# Rendu Technique de FGTW

Projet Fortins - AP4.1

# Configuration ip & Dashboard :

## 1. Configuration IP & Dashboard

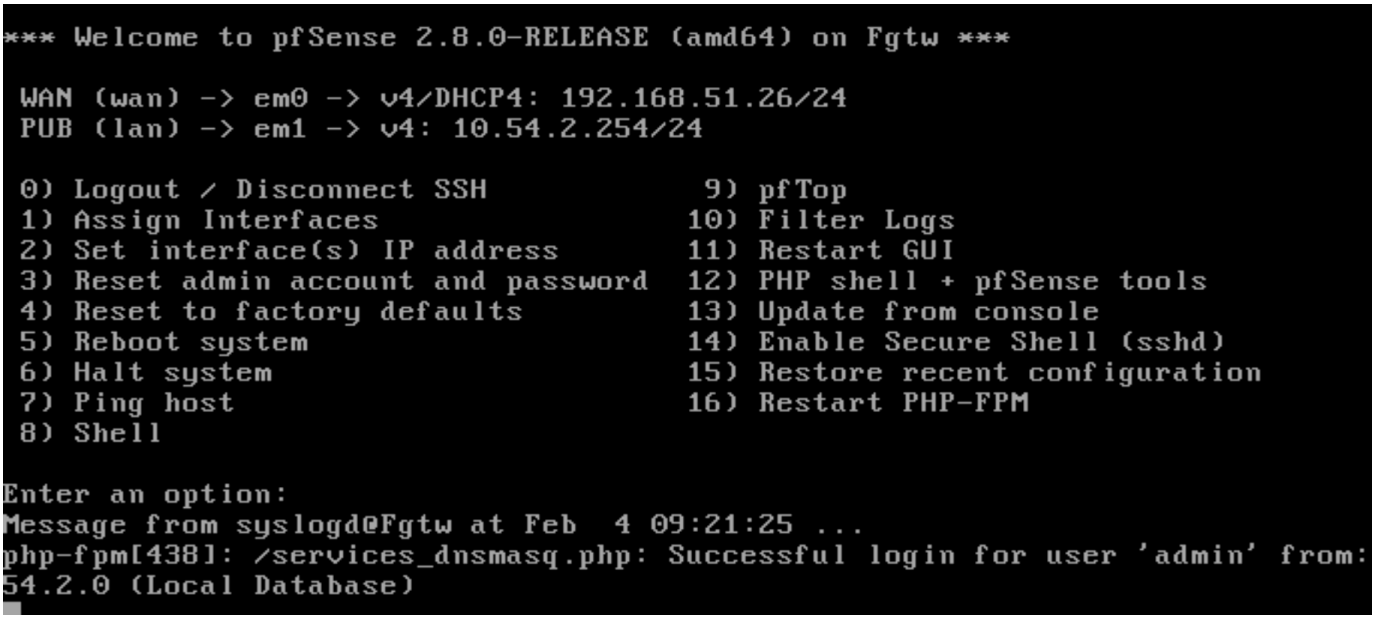
**Configuration des interfaces**

La passerelle FGTW est configurée avec deux interfaces conformément au cahier des charges :

- **WAN** : adresse obtenue via DHCP depuis le réseau SIO (fournisseur local).

- **PUB** : interface statique associée à la DMZ publique en **10.54.2.254/24**.

Cette configuration permet à FGTW d'assurer la communication entre Internet et la DMZ publique tout en servant de point d'entrée principal pour les flux HTTPS et VPN.

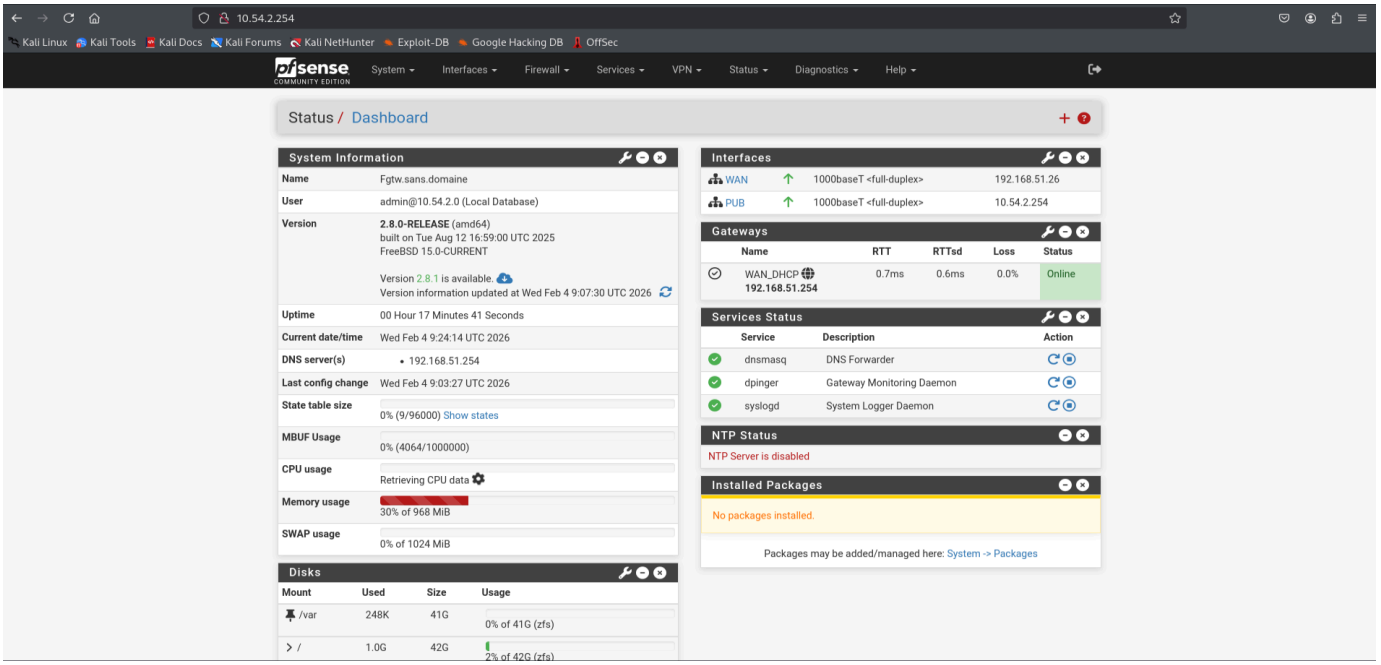



**Dashboard**

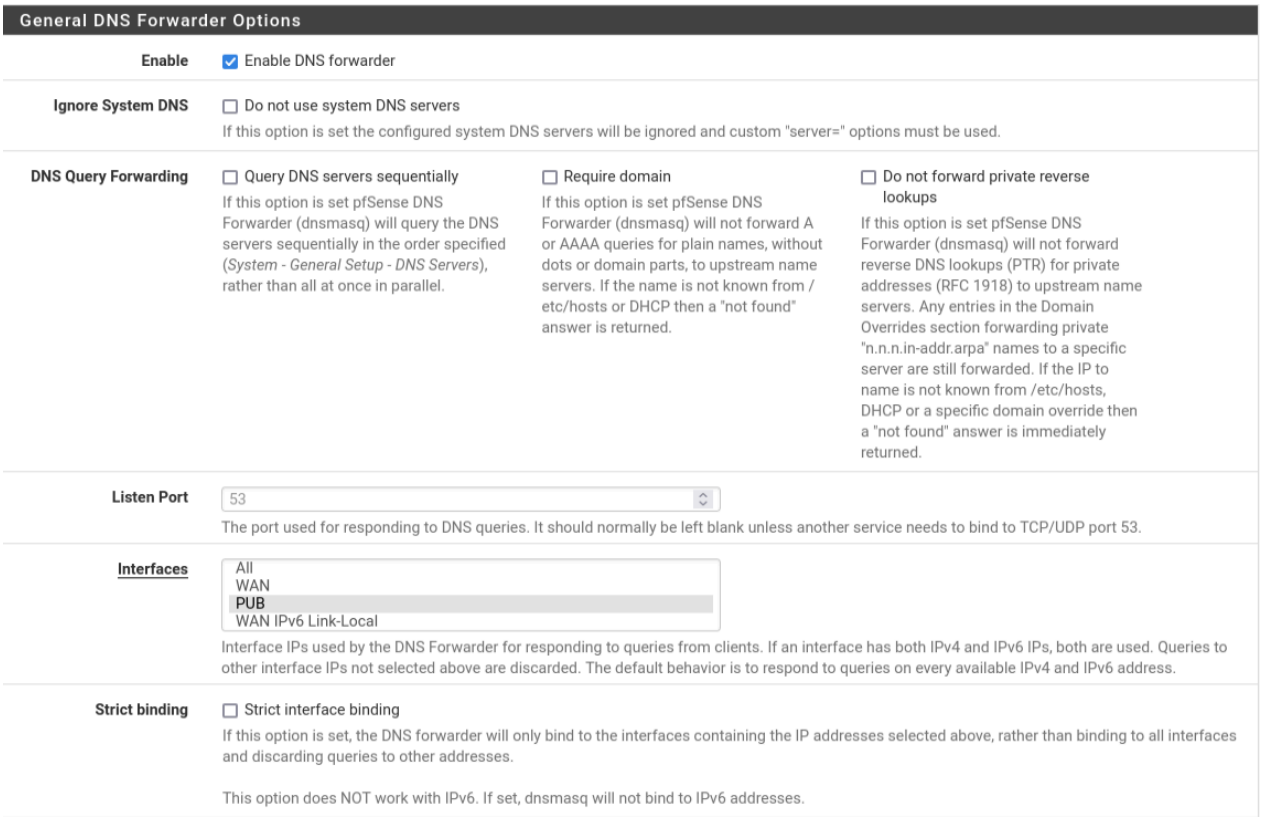
Le tableau de bord pfSense confirme le bon fonctionnement de la passerelle :

- interfaces actives,
- gateways opérationnelles,
- services DNS Forwarder et NTP actifs,
- absence d'erreurs critiques dans les logs.

Cela valide la stabilité de FGTW et son adéquation aux exigences d'administration sécurisée.


10.54.2.254
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
System Information
Name
Fgtw.sans.domaine
User
admin@10.54.2.0 (Local Database)
Version
2.8.0-RELEASE (amd64)
built on Tue Aug 12 16:59:00 UTC 2025
FreeBSD 15.0-CURRENT
Version 2.8.1 is available.
Version information updated at Wed Feb 4 9:07:30 UTC 2026
Uptime
00 Hour 17 Minutes 41 Seconds
Current date/time
Wed Feb 4 9:24:14 UTC 2026
DNS server(s)
192.168.51.254
Last config change
Wed Feb 4 9:03:27 UTC 2026
State table size
0% (9/96000) Show states
MBUF Usage
0% (4064/1000000)
CPU usage
Retrieving CPU data
Memory usage
30% of 968 MiB
SWAP usage
0% of 1024 MiB
Disks
Mount
Used
Size
Usage
/var
248K
41G
0% of 41G (zfs)
/
1.0G
42G
2% of 42G (zfs)
Interfaces
WAN
1000baseT <full-duplex>
192.168.51.26
PUB
1000baseT <full-duplex>
10.54.2.254
Gateways
Name
RTT
RTTsd
Loss
Status
WAN_DHCP
192.168.51.254
0.7ms
0.6ms
0.0%
Online
Services Status
Service
Description
Action
dnsmasq
DNS Forwarder
dpinger
Gateway Monitoring Daemon
syslogd
System Logger Daemon
NTP Status
NTP Server is disabled
Installed Packages
No packages installed.
Packages may be added/managed here: System -> Packages

Dns fowarder & NTP




## DNS Forwarder

Le service **dnsmasq** est activé pour la résolution et le relais DNS.
Les options clés configurées sont :

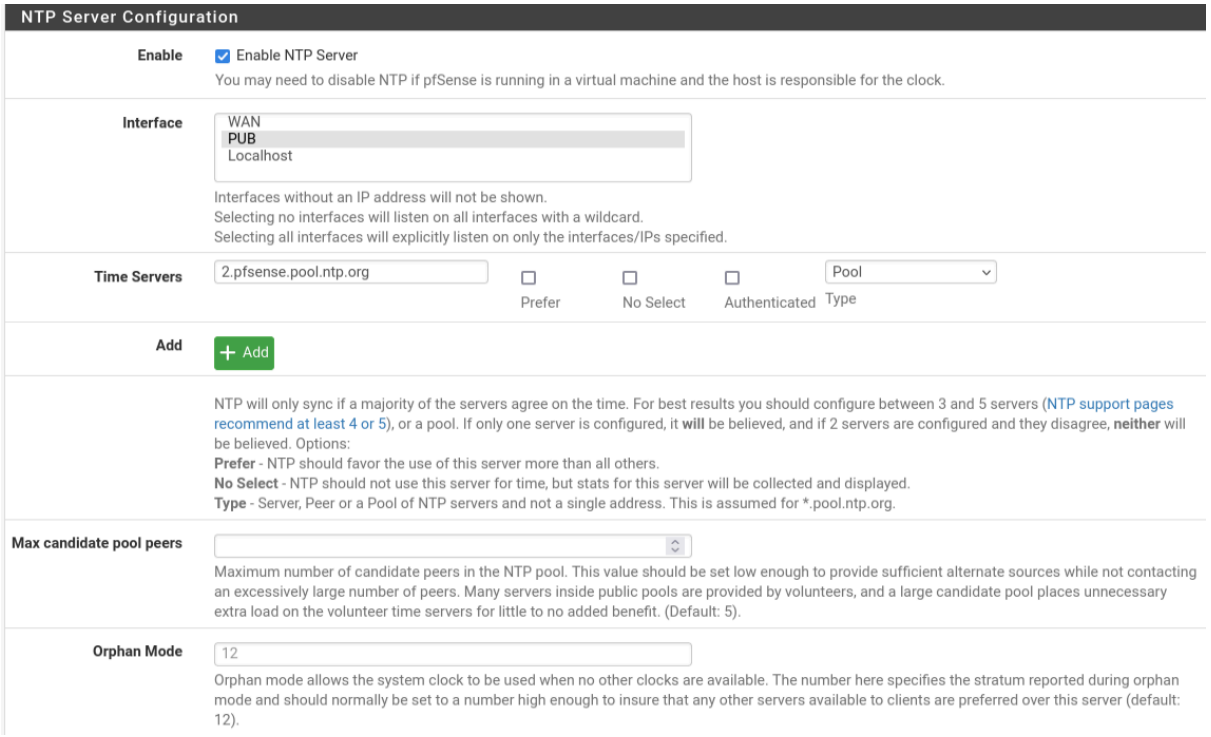
- *Enable DNS Forwarder*
- *Query DNS servers sequentially*
- *Strict interface binding*
- Écoute sur WAN et PUB

Ce service permet aux hôtes internes et DMZ d'obtenir une résolution DNS fiable tout en respectant l'architecture cloisonnée de la DMZ.

## NTP

Le service NTP est activé sur les interfaces WAN et PUB.
Les serveurs `*.pool.ntp.org` sont utilisés pour synchroniser l'horloge de la passerelle.

Cette synchronisation est essentielle pour la validité des certificats SSL/TLS et VPN.



**3. Gateways & Routes**

## Gateways

Deux passerelles sont définies :

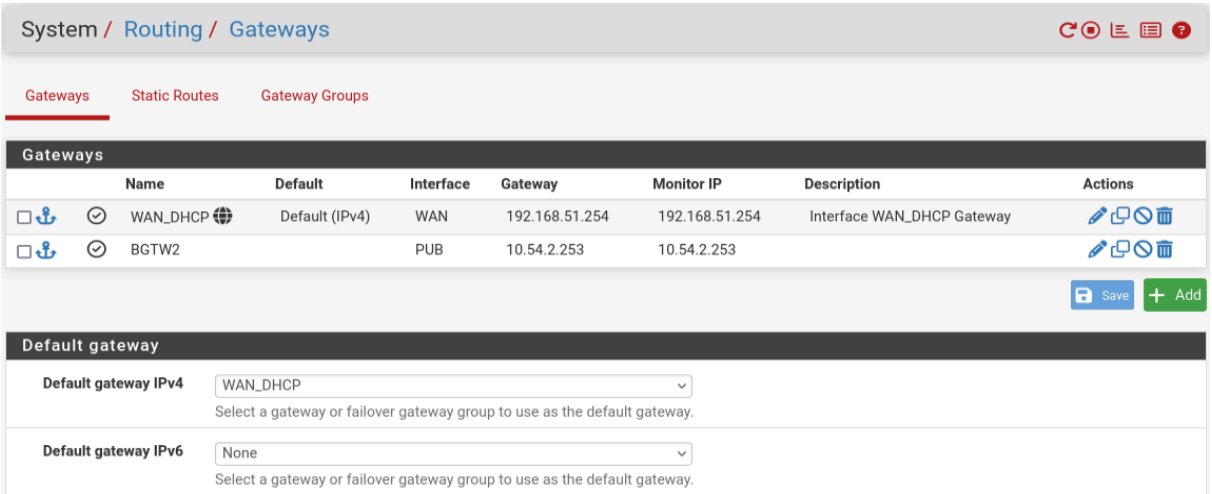
- **WAN_DHCP** comme route par défaut vers Internet.
- **BGTW2** sur l'interface PUB pour accéder aux réseaux internes situés derrière la passerelle dorsale.

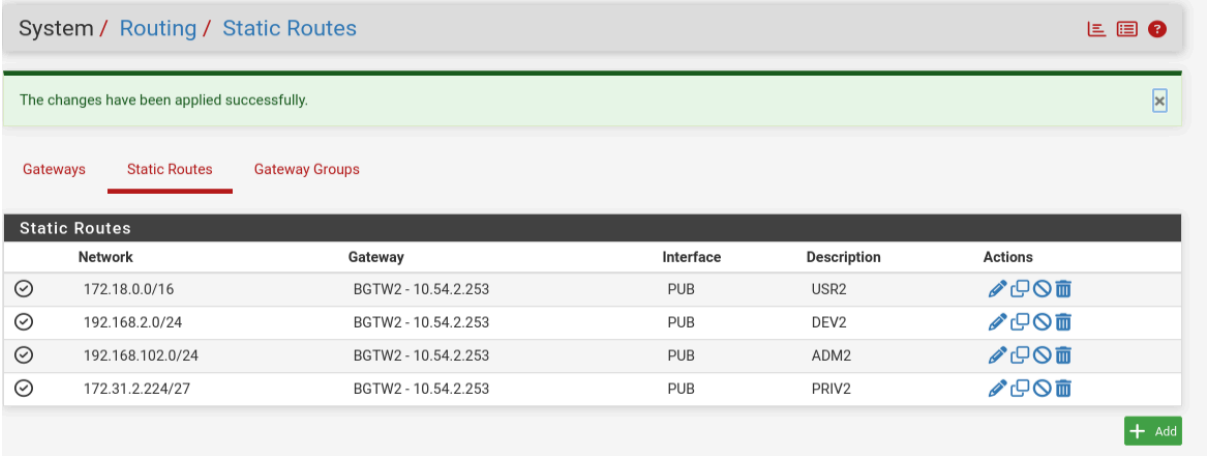
## Routes statiques

Des routes statiques sont ajoutées via **BGTW2** afin d'atteindre tous les sous-réseaux internes :

- 172.18.0.0/16 (Usr)
- 192.168.2.0/24 (Dev)
- 192.168.102.0/24 (Adm)
- 172.31.2.224/27 (Priv)

Ces routes permettent à FGTW de rediriger correctement les flux vers BGTW conformément à l'architecture hiérarchisée de la DMZ.





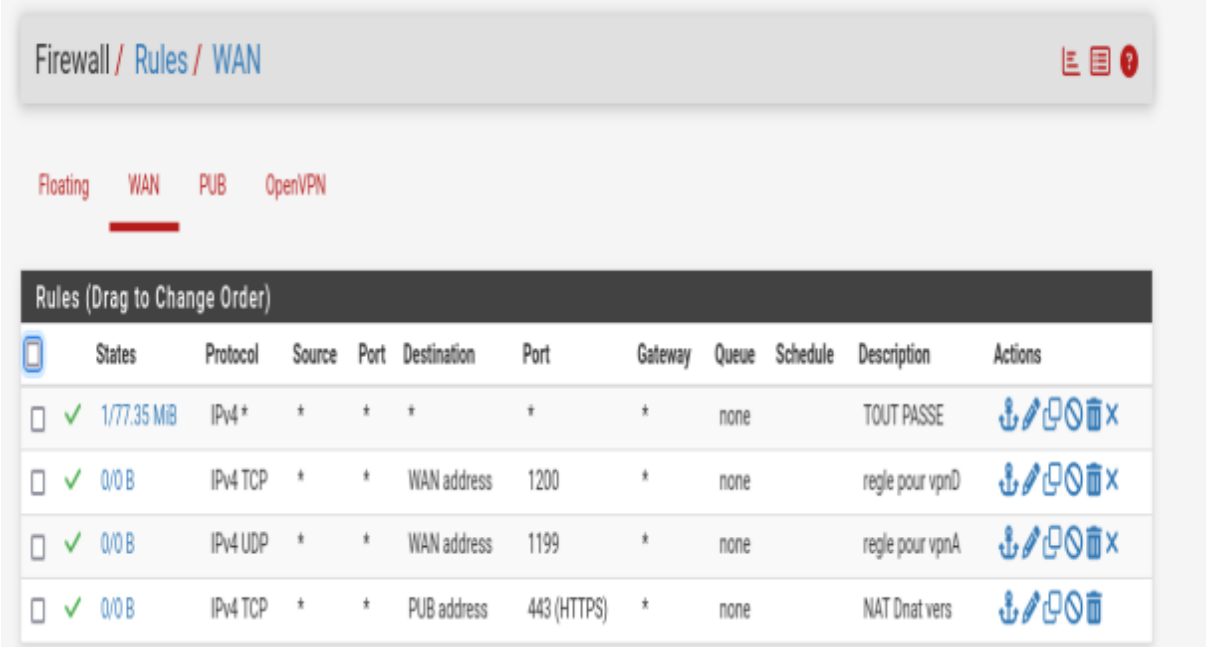

# Rules firewall

## wan :

Les règles configurées permettent :

- le passage temporaire de tous les flux (phase d'intégration),
- les connexions VPN : **UDP/1199** pour VpnA et **UDP/1200** pour VpnD,
- la redirection HTTPS (443) vers le serveur Web en DMZ publique (WebR).

Ces règles assurent l'accessibilité externe tout en respectant les protocoles imposés.

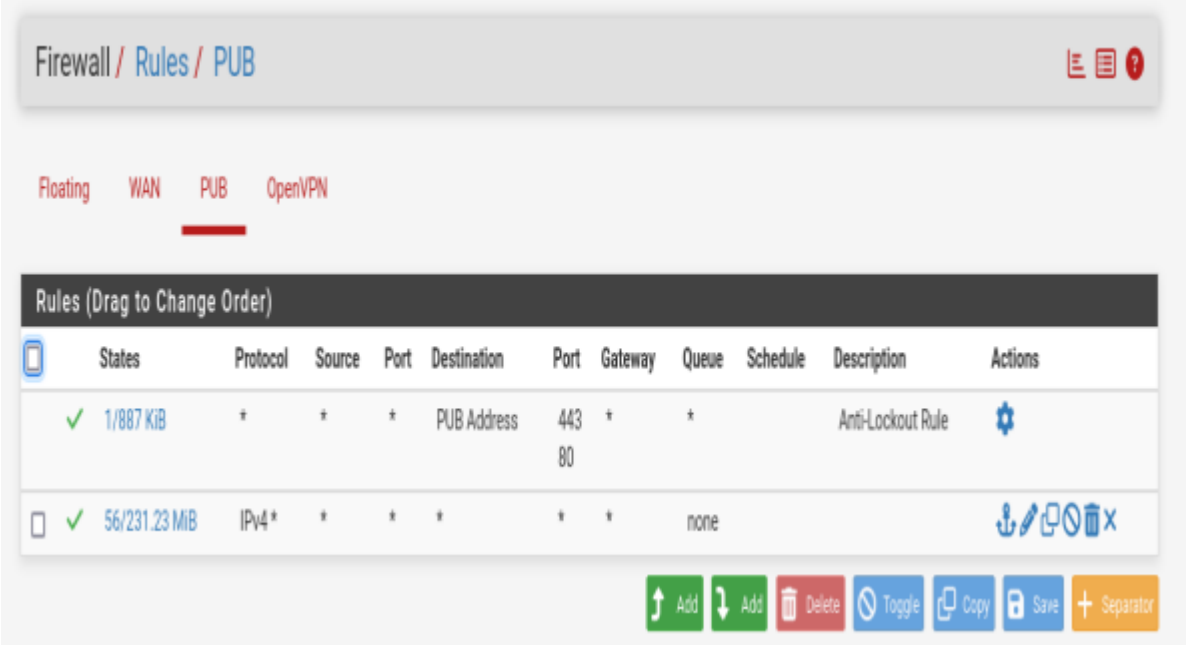



pub :

Les règles filtrent le trafic à destination de la DMZ publique en autorisant :

- le HTTPS sur **443**,
- le trafic interne nécessaire aux serveurs.

Les flux non autorisés sont bloqués pour empêcher les contournements en DMZ.




# Snat & DNAT

**DNAT (Port Forwarding)**

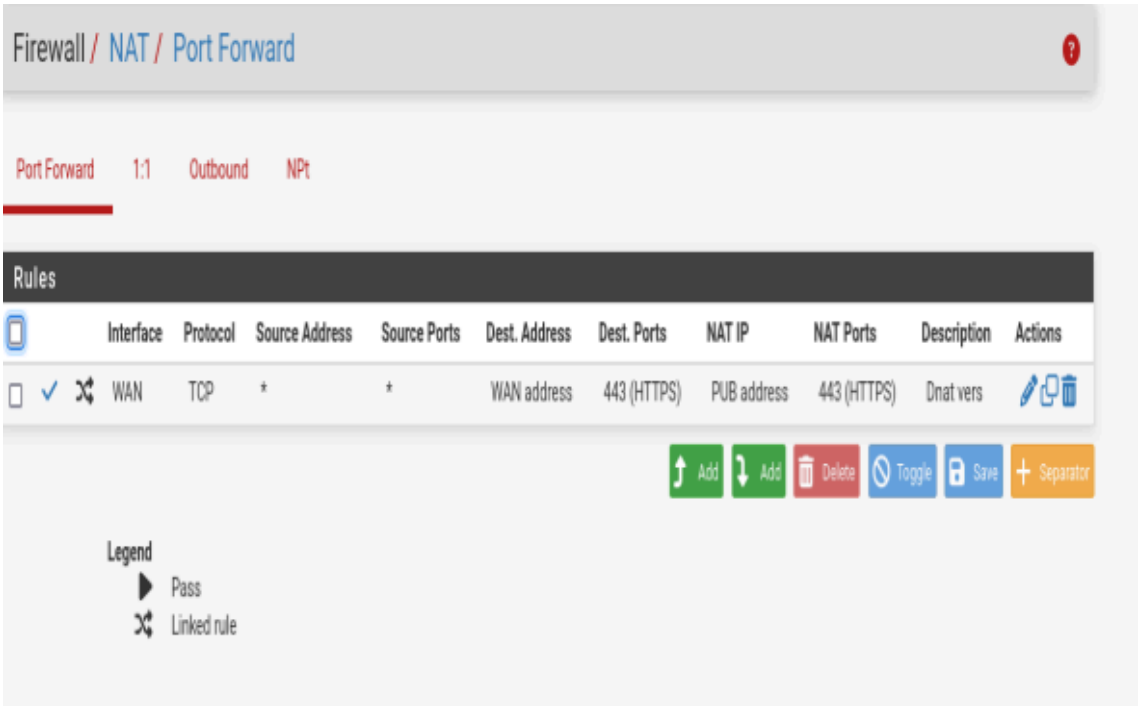
Une règle de redirection NAT est configurée pour exposer le serveur Web sécurisé :

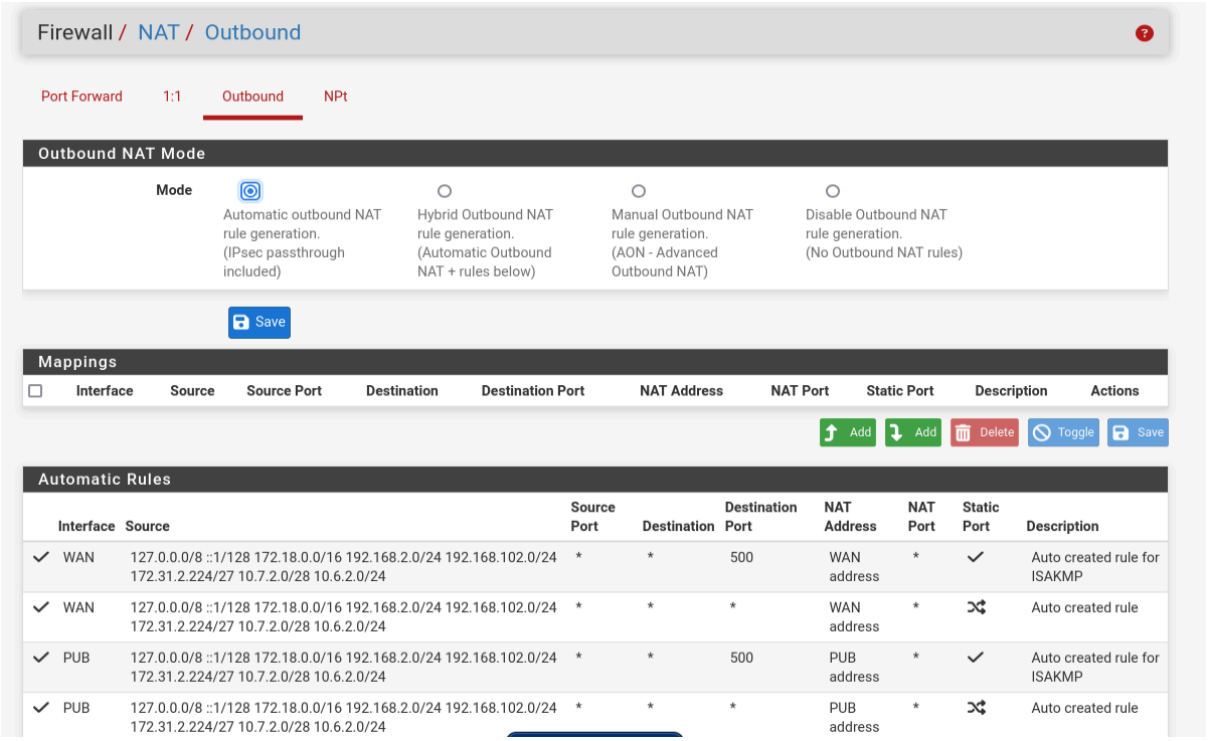
**WAN:443 → PUB:443 → WebR**

Cela permet l'accès externe à l'application Reservator en HTTPS sécurisé.

**SNAT**

Le mode NAT sortant automatique est activé.
Il garantit que tous les réseaux internes (Usr, Dev, Adm, Priv, VPN) utilisent l'adresse WAN de FGTW pour sortir sur Internet.




Firewall / NAT / Outbound
Port Forward
1:1
Outbound
NPt
Outbound NAT Mode
Mode
Automatic outbound NAT rule generation. (IPsec passthrough included)
Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
Disable Outbound NAT rule generation. (No Outbound NAT rules)
Save
Mappings
Interface Source Source Port Destination Destination Port NAT Address NAT Port Static Port Description Actions
Add
Add
Delete
Toggle
Save
Automatic Rules
Interface Source Source Port Destination Destination Port NAT Address NAT Port Static Port Description
WAN 127.0.0.0/8 ::1/128 172.18.0.0/16 192.168.2.0/24 192.168.102.0/24 172.31.2.224/27 10.7.2.0/28 10.6.2.0/24 * * 500 WAN address * Auto created rule for ISAKMP
WAN 127.0.0.0/8 ::1/128 172.18.0.0/16 192.168.2.0/24 192.168.102.0/24 172.31.2.224/27 10.7.2.0/28 10.6.2.0/24 * * * WAN address * Auto created rule
PUB 127.0.0.0/8 ::1/128 172.18.0.0/16 192.168.2.0/24 192.168.102.0/24 172.31.2.224/27 10.7.2.0/28 10.6.2.0/24 * * 500 PUB address * Auto created rule for ISAKMP
PUB 127.0.0.0/8 ::1/128 172.18.0.0/16 192.168.2.0/24 192.168.102.0/24 172.31.2.224/27 10.7.2.0/28 10.6.2.0/24 * * * PUB address * Auto created rule

# vpn serv & client :

**Serveurs OpenVPN**

Deux serveurs VPN routés sont configurés :

- **VpnA** pour les administrateurs (*UDP/1199*, réseau 10.7.2.0/28)
- **VpnD** pour les développeurs (*UDP/1200*, réseau 10.6.2.0/28)

Configurations :

- chiffrement **AES-256-GCM**
- authentification TLS + utilisateur
- clés DH 2048 bits

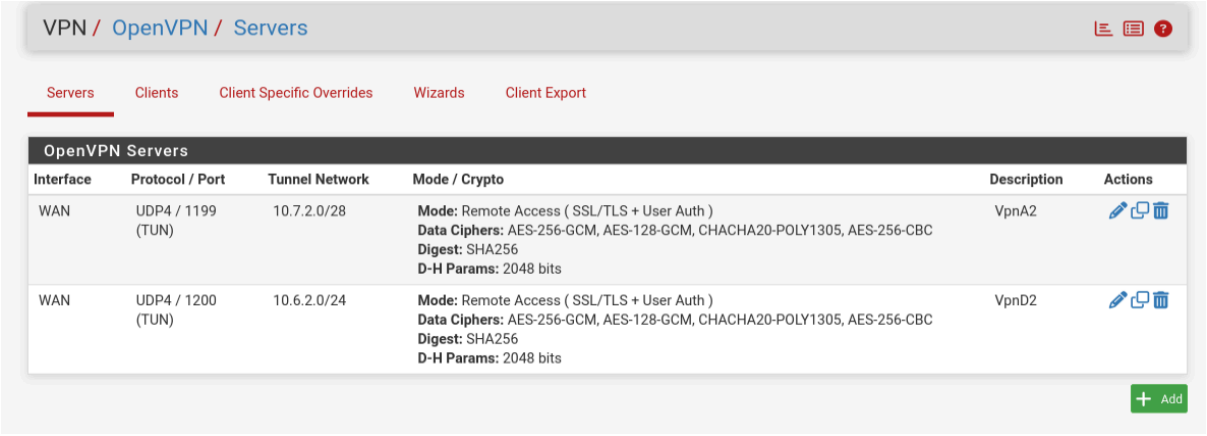
Ces VPN permettent un accès sécurisé aux ressources internes selon les rôles.

**Connexions clients**

Les captures montrent :

- une connexion réussie,
- l'attribution des IP virtuelles correctes (ex. 10.7.2.2 et 10.6.2.2),
- la communication opérationnelle vers la DMZ (Ping → 10.54.2.252 réussi).

Cela valide entièrement le routage, le filtrage et l'intégration VPN/DMZ.



connexion des vpn client :