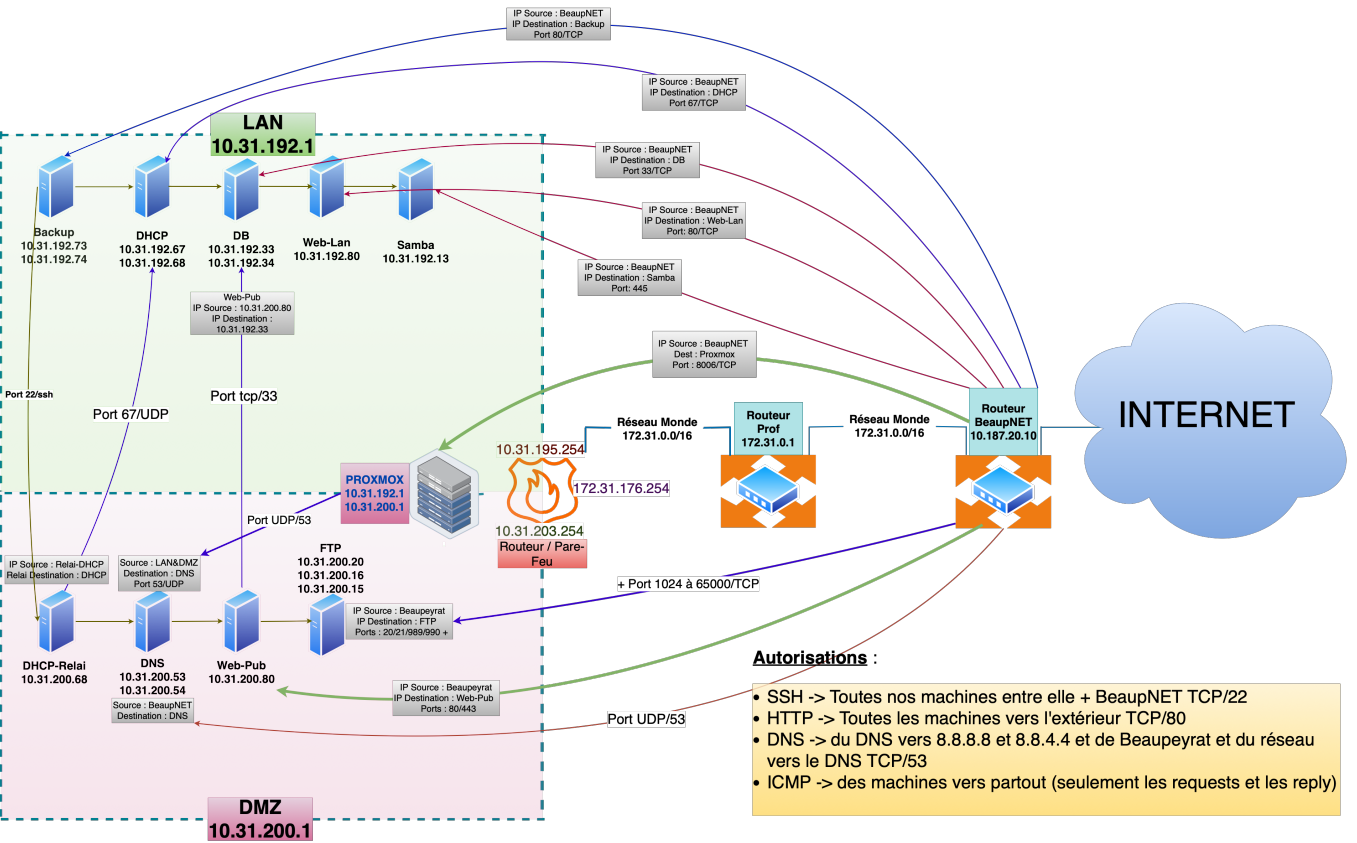


SCHÉMA RÉSEAU



Liste de règle de pare-feu

Routeur:

source	Destination	
172.31.195.254	<- 10.187.20.0/24	tcp:ssh
10.31.192.254	<- 10.187.20.0/24	tcp:ssh
10.31.203.254	<- 10.187.20.0/24	tcp:ssh

Proxmox:

10.31.192.1	<- 10.187.20.0/24	tcp: ssh
10.31.200.1	<- 10.187.20.0/24	tcp: ssh

RÉSEAU PRIVÉ LAN #Backup

Source :	Destination :	
10.31.192.73	<- 10.187.20.0/24	tcp: 80
10.31.192.74	<- 10.187.20.0/24	tcp: 80

#DHCP

10.31.192.67	<-	10.187.20.0/24		udp: 67
--------------	----	----------------	--	---------

#BDD

10.31.192.33	<-	10.187.20.0/24		tcp: 80/33
10.31.192.34	<-	10.187.20.0/24		tcp: 80/33

#Web-priv

10.31.192.80	<-	10.187.20.0/24		tcp: 80/443
--------------	----	----------------	--	-------------

#Samba

10.31.192.13	<-	10.187.20.0/24		tcp: 445
--------------	----	----------------	--	----------

RÉSEAU PUBLIC DMZ

#DNS

10.31.200.53	<-	8.8.8.8		udp:domain :53
10.31.200.54	<-	8.8.8.8		udp:domain :53

#DHCP Relay

10.31.200.68	<-	10.187.20.0/24		tcp : 67
--------------	----	----------------	--	----------

#Web-pub

10.31.200.80	<-	10.187.20.0/24		tcp:http :80/443
--------------	----	----------------	--	------------------

#FTP

10.31.200.20	<-	10.187.20.0/24		tcp: 20/21
10.31.200.15	<-	10.187.20.0/24		tcp: 20/21
10.31.200.16	<-	10.187.20.0/24		tcp: 20/21

Installation de OPNSense

Pour installer OPNSense sur notre routeur nous devons posséder le logiciel dans une clé USB et le booter sur notre machine en cliquant sur le bouton F12. Cela nous affichera ou une page ou l'on devra choisir Entre Debian/Linux et OpnSense. Notre choix se portera sur le deuxième.

- Ensuite on se connecte avec l'utilisateur : installer
- Le mot de passe : opnsense

```
>>> invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Tue Feb 21 06:21:18 UTC 2023

*** OPNsense.localdomain: OPNsense 23.1 ***

LAN (vnx0)    -> v4: 192.168.1.1/24
WAN (vnx1)    -> v4/DHCP4: 10.13.37.77/24

HTTPS: SHA256 7E 2D 39 6D FC E7 EA 6B 30 F1 63 6E 54 31 E7 D5
7B B6 3E 79 9F E5 6A E5 7C 21 FD EF 21 6F 50 9E
SSH:  SHA256 xQ22eJv2CJdo0LMrzsTEpLqnt6DFxh00RYQ6Qbf0CaM (ECDSA)
SSH:  SHA256 zJfq7vlib6U1/d20cXuaB/auM2nbMTJe2+uUGQKeWAA (ED25519)
SSH:  SHA256 mF4MC2pbxMrYuEhtBSB11D3Xsb0N6eDr2Np41dhxill (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █
```

* Un menu sera dans la console:

- | | |
|----------------------------------|-----------------------------|
| * 0) Logout | 7) Ping host |
| * 1) Assign interfaces | 8) Shell |
| * 2) Set interface(s) IP address | 9) pfTop |
| * 3) Reset the root password | 10) Filter logs |
| * 4) Reset to factory defaults | 11) Restart web interface |
| * 5) Reboot system | 12) Upgrade from console |
| * 6) Halt system | 13) Restore a configuration |

Nous devons choisir le N°1

Puis on assigne toute les interfaces avec les adresses MAC de chaque réseaux. Pour l'interface WAN d'OPNsense, on mettra en gateway l'IP du routeur de prof 172.31.0.1 ; En ce qui concerne les autres interfaces LAN et DMZ on ne met pas de gateway.

```
Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished): em2

Enter the Optional interface 2 name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1
OPT1 -> em2
```

Chez nous ce sera :

- WAN : re0
- LAN : re1
- OPT1: re2
- Puis on valide la configuration

Ensuite en retourne sur le menu départ

* Un menu sera dans la console:

* 0) Logout	7) Ping host
* 1) Assign interfaces	8) Shell
* 2) Set interface(s) IP address	9) pfTop
* 3) Reset the root password	10) Filter logs
* 4) Reset to factory defaults	11) Restart web interface
* 5) Reboot system	12) Upgrade from console
* 6) Halt system	13) Restore a

configuration

On choisi cette fois l'option 2 pour configurer les IP de chaque interface:

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

- On entre le nombre d'interface à configurer : 3
- Configurer l'adresse IPV4 de l'interface WAN via DHCP : N
- On entre la nouvelle adresse IPV4 du WAN : 172.31.192.254

Puis on choisi le nombre de bit pour la notation CIDR entre :

- 255.255.255.0 = 24
- 255.255.0.0 = 16
- 255.0.0.0 = 8
- On choisi 16

Puis on entre l'adresse de la Gateway du WAN qui sera 172.31.0.1

- Do you want to use the gateway as the IPV4 name server, too? [Y/n] : n
- Enter the IPv4 name server or press <ENTER> for none:

> 8.8.8.8

- Configure IPv6 address WAN interface via DHCP6 [Y/n] : n
- Puis on clique à chaque fois sur la touche Entrée

Une fois la configuration terminée, on obtient ce résultat :

- <https://172.31.192.254>
- DMZ (re2) → v4: 10.31.203.254/22
- LAN (re1) → v4: 10.31.195.254/22
- WAN (re0) → v4: 172.31.192.254/24

Interface web d'OPNSense

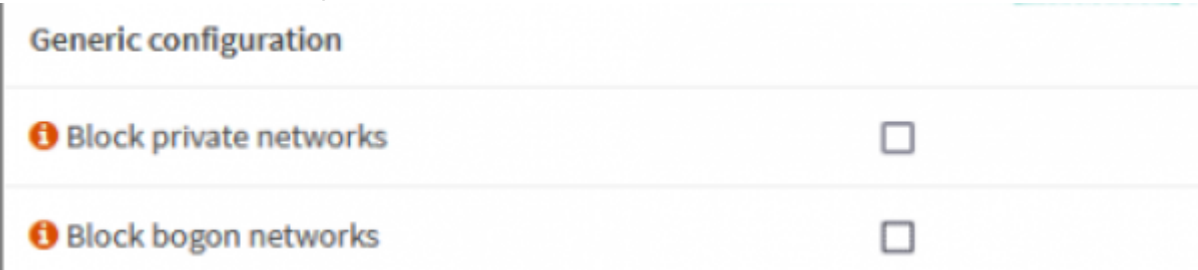
On commence d'abord par désactiver temporairement le pare-feu pour accéder à la GUI depuis l'interface.

```
pfctl -d
pf disabled
```

Puis on va sur notre navigateur et on entre l'adresse suivante : <https://172.31.192.254>


Configuration

On autorise les réseaux privés sur WAN. Pour ce faire il faut aller dans Interface → WAN



On fait la règle de NAT pour accéder à la GUI depuis l'interface WAN :

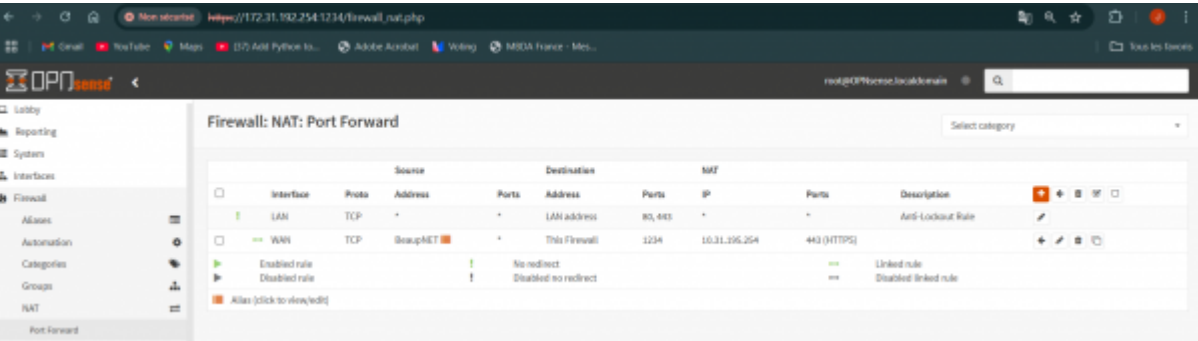
Firewall → NAT → PortForward



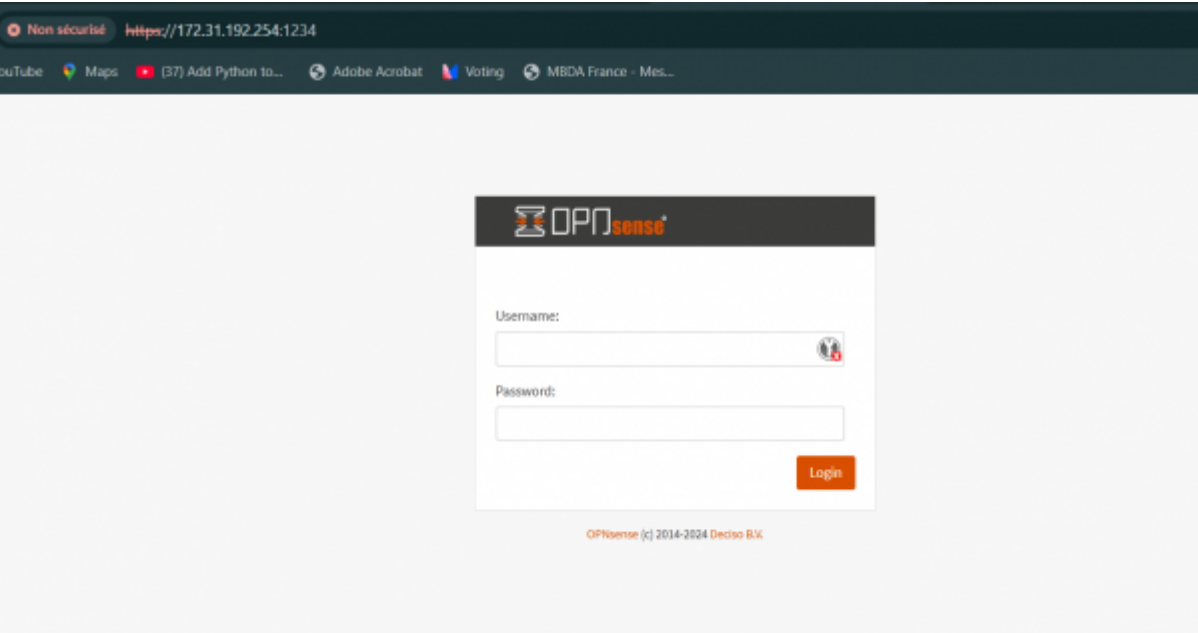
Source : WAN net ; port source :*

Dest : This firewall ; port dest : 1234

Redirect : IP_LAN_OPNSense ; redirect port : 443



On somme, on accède à la GUI depuis l'adresse WAN, le pare-feu est activé



Règles de pare-feu sur OPNSense

Pour crée des règles de pare-feu sur nos 3 interfaces on va dans **Firewall → Rules**

Firewall : Rules : WAN

Firewall: Rules: WAN										Select category	Inspect
<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description			
Automatically generated rules											
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	10.31.192.254	443 (HTTPS)	*	*				
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	10.31.192.1	22 (SSH)	*	*	connexion ssh depuis le réseau de beaup vers le serveur PVE			
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	DMZ net	22 (SSH)	*	*	connexion ssh à toutes les adresses sur la dmz			
<input type="checkbox"/>	IPv4 ICMP	BeaupNET	*	LAN net	*	*	*	Permet les ping depuis Beaup sur le LAN			
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	LAN net	22 (SSH)	*	*	Connexion ssh depuis beaup sur les machine du réseau LAN			
<input type="checkbox"/>	IPv4 ICMP	BeaupNET	*	DMZ net	*	*	*	Permet le ping de DMZ depuis Beaup			
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	10.31.192.1	any - 8006	*	*	Permet de se connecter à proemox avec le réseau de beaup			
<input type="checkbox"/>	IPv4 TCP	10.187.20.15	*	10.31.192.1	8006	*	*	Permet de se connecter à proemox grace au vpn			
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	10.31.192.0/20	22 (SSH)	*	*	connexion au routeur depuis Beaup			
<input type="checkbox"/>	IPv4 UDP	BeaupNET	*	10.31.200.53	53 (DNS)	*	*	Allow DNS request from BeaupNet to DNS#1			
<input type="checkbox"/>	IPv4 UDP	BeaupNET	*	10.31.200.54	53 (DNS)	*	*	Allow DNS request from BeaupNet to DNS#2			
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	10.31.200.80	80 (HTTP)	*	*	Allow HTTP request			
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	10.31.200.80	443 (HTTPS)	*	*	Allow HTTPS request			
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	10.31.192.33	3306	*	*	connexion à la base de donnée depuis une machine du réseau de Beaup			
<input type="checkbox"/>	IPv4 TCP	BeaupNET	*	10.31.192.34	3306	*	*	connexion à la base de donnée depuis une machine du réseau de Beaup			

		IPv4 TCP	BeaupNET	*	10.31.192.34	3306	*	*	connexion à la base de donnée depuis une machine du réseau de Beaup			
		IPv4 TCP	BeaupNET	*	10.31.192.80	80 (HTTP)	*	*	connexion au web-priv depuis une machine du réseau de beaup			
		IPv4 TCP	BeaupNET	*	10.31.192.80	443 (HTTPS)	*	*	connexion au web-priv depuis une machine du réseau de beaup			
		IPv4 TCP	BeaupNET	*	10.31.200.80	80 (HTTP)	*	*	connexion à web-pub avec une machine sur le réseau de Beaup			
		IPv4 TCP	BeaupNET	*	10.31.200.80	443 (HTTPS)	*	*	connexion à web-pub avec une machine sur le réseau de Beaup			
		IPv4 TCP	BeaupNET	*	10.31.200.20	20	*	*	connexion à ftp-pub sur une machine de beaup			
		IPv4 TCP	BeaupNET	*	10.31.200.20	21 (FTP)	*	*	connexion à ftp-pub sur une machine de beaup			
		IPv4 TCP	BeaupNET	*	10.31.200.15	21 (FTP)	*	*	connexion à ftp-pub sur une machine de beaup			
		IPv4 TCP	BeaupNET	*	10.31.200.16	21 (FTP)	*	*	connexion à ftp-pub sur une machine de beaup			
		IPv4 TCP	BeaupNET	*	10.31.192.74	80 (HTTP)	*	*	Activation de backupPC2			
		IPv4 TCP	BeaupNET	*	10.31.192.73	80 (HTTP)	*	*	Activation de BackupPC1			
		IPv4 TCP	BeaupNET	*	10.31.200.20	49152 - 65534	*	*	activation du compte std sur ftp			
		IPv4 TCP	BeaupNET	*	10.31.200.15	49152 - 65534	*	*	activation du compte intra sur ftp			
		IPv4 TCP	BeaupNET	*	10.31.200.16	49152 - 65534	*	*	activation du compte extra sur ftp			
		IPv4 TCP	BeaupNET	*	10.31.192.13	445 (MS DS)	*	*	Allow samba's service			
		IPv4 TCP/UDP	BeaupNET	*	10.31.192.200	3389 (MS RDP)	*	*	Connexion Bureau A Distance a Partir de nos machine BEAUPNET			
		pass		block		reject		log			first match	
		pass (disabled)		block (disabled)		reject (disabled)		log (disabled)			last match	
Active/Inactive Schedule (click to view/edit)												
Alias (click to view/edit)												

Firewall : Rules : LAN

Firewall: Rules: LAN										Select category	Inspect		
<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description					
	Automatically generated rules												
	IPv4 UDP	LAN net	*	10.31.200.53	53 (DNS)	*	*	Allow DNS request from LAN Net to DNS#1					
	IPv4 UDP	LAN net	*	10.31.200.54	53 (DNS)	*	*	Allow DNS request from LAN Net to DNS#2					
	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	*	pour autoriser les MAJ sur le reseau lan					
	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	*	pour autoriser les MAJ sur le reseau lan					
	IPv4 TCP/UDP	10.31.192.74	*	DMZ net	22 (SSH)	*	*	Permet à l'user backup de se connecter à toute les machines du réseau DMZ					
	IPv4 TCP/UDP	10.31.192.73	*	DMZ net	22 (SSH)	*	*	Permet à l'user backup de se connecter à toute les machines du réseau DMZ					
	IPv4 ICMP	10.31.192.73	*	DMZ net	*	*	*	Permet à Backuppc de ping les machines de la DMZ sinon y'as pas de backup					
	IPv4 ICMP	10.31.192.74	*	DMZ net	*	*	*	Permet à l'utilisateur backuppc de ping les machines du réseau DMZ					
	pass	block			reject			log			first match		
	pass (disabled)	block (disabled)			reject (disabled)			log (disabled)			last match		
Active/Inactive Schedule (click to view/edit)													
Alias (click to view/edit)													

Firewall : Rules : DMZ

Firewall: Rules: DMZ

Select category

Inspect

		Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description				
										Automatically generated rules				
			</											

From:

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

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr2-europe:opnsense>

Last update: **2024/12/16 13:01**

