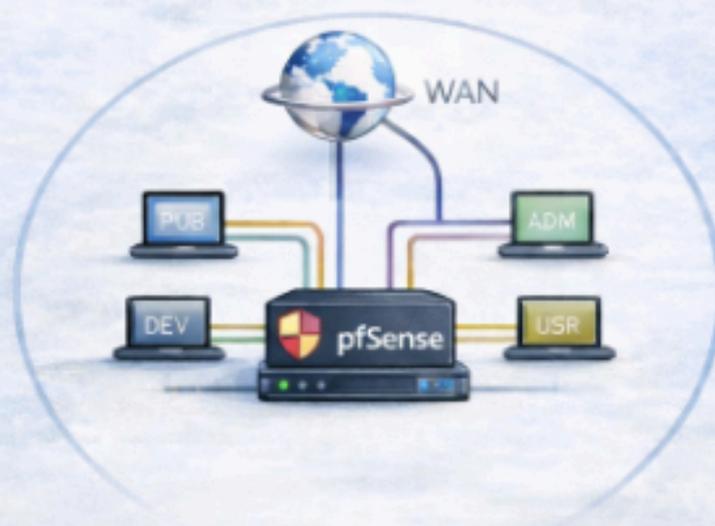




Rendu Technique de FGTW

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.

```
*** Welcome to pfSense 2.8.0-RELEASE (amd64) on Fgtw ***  
  
WAN (wan) -> em0 -> v4/DHCP4: 192.168.51.26/24  
PUB (lan) -> em1 -> v4: 10.54.2.254/24  
  
0) Logout / Disconnect SSH          9) pfTop  
1) Assign Interfaces                10) Filter Logs  
2) Set interface(s) IP address      11) Restart GUI  
3) Reset admin account and password 12) PHP shell + pfSense tools  
4) Reset to factory defaults        13) Update from console  
5) Reboot system                    14) Enable Secure Shell (sshd)  
6) Halt system                      15) Restore recent configuration  
7) Ping host                        16) Restart PHP-FPM  
8) Shell  
  
Enter an option:  
Message from syslogd@Fgtw at Feb  4 09:21:25 ...  
php-fpm[4381]: /services_dnsmasq.php: Successful login for user 'admin' from:  
54.2.0 (Local Database)
```

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 FGFW 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	Refresh
dpinger	Gateway Monitoring Daemon	Refresh
syslogd	System Logger Daemon	Refresh

NTP Status

NTP Server is disabled

Installed Packages

No packages installed.

Packages may be added/managed here: [System -> Packages](#)

Dns forwarder & NTP

General DNS Forwarder Options		
Enable	<input checked="" type="checkbox"/> Enable DNS forwarder	
Ignore System DNS	<input type="checkbox"/> Do not use system DNS servers If this option is set the configured system DNS servers will be ignored and custom "server=" options must be used.	
DNS Query Forwarding	<input type="checkbox"/> Query DNS servers sequentially If this option is set pfSense DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (System - General Setup - DNS Servers), rather than all at once in parallel.	<input type="checkbox"/> Require domain If this option is set pfSense DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned.
		<input type="checkbox"/> Do not forward private reverse lookups If this option is set pfSense DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the Domain Overrides section forwarding private "n.n.n.in-addr.arpa" names to a specific server are still forwarded. If the IP to name is not known from /etc/hosts, DHCP or a specific domain override then a "not found" answer is immediately returned.
Listen Port	<input type="text" value="53"/> The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.	
Interfaces	<div style="border: 1px solid #ccc; padding: 2px;"><input type="checkbox"/> All <input type="checkbox"/> WAN <input checked="" type="checkbox"/> PUB <input type="checkbox"/> WAN IPv6 Link-Local</div> Interface IPs used by the DNS Forwarder for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected above are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.	
Strict binding	<input type="checkbox"/> Strict interface binding If this option is set, the DNS forwarder will only bind to the interfaces containing the IP addresses selected above, rather than binding to all interfaces and discarding queries to other addresses. This option does NOT work with IPv6. If set, dnsmasq will not bind to IPv6 addresses.	

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](https://www.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.

NTP Server Configuration	
Enable	<input checked="" type="checkbox"/> Enable NTP Server You may need to disable NTP if pfSense is running in a virtual machine and the host is responsible for the clock.
Interface	<div style="border: 1px solid #ccc; padding: 5px;"><p>WAN PUB Localhost</p></div> <p>Interfaces without an IP address will not be shown. Selecting no interfaces will listen on all interfaces with a wildcard. Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.</p>
Time Servers	<input type="text" value="2.pfsense.pool.ntp.org"/> <input type="checkbox"/> Prefer <input type="checkbox"/> No Select <input type="checkbox"/> Authenticated <input type="text" value="Pool"/> Type
Add	<input type="button" value="+ Add"/>
	<p>NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers (NTP support pages recommend at least 4 or 5), or a pool. If only one server is configured, it will be believed, and if 2 servers are configured and they disagree, neither will be believed. Options: Prefer - NTP should favor the use of this server more than all others. No Select - NTP should not use this server for time, but stats for this server will be collected and displayed. Type - Server, Peer or a Pool of NTP servers and not a single address. This is assumed for *.pool.ntp.org.</p>
Max candidate pool peers	<input type="text" value="5"/> Maximum number of candidate peers in the NTP pool. This value should be set low enough to provide sufficient alternate sources while not contacting an excessively large number of peers. Many servers inside public pools are provided by volunteers, and a large candidate pool places unnecessary extra load on the volunteer time servers for little to no added benefit. (Default: 5).
Orphan Mode	<input type="text" value="12"/> Orphan mode allows the system clock to be used when no other clocks are available. The number here specifies the stratum reported during orphan mode and should normally be set to a number high enough to insure that any other servers available to clients are preferred over this server (default: 12).

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.

System / Routing / Gateways

Gateways Static Routes Gateway Groups

Gateways							
	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input type="checkbox"/>	WAN_DHCP	Default (IPv4)	WAN	192.168.51.254	192.168.51.254	Interface WAN_DHCP Gateway	
<input type="checkbox"/>	BGTW2		PUB	10.54.2.253	10.54.2.253		

Save Add

Default gateway

Default gateway IPv4: WAN_DHCP
Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6: None
Select a gateway or failover gateway group to use as the default gateway.

System / Routing / Static Routes

The changes have been applied successfully.

Gateways **Static Routes** Gateway Groups

Static Routes					
	Network	Gateway	Interface	Description	Actions
✓	172.18.0.0/16	BGTW2 - 10.54.2.253	PUB	USR2	  
✓	192.168.2.0/24	BGTW2 - 10.54.2.253	PUB	DEV2	  
✓	192.168.102.0/24	BGTW2 - 10.54.2.253	PUB	ADM2	  
✓	172.31.2.224/27	BGTW2 - 10.54.2.253	PUB	PRIV2	  

+ Add

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.

Firewall / Rules / WAN ☰ ☰ ?

Floating **WAN** PUB OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/77.35 MIB	IPv4*	*	*	*	*	*	none		TOUT PASSE	📌 ✎ 🔄 🗑️ ✕
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	WAN address	1200	*	none		regle pour vpnD	📌 ✎ 🔄 🗑️ ✕
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1199	*	none		regle pour vpnA	📌 ✎ 🔄 🗑️ ✕
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	PUB address	443 (HTTPS)	*	none		NAT Dnat vers	📌 ✎ 🔄 🗑️ ✕

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.

Firewall / Rules / PUB ☰ ⓘ

Floating WAN **PUB** OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/887 KiB	*	*	*	PUB Address	443 80	*	*		Anti-Lockout Rule	⚙️
☐ ✓ 56/231.23 MiB	IPv4*	*	*	*	*	*	none			⬇️ ✎ 📄 🗑️ ✕

⬆️ Add
⬇️ Add
🗑️ Delete
🔄 Toggle
📄 Copy
💾 Save
⊕ Separator

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.

The screenshot shows the Mikrotik Firewall configuration page for NAT Port Forward. The breadcrumb navigation is "Firewall / NAT / Port Forward". The current configuration is for a "Port Forward" rule with a "1:1" NAT type, "Outbound" direction, and "NPT" mode. The "Rules" table below shows a single rule with the following details:

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
WAN	TCP	*	*	WAN address	443 (HTTPS)	PUB address	443 (HTTPS)	Dnat vers	[Edit] [Delete]

Below the table, there are control buttons: "Add" (up arrow), "Add" (down arrow), "Delete" (trash), "Toggle" (power), "Save" (lock), and "Separator" (+). A legend indicates that a play button icon means "Pass" and a linked rule icon means "Linked rule".



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

<input type="checkbox"/>	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

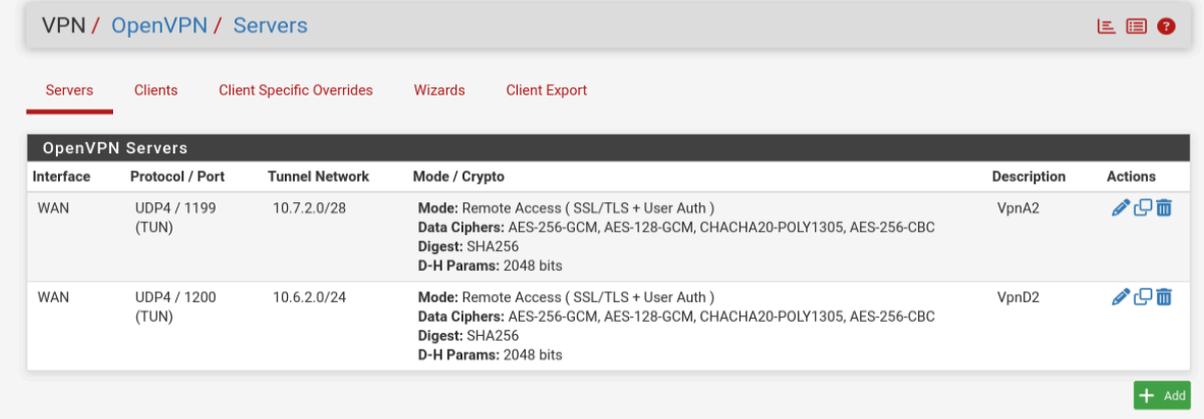
Ces VPN permettent un accès sécurisé aux ressources internes selon les rôles.

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.



The screenshot shows the OpenVPN web interface with the following configuration details:

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1199 (TUN)	10.7.2.0/28	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VpnA2	  
WAN	UDP4 / 1200 (TUN)	10.6.2.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VpnD2	  

At the bottom right of the interface, there is a green '+ Add' button.

