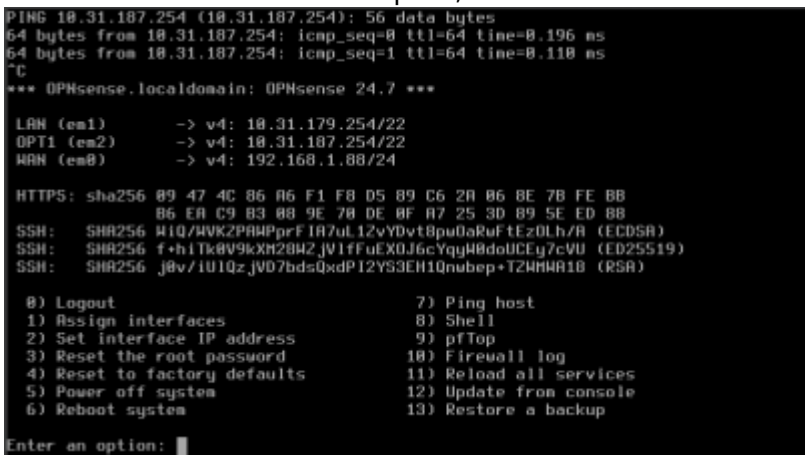
OPNsense

Installation de OPNsense

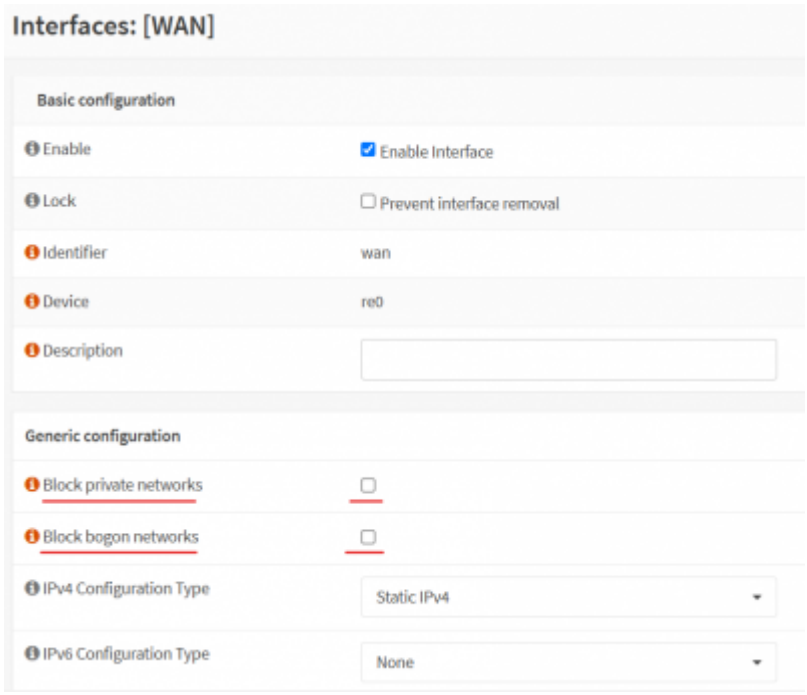
Pour commencer l'installation de OPNsense, il faut télécharger l'iso de OPNsense sur une clé USB pour pouvoir bouter l'iso et l'installer.
Ensuite, une fois que l'iso sera bouter sur notre machine, il faudra remplir plusieurs informations avant de faire la configuration des interfaces avec les réseaux.
Une fois les informations remplies, on va tomber sur l'interface ci-dessous :



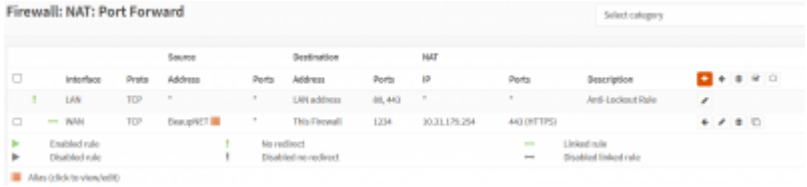
Pour commencer, il faut taper “1) Assign interfaces” pour attribuer les interfaces avec nos réseaux LAN, DMZ et WAN.
Pour cela, il faut regarder les adresses MAC de la LAN, DMZ et WAN afin d'attribuer plus facilement les interfaces sinon faut faire au pif.
Ensuite, il faut taper “2) Set interface IP address” pour configurer les IP de chaque interfaces puis suivre les indications suivantes :
- Choisir l'interface à configurer
- Choisir n
- Entrer l'adresse IPv4
- Choisir le masque du réseau
- Entrer l'IP de la gateway
- Choisir n
- Entrer 8.8.8.8 pour l'IP de name server
- Choisir n
- Faire entrée
- Choisir n jusqu'à la fin

Faire a même chose pour les autres interfaces à configurer.
Ne pas oublier de faire “8)” pour se déconnecter et désactiver le pare-feu avec la commande pfctl -d. (pftcl -e pour l'activer)

Une fois les configurations terminées, il faut se connecter à OPNsense avec l'IP de WAN sur internet.
Ensuite, il faut autoriser les réseaux privés sur WAN



Puis, faire la règle de NAT pour accéder à la GUI depuis l'interface WAN même le pare-feu activé



Si tout est bon, il est possible d'accéder à OPNsense avec le pare-feu activé.

Règles de pare-feu

Règles de pare-feu LAN

Protocol	Source	Source Port	Destination	Destination Port	Gateway	Schedule	Description
IPv4 UDP	LAN net	*	10.31.184.53	53 (DNS)	*	*	Règles pour le DNS
IPv4 UDP	LAN net	*	10.31.184.54	53 (DNS)	*	*	Règles pour le DNS
IPv4 TCP	10.31.176.73	*	DMZ net	22 (SSH)	*	*	Règle backup PC
IPv4 ICMP	10.31.176.73	*	DMZ net	*	*	*	Règle backup PC
IPv4 ICMP	LAN net	*	DMZ net	*	*	*	Ping vers DMZ
IPv4 TCP	LAN net	*	*	80 (HTTP)	*	*	Vers Internet pour MAJ
IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	*	Vers Internet pour MAJ

Protocol	Source	Source Port	Destination	Destination Port	Gateway	Schedule	Description
IPv4 TCP/UDP	10.31.176.201	*	8.8.8.8	*	*	*	

Règles de pare-feu DMZ

Protocol	Source	Source Port	Destination	Destination Port	Gateway	Schedule	Description
IPv4 UDP	10.31.184.53	*	8.8.8.8	53 (DNS)	*	*	Règle pour DNS
IPv4 UDP	10.31.184.54	*	8.8.8.8	53 (DNS)	*	*	Règle pour DNS
IPv4 UDP	10.31.184.53	*	8.8.4.4	53 (DNS)	*	*	Règle pour DNS
IPv4 UDP	10.31.184.54	*	8.8.4.4	53 (DNS)	*	*	Règle pour DNS
IPv4 ICMP	DMZ net	*	LAN net	*	*	*	Ping DMZ vers LAN
IPv4 ICMP	DMZ net	*	*	*	*	*	Ping DMZ vers extérieur
IPv4 TCP	DMZ net	*	*	80 (HTTP)	*	*	Vers Internet pour MAJ
IPv4 TCP	DMZ net	*	*	443 (HTTPS)	*	*	Vers Internet pour MAJ
IPv4 TCP	10.31.184.80	*	10.31.176.33	3306	*	*	Web Pub vers base de données
IPv4 TCP	10.31.184.80	*	10.31.176.34	3306	*	*	Web Pub vers base de données
IPv4 UDP	10.31.184.67	*	10.31.176.67	67	*	*	DHCP Relais vers DHCP
IPv4 UDP	10.31.184.67	*	10.31.176.68	67	*	*	DHCP Relais vers DHCP
IPv4 TCP/UDP	10.31.184.200	*	8.8.8.8	*	*	*	Règle pour que serveur Windows contacte Google
IPv4 TCP/UDP	10.31.184.201	*	10.31.176.200	389 (LDAP)	*	*	
IPv4 TCP/UDP	10.31.184.201	*	10.31.176.200	88	*	*	
IPv4 TCP/UDP	10.31.184.201	*	10.31.176.200	53 (DNS)	*	*	
IPv4 TCP/UDP	10.31.184.201	*	10.31.176.200	445 (MS DS)	*	*	
IPv4 TCP/UDP	10.31.184.201	*	10.31.176.200	135	*	*	

Règles de pare-feu WAN

Protocol	Source	Source Port	Destination	Destination Port	Gateway	Schedule	Description
IPv4 TCP	BeaupNET	*	10.31.179.254	443 (HTTPS)	*	*	
IPv4 ICMP	BeaupNET	*	LAN net	*	*	*	Allow ping from Beaup to LAN
IPv4 ICMP	BeaupNET	*	DMZ net	*	*	*	Allow ping from Beaup to DMZ
IPv4 TCP	BeaupNET	*	10.31.176.1	8006	*	*	Règle pour Proxmox
IPv4 UDP	BeaupNET	*	10.31.184.53	53 (DNS)	*	*	Règle pour DNS
IPv4 UDP	BeaupNET	*	10.31.184.54	53 (DNS)	*	*	Règle pour DNS
IPv4 TCP	BeaupNET	*	LAN net	22 (SSH)	*	*	Règle SSH pour LAN
IPv4 TCP	BeaupNET	*	DMZ net	22 (SSH)	*	*	Règle SSH pour DMZ
IPv4 TCP	BeaupNET	*	10.31.176.73	80 (HTTP)	*	*	Règle pour BackupPC
IPv4 TCP	BeaupNET	*	10.31.176.50	80 (HTTP)	*	*	Règle pour Zabbix HTTP
IPv4 TCP	BeaupNET	*	10.31.176.13	445 (MS DS)	*	*	Règle Samba
IPv4 TCP	BeaupNET	*	10.31.184.80	443 (HTTPS)	*	*	Web Pub vers l'extérieur
IPv4 TCP	BeaupNET	*	10.31.184.80	80 (HTTP)	*	*	Web Pub vers l'extérieur
IPv4 TCP	BeaupNET	*	10.31.176.80	443 (HTTPS)	*	*	Web Priv vers l'extérieur
IPv4 TCP	BeaupNET	*	10.31.176.50	443 (HTTPS)	*	*	Zabbix HTTPS
IPv4 TCP	BeaupNET	*	10.31.176.80	80 (HTTP)	*	*	Web Priv vers l'extérieur
IPv4 TCP	BeaupNET	*	10.31.184.20	21 (FTP)	*	*	FTP
IPv4 TCP	BeaupNET	*	10.31.184.20	*	*	*	FTP
IPv4 TCP	BeaupNET	*	10.31.184.15	21 (FTP)	*	*	FTP INTRA
IPv4 TCP	BeaupNET	*	10.31.184.16	21 (FTP)	*	*	FTP EXTRA
IPv4 TCP	BeaupNET	*	10.31.184.20	60000 - 61000	*	*	FTP
IPv4 TCP	BeaupNET	*	10.31.184.15	60000 - 61000	*	*	FTP INTRA
IPv4 TCP	BeaupNET	*	10.31.184.16	60000 - 61000	*	*	FTP EXTRA
IPv4 TCP	BeaupNET	*	10.31.184.20	990	*	*	FTP
IPv4 TCP	BeaupNET	*	10.31.184.15	990	*	*	FTP INTRA
IPv4 TCP	BeaupNET	*	10.31.184.16	990	*	*	FTP EXTRA
IPv4 TCP	BeaupNET	*	This Firewall	22 (SSH)	*	*	
IPv4 TCP/UDP	BeaupNET	*	10.31.176.200	3389 (MS RDP)	*	*	
IPv4 TCP/UDP	BeaupNET	*	10.31.176.200	3389 (MS RDP)	*	*	Connexion bureau à distance

Protocol	Source	Source Port	Destination	Destination Port	Gateway	Schedule	Description
IPv4 TCP/UDP	BeaupNET	*	10.31.184.201	3389 (MS RDP)	*	*	Connexion bureau à distance
IPv4 TCP/UDP	BeaupNET	*	10.31.176.201	3389 (MS RDP)	*	*	Connexion bureau à distance