



**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 - 02/2024

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, <u>https://ip\_pfsense</u>

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) :

System / Adva	anced / Admin Access	
Admin Access Firewa	all & NAT Networking Miscellaned	
webConfigurator		
Protocol	ОНТТР	
SSL/TLS Certificate	GUI default (65b67496d90b5) Certificates known to be incompatibl incompatible ECDSA curves of weak	Indiquez, ici, le numéro du port TCP souhaité pour l'accès à la console de votre pfSENSE.
TCP port	4444 Enter a custom port number for the v will take effect immediately after sav	

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



© TUTOS-INFO.FR – CONFIGURER L'ACCES A PFSENSE DEPUIS L'EXTERIEUR

#### 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 » Cette règle DNAT permettra de rediriger le 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 :

Fire	ewall / Ru	les / L/	AN								Lill 🔚 🕄
Floatir	ng WAN L/	AN									
Rule	es (Drag to (	Change O	order)								
0	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	States 5/999 KiB	Protocol *	source	Port *	Destination LAN Address	<b>Port</b> 4444 80	Gateway	Queue *	Schedule	Description Anti-Lockout Rule	Actions

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, <u>pfSENSE n'autorise</u> aucun trafic entrant sur l'interface « WAN » :

ating	WAN	N N	AN	l	Par défa trafic e l'interfa	nut o entra ce «	lans p ant es WAN	fSEN st bl ».	SE, toı oqué	ut le 🔟 sur	■ 8
ules (	Drag to C	hange (	Order)		/	/					
Sta	ates	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<b>X</b> 0,	/0 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	\$
<b>X</b> 0,	/1.75 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	\$

La création de la règle DNAT s'effectue ainsi :

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

Firewall / NAT / Port Forward		0
Port Forward I:1 Outbound NPt Rules	Ş	
Interface Protocol Source Address Sou	rce Ports Dest. Address Dest. Po	rts NAT IP NAT Ports Description Actions
	Add 🕽 Add	dd 🛅 Delete 🚫 Toggle 🖬 Save 🕂 Separator

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

Edit Redirect E	intry
Disabled	Disable this rule
No RDR (NOT)	<ul> <li>Disable redirection for traffic matching this rule</li> <li>This option is rarely needed. Don't use this without thorough</li> <li>On choisit "WAN" car le trafic arrive par</li> </ul>
Interface	Cette interface.
Address Family	Select the Internet Protocol version this rule applies to. On stipule la famille d'adresses autorisées et le port au piveau des flux entrants
Protoco	TCP Choose which protocol this rule should match. In most cases "TCP" is specified.
Source	Display Advanced
Destination	On indique ici que les flux arrivant sur la WAN address Type WAN address Type WAN (avec leurs adresses publiques) seront redirigés vers le port TCP de
Destination por range	Other       Other       redirection (le 4444 que l'on a défini précédemment lors de la configuration de pfSENSE).
Redirect target IP	Address or Alias
Redirect target port	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.*) o local s Other Port Specify the port on the machine with the IP address entered above. In case of a p
Description	Accès <u>pfSense</u> via ward A description may be entered here for administrative reference (not p

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

Firewall	/ NAT	/ Port	Forwar	d						0
The NAT cor The changes	nfiguration s must be a	has been o applied for	changed. them to take	effect.					Apply	Changes
Port Forward	1:1 0	utbound	NPt							
Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□ ✓ ≭	WAN	TCP	*	*	WAN	4444	192.168.1.1	4444	Accès pfSense via	Ø 🗋
					address				wan	Î

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

F	irev	wall / F	Rules / \	WAN								iii 🗐 😧
Fl	pating	WAN	LAN									
F	ules	: (Drag to	o Change	Order)								
D		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	×	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	\$
	×	0/1.80 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	٥
	~	0/0 B	IPv4 TCP	*	×	192.168.1.1	4444	*	none		NAT Accès pfSense via wan	₺∥©© 1
						t	Add	l Add	🔲 Delet	e 🛇 Tog	ggle 🚺 Copy 🕞 Save	e + 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 <u>https://ip\_wan:4444</u> Le navigateur affichera le message d'alerte pour le certificat autosigné 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 (par exemple, les mots de passe, les messages ou les cartes de crédit).	pfsense.sio-ndlp.fr
Avancé	Retour

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



#### SIGN IN

Username

Password

SIGN IN

© TUTOS-INFO.FR – CONFIGURER L'ACCES A PFSENSE DEPUIS L'EXTERIEUR