

OPNsense

OPNsense est une plate-forme de routage et de pare-feu open source

Installation

Après avoir mis l'image ISO d'OPNsense sur une clé USB, on doit la connecter à notre routeur et booter dessus. Puis l'installer :

On se connecte avec le compte installateur (user : installer ; password : opnsense).

Il nous a demandé notre keyboard map : Français.

Puis on choisit l'installation "Install (UFS)"

On choisit le disque sur lequel on veut installer OPNsense

Après l'installation nous pouvons entrer un nouveau mot de passe du compte root et cliquer sur "Complete Install".

Après que la machine ait redémarrer, on choisit l'option 1 :

```
8) Logout                                7) Ping host
1) Assign interfaces                     8) Shell
2) Set interface IP address             9) pfTop
3) Reset the root password              10) Firewall log
4) Reset to factory defaults            11) Reload all services
5) Power off system                    12) Update from console
6) Reboot system                       13) Restore a backup

Enter an option: 1

Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n
```

Nous devons configurer les interfaces réseaux : rentrer deux interfaces réseaux :

- en0 est l'interface (WAN) du côté d'Internet
- en1 est l'interface du réseau LAN
- en2 est l'interface du réseau DMZ

```
Valid interfaces are:

en0      08:00:27:97:c8:09 Intel(R) Legacy PRO/1000 MT 82540EM
en1      08:00:27:cf:ed:cc Intel(R) Legacy PRO/1000 MT 82540EM
en2      08:00:27:be:9a:21 Intel(R) Legacy PRO/1000 MT 82540EM

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: en0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): en1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished): en2
```

Il faut maintenant associer les interfaces. On tape 2 :

```
8) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option: 2

Available interfaces:
1 - LAN (en1 - static, track6)
2 - OPT1 (en2)
3 - WAN (en0 - dhcp, dhcp6)
```

On associe les bonnes IPs aux bonnes interfaces et on change le nom de l'interface OPT1 en DMZ.

- en0 est l'interface (WAN) du côté d'Internet, on lui donnera donc l'IP '172.31.208.254/16'
- en1 est l'interface du réseau LAN, on lui donnera donc l'IP '10.31.211.254/22'
- en2 est l'interface du réseau DMZ, on lui donnera donc l'IP '10.31.219.254/22'

Configuration

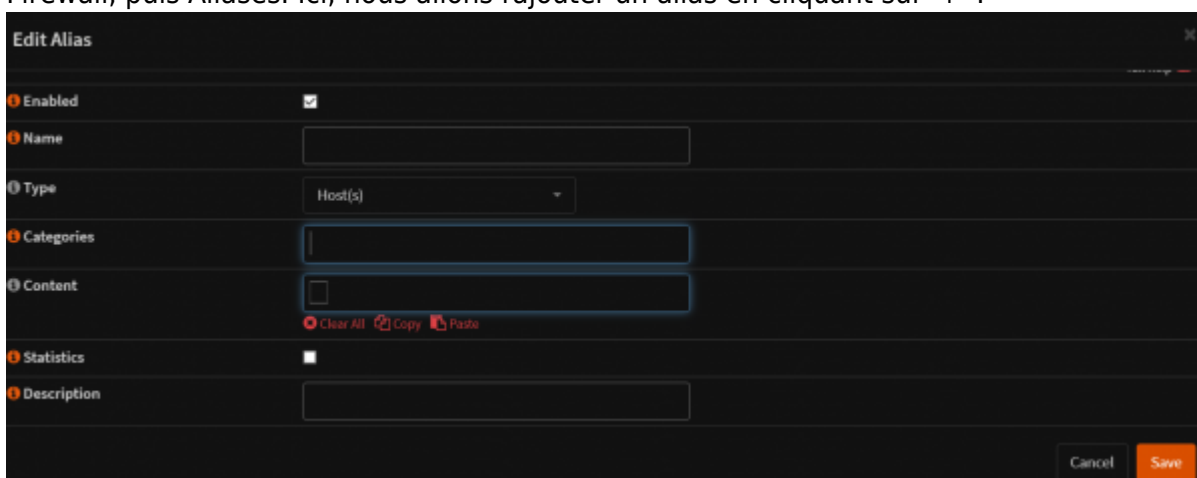
Maintenant nous devons accéder à l'interface d'OPNsense. Pour cela on rend inactif le parefeu qui par défaut refuse toutes les requêtes passantes. On se rend dans le shell et on tape :

```
pfctl -d
```

Maintenant depuis une autre machine nous pouvons nous rendre sur l'interface web en entrant dans la barre d'URL :

```
https://172.31.208.254
```

On rentre les identifiants du compte root. On admire cette belle interface et on se rend dans l'onglet Firewall, puis Aliases. Ici, nous allons rajouter un alias en cliquant sur '+' :



On va créer un alias pour le réseau de Beaupeyrat Dans 'name' on met le nom correspondant : BeaupNET

Dans 'type' on met Network.

Dans Content on met le réseau de Beaupeyrat : 10.187.20.0/24 On rajoute une description qui

explique cet alias. Puis on clique sur 'Save' puis sur 'Apply'. (On peut en créer 4 autres :

- OceanieNET : 10.31.208.0/20
- DMZNET : 10.31.216.0/22
- LANNET : 10.31.208.0/22
- MondeNET : 172.31.0.0/16)

On se rend dans l'onglet Firewall, puis NAT, puis Port forward.

Ici, nous allons rajouter une règle en cliquant sur '+' :

Firewall: NAT: Port Forward

Edit Redirect entry [full help](#)

☐ Disabled ☐ Disable this rule

☐ No RDR (NOT) ☐

☐ Interface WAN

☐ TCP/IP Version IPv4

☐ Protocol TCP

☐ Source / Invert ☐

☐ Source BeaupNET

☐ Source port range

from: any to: any

☐ Destination / Invert ☐

☐ Destination This Firewall

☐ Destination port range

from: (other) to: (other)

1234 1234

☐ Redirect target IP Single host or Network

10.31.211.254

☐ Redirect target port HTTPS

- Interface : WAN
- Protocole : TCP
- Source : BeaupNET
- Destination : This Firewall
- Destination port range :
 - From : 1234
 - To : 1234
- Redirect target IP : Single host or Network
 - 10.31.211.254
- Redirect target port : HTTPS

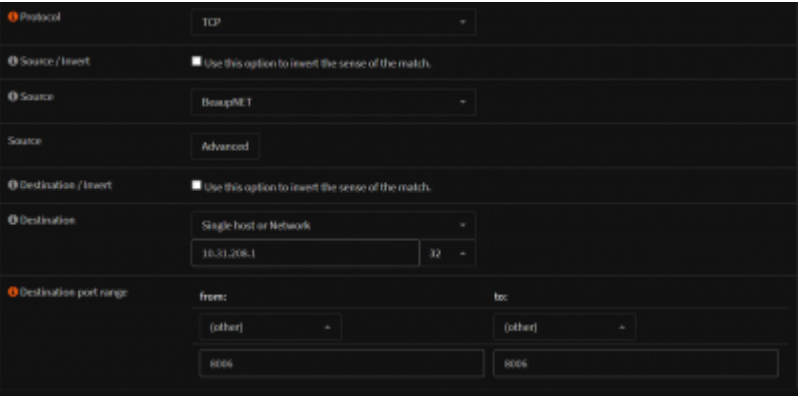
Cette règle signifie que pour toutes les requêtes TCP à destination du routeur entrante par l'interface

WAN sur le port 1234 on le redirige sur l'interface ayant l'IP 10.31.211.254 sur le port 443 (HTTPS). On clique sur 'Save' puis 'Apply' et nous pouvons réactiver le parefeu du routeur sur son shell on tapant la commande :

```
pfctl -e
```

Règles de pare-feu

Pour mettre en place des règles de pare-feu on se rend dans l'onglet Firewall, puis Rules. On retrouve nos 3 interfaces (WAN, DMZ, LAN). Etant donné qu'on va configurer toutes nos règles avec une direction 'in' (signifie que les règles s'appliquent à l'entrée du routeur donc par la première interface touché par les requêtes) alors on va mettre les règles en fonction de ça.
Pour ajouter une règle (par exemple dans WAN) on clique sur '+' :



Ici on permet au réseau BeaupNET de se connecter à la machine 10.31.208.1 sur le port 8006 en TCP. Voici la liste des règles :

WAN

| Source | Destination | Port | Protocole |
|----------|--------------|-------------|-----------|
| BeaupNET | 10.31.208.1 | 8006 | TCP |
| BeaupNET | 10.31.216.1 | 8006 | TCP |
| BeaupNET | OceanieNET | 22 | TCP |
| BeaupNET | LANNET | 80 | TCP |
| BeaupNET | LANNET | 443 | TCP |
| BeaupNET | 10.31.208.33 | 3306 | TCP |
| BeaupNET | 10.31.208.34 | 3306 | TCP |
| BeaupNET | 10.31.208.13 | 445 | TCP |
| BeaupNET | 10.31.216.53 | 53 | UDP |
| BeaupNET | 10.31.216.54 | 53 | UDP |
| BeaupNET | 10.31.216.80 | 80 | TCP |
| BeaupNET | 10.31.216.80 | 443 | TCP |
| BeaupNET | 10.31.216.20 | 990 | TCP |
| BeaupNET | 10.31.216.20 | 49100-49199 | TCP |
| BeaupNET | 10.31.216.20 | 21 | TCP |
| BeaupNET | 10.31.216.15 | 990 | TCP |
| BeaupNET | 10.31.216.15 | 49200-49299 | TCP |
| BeaupNET | 10.31.216.15 | 21 | TCP |

| Source | Destination | Port | Protocole |
|----------|---------------|-------------|-----------|
| BeaupNET | 10.31.216.16 | 990 | TCP |
| BeaupNET | 10.31.216.16 | 49300-49399 | TCP |
| BeaupNET | 10.31.216.16 | 21 | TCP |
| MondeNET | 10.31.216.53 | 54 | UDP |
| MondeNET | 10.31.216.54 | 54 | UDP |
| BeaupNET | This firewall | * | ICMP |
| BeaupNET | This firewall | 22 | TCP |

LAN

| Source | Destination | Port | Protocole |
|--------------|---------------|------|-----------|
| 10.31.208.1 | DMZNET | 22 | TCP |
| LANNET | * | 80 | TCP |
| LANNET | * | 443 | TCP |
| LANNET | * | * | ICMP |
| LANNET | 10.31.216.53 | 53 | UDP |
| LANNET | 10.31.216.54 | 53 | UDP |
| 10.31.208.73 | DMZNET | 22 | TCP |
| 10.31.208.74 | DMZNET | 22 | TCP |
| LANNET | This Firewall | * | ICMP |
| LANNET | MondeNET | * | ICMP |

DMZ

| Source | Destination | Port | Protocole |
|--------------|---------------|------|-----------|
| DMZNET | * | 80 | TCP |
| DMZNET | * | 443 | TCP |
| 10.31.216.1 | LANNET | 22 | TCP |
| DMZNET | * | * | ICMP |
| 10.31.216.53 | 8.8.8.8 | 53 | UDP |
| 10.31.216.54 | 8.8.8.8 | 53 | UDP |
| 10.31.216.53 | 8.8.4.4 | 53 | UDP |
| 10.31.216.54 | 8.8.4.4 | 53 | UDP |
| 10.31.216.67 | 10.31.208.67 | 67 | UDP |
| 10.31.216.67 | 10.31.208.68 | 67 | UDP |
| 10.31.216.80 | 10.31.208.33 | 3306 | TCP |
| 10.31.216.80 | 10.31.208.34 | 3306 | TCP |
| DMZNET | This Firewall | * | ICMP |
| 10.31.216.53 | LANNET | 53 | UDP |
| 10.31.216.54 | LANNET | 53 | UDP |
| DMZNET | MondeNET | * | ICMP |

Concernant le serveur FTP nous avons du mettre en place les ports passifs.
Pour cela on se rend sur le serveur FTP puis dans le fichier proftpd.conf :

```
nano /etc/proftpd/proftpd.conf
```

On décommente la ligne 'PassivePorts' :

```
# In some cases you have to specify passive ports range to by-pass  
# firewall limitations. Ephemeral ports can be used for that, but  
# feel free to use a more narrow range.  
PassivePorts 49100 49199
```

C'est suivi d'un rang de ports, ici 49100 à 49199. Cela signifie que lorsqu'un client va vouloir communiquer avec le serveur FTP le serveur va répondre sur un port au hasard dans ce rang. On rajoute la même directive dans les VHosts intra et extra pour une rangé de port de différent.

```
systemctl restart proftpd
```



From:

<https://sisr2.beaupeyrat.com/> - Documentations SIO2 option SISR

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr2-oceanie:mission12>

Last update: **2024/11/29 10:50**

