

Configuration Translation de port

Présentation

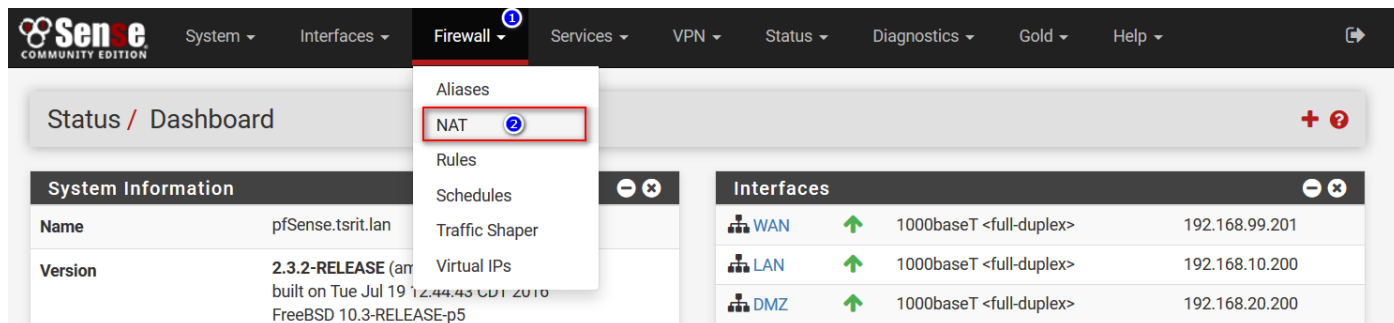
Nous allons mettre en place le « **Port Forwardings** » sous pfsense. Le cas d'utilisation le plus courant du port Forwarding étant le fait de mettre un serveur web (ou autre) dans le côté LAN ou DMZ d'un routeur Pfsense. On souhaite alors que les flux venant du WAN sur le port 80 ou 443 par exemple soient redirigés vers notre serveur web en interne. Le port forwarding se distingue de la redirection 1 à 1 (ou 1" to 1") car cette dernière redirige tous les flux vers une IP donnée alors que le port forwarding ne redirige que les flux venant ou allant vers un port donné.

Petit rappel sur le DMZ : une zone démilitarisée (ou **DMZ**, de l'anglais demilitarized zone) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu (dans notre exemple PfSense). Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. (Source Wikipedia)

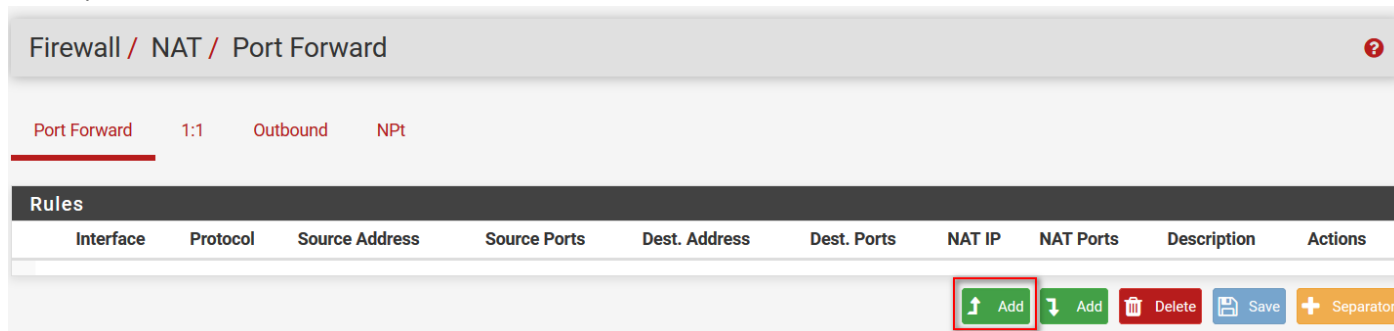
Procédure

Ce que nous allons faire et donc de rediriger tout ce qui vient du WAN sur le port 80 vers notre serveur web en interne.

Donc on commence par se connecter sur l'interface web de gestion de **Pfsense** puis on va dans « **Firewall** » puis « **NAT** » :



On clique ensuite sur « Add »



Dans le cadre « **Protocole** » on va sélectionner « **TCP** » car l'HTTP est un protocole utilisant le protocole de transport TCP.

On va ensuite modifier le « **Destination port range** » en mettant le protocole HTTP, cela signifie que notre règle concerne tout ce qui vient vers le **port 80 (HTTP)**. Pour un autre port, on peut sélectionner (other) puis mettre le numéro de port dans les cases de droite.

On va pouvoir par la suite mettre dans « **Redirect target IP** » l'IP de notre serveur web en interne, c'est vers cette IP que seront redirigées les requêtes. Enfin, on va mettre vers quel port seront redirigées nos requêtes, il arrive dans certaine configuration que l'on redirige les paquets arrivant sur un certain port vers un autre port en interne, les cadres modifiés ressembleront donc à cela :

Edit Redirect Entry			
Disabled	<input type="checkbox"/> Disable this rule		
No RDR (NOT)	<input type="checkbox"/> 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.		
Protocol	TCP Choose which protocol this rule should match. In most cases "TCP" is specified.		
Source	Display Advanced		
Destination	<input type="checkbox"/> Invert match. WAN address Type Address/mask		
Destination port range	HTTP HTTP From port Custom 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	192.168.20.10 Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12		
Redirect target port	HTTP Port Custom Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.		
Description	Intranet depuis le Wan A description may be entered here for administrative reference (not parsed).		
No XMLRPC Sync	<input type="checkbox"/> Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.		
NAT reflection	Use system default		
Filter rule association	Add associated filter rule The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.		

Remarque : N'oubliez pas de donner toujours des « description » bref sur vos règles pour une meilleure lecture.

Cliquer sur « Apply changes »

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

✓ Apply Changes

Suite à l'application de cette règle, on pourra tester notre redirection en allant sur le port 80 sur l'IP WAN de notre **PfSense**, qui devrait nous rediriger vers notre serveur web.

Port Forward

1:1

Outbound

NPT

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<div><div><input type="checkbox"/></div><div><input checked="" type="checkbox"/></div><div></div></div>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.20.10	80 (HTTP)	Intranet depuis le Wan	<div><div></div><div></div><div></div></div>

Add

Add

Delete

Save

Separator

Nous pouvons remarquer l'ajout d'une règle dans l'interface « WAN » de notre pfsense qui autorise le trafic sur le port 80 vers notre serveur web :

System Information

Name

pfSense.tsrit.lan

Version

2.3.2-RELEASE (amd64)
built on Tue Jul 19 12:44:43 CDT 2016
FreeBSD 10.3-RELEASE-p5

Aliases

NAT

Rules

Schedules

Traffic Shaper

Virtual IPs

Interfaces

WAN

1000baseT <full-duplex>

192.168.99.201

LAN

1000baseT <full-duplex>

192.168.10.200

DMZ




1000baseT <full-duplex>






192.168.20.200

Firewall / Rules / WAN

Floating WAN LAN DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	6/11 KiB	IPv4 TCP	*	*	192.168.20.10	80 (HTTP)	*	none	NAT Intranet depuis le Wan	  

 Add  Add  Delete  Save  Separator

Pour déboguer, on pourra aller voir dans « **Status** » puis dans « **System logs** » puis dans l'onglet « **Firewall** », nous pourrons y avoir les redirections des paquets effectuées.

Firewall / NAT / Port Forward


The changes have been applied successfully.
[Monitor](#) the filter reload progress.


Port Forward 1:1 Outbound NPT

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports					
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.20.10	80 (HTTP)

Legend

 Pass

 Linked rule

Status

Captive Portal

CARP (failover)

Dashboard

DHCP Leases

DHCPv6 Leases

Filter Reload

Gateways

Interfaces

IPsec

Load Balancer

Monitoring

NAT

NTP

OpenVPN

Package Logs

Queues

Services

System Logs

Status / System Logs / Firewall / Normal View

SystemFirewallDHCP

Captive Portal AuthIPsecPPPVPNLoad BalancerOpenVPNNTPSettings

Normal ViewDynamic ViewSummary View

Last 50 Firewall Log Entries. (Maximum 50)

Action	Time	Interface	Source	Destination	Protocol
✖	Nov 10 00:31:39	DMZ	192.168.20.1:137	192.168.20.255:137	UDP
✖	Nov 10 00:31:38	DMZ	192.168.20.1:137	192.168.20.255:137	UDP
✖	Nov 10 00:31:37	DMZ	192.168.20.1:137	192.168.20.255:137	UDP
✖	Nov 10 00:31:36	WAN	192.168.99.1:137	192.168.99.255:137	UDP
✖	Nov 10 00:31:36	WAN	192.168.99.1:137	192.168.99.255:137	UDP
✖	Nov 10 00:31:35	WAN	192.168.99.1:137	192.168.99.255:137	UDP
✖	Nov 10 00:31:25	DMZ	192.168.20.1:137	192.168.20.255:137	UDP

On pourra également faire une analyse de port sur le côté WAN de notre Pfsense pour voir si le port est ouvert.