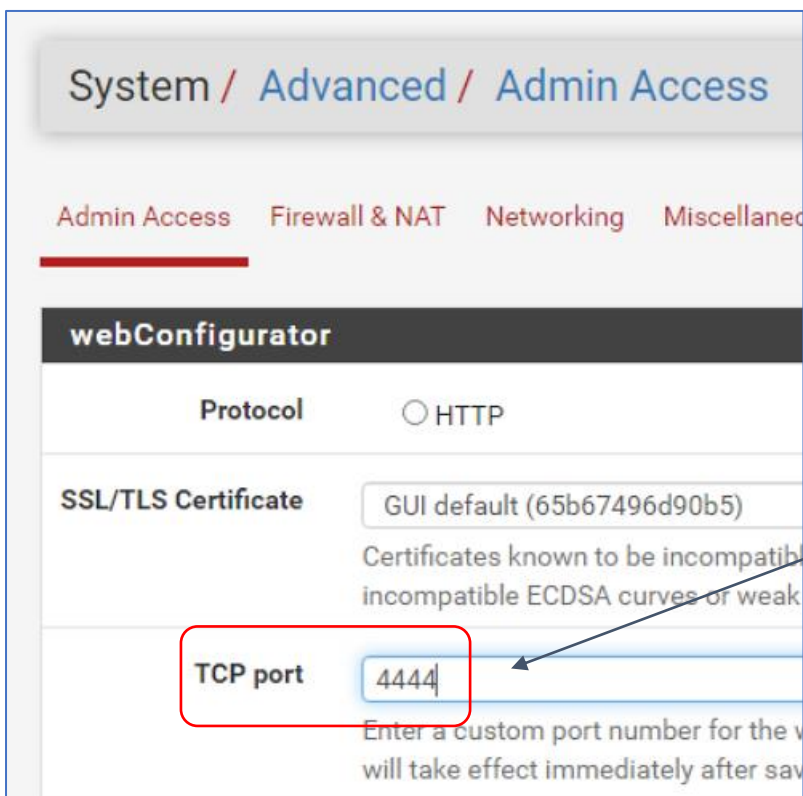
Pour accéder à la console d'administration de pfSENSE via le réseau local (« LAN ») il suffit de lancer un navigateur et de saisir, dans la barre d'adresses, [https://ip\\_pfsense](https://ip_pfsense)

Il est possible d'accéder à pfSENSE depuis un ordinateur connecté à l'Internet mais il est vivement déconseillé de laisser le port TCP n° 443 (HTTPS) par défaut (connu des administrateurs systèmes).

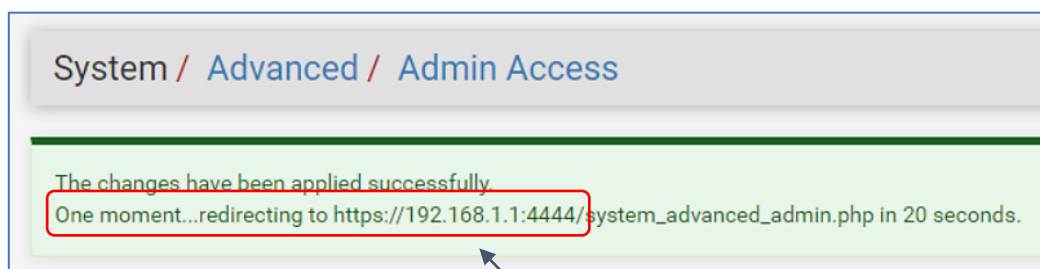
Dans ce tutoriel, nous allons modifier le port par défaut et créer une règle dans le pare-feu de pfSENSE qui nous autorisera à nous connecter depuis l'extérieur. Nous utiliserons, ici, un sous-domaine mais vous pouvez effectuer la manipulation avec l'adresse IP publique de votre routeur si cette dernière est fixe.

La modification du port s'effectue ainsi :

- Connectez-vous, depuis une machine du réseau local, en tant qu'administrateur sur pfSENSE
- Cliquez le menu « **System** » - « **Advanced** »
- Saisissez, dans la rubrique « **TCP port** » le numéro de port TCP souhaité (ici nous avons indiqué 4444) :



- Cliquez le bouton « **Save** » dans le bas de la fenêtre et patientez le temps du rechargement de la page :



La nouvelle URL est enregistrée et s'affiche :

<https://192.168.1.1:4444/>

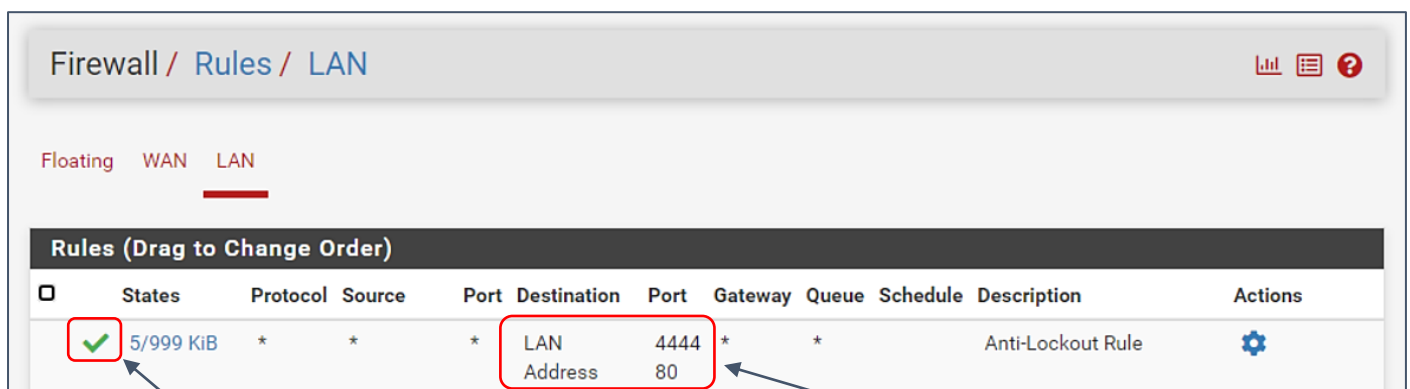
## 2 – CREATION D'UNE REGLE « DNAT » DANS LE PARE-FEU pfSENSE

Comme nous pouvons le constater, le changement de port n'a pas affecté l'accès à la console depuis le réseau local « LAN ». Cela est normal car pfSENSE autorise par défaut les flux à l'intérieur du réseau local. **Il est donc possible de se connecter depuis le réseau local sans procédure particulière** au niveau du pare-feu.

Pour accéder à votre console pfSENSE depuis l'extérieur, **il sera nécessaire de créer une règle NAT dans le pare-feu au niveau du trafic entrant** sur la « WAN ». **Cette règle DNAT permettra de rediriger le trafic entrant sur la « WAN » vers une machine spécifique du réseau local** (notre pfSENSE avec le port 4444).

En effet, **pfSENSE bloque**, par défaut, **tous les flux entrants** sur l'interface « WAN ».

- Cliquez sur le menu « Firewall » - « Rules »
- Cliquez sur l'interface « LAN » ; on constate que la règle est déjà présente et laisse passer le flux en provenance du réseau local vers l'interface pfSENSE avec le port 4444 :



Firewall / Rules / LAN

Floating WAN LAN

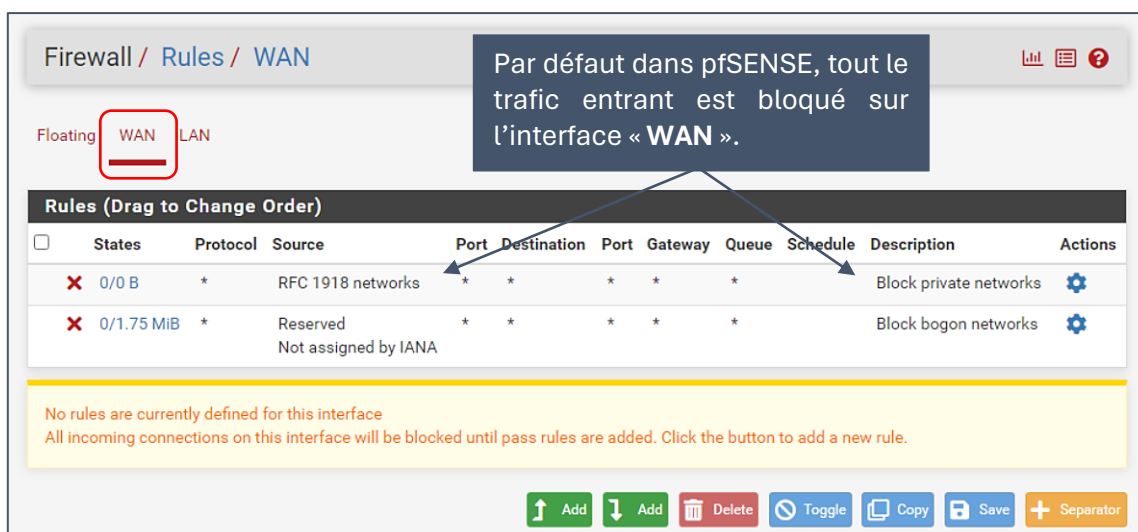
Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 5/999 KiB	*	*	*	LAN Address	4444 80	*	*		Anti-Lockout Rule	

L'encoche verte  indique que **le flux est autorisé** (mode « pass ») au sein du « LAN » vers le port 4444

- Cliquez sur le menu « Firewall » - « Rules »
- Cliquez sur l'interface « WAN »

On constate que l'interface « WAN » ne possède aucune règle de trafic entrant. Par défaut, **pfSENSE n'autorise aucun trafic entrant sur l'interface « WAN »** :



Firewall / Rules / WAN

Floating WAN LAN

Par défaut dans pfSENSE, tout le trafic entrant est bloqué sur l'interface « WAN ».

Rules (Drag to Change Order)

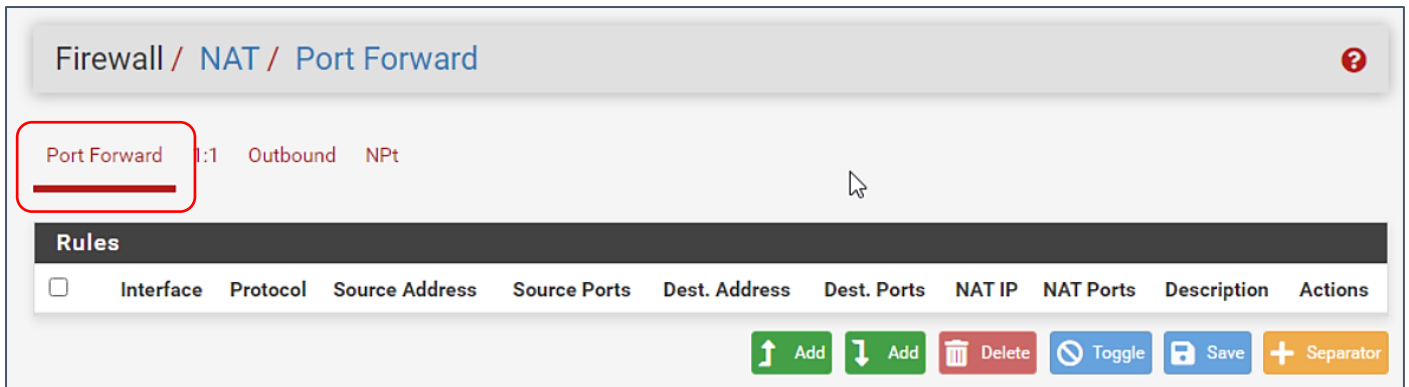
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/0 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
<input checked="" type="checkbox"/> 0/1.75 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	

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.

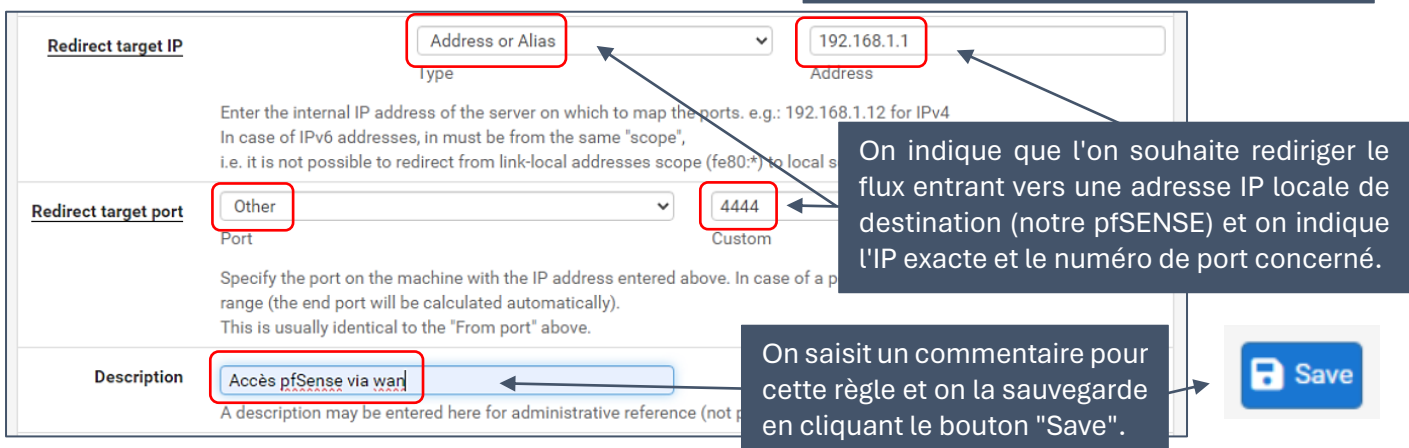
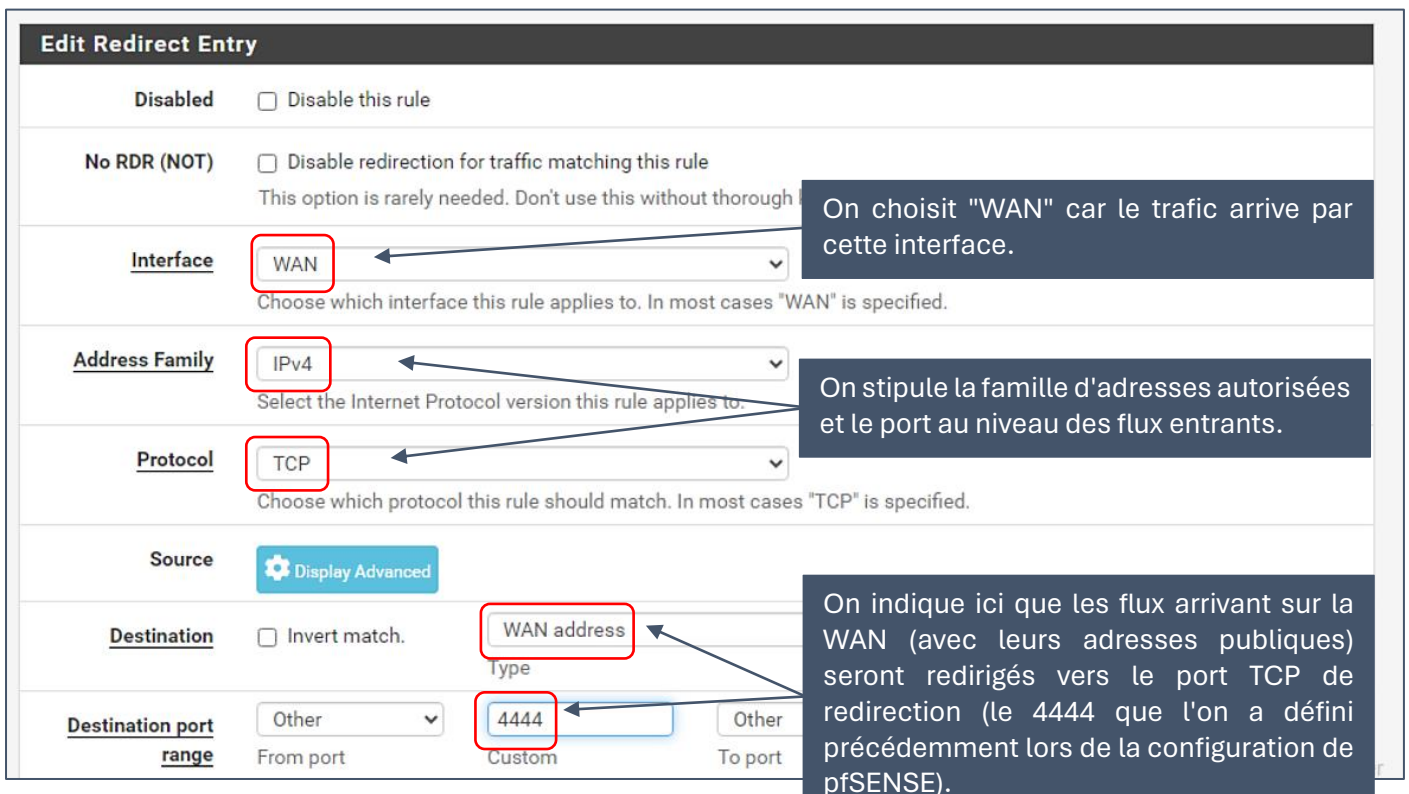
Add Add Delete Toggle Copy Save Separator

La création de la règle DNAT s'effectue ainsi :

- Cliquez le menu « **Firewall** » - « **NAT** »
- Cliquez sur « **Port forward** » :



- Cliquez le bouton vert « **Add** » dans le bas de la fenêtre et saisissez la règle DNAT suivante :



Une fois la règle DNAT créée, il faut l'appliquer en cliquant le bouton vert "Apply Changes" :

Firewall / NAT / Port Forward

The NAT configuration has been changed.  
The changes must be applied for them to take effect.

Apply Changes

Port Forward 1:1 Outbound NPT

Rules										
<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	4444	192.168.1.1	4444	Accès pfSense via wan	

↑ Add ↓ Add Delete Toggle Save + Separator

La règle DNAT s'affiche au niveau de l'interface "WAN" :

Firewall / Rules / WAN

Floating **WAN** LAN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/1.80 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.1.1	4444	*	none		NAT Accès pfSense via wan	

↑ Add ↓ Add Delete Toggle Copy Save + Separator

Il ne reste plus qu'à tester l'accès via un navigateur web en saisissant votre IP WAN suivie du numéro de port. Pour nous, cela donne [https://ip\\_wan:4444](https://ip_wan:4444). Le navigateur affichera le message d'alerte pour le certificat auto-signé envoyé par pfSENSE ; il suffira de valider l'exception pour accéder à la console d'identification :

**Votre connexion n'est pas privée**


Les utilisateurs malveillants essaient peut-être de voler vos informations de pfsense.sio-ndlp.fr (par exemple, les mots de passe, les messages ou les cartes de crédit).

NET-ERR\_CERT\_AUTHORITY\_INVALID

Avancé Retour

Validez, ici, l'exception dans votre navigateur (certificat auto-signé) pour accéder à la console de pfSENSE.

Vous avez maintenant accès à votre pfSENSE à distance. Pensez à sécuriser votre mot de passe !



SIGN IN

*Username*

---

*Password*

---

SIGN IN