Installation et Configuration

pfSense — Pare-feu & NAT

Clarac Matheo — BTS SIO 1ère année SISR

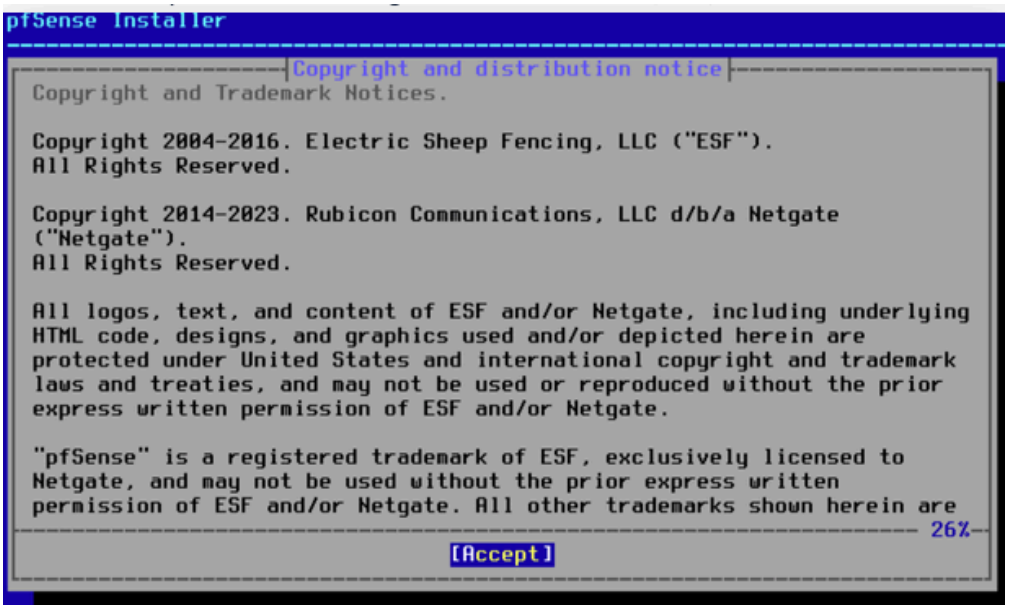
Objectif

Installer et configurer pfSense comme pare-feu/routeur, mettre en place une architecture réseau avec une zone WAN, LAN et DMZ, puis créer des règles de pare-feu permettant l'accès au serveur web via NAT.

1. Installation de pfSense

pfSense est un système d'exploitation basé sur FreeBSD, utilisé comme pare-feu et routeur. L'installation se fait depuis une image ISO bootable.

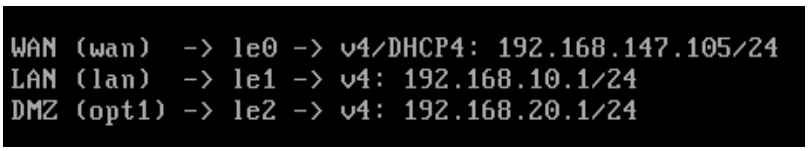
1. Démarrer la machine sur l'ISO pfSense.
2. Accepter les termes de la licence (Copyright and distribution notice).
3. Suivre l'assistant d'installation : choix du clavier, partitionnement, installation.
4. Redémarrer après installation.



L'écran d'installation affiche l'avertissement de copyright et de distribution de pfSense. Cliquer sur [Accept] pour continuer.

2. Configuration des interfaces réseau

Après redémarrage, pfSense affiche l'assignation des interfaces réseau depuis la console. Les trois interfaces sont configurées comme suit :



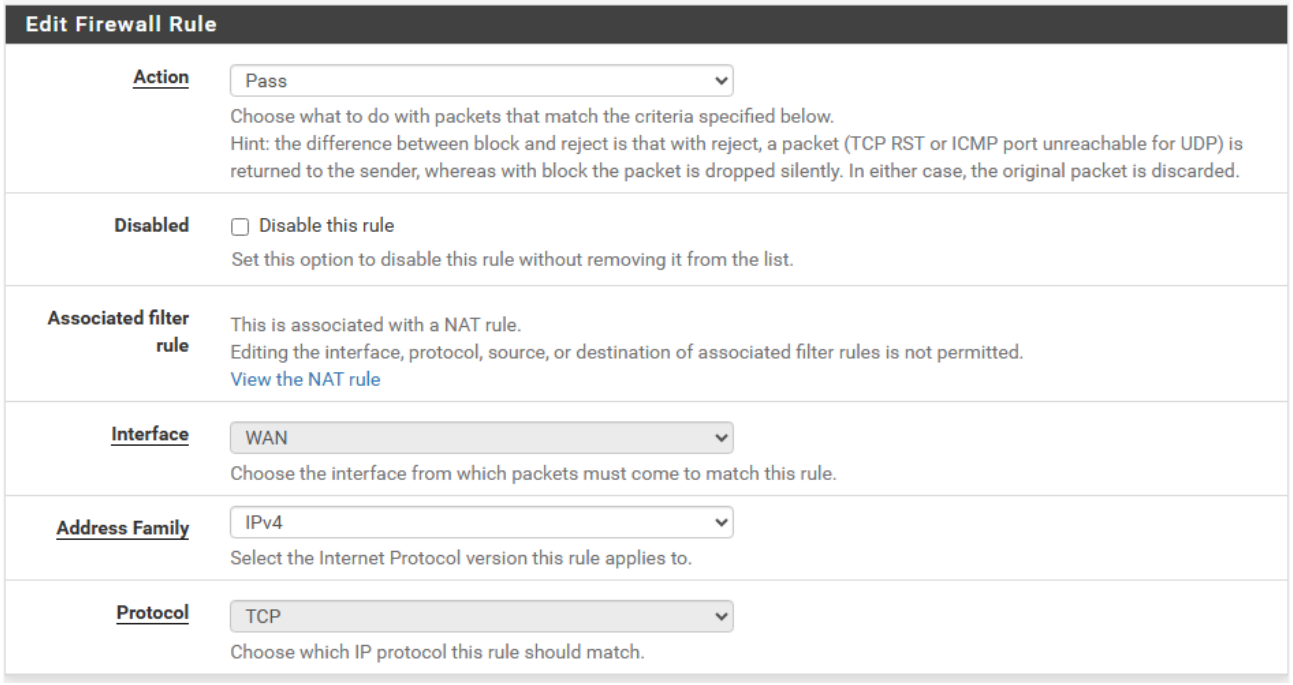
Zone	Interface	Carte	Adresse IP
WAN	wan	le0	192.168.147.105/24 (DHCP)
LAN	lan	le1	192.168.10.1/24
DMZ (opt1)	opt1	le2	192.168.20.1/24

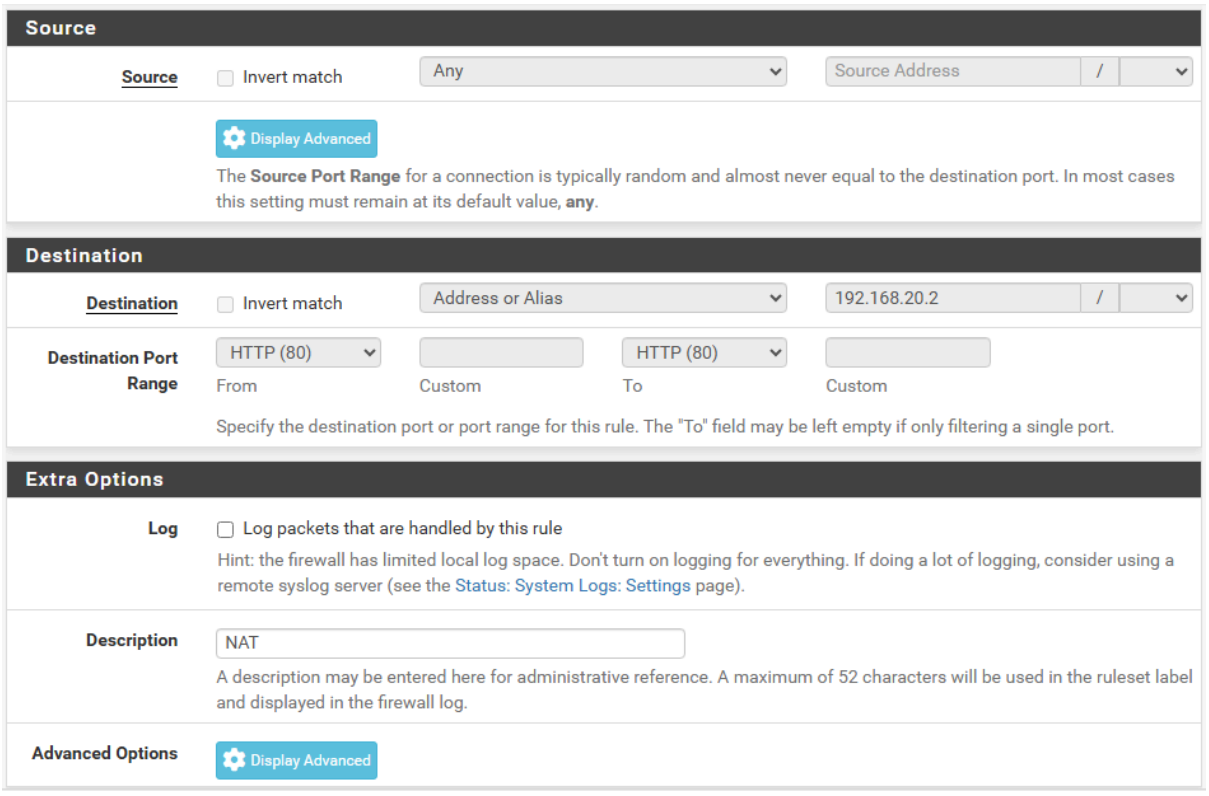
⚠ Le serveur web se trouve dans la DMZ à l'adresse 192.168.20.2. La DMZ isole les serveurs accessibles depuis l'extérieur du réseau LAN interne.

3. Règle de pare-feu — Accès au serveur web

Cette règle permet aux connexions provenant d'Internet (WAN) d'atteindre le serveur web situé en DMZ via un NAT de redirection de port (Port Forward).

Configuration de la règle



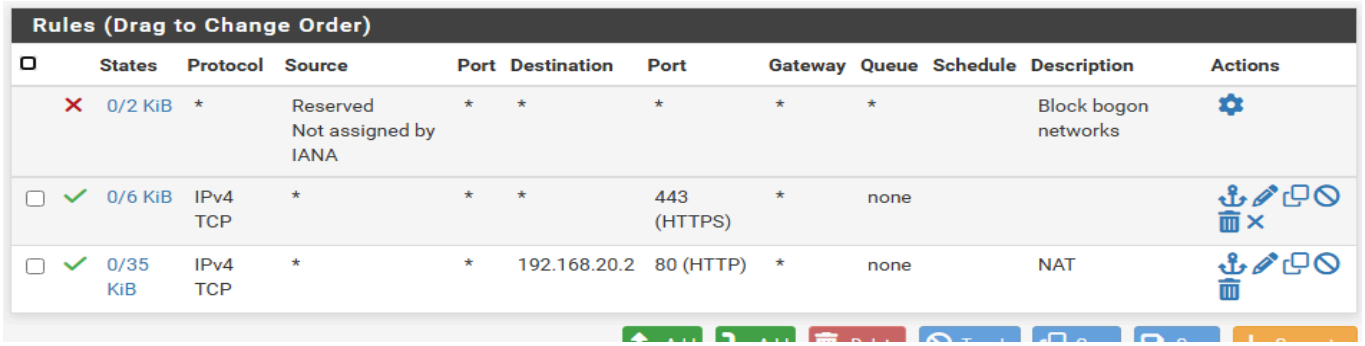


Détail des paramètres

Paramètre	Valeur
Action	Pass (Autoriser)
Interface	WAN
Address Family	IPv4
Protocole	TCP
Source	Any (toute source)
Destination	192.168.20.2 (serveur web DMZ)
Port destination	HTTP (80)
Description	NAT
Tracking ID	1747063536
Créée le	5/12/25 15:25:36 par NAT Port Forward

4. Récapitulatif des règles WAN

Le tableau ci-dessous liste l'ensemble des règles actives sur l'interface WAN de pfSense.



État	Protocol	Source	Port	Destination	Port dest.	Description
❌ Bloqué	*	Reserved / Not assigned by IANA	*	*	*	Block bogon networks
✅ Autorisé	IPv4 TCP	*	*	*	443 (HTTPS)	—
✅ Autorisé	IPv4 TCP	*	*	192.168.20.2	80 (HTTP)	NAT

Explication des règles :

- Block bogon networks : bloque les adresses IP réservées ou non attribuées par l'IANA (protection par défaut).
- Port 443 (HTTPS) : autorise les connexions HTTPS entrantes depuis n'importe quelle source.
- Port 80 (HTTP) → 192.168.20.2 (NAT) : redirige le trafic HTTP entrant vers le serveur web en DMZ.

⚠ La règle NAT (port 80) a été créée automatiquement lors de la configuration du Port Forward dans le menu Firewall > NAT > Port Forward.