pfSense Plus : Firewall Open Source — Guide Complet

Guide complet pfSense Plus : installation, configuration du pare-feu, interfaces, VIP, règles, NAT, services réseaux, VPN IPsec et OpenVPN, Multi-WAN, Traffic Shaping et haute disponibilité. 9 chapitres avec travaux pratiques.

Systèmes Réseau 120 min de lecture Niveau Intermédiaire

Document généré le 11/07/2026 à 20h43 · nouvy.fr/wiki/pfsense-plus-firewall-guide-complet

Sommaire

120 section(s) · 120 min de lecture

Compétences à acquérir

À l'issue de ce guide, vous serez capable de :

- **Installer et configurer** pfSense Plus en tant que firewall/routeur
- **Créer et gérer** des règles de pare-feu, interfaces et adresses IP virtuelles
- **Maîtriser le NAT** (Port Forward, 1:1 NAT, Outbound NAT)
- **Configurer les services réseaux** (DHCP, DNS, NTP, SNMP)
- **Déployer des VPN** IPsec et OpenVPN (Site-to-Site et Point-to-Site)
- **Mettre en œuvre** le Multi-WAN, le Traffic Shaping et la haute disponibilité (CARP)

Table des matières

Chapitre 1 : Introduction à pfSense Plus

1.1 Qu'est-ce que pfSense ?

pfSense est une distribution **FreeBSD** spécialisée, transformant un ordinateur standard en un **firewall/routeur** de classe entreprise. pfSense Plus est la version commerciale supportée par **Netgate**.

> ***pfSense** signifie « **making sense of pf** » — pf étant le **Packet Filter** de OpenBSD/FreeBSD.*

Comparatif pfSense vs solutions commerciales

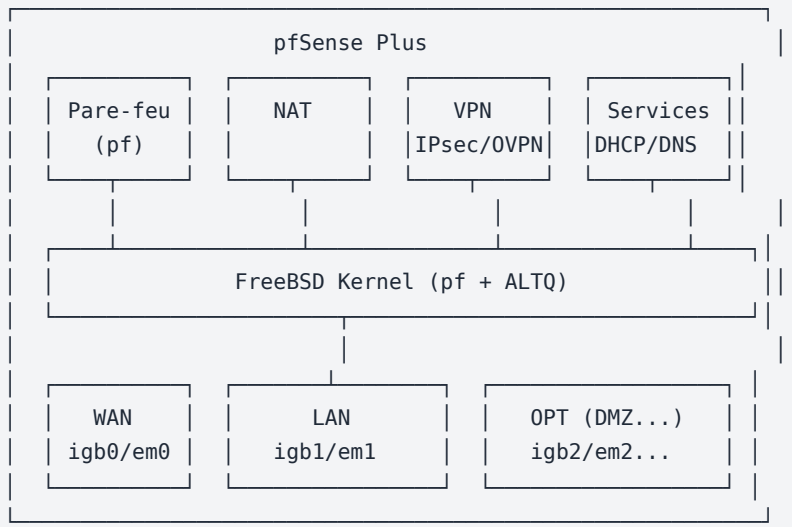
Critère	pfSense Plus	Cisco ASA	Fortinet FortiGate	Sophos XG
Coût licence	Gratuit (CE) / Abordable (Plus)	Élevé	Élevé	Moyen
Open Source	□ Oui (CE)	□ Non	□ Non	□ Non
Interface Web	□ Complète	⚠ ASDM	□ Complète	□ Complète
VPN intégré	□ IPsec + OpenVPN	□ AnyConnect	□ FortiClient	□ SSL VPN
Communauté	□ Très active	⚠ Moyenne	⚠ Moyenne	⚠ Moyenne
Mises à jour	□ Fréquentes	⚠ Payantes	⚠ Payantes	⚠ Payantes

1.2 Fonctionnalités principales

pfSense offre un ensemble complet de fonctionnalités :

Catégorie	Fonctionnalités
Pare-feu	Filtrage stateful, règles par interface, aliases, schedules
NAT	Port Forward, 1:1 NAT, Outbound NAT, NPt (IPv6)
VPN	IPsec, OpenVPN, WireGuard (via package)
Routage	Statique, OSPF, BGP (via FRR), Multi-WAN
Services	DHCP, DNS Resolver/Forwarder, NTP, SNMP
Monitoring	Logs temps réel, graphiques RRD, packet capture
HA	CARP, pfsync, XMLRPC sync
Packages	Squid, Snort/Suricata, HAProxy, pfBlockerNG, ntopng

1.3 Architecture de pfSense



Copier

1.4 Prérequis matériels

Configuration minimale

Composant	Minimum	Recommandé
CPU	64-bit (amd64)	Multi-core Intel/AMD
RAM	1 Go	4 Go+ (8 Go avec packages)
Stockage	8 Go	32 Go+ SSD
Interfaces réseau	2 (WAN + LAN)	3+ (WAN, LAN, DMZ)
Compatibilité	FreeBSD 14.x drivers	Intel NICs (igb, ix, ixl)

> ⚠ ***Cartes réseau** : Les cartes Intel (igb, em, ix, ixl) sont les plus fiables. Éviter les Realtek (re) en production.*

1.5 Installation de pfSense Plus

Étape 1 : Téléchargement de l'image

1. Se rendre sur https://www.pfsense.org/download/
2. Choisir :
    - **Architecture** : AMD64 (64-bit)
    - **Type d'image** : USB Memstick Installer (pour clé USB) ou ISO (pour VM)
    - **Console** : VGA (interface graphique d'installation)

Étape 2 : Création du média bootable

```
# Sous Linux/macOS — écrire l'image sur une clé USB
dd if=pfSense-CE-2.7.2-RELEASE-amd64.img.gz of=/dev/sdX bs=4M status=progress

# Sous Windows — utiliser Rufus ou Etcher
```

Copier

Étape 3 : Installation

Écran	Action
Boot	Sélectionner **Boot Multi User**
Copyright	Accepter les termes
Bienvenue	Choisir **Install pfSense**
Keymap	Sélectionner le clavier (French ISO)
Partitionnement	**Auto (ZFS)** recommandé pour la fiabilité
ZFS Configuration	stripe (1 disque) ou mirror (2 disques RAID1)
Installation	Attendre la copie des fichiers
Fin	**Reboot** et retirer le média

Étape 4 : Configuration initiale (console)

Après le premier démarrage, pfSense présente un menu console :

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) ***

 WAN (wan)       -> em0        -> v4: DHCP
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator 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
```

Copier

Configuration réseau initiale :

1. Option **1** — Assigner les interfaces :
   - WAN : `em0` (ou `igb0`)
   - LAN : `em1` (ou `igb1`)
2. Option **2** — Configurer les IP :
   - LAN : `192.168.1.1/24`, activer DHCP (plage : `.100` à `.254`)
   - WAN : DHCP (automatique) ou IP statique selon l'ISP

1.6 Interface Web (webConfigurator)

Accéder à l'interface depuis un poste connecté au LAN :

```
https://192.168.1.1
```

Copier

Paramètre	Valeur par défaut
URL	`https://192.168.1.1`
Utilisateur	`admin`
Mot de passe	`pfsense`

Assistant de configuration (Setup Wizard)

L'assistant guide les premiers paramétrages :

Étape	Configuration
1	Nom d'hôte (ex: `fw01`), domaine (ex: `local.lan`)
2	Serveurs DNS (ex: `1.1.1.1`, `8.8.8.8`)
3	Configuration du fuseau horaire et serveur NTP
4	Configuration de l'interface WAN (DHCP/Static/PPPoE)
5	Configuration de l'interface LAN (IP, masque)
6	Changement du mot de passe admin
7	Rechargement de la configuration

> ***IMPORTANT** : Toujours changer le mot de passe admin par défaut dès la première connexion !*

1.7 Navigation dans l'interface

L'interface webConfigurator est organisée en menus :

Menu	Contenu
System	Configuration générale, utilisateurs, certificats, packages, mises à jour
Interfaces	Configuration des interfaces réseau (WAN, LAN, OPTx)
Firewall	Règles, NAT, Aliases, Schedules, Traffic Shaper, Virtual IPs
Services	DHCP, DNS, NTP, SNMP, Dynamic DNS, IGMP Proxy
VPN	IPsec, OpenVPN, WireGuard
Status	Dashboard, logs, trafic, services, CARP, queues
Diagnostics	Ping, Traceroute, Packet Capture, DNS Lookup, pfTop

TP 1 : Mise en place d'un firewall pfSense

Objectifs

- Installer pfSense dans un environnement virtualisé
- Configurer les interfaces WAN et LAN
- Accéder à l'interface web et réaliser la configuration initiale
- Tester la connectivité de base

Topologie du lab

```
Internet
    |
    |  (NAT / Bridged)
    |
┌──────────────────┐
|   pfSense VM     |
|  WAN: DHCP (em0) |
|  LAN: 10.0.0.1/24|
|       (em1)      |
└──────────────────┘
    |
    | Réseau interne (Host-Only / Internal)
    |
┌──────────────────┐
|   Client VM      |
|  (Windows/Linux) |
|  IP: DHCP        |
|  10.0.0.x/24     |
└──────────────────┘
```

Copier

Étape 1 : Création de la VM pfSense

VirtualBox :

Paramètre	Valeur
Type	BSD → FreeBSD (64-bit)
RAM	2048 Mo
Disque	20 Go (VDI, dynamique)
Réseau Adapter 1	NAT (WAN)
Réseau Adapter 2	Réseau interne ou Host-Only (LAN)
ISO	pfSense-CE-2.7.2-RELEASE-amd64.iso

VMware Workstation :

Paramètre	Valeur
Type	Other → FreeBSD 14 64-bit
RAM	2048 Mo
Disque	20 Go
Network Adapter 1	NAT (WAN)
Network Adapter 2	Host-Only ou Custom (LAN)

Étape 2 : Installation

1. Démarrer la VM sur l'ISO
2. Suivre l'assistant d'installation (cf. section 1.5)
3. Redémarrer après installation

Étape 3 : Configuration des interfaces

Via la console pfSense :

```
Assign Interfaces:
  WAN -> em0
  LAN -> em1

Set LAN IP:
  IPv4 Address: 10.0.0.1
  Subnet: 24
  Enable DHCP: yes
  Start: 10.0.0.100
  End:   10.0.0.200
```

Copier

Étape 4 : Configuration du client

Sur la VM cliente (connectée au réseau LAN) :

```
# Vérifier l'obtention d'une IP via DHCP
ip addr show    # Linux
ipconfig        # Windows

# Résultat attendu : IP dans la plage 10.0.0.100-200
# Passerelle : 10.0.0.1
# DNS : 10.0.0.1
```

Copier

Étape 5 : Accès à l'interface web

1. Ouvrir un navigateur sur le client : `https://10.0.0.1`
2. Accepter l'avertissement de certificat auto-signé
3. Se connecter : `admin` / `pfsense`
4. Compléter le **Setup Wizard**

Étape 6 : Vérifications

Test	Commande / Action	Résultat attendu
Ping passerelle	`ping 10.0.0.1`	✅ Réponse
Ping Internet	`ping 8.8.8.8`	✅ Réponse
Résolution DNS	`nslookup google.com`	✅ Résolution
Accès web	Naviguer sur un site	✅ Page affichée

Livrables du TP

- ✅ pfSense installé et accessible via l'interface web
- ✅ Client obtient une IP via DHCP
- ✅ Client accède à Internet via pfSense
- ✅ Capture d'écran du Dashboard pfSense

Chapitre 2 : Le pare-feu — Interfaces, VIP et règles

2.1 Les interfaces réseau

Types d'interfaces

Type	Description	Exemple
WAN	Interface côté Internet	`em0` / `igb0`
LAN	Réseau local principal	`em1` / `igb1`
OPTx	Interfaces optionnelles (DMZ, WiFi, etc.)	`em2`, `em3`...
VLAN	Interface virtuelle 802.1Q	`em1.10`, `em1.20`
Bridge	Pont entre interfaces	`bridge0`
GIF	Tunnel GIF (IPv6 over IPv4)	`gif0`
GRE	Tunnel GRE	`gre0`
LAGG	Agrégation de liens (LACP)	`lagg0`

Configuration d'une interface

Interfaces → WAN (ou LAN, OPTx) :

Paramètre	Description
Enable	Activer l'interface
Description	Nom personnalisé (ex: `DMZ`, `WIFI`)
IPv4 Type	Static, DHCP, PPPoE, PPTP, None
IPv6 Type	Static, DHCP6, SLAAC, 6rd, Track Interface, None
MAC Address	Spoofing MAC si nécessaire
MTU	Taille maximale des trames (défaut: 1500)
MSS	Maximum Segment Size
Speed and Duplex	Négociation automatique ou forcée

Configuration d'un VLAN

Interfaces → VLANs → Add :

Champ	Valeur exemple
Parent Interface	`em1` (LAN physique)
VLAN Tag	`10`
VLAN Priority	`0` (défaut)
Description	`VLAN_SERVEURS`

Après création, assigner le VLAN via **Interfaces → Assignments** → onglet **Interface Assignments** → ajouter le VLAN comme nouvelle interface OPT.

```
Exemple de topologie VLAN :
                    ┌── VLAN 10 (Serveurs) : 10.10.10.0/24
em1 (trunk) ────────┼── VLAN 20 (Postes)   : 10.10.20.0/24
                    └── VLAN 30 (VoIP)     : 10.10.30.0/24
```

Copier

2.2 Adresses IP Virtuelles (VIP)

Les VIP permettent d'ajouter des adresses IP supplémentaires à pfSense, utiles pour le NAT, le HA ou l'hébergement multi-services.

Types de VIP

Type	Usage	Détails
IP Alias	Ajouter une IP sur une interface existante	Pas de failover, simple alias
CARP	Haute disponibilité (HA)	IP partagée entre 2 firewalls, failover automatique
Proxy ARP	NAT sans ajouter l'IP au système	pfSense répond aux requêtes ARP pour cette IP
Other	Usage spécial (IPsec, etc.)	IP de type « autre », pas de réponse ARP

Créer une VIP (IP Alias)

Firewall → Virtual IPs → Add :

Champ	Valeur
Type	IP Alias
Interface	WAN
Address(es)	`203.0.113.10/32`
Description	`VIP Web Server`

Créer une VIP CARP (pour HA)

Champ	Valeur
Type	CARP
Interface	LAN
Address(es)	`10.0.0.254/24`
Virtual IP Password	`secret123`
VHID Group	`1`
Advertising Frequency	Base: `1`, Skew: `0` (master)
Description	`CARP LAN VIP`

2.3 Aliases

Les **aliases** simplifient la gestion des règles en regroupant des IP, ports ou URL sous un nom logique.

Types d'aliases

Type	Contenu	Exemple
Host(s)	Adresses IP ou FQDN	`10.0.0.10`, `server.example.com`
Network(s)	Réseaux CIDR	`10.0.0.0/24`, `172.16.0.0/12`
Port(s)	Ports ou plages	`80`, `443`, `8000:8999`
URL (IPs)	Liste d'IP depuis une URL	URL vers une blocklist
URL Table (IPs)	Grande liste d'IP (optimisée)	Listes de menaces (>3000 entrées)

Créer un alias

Firewall → Aliases → Add :

```
Nom      : SERVEURS_WEB
Type     : Host(s)
Entrées  : 10.0.0.10, 10.0.0.11, 10.0.0.12
Description : Serveurs web internes
```

Copier

```
Nom      : PORTS_WEB
Type     : Port(s)
Entrées  : 80, 443, 8080
Description : Ports HTTP/HTTPS
```

Copier

2.4 Règles de pare-feu

Principes fondamentaux

Principe	Description
Évaluation top-down	Les règles sont évaluées de haut en bas, la première correspondance gagne
Deny implicite	Tout trafic non autorisé est bloqué (sauf sur le LAN par défaut)
Stateful	pfSense maintient une table d'états — le trafic retour est automatiquement autorisé
Par interface	Les règles s'appliquent au trafic **entrant** sur chaque interface
Anti-lockout	Règle spéciale sur le LAN empêchant de se bloquer soi-même (désactivable)

> ⚠ ***IMPORTANT*** *: Les règles sont évaluées sur le trafic* ***ENTRANT*** *de l'interface. Une règle sur WAN filtre le trafic venant d'Internet. Une règle sur LAN filtre le trafic venant du réseau local.*

Structure d'une règle

Champ	Options	Description
Action	Pass / Block / Reject	Autoriser / Bloquer (silencieux) / Rejeter (RST/ICMP)
Disabled	Checkbox	Désactiver sans supprimer
Interface	WAN, LAN, OPTx	Interface d'application
Address Family	IPv4, IPv6, IPv4+IPv6	Version IP
Protocol	TCP, UDP, ICMP, Any...	Protocole ciblé
Source	Any, Network, Alias, IP	Origine du trafic
Destination	Any, Network, Alias, IP	Destination du trafic
Dest. Port Range	Port, plage, alias	Port(s) de destination
Log	Checkbox	Journaliser les correspondances
Description	Texte libre	Toujours documenter vos règles !

Options avancées des règles

Option	Description
OS fingerprinting	Filtrer par système d'exploitation détecté
Schedule	Appliquer la règle selon un calendrier
Gateway	Forcer le trafic vers une passerelle spécifique (Policy Routing)
In/Out pipe	Appliquer un limiteur de bande passante
Ackqueue/Queue	Assigner à une queue de Traffic Shaping
Tag / Tagged	Marquer les paquets pour traitement ultérieur
State Type	Keep State, Sloppy State, Synproxy State, None
Max states	Limiter le nombre de connexions simultanées

Règles par défaut

Interface	Règle par défaut	Effet
WAN	Block all (implicite)	Tout est bloqué sauf le trafic de retour
LAN	Anti-lockout + Pass any to any	Tout le trafic LAN est autorisé
OPTx	Block all (implicite)	Tout est bloqué, à configurer manuellement

Exemples de règles courantes

Autoriser uniquement HTTP/HTTPS depuis le LAN :

Champ	Valeur
Action	Pass
Interface	LAN
Protocol	TCP
Source	LAN net
Destination	Any
Dest. Port Range	PORTS_WEB (alias)
Description	Autoriser navigation web

Bloquer l'accès à un réseau spécifique :

Champ	Valeur
Action	Block
Interface	LAN
Protocol	Any
Source	LAN net
Destination	10.10.30.0/24
Description	Bloquer accès au VLAN VoIP

> ***Bonnes pratiques*** *:*
>
> - Placer les règles **Block** avant les règles **Pass**
> - Toujours utiliser des **aliases** plutôt que des IP en dur
> - **Documenter** chaque règle avec une description claire
> - Activer le **log** sur les règles sensibles
> - Restreindre le LAN (supprimer le « pass any ») en production

2.5 Floating Rules

Les **Floating Rules** sont des règles spéciales qui peuvent s'appliquer sur plusieurs interfaces et dans les deux directions (in/out).

Caractéristique	Règle normale	Floating Rule
Interface	Une seule	Une ou plusieurs
Direction	In uniquement	In, Out, ou Any
Priorité	Après floating	Avant les règles normales
Quick	Toujours	Optionnel (si non Quick, continue l'évaluation)

Cas d'usage des Floating Rules

- Bloquer un trafic sur **toutes** les interfaces à la fois
- Appliquer du Traffic Shaping (direction Out)
- Règles de politique globale (ex: bloquer un pays)

Chapitre 3 : NAT 101 — Traduction de réseau

3.1 Rappel : qu'est-ce que le NAT ?

Le **NAT (Network Address Translation)** permet de traduire les adresses IP entre le réseau privé (LAN) et le réseau public (WAN). C'est une fonctionnalité essentielle de tout firewall.

Types de NAT dans pfSense

Type	Direction	Usage
Outbound NAT	LAN → WAN	Permet aux clients internes d'accéder à Internet
Port Forward	WAN → LAN	Redirige un port public vers un serveur interne
1:1 NAT	Bidirectionnel	Mappe une IP publique complète vers une IP privée
NPt	IPv6	Network Prefix Translation pour IPv6

3.2 Outbound NAT (Source NAT)

L'Outbound NAT traduit les adresses IP sources privées en adresse IP publique WAN lors de la sortie vers Internet.

Modes de l'Outbound NAT

Mode	Description
Automatic	pfSense crée automatiquement les règles NAT pour tous les réseaux internes
Hybrid	Règles automatiques + règles manuelles personnalisées (recommandé)
Manual	Uniquement les règles manuelles — contrôle total
Disable	Aucun NAT sortant — pour routage pur

> ***Recommandation** : Utiliser le mode **Hybrid** pour conserver les règles automatiques tout en ajoutant des règles personnalisées.*

Firewall → NAT → Outbound :

Créer une règle Outbound NAT manuelle

Champ	Valeur	Description
Interface	WAN	Interface de sortie
Address Family	IPv4	
Protocol	Any	
Source	10.0.0.0/24	Réseau source (LAN)
Destination	Any	
Translation Address	Interface Address	Utiliser l'IP WAN
Translation Port	(vide)	Port source aléatoire
Static Port	☐	Cocher pour SIP/gaming si besoin

> ⚠ ***Static Port** : Certaines applications (SIP, jeux en ligne, IPsec passthrough) nécessitent que le port source ne soit pas modifié. Cocher cette option dans ce cas.*

3.3 Port Forward (Destination NAT)

Le **Port Forward** redirige le trafic arrivant sur un port spécifique de l'IP WAN vers un serveur interne.

Firewall → NAT → Port Forward → Add :

Exemple : Rediriger le trafic web vers un serveur interne

Champ	Valeur
Interface	WAN
Address Family	IPv4
Protocol	TCP
Destination	WAN Address
Dest. Port Range	HTTP (80)
Redirect Target IP	10.0.0.10
Redirect Target Port	HTTP (80)
Description	Port Forward HTTP vers serveur web
Filter Rule Association	Add associated filter rule

> 💡 *L'option **Filter Rule Association** crée automatiquement la règle de firewall correspondante sur l'interface WAN. Choisir « Add associated filter rule » pour simplifier la configuration.*

Exemples courants de Port Forward

Service	Port externe	IP interne	Port interne
Serveur Web (HTTP)	80	10.0.0.10	80
Serveur Web (HTTPS)	443	10.0.0.10	443
Serveur SSH	2222	10.0.0.20	22
Bureau à distance (RDP)	33389	10.0.0.30	3389
Serveur Mail (SMTP)	25	10.0.0.40	25
Serveur FTP	21	10.0.0.50	21
Minecraft	25565	10.0.0.60	25565

> ⚠ ***Sécurité** : Ne jamais exposer directement des ports sensibles (SSH 22, RDP 3389) sur les ports standards. Utiliser des ports non standard (ex: 2222 pour SSH) et activer le log.*

3.4 NAT 1:1

Le NAT 1:1 crée un mapping complet entre une **IP publique** et une **IP privée**. Tout le trafic entrant sur l'IP publique est redirigé vers l'IP privée, et tout le trafic sortant de l'IP privée utilise cette IP publique.

Firewall → NAT → 1:1 → Add :

Champ	Valeur
Interface	WAN
External subnet IP	203.0.113.10
Internal IP	10.0.0.10
Destination	Any
Description	NAT 1:1 pour serveur web principal

Quand utiliser le NAT 1:1 ?

Scénario	Port Forward	1:1 NAT
Rediriger quelques ports	Idéal	Overkill
Serveur avec beaucoup de ports	⚠ Fastidieux	Idéal
IP publique dédiée par serveur		Parfait
Conservation des ports source		Automatique

> ***Prérequis** : Le NAT 1:1 nécessite une **VIP** (Virtual IP) sur l'interface WAN pour l'adresse IP publique externe (sauf si c'est l'IP WAN principale).*

3.5 NAT Reflection

Le **NAT Reflection** (ou **NAT Hairpinning**) permet aux clients internes d'accéder aux services internes via l'adresse IP **publique** (WAN).

Problème sans NAT Reflection

```
Client LAN (10.0.0.50) → accède à http://203.0.113.1 (IP publique)
  → Le paquet arrive sur le WAN de pfSense
  → Port forward vers 10.0.0.10 (serveur web)
  → Le serveur répond directement à 10.0.0.50 (même LAN)
  → Le client rejette la réponse (source IP inattendue) 
```

Copier

Configuration

System → Advanced → Firewall & NAT :

Option	Recommandation
NAT Reflection mode for port forwards	**Pure NAT**
NAT Reflection mode for 1:1	**Enable**
Automatic outbound NAT for Reflection	**Enable**

3.6 NPt (Network Prefix Translation IPv6)

Le NPt traduit les préfixes IPv6 entre réseaux, permettant une forme de NAT pour IPv6 (bien que controversée).

Firewall → NAT → NPt → Add :

Champ	Valeur
Interface	WAN
Internal IPv6 Prefix	`fd00:1::/64` (ULA)
Destination IPv6 Prefix	`2001:db8:1::/64` (GUA du FAI)

3.7 Dépannage du NAT

Outils de diagnostic

Outil	Chemin	Usage
States	Diagnostics → States	Voir les connexions NAT actives
Packet Capture	Diagnostics → Packet Capture	Capturer le trafic sur une interface
pfTop	Diagnostics → pfTop	Voir les connexions en temps réel
System Logs	Status → System Logs → Firewall	Vérifier les règles bloquantes

Checklist de dépannage Port Forward

1. ☐ La règle de Port Forward existe dans **Firewall → NAT → Port Forward**
2. ☐ Une règle de firewall correspondante existe sur l'interface WAN
3. ☐ Le serveur interne écoute bien sur le bon port
4. ☐ La passerelle par défaut du serveur interne pointe vers pfSense
5. ☐ Pas de firewall local sur le serveur bloquant le port
6. ☐ NAT Reflection configuré si test depuis le LAN
7. ☐ Vérifier dans **Diagnostics → States** si la connexion apparaît

---

Chapitre 4 : pfSense — Les Services réseaux

4.1 Serveur DHCP

pfSense intègre un serveur DHCP complet basé sur **ISC DHCP** (ou Kea DHCP dans les versions récentes).

Services → DHCP Server (onglet par interface) :

Configuration du pool DHCP

Paramètre	Valeur exemple	Description
Enable	☑	Activer le DHCP sur cette interface
Range From	`10.0.0.100`	Début de la plage
Range To	`10.0.0.200`	Fin de la plage
DNS Servers	`10.0.0.1`	Serveurs DNS distribués aux clients
Gateway	`10.0.0.1`	Passerelle par défaut
Domain Name	`local.lan`	Nom de domaine
Default Lease Time	`7200`	Bail par défaut (secondes)
Maximum Lease Time	`86400`	Bail maximum (secondes)
NTP Servers	`10.0.0.1`	Serveur NTP
TFTP Server	`10.0.0.5`	Pour le boot PXE

Mappages statiques (réservation DHCP)

Permet d'attribuer toujours la même IP à un périphérique via son adresse MAC.

Services → DHCP Server → [interface] → DHCP Static Mappings :

Champ	Valeur
MAC Address	`aa:bb:cc:dd:ee:ff`
IP Address	`10.0.0.10`
Hostname	`srv-web01`
Description	`Serveur Web principal`

Options avancées DHCP

Option	Usage
DHCP Relay	Relayer les requêtes vers un serveur DHCP externe
Additional Pools	Créer plusieurs plages sur la même interface
Custom Options	Options DHCP personnalisées (option 66, 150 pour VoIP, PXE)
MAC Allow/Deny	Contrôle d'accès par adresse MAC
Dynamic DNS	Enregistrement automatique des clients dans le DNS

4.2 DNS Resolver (Unbound)

Le **DNS Resolver** utilise **Unbound**, un résolveur DNS récursif, validant et cachant les requêtes DNS.

Services → DNS Resolver :

Configuration principale

Paramètre	Recommandation	Description
Enable	☑	Activer le résolveur DNS
Listen Port	53	Port d'écoute
Network Interfaces	All	Interfaces d'écoute
Outgoing Interfaces	WAN	Interface pour les requêtes sortantes
DNSSEC	☑ Enable	Validation DNSSEC (sécurité DNS)
DNS Query Forwarding	☐ ou ☑ selon besoin	Transférer les requêtes vers un serveur upstream
TLS for forwarding	☑ si forwarding activé	DNS over TLS (DoT) vers le serveur upstream

Host Overrides (entrées DNS locales)

Permet de créer des entrées DNS personnalisées :

Champ	Valeur
Host	`srv-web01`
Domain	`local.lan`
IP Address	`10.0.0.10`
Description	`Serveur Web`

→ `srv-web01.local.lan` résoudra en `10.0.0.10`

Domain Overrides

Redirige les requêtes DNS d'un domaine vers un serveur DNS spécifique :

Champ	Valeur
Domain	`ad.corp.local`
IP Address	`10.10.10.5`
Description	`Serveur AD pour le domaine interne`

> ☑ *Utile pour les environnements avec Active Directory : les requêtes pour le domaine AD sont envoyées au contrôleur de domaine.*

DNS Resolver vs DNS Forwarder

Caractéristique	DNS Resolver (Unbound)	DNS Forwarder (dnsmasq)
Type	Récursif	Forwarding uniquement
DNSSEC	✅ Natif	❌ Non supporté
Performance	Excellent (cache)	Bon (léger)
Contrôle	Très granulaire	Basique
Cas d'usage	Production	Petits réseaux / split DNS

4.3 Serveur NTP

pfSense peut servir de serveur NTP pour synchroniser l'horloge de tous les périphériques du réseau.

Services → NTP :

Paramètre	Valeur recommandée
Interface	LAN (et OPTx si besoin)
Time Servers	`0.fr.pool.ntp.org`, `1.fr.pool.ntp.org`, `2.fr.pool.ntp.org`
Orphan Mode	`12`
NTP Graphs	✅ Enable (monitoring RRD)

> ✅ *Configurer les clients (Windows, Linux) pour pointer vers l'IP LAN de pfSense comme serveur NTP unique.*

4.4 SNMP

Le service **SNMP** permet la supervision de pfSense par des outils comme Zabbix, PRTG, LibreNMS ou Nagios.

Services → SNMP :

Paramètre	Valeur
Enable	✅
Polling Port	`161`
System Location	`Salle serveur Paris`
System Contact	`admin@example.com`
Community String	`maCommunauteSNMP` (changer le défaut !)
Bind Interfaces	LAN uniquement

> ⚠ ***Sécurité** : Ne jamais exposer SNMP sur le WAN. Utiliser SNMPv3 si disponible pour le chiffrement.*

4.5 Dynamic DNS

Permet de mettre à jour automatiquement un nom de domaine avec l'IP WAN dynamique.

Services → Dynamic DNS → Add :

Champ	Valeur
Service Type	Cloudflare, DynDNS, No-IP, OVH, etc.
Interface to Monitor	WAN
Hostname	`firewall.example.com`
Username	(selon fournisseur)
Password	(selon fournisseur)
Update URL	(auto-rempli selon le service)

4.6 Wake on LAN

Services → Wake on LAN :

Permet de réveiller des machines du réseau à distance en envoyant un **Magic Packet**.

Champ	Valeur
Interface	LAN
MAC Address	`aa:bb:cc:dd:ee:ff`

4.7 IGMP Proxy

Pour relayer le trafic **multicast** (IPTV, streaming) entre les interfaces.

Services → IGMP Proxy :

Interface	Type	Description
WAN	Upstream	Reçoit le multicast du FAI
LAN	Downstream	Distribue le multicast au réseau local

TP 1 : Configuration avancée du firewall pfSense

Objectifs

- Créer des VLANs (DATA, VOIX, MGMT) et configurer le routage inter-VLAN
- Mettre en place des aliases et des règles de firewall granulaires
- Configurer le NAT (Port Forward + Outbound)
- Configurer les services DHCP et DNS

Adressage par groupe

Chaque groupe travaille avec sa propre plage d'adresses. Repérez votre groupe et utilisez les adresses correspondantes pour tout le TP.

Groupe 1 — Plage : 10.1.10.0 — 10.1.30.0

VLAN ID	Rôle	Réseau	Passerelle
10	DATA	10.1.10.0/24	10.1.10.1
20	VOIX	10.1.20.0/24	10.1.20.1
30	MGMT	10.1.30.0/24	10.1.30.1

Groupe 2 — Plage : 10.2.10.0 — 10.2.30.0

VLAN ID	Rôle	Réseau	Passerelle
40	DATA	10.2.10.0/24	10.2.10.1
50	VOIX	10.2.20.0/24	10.2.20.1
60	MGMT	10.2.30.0/24	10.2.30.1

Groupe 3 — Plage : 10.3.10.0 — 10.3.30.0

VLAN ID	Rôle	Réseau	Passerelle
70	DATA	10.3.10.0/24	10.3.10.1
80	VOIX	10.3.20.0/24	10.3.20.1
90	MGMT	10.3.30.0/24	10.3.30.1

Groupe 4 — Plage : 10.4.10.0 — 10.4.30.0

VLAN ID	Rôle	Réseau	Passerelle
100	DATA	10.4.10.0/24	10.4.10.1
110	VOIX	10.4.20.0/24	10.4.20.1
120	MGMT	10.4.30.0/24	10.4.30.1

Groupe 5 — Plage : 10.5.10.0 — 10.5.30.0

VLAN ID	Rôle	Réseau	Passerelle
130	DATA	10.5.10.0/24	10.5.10.1
140	VOIX	10.5.20.0/24	10.5.20.1
150	MGMT	10.5.30.0/24	10.5.30.1

Groupe 6 — Plage : 10.6.10.0 — 10.6.30.0

VLAN ID	Rôle	Réseau	Passerelle
160	DATA	10.6.10.0/24	10.6.10.1
170	VOIX	10.6.20.0/24	10.6.20.1
180	MGMT	10.6.30.0/24	10.6.30.1

Groupe 7 — Plage : 10.7.10.0 — 10.7.30.0

VLAN ID	Rôle	Réseau	Passerelle
190	DATA	10.7.10.0/24	10.7.10.1
200	VOIX	10.7.20.0/24	10.7.20.1
210	MGMT	10.7.30.0/24	10.7.30.1

> 📝 ***Convention de notation** : dans les exercices ci-dessous, `VLAN_DATA`, `VLAN_VOIX` et `VLAN_MGMT` font référence aux VLANs de **votre groupe**. Remplacez par vos valeurs réelles.*

Topologie

Copier

Exercice 1 : Configuration des VLANs

1. Créer les 3 VLANs sur pfSense (les tags correspondent à votre groupe) :
   - **VLAN DATA** sur l'interface parent LAN (`em1`) → description : `DATA`
   - **VLAN VOIX** sur l'interface parent LAN (`em1`) → description : `VOIX`
   - **VLAN MGMT** sur l'interface parent LAN (`em1`) → description : `MGMT`

2. Assigner les VLANs comme interfaces OPT1, OPT2 et OPT3
3. Configurer les IP passerelle sur chaque interface (selon votre tableau de groupe)
4. Activer le **DHCP** sur chaque VLAN :

VLAN	Plage DHCP (exemple Groupe 1)	Passerelle	DNS
DATA	`.100` → `.200`	`.1`	`.1`
VOIX	`.100` → `.200`	`.1`	`.1`
MGMT	`.100` → `.200`	`.1`	`.1`

> ⚠ *Sur le VLAN VOIX, ajouter l'**option DHCP 66** (TFTP Server) si des téléphones IP sont présents, et l'**option 150** pour les téléphones Cisco.*

Exercice 2 : Règles de firewall avec aliases

1. Créer les aliases (adapter les IP à votre groupe) :
   - `SERVEURS_WEB` (Hosts) : premier et deuxième serveur du VLAN DATA (ex G1 : `10.1.10.10`, `10.1.10.11`)
   - `PORTS_WEB` (Ports) : `80`, `443`
   - `PORTS_VOIP` (Ports) : `5060`, `5061`, `10000:20000`
   - `DNS_PUBLICS` (Hosts) : `1.1.1.1`, `8.8.8.8`
   - `VLAN_ALL` (Networks) : les 3 réseaux de votre groupe
2. Configurer les règles sur le **VLAN DATA** :

#	Action	Source	Destination	Port	Description
1	Pass	DATA net	DNS_PUBLICS	53 (TCP/UDP)	Autoriser DNS
2	Pass	DATA net	Any	PORTS_WEB	Navigation Internet + mises à jour
3	Block	DATA net	VLAN VOIX net	Any	Isoler le VLAN VOIX
4	Block	DATA net	VLAN MGMT net	Any	Isoler le VLAN MGMT
5	Block	DATA net	Any	Any	Bloquer tout le reste

3. Configurer les règles sur le **VLAN VOIX** :

#	Action	Source	Destination	Port	Description
1	Pass	VOIX net	Any	PORTS_VOIP	Autoriser SIP + RTP
2	Pass	VOIX net	DNS_PUBLICS	53	DNS pour les téléphones
3	Block	VOIX net	DATA net	Any	Isoler le VLAN DATA
4	Block	VOIX net	MGMT net	Any	Isoler le VLAN MGMT
5	Block	VOIX net	Any	Any	Bloquer tout le reste

4. Configurer les règles sur le **VLAN MGMT** :

#	Action	Source	Destination	Port	Description
1	Pass	MGMT net	VLAN_ALL	443	Accès HTTPS aux équipements
2	Pass	MGMT net	VLAN_ALL	22	Accès SSH aux équipements
3	Pass	MGMT net	Any	PORTS_WEB	Navigation Internet
4	Pass	MGMT net	DNS_PUBLICS	53	DNS
5	Block	MGMT net	Any	Any	Bloquer tout le reste

> ⚠ *L'ordre est crucial : les règles **Pass** spécifiques doivent toujours être **avant** les règles **Block** générales. Le VLAN MGMT est le seul à pouvoir accéder aux autres VLANs (administration).*

Exercice 3 : Port Forward

Rendre le serveur web interne du VLAN DATA accessible depuis Internet (adapter l'IP à votre groupe) :

1. Créer le Port Forward :
    - Interface : WAN
    - Port externe : `80` et `443`
    - IP cible : premier serveur du VLAN DATA (ex G1 : `10.1.10.10`)
    - Port cible : `80` et `443`
2. Vérifier que la règle WAN associée a été créée
3. Tester depuis une machine externe ou depuis pfSense (Diagnostics → Test Port)

Exercice 4 : DNS Resolver

1. Configurer les Host Overrides (adapter à votre groupe) :
    - `srv-web01.local.lan` → IP du premier serveur DATA
    - `srv-web02.local.lan` → IP du deuxième serveur DATA
    - `phone01.local.lan` → IP du premier téléphone VOIX
2. Activer le DNSSEC
3. Tester la résolution depuis un client :

```
nslookup srv-web01.local.lan <IP_PASSERELLE_DATA>
```

Copier

Exercice 5 : Vérifications et tests inter-VLAN

Valider l'isolation et les accès autorisés :

Depuis	Vers	Test	Résultat attendu
DATA	Internet	`ping 8.8.8.8`	✅ Autorisé
DATA	VOIX	`ping <IP_VOIX>`	❌ Bloqué
DATA	MGMT	`ping <IP_MGMT>`	❌ Bloqué
VOIX	DATA	`ping <IP_DATA>`	❌ Bloqué
VOIX	Internet (port 5060)	Test SIP	✅ Autorisé
MGMT	DATA	`ping <IP_DATA>`	❌ Bloqué (ICMP non autorisé)
MGMT	DATA	`https://<IP_DATA>`	✅ Autorisé (port 443)
MGMT	VOIX	`ssh <IP_VOIX>`	✅ Autorisé (port 22)
MGMT	Internet	Navigation web	✅ Autorisé

Livrables

- ✅ 3 VLANs créés (DATA, VOIX, MGMT) avec les adressages de votre groupe
- ✅ DHCP fonctionnel sur chaque VLAN
- ✅ Règles de firewall avec aliases testées et validées
- ✅ Isolation inter-VLAN vérifiée (DATA ↔ VOIX bloqué, MGMT → tous autorisé en HTTPS/SSH)
- ✅ Port Forward fonctionnel vers le serveur DATA
- ✅ Résolution DNS personnalisée fonctionnelle
- ✅ Captures d'écran des règles, tests ping et logs firewall

TP 2 : Sécurité et troubleshooting du firewall pfSense

Objectifs

- Renforcer la sécurité de pfSense
- Utiliser les outils de diagnostic intégrés
- Dépanner des problèmes courants

Exercice 1 : Hardening (renforcement de la sécurité)

1.1 Sécurisation de l'accès web

System → Advanced → Admin Access :

Paramètre	Recommandation
Protocol	HTTPS uniquement
TCP Port	Changer le port par défaut (ex: 8443)
Max Processes	2
Anti-lockout	Garder activé sauf si accès console disponible
DNS Rebind Check	□ Activé
HTTP Referer Check	□ Activé
Browser HTTP_REFERER enforcement	□ Activé

1.2 Gestion des utilisateurs

System → User Manager :

1. Créer un utilisateur administrateur personnalisé
2. Désactiver ou renommer le compte `admin` par défaut
3. Activer l'authentification à deux facteurs (TOTP) si disponible
4. Créer des groupes avec des privilèges limités :

Groupe	Privilèges
`fw-admins`	Accès complet
`fw-readonly`	Dashboard + Status + Diagnostics (lecture seule)
`vpn-admins`	Gestion VPN uniquement

1.3 Sécurisation SSH

System → Advanced → Secure Shell :

Paramètre	Recommandation
Enable SSH	□ (si besoin)
SSHd Key Only	□ Public Key Only
SSH Port	2222 (changer le port par défaut)
Listen Interfaces	LAN uniquement

1.4 Blocage des bogons et réseaux privés

Interfaces → WAN :

Option	Action
Block private networks	□ Cocher
Block bogon networks	□ Cocher

Exercice 2 : Outils de diagnostic

2.1 Packet Capture

Diagnostics → Packet Capture :

Champ	Valeur exemple
Interface	LAN
Protocol	Any (ou TCP/UDP/ICMP)
Host Address	`10.0.0.50`
Port	`80`
Packet Count	`100`
Level of Detail	Normal

1. Lancer une capture sur l'interface LAN, filtrer sur un client spécifique
2. Depuis le client, naviguer sur un site web
3. Arrêter la capture et analyser les résultats
4. Télécharger le fichier `.pcap` et l'ouvrir dans **Wireshark**

2.2 pfTop

Diagnostics → pfTop :

Affiche les connexions actives en temps réel, triées par :

- Bytes (volume de données)
- Rate (débit)
- Age (ancienneté)
- Peak (pic de bande passante)

2.3 States Table

Diagnostics → States :

Affiche la table d'états du firewall (connexions actives) :

```
Interface  Protocol  Source               Destination          State
WAN        TCP       10.0.0.50:52341  →   93.184.216.34:443    ESTABLISHED:ESTABLISHED
LAN        UDP       10.0.0.50:45123  →   1.1.1.1:53           SINGLE:MULTIPLE
```

Copier

Filtrer par IP source, destination ou interface pour le dépannage.

2.4 DNS Lookup

Diagnostics → DNS Lookup :

Tester la résolution DNS directement depuis pfSense :

```
Hostname: google.com
→ A: 142.250.179.110 (résolu en 12ms)
→ AAAA: 2a00:1450:4007:818::200e
```

Copier

2.5 Ping et Traceroute

Diagnostics → Ping / Traceroute :

Test	Depuis pfSense	Vérification
`ping 8.8.8.8`	Connectivité WAN	□ Si réponse
`ping 10.0.0.50`	Connectivité LAN	□ Si réponse
`traceroute google.com`	Chemin réseau	Vérifier les sauts

Exercice 3 : Scénarios de dépannage

Scénario A : « Le client n'a pas Internet »

Étape	Vérification	Commande/Outil
1	Le client a une IP ?	`ipconfig` / `ip addr`
2	Ping vers la passerelle (pfSense) ?	`ping 10.0.0.1`
3	Ping vers Internet (IP) ?	`ping 8.8.8.8`
4	Résolution DNS ?	`nslookup google.com`
5	Règle de firewall bloquante ?	Status → System Logs → Firewall
6	NAT fonctionnel ?	Diagnostics → States

Scénario B : « Le Port Forward ne fonctionne pas »

Étape	Vérification
1	La règle Port Forward existe ?
2	La règle WAN firewall associée existe et est en Pass ?
3	Le serveur cible est joignable depuis pfSense ? (Diagnostics → Ping)
4	Le service écoute sur le bon port ? (vérifier sur le serveur)
5	Pas de firewall local sur le serveur ?
6	La connexion apparaît dans States ?
7	Packet Capture sur WAN montre le trafic entrant ?

Scénario C : « Les VLANs ne communiquent pas »

Étape	Vérification
1	Les interfaces VLAN sont activées et ont une IP ?
2	Le DHCP distribue les bonnes infos (IP, passerelle, DNS) ?
3	Le switch est configuré en trunk sur le port vers pfSense ?
4	Les règles de firewall autorisent le trafic inter-VLAN ?
5	Packet Capture sur l'interface VLAN montre-t-il du trafic ?

Livrables

- □ Paramètres de sécurité appliqués (HTTPS, port personnalisé, SSH sécurisé)
- □ Capture de paquets réalisée et analysée dans Wireshark
- □ Trois scénarios de dépannage documentés avec résolution
- □ Rapport de synthèse sur l'état de sécurité du firewall

Chapitre 5 : VPN et IPsec

5.1 Introduction aux VPN

Un **VPN (Virtual Private Network)** crée un tunnel chiffré entre deux points à travers un réseau non sécurisé (Internet).

Types de VPN

Type	Description	Cas d'usage
Site-to-Site	Connexion permanente entre 2 réseaux	Relier 2 sites distants
Point-to-Site (Remote Access)	Connexion d'un client distant au réseau	Télétravail
Point-to-Point	Tunnel entre 2 machines spécifiques	Lien dédié

Protocoles VPN supportés par pfSense

Protocole	Sécurité	Performance	Complexité	Port
IPsec	□ Très forte	□ Excellente (hardware accel.)	⚠ Complexe	UDP 500, 4500
OpenVPN	□ Forte	⚠ Bonne	□ Simple	UDP 1194 (configurable)
WireGuard	□ Forte	□ Excellente	□ Simple	UDP 51820

5.2 Concepts IPsec

IPsec fonctionne en deux phases :

Phase 1 (IKE — Internet Key Exchange)

Établit le tunnel sécurisé pour la négociation :

Paramètre	Options courantes
Key Exchange	IKEv1, IKEv2 (recommandé)
Authentication	Pre-Shared Key (PSK), Certificats
Encryption	AES-256-GCM (recommandé), AES-256-CBC, AES-128
Hash	SHA-256, SHA-384, SHA-512
DH Group	14 (2048-bit), 19 (ECP-256), 20 (ECP-384)
Lifetime	28800 secondes (8 heures)
Dead Peer Detection	☑ Activer (détection de panne)

Phase 2 (IPsec SA — Security Association)

Définit le tunnel de données :

Paramètre	Options courantes
Protocol	ESP (chiffrement + auth), AH (auth uniquement)
Encryption	AES-256-GCM (recommandé), AES-256-CBC
Hash	SHA-256
PFS Key Group	14 (2048-bit) — Perfect Forward Secrecy
Lifetime	3600 secondes (1 heure)
Local Network	Réseau local à partager (ex: `10.0.0.0/24`)
Remote Network	Réseau distant (ex: `192.168.0.0/24`)

```
Phase 1 : Négociation du tunnel sécurisé (IKE)
┌──────────────┐          IKE (UDP 500/4500)          ┌──────────────┐
│  Site A      │◄─────────────────────────────────────►│  Site B      │
│  pfSense     │  Authentification + Chiffrement      │  pfSense     │
└──────────────┘                                      └──────────────┘

Phase 2 : Tunnel de données (ESP)
┌──────────────┐          ESP (protocole 50)          ┌──────────────┐
│ 10.0.0.0     │◄═════════════════════════════════════►│192.168.0.0   │
│   /24        │      Données chiffrées (AES)         │   /24        │
└──────────────┘                                      └──────────────┘
```

Copier

5.3 Configuration IPsec Site-to-Site

Schéma

```
Site A (Paris)                              Site B (Lyon)
LAN: 10.0.0.0/24                          LAN: 192.168.0.0/24
pfSense WAN: 203.0.113.1      ◄──IPsec──►  pfSense WAN: 198.51.100.1
```

Copier

Configuration sur le Site A (Paris)

VPN → IPsec → Tunnels → Add P1 :

Phase 1 :

Champ	Valeur
Key Exchange version	IKEv2
Internet Protocol	IPv4
Interface	WAN
Remote Gateway	`198.51.100.1` (IP WAN Site B)
Authentication Method	Mutual PSK
Pre-Shared Key	`SuperSecretKey2024!`
Encryption Algorithm	AES 256-GCM / 128 bits
Hash Algorithm	SHA256
DH Group	14 (2048 bit)
Lifetime	28800
Dead Peer Detection	☑ Enable
DPD delay	10
DPD retries	5

Phase 2 (Show Phase 2 → Add P2) :

Champ	Valeur
Mode	Tunnel IPv4
Local Network	LAN subnet (10.0.0.0/24)
Remote Network	Network `192.168.0.0/24`
Protocol	ESP
Encryption	AES 256-GCM / 128 bits
Hash	SHA256
PFS Key Group	14 (2048 bit)
Lifetime	3600

Configuration sur le Site B (Lyon)

Configuration **miroir** :

- Remote Gateway : `203.0.113.1` (IP WAN Site A)
- Même Pre-Shared Key
- Local Network : `192.168.0.0/24`
- Remote Network : `10.0.0.0/24`
- Mêmes algorithmes de chiffrement

Règles de firewall pour IPsec

Firewall → Rules → IPsec :

Champ	Valeur
Action	Pass
Protocol	Any
Source	`192.168.0.0/24` (réseau distant)
Destination	LAN net (`10.0.0.0/24`)
Description	Autoriser trafic IPsec depuis Site B

> *Créer cette règle sur les **deux** sites pfSense.*

Vérification du tunnel

Status → IPsec :

État	Signification
ESTABLISHED	Phase 1 connectée
INSTALLED	Phase 2 active, trafic peut passer
CONNECTING	Tentative de connexion en cours
Aucun affichage	Tunnel non initié

```
# Depuis un poste du Site A, pinger un poste du Site B
ping 192.168.0.10

# Depuis pfSense (Diagnostics → Ping)
Source: LAN
Host: 192.168.0.1
```

Copier

5.4 Dépannage IPsec

Logs IPsec

Status → System Logs → IPsec :

Message	Cause probable
`NO_PROPOSAL_CHOSEN`	Mismatch d'algorithmes (Phase 1 ou Phase 2)
`AUTHENTICATION_FAILED`	Pre-Shared Key différente
`PEER_NOT_RESPONDING`	IP distante injoignable ou port 500/4500 bloqué
`TS_UNACCEPTABLE`	Réseaux locaux/distants ne correspondent pas
`INVALID_KE_PAYLOAD`	Groupe DH différent entre les deux sites

Checklist de dépannage

1. □ Les deux sites ont la **même** Pre-Shared Key
2. □ Les algorithmes Phase 1 sont **identiques** des deux côtés
3. □ Les algorithmes Phase 2 sont **identiques** des deux côtés
4. □ Les réseaux Local/Remote sont **inversés** (miroir) entre les sites
5. □ Les ports **UDP 500 et 4500** sont ouverts sur le WAN
6. □ Les règles de firewall sur l'onglet **IPsec** autorisent le trafic
7. □ Pas de conflit d'adresses entre les réseaux des deux sites
8. □ **NAT-T** (NAT Traversal) activé si un site est derrière un NAT

Chapitre 6 : OpenVPN

6.1 Pourquoi OpenVPN ?

Critère	IPsec	OpenVPN
Facilité de configuration	⚠ Complexe	□ Simple
Traversée NAT/Proxy	⚠ Problématique	□ Facile (TCP 443)
Clients multiplateformes	⚠ Variable	□ Excellent
Performance brute	□ Meilleure (hardware)	⚠ Bonne (userspace)
Interopérabilité	□ Standard	⚠ OpenVPN uniquement
Certificats	⚠ Complexe	□ PKI intégrée

6.2 Infrastructure à clé publique (PKI)

Avant de configurer OpenVPN, il faut créer une **autorité de certification (CA)** et des certificats.

Créer la CA (Certificate Authority)

System → Cert. Manager → CAs → Add :

Champ	Valeur
Descriptive Name	`CA-VPN-pfSense`
Method	Create an internal Certificate Authority
Key type	RSA
Key length	4096
Digest Algorithm	SHA256
Lifetime	3650 (10 ans)
Common Name	`CA-VPN-pfSense`
Country	FR
State	Ile-de-France
City	Paris
Organization	MonEntreprise

Créer le certificat serveur

System → Cert. Manager → Certificates → Add/Sign :

Champ	Valeur
Method	Create an internal Certificate
Descriptive Name	`Cert-OpenVPN-Server`
Certificate Authority	`CA-VPN-pfSense`
Key type	RSA
Key length	4096
Digest Algorithm	SHA256
Lifetime	3650
Common Name	`vpn.example.com`
Certificate Type	Server Certificate

Créer les certificats utilisateurs

Pour chaque utilisateur VPN :

System → Cert. Manager → Certificates → Add/Sign :

Champ	Valeur
Method	Create an internal Certificate
Descriptive Name	`Cert-User-JDupont`
Certificate Authority	`CA-VPN-pfSense`
Common Name	`jdupont`
Certificate Type	User Certificate

6.3 Configuration OpenVPN Remote Access (Point-to-Site)

Utilisation du Wizard

VPN → OpenVPN → Wizards :

Le wizard simplifie la configuration. Sinon, configuration manuelle :

VPN → OpenVPN → Servers → Add :

Champ	Valeur
Server Mode	Remote Access (SSL/TLS + User Auth)
Backend for Authentication	Local Database
Protocol	UDP on IPv4 only
Device Mode	tun (Layer 3 Tunnel)
Interface	WAN
Local Port	`1194`
Description	`VPN Remote Access`

Cryptographic Settings :

Champ	Valeur
TLS Configuration	☑ Use a TLS Key
Auto generate TLS Key	☑
Peer Certificate Authority	`CA-VPN-pfSense`
Server Certificate	`Cert-OpenVPN-Server`
DH Parameter Length	4096
Data Encryption Algorithms	AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305
Fallback Algorithm	AES-256-CBC
Auth Digest	SHA256

Tunnel Settings :

Champ	Valeur
IPv4 Tunnel Network	`10.8.0.0/24`
Redirect IPv4 Gateway	□ (full tunnel) ou □ (split tunnel)
IPv4 Local Network(s)	`10.0.0.0/24` (réseaux accessibles via VPN)
Concurrent Connections	`50`
Compression	□ Refuse (sécurité : éviter VORACLE)
DNS Default Domain	`local.lan`
DNS Server 1	`10.0.0.1`

Créer les utilisateurs VPN

System → User Manager → Users → Add :

Champ	Valeur
Username	`jdupont`
Password	(mot de passe fort)
Certificate	□ Click to create a user certificate

Règles de firewall

Firewall → Rules → WAN :

Champ	Valeur
Action	Pass
Protocol	UDP
Source	Any
Destination	WAN Address
Dest. Port	1194
Description	Autoriser OpenVPN

Firewall → Rules → OpenVPN :

Champ	Valeur
Action	Pass
Protocol	Any
Source	`10.8.0.0/24` (tunnel network)
Destination	LAN net
Description	Autoriser clients VPN vers LAN

Export du client (Client Export Package)

Installer le package **openvpn-client-export** :

System → Package Manager → Available Packages → chercher `openvpn-client-export` → Install

Puis **VPN → OpenVPN → Client Export** :

Format	Usage
Inline Configurations	Fichier `.ovpn` tout-en-un
Windows Installer	Installeur avec config intégrée
Viscosity	Client macOS
Android	Config pour OpenVPN Connect
iOS	Config pour OpenVPN Connect

6.4 Configuration OpenVPN Site-to-Site

Architecture

```
Site A (Paris)                              Site B (Lyon)
LAN: 10.0.0.0/24                          LAN: 192.168.0.0/24
pfSense (Serveur OpenVPN)   ◄──OpenVPN──►  pfSense (Client OpenVPN)
Tunnel: 10.9.0.1                           Tunnel: 10.9.0.2
```

Copier

Côté Serveur (Site A)

VPN → OpenVPN → Servers → Add :

Champ	Valeur
Server Mode	Peer to Peer (SSL/TLS)
Protocol	UDP on IPv4 only
Device Mode	tun
Interface	WAN
Local Port	`1195` (différent du Remote Access)
Peer Certificate Authority	`CA-VPN-pfSense`
Server Certificate	`Cert-OpenVPN-Server`
IPv4 Tunnel Network	`10.9.0.0/24`
IPv4 Remote Network(s)	`192.168.0.0/24`

Côté Client (Site B)

VPN → OpenVPN → Clients → Add :

Champ	Valeur
Server Mode	Peer to Peer (SSL/TLS)
Protocol	UDP on IPv4 only
Device Mode	tun
Interface	WAN
Server Host	`203.0.113.1` (IP WAN Site A)
Server Port	`1195`
Peer Certificate Authority	`CA-VPN-pfSense` (même CA)
Client Certificate	Certificat client généré sur la CA du Site A
IPv4 Tunnel Network	`10.9.0.0/24`
IPv4 Remote Network(s)	`10.0.0.0/24`

6.5 Surveillance OpenVPN

Status → OpenVPN :

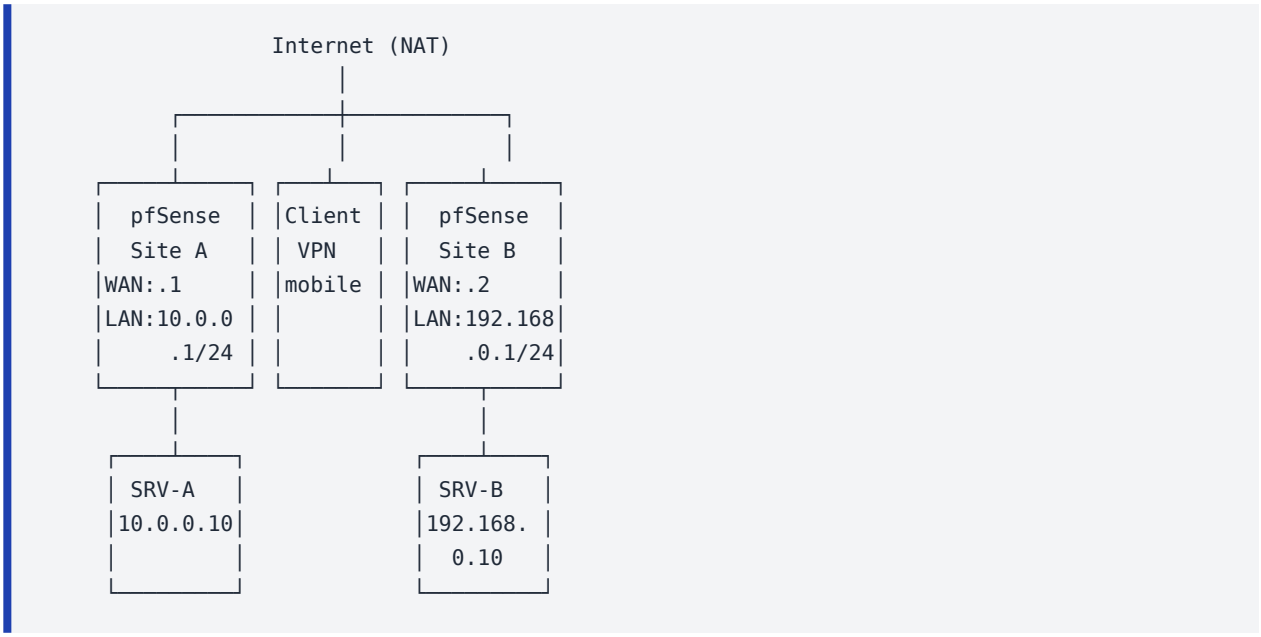
Information	Description
Virtual Address	IP du tunnel attribuée au client
Remote Host	IP publique du client
Connected Since	Durée de connexion
Bytes Sent/Received	Volume de données échangées
Actions	Déconnecter le client

TP 1 : Mise en place d'une solution VPN — Point To Site et Site To Site

Objectifs

- Configurer un VPN Remote Access (Point-to-Site) avec OpenVPN
- Configurer un VPN Site-to-Site avec IPsec
- Tester la connectivité et le routage à travers les tunnels

Topologie du lab



Copier

Partie 1 : VPN Remote Access (Point-to-Site) avec OpenVPN

Étape 1 : Créer la PKI

1. Créer la **CA** : `CA-Lab-VPN` (RSA 4096, SHA256, 10 ans)
2. Créer le **certificat serveur** : `Cert-OVPN-Server` (Server Certificate)
3. Créer un **utilisateur** `testuser` avec certificat utilisateur

Étape 2 : Configurer le serveur OpenVPN

1. **VPN → OpenVPN → Servers → Add** avec les paramètres :
    - Mode : Remote Access (SSL/TLS + User Auth)
    - Protocol : UDP, Port : 1194
    - Tunnel Network : `10.8.0.0/24`
    - Local Network : `10.0.0.0/24`
    - DNS : `10.0.0.1`

Étape 3 : Règles de firewall

1. WAN : Autoriser UDP 1194 vers WAN Address
2. OpenVPN : Autoriser tout le trafic du tunnel `10.8.0.0/24` vers le LAN

Étape 4 : Installer le Client Export Package

1. Installer `openvpn-client-export`
2. Exporter la configuration pour `testuser`
3. Installer OpenVPN sur le client
4. Importer la configuration `.ovpn`

Étape 5 : Test du VPN Remote Access

Test	Commande	Résultat attendu
Connexion VPN	Connecter le client OpenVPN	□ Tunnel établi
IP tunnel	`ipconfig` / `ip addr`	`10.8.0.x` attribuée
Ping pfSense LAN	`ping 10.0.0.1`	□ Réponse
Ping serveur interne	`ping 10.0.0.10`	□ Réponse
Accès service	`http://10.0.0.10`	□ Page affichée

Partie 2 : VPN Site-to-Site avec IPsec

Étape 1 : Configurer le tunnel IPsec

Sur **Site A** :

1. Phase 1 : IKEv2, PSK `LabIPsecKey2024!`, AES-256-GCM, SHA256, DH14
2. Phase 2 : Local `10.0.0.0/24`, Remote `192.168.0.0/24`, ESP, AES-256-GCM

Sur **Site B** :

1. Configuration miroir (inverser Local/Remote)

Étape 2 : Règles IPsec

Sur chaque site, créer une règle sur l'onglet IPsec :

- Pass Any depuis le réseau distant vers le réseau local

Étape 3 : Test du tunnel Site-to-Site

Test	Depuis	Vers	Résultat
Ping inter-site	SRV-A (`10.0.0.10`)	SRV-B (`192.168.0.10`)	□
Ping inter-site	SRV-B (`192.168.0.10`)	SRV-A (`10.0.0.10`)	□
Status IPsec	Status → IPsec		Phase 1: ESTABLISHED, Phase 2: INSTALLED
Traceroute	SRV-A	`192.168.0.10`	Un seul saut (tunnel)

Livrables

- □ VPN Remote Access fonctionnel — un client se connecte et accède au LAN
- □ VPN Site-to-Site IPsec fonctionnel — les deux réseaux communiquent
- □ Captures d'écran : Status OpenVPN, Status IPsec, tests ping
- □ Fichier de configuration OpenVPN client exporté

Chapitre 7 : Multi-WAN

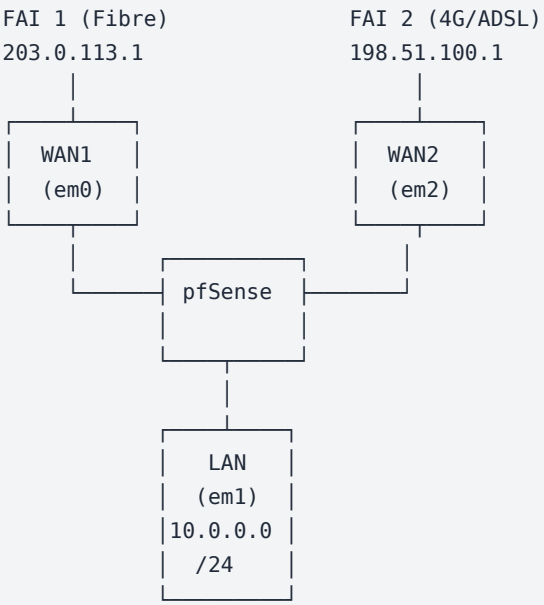
7.1 Concepts du Multi-WAN

Le **Multi-WAN** permet de connecter pfSense à plusieurs fournisseurs d'accès Internet (FAI) simultanément, offrant **redondance** et/ou **répartition de charge**.

Modes de fonctionnement

Mode	Description	Cas d'usage
Failover	Bascule automatique sur le WAN de secours si le principal tombe	Continuité de service
Load Balancing	Répartition du trafic entre les WAN	Augmenter la bande passante
Mixte	Combinaison des deux modes	Optimisation + redondance

Architecture typique



Copier

7.2 Configuration de la deuxième interface WAN

Étape 1 : Assigner l'interface

Interfaces → Assignments → Ajouter la nouvelle interface (ex: em2) → Sauvegarder

Interfaces → OPT1 (renommer en WAN2) :

Champ	Valeur
Enable	☑
Description	WAN2
IPv4 Configuration Type	DHCP ou Static selon le FAI
IPv4 Address (si static)	Adresse fournie par le FAI
Gateway	IP de la passerelle du FAI

> ⚠ *Cocher **Block private networks** et **Block bogon networks** sur WAN2 (comme sur WAN1).*

Étape 2 : Configurer les passerelles

System → Routing → Gateways :

Les passerelles WAN et WAN2 sont normalement créées automatiquement. Vérifier :

Passerelle	Interface	Gateway IP	Monitor IP	Default
WAN_DHCP	WAN	(auto)	8.8.8.8	☐
WAN2_DHCP	WAN2	(auto)	1.1.1.1	☐

> ☐ ***Monitor IP** : Utiliser une IP publique fiable et différente pour chaque WAN. pfSense pingue cette adresse pour déterminer si le WAN est bien accessible (up).*

7.3 Gateway Groups

Les **Gateway Groups** définissent le comportement Multi-WAN (failover, load balancing, ou mixte).

System → Routing → Gateway Groups → Add :

Configuration Failover (WAN1 prioritaire)

Champ	Valeur
Group Name	`FAILOVER_GROUP`
Gateway Priority	

Gateway	Tier	Virtual IP
WAN_DHCP	Tier 1 (prioritaire)	Interface Address
WAN2_DHCP	Tier 2 (secours)	Interface Address

| Trigger Level | `Member Down` | | Description | `WAN1 principal, WAN2 secours` |

> ☐ ***Tier** : Les passerelles du même Tier sont en **load balancing**. Les Tiers supérieurs sont en **failover**.*
>
> - Tier 1 + Tier 2 = Failover
> - Tier 1 + Tier 1 = Load Balancing

Configuration Load Balancing

Gateway	Tier
WAN_DHCP	Tier 1
WAN2_DHCP	Tier 1

→ Le trafic est réparti entre les deux WAN.

Configuration Mixte (Load Balancing + Failover)

Gateway	Tier
WAN_DHCP	Tier 1
WAN2_DHCP	Tier 1
WAN3_DHCP	Tier 2

→ WAN1 et WAN2 en load balancing, WAN3 en secours si les deux tombent.

Trigger Levels

Niveau	Déclenchement
Member Down	Bascule uniquement quand le WAN est complètement down
Packet Loss	Bascule si perte de paquets détectée
High Latency	Bascule si latence trop élevée
Packet Loss or High Latency	Bascule sur l'un ou l'autre (recommandé)

7.4 Policy Routing (routage par politique)

Le **Policy Routing** permet de forcer certains types de trafic vers un WAN spécifique.

Application via les règles de firewall

Dans une règle de firewall, section **Advanced** → **Gateway** :

Scénario	Règle LAN	Gateway
Tout le trafic via failover	Source: LAN net, Dest: Any	`FAILOVER_GROUP`
VoIP via WAN1 (fibre)	Source: VLAN_VOIP, Dest: Any	`WAN_DHCP`
Backup via WAN2 (ADSL)	Source: SRV_BACKUP, Dest: Any	`WAN2_DHCP`
Navigation via load balancing	Source: LAN net, Dest: Any, Port: 80,443	`LOADBAL_GROUP`

> ⚠ ***Ordre des règles** : Les règles avec des passerelles spécifiques doivent être **avant** la règle générale avec le Gateway Group.*

7.5 DNS Multi-WAN

Chaque WAN peut avoir ses propres serveurs DNS. Configurer correctement le DNS est crucial.

System → General Setup :

DNS Server	Gateway
8.8.8.8	WAN_DHCP
8.8.4.4	WAN_DHCP
1.1.1.1	WAN2_DHCP
1.0.0.1	WAN2_DHCP

> *Associer chaque serveur DNS à sa passerelle respective pour que les requêtes DNS sortent par le bon WAN.*

7.6 Outbound NAT Multi-WAN

En mode **Hybrid** ou **Manual**, créer des règles Outbound NAT pour chaque WAN :

Interface	Source	Translation
WAN	LAN net (10.0.0.0/24)	WAN Address
WAN2	LAN net (10.0.0.0/24)	WAN2 Address

7.7 Monitoring et dépannage Multi-WAN

Status → Gateways :

Colonne	Description
Name	Nom de la passerelle
Gateway	IP de la passerelle
Monitor	IP surveillée
RTT	Round Trip Time (latence)
RTTsd	Écart-type de la latence
Loss	Pourcentage de perte de paquets
Status	Online / Offline / Warning

Problèmes courants Multi-WAN

Problème	Cause	Solution
Trafic ne bascule pas	Trigger Level trop strict	Changer en « Packet Loss or High Latency »
Sites ne chargent pas	Asymmetric routing	Activer « Sticky connections » dans System → Advanced
VPN ne fonctionne plus	VPN lié à l'IP d'un WAN spécifique	Configurer le VPN sur une interface spécifique
DNS lent après bascule	DNS associé au WAN down	Associer les DNS aux bonnes passerelles

Chapitre 8 : Traffic Shaping

8.1 Introduction au Traffic Shaping

Le **Traffic Shaping** (ou QoS — Quality of Service) permet de contrôler et prioriser le trafic réseau pour garantir la qualité des applications critiques.

Pourquoi le Traffic Shaping ?

Sans QoS	Avec QoS
Un gros téléchargement sature le lien	La bande passante est répartie équitablement
La VoIP est saccadée	La VoIP est priorisée, qualité constante
Les vidéoconférences lagguent	Le trafic temps réel est garanti
Premier arrivé, premier servi	Trafic classifié et priorisé

8.2 Concepts ALTQ

pfSense utilise **ALTQ** (Alternate Queuing) intégré au noyau FreeBSD pour le Traffic Shaping.

Schedulers (disciplines de file d'attente)

Scheduler	Description	Cas d'usage
PRIQ (Priority Queuing)	Files d'attente par priorité stricte	Simple, VoIP prioritaire
CBQ (Class-Based Queuing)	Bande passante allouée par classe	Partage équitable
HFSC (Hierarchical Fair Service Curve)	Garanties de bande passante + délai	Le plus flexible et recommandé
FAIRQ	Fair Queuing	Équité entre flux
CODELQ	CoDel Active Queue Management	Anti-bufferbloat

> ***Recommandation** : Utiliser **HFSC** pour la plupart des scénarios. C'est le scheduler le plus polyvalent.*

8.3 Configuration avec le Wizard

Firewall → Traffic Shaper → Wizards :

Le wizard crée automatiquement les queues en fonction de vos besoins.

Wizard « Traffic Shaper »

Étape	Configuration
1	Nombre d'interfaces WAN (1 ou 2 pour Multi-WAN)
2	Scheduler : **HFSC**
3	Bande passante WAN Upload : ex. `20 Mbit/s`
4	Bande passante WAN Download : ex. `100 Mbit/s`
5	Priorité VoIP : ☑ Enable, DSCP: EF
6	Penalty Box : IP à limiter (optionnel)
7	Peer-to-Peer : ☑ Limiter (catch-all ou par application)
8	Jeux en ligne : ☑ Prioriser
9	Autres applications : personnaliser

> ⚠ ***IMPORTANT** : Configurer la bande passante à **90-95%** de la capacité réelle du lien. Si votre connexion est de 100 Mbps, configurer 95 Mbps. Cela garantit que pfSense contrôle la mise en file d'attente plutôt que le routeur du FAI.*

8.4 Configuration manuelle des queues

Firewall → Traffic Shaper → By Interface :

Créer la queue racine (Root Queue)

Champ	Valeur
Enable	☑
Scheduler	HFSC
Bandwidth	`95 Mbit/s` (95% du lien)
Queue Limit	`50` paquets

Créer les sous-queues

Queue	Bandwidth	Priority	Realtime	Upperlimit	Description
`qVoIP`	10%	7	2 Mbit/s	—	VoIP / Temps réel
`qACK`	5%	6	1 Mbit/s	—	ACK TCP (accélère les transferts)
`qDefault`	40%	3	—	—	Trafic général
`qWeb`	25%	4	—	—	Navigation HTTP/HTTPS
`qP2P`	10%	1	—	10 Mbit/s	Peer-to-Peer (limité)
`qBulk`	10%	2	—	15 Mbit/s	Téléchargements volumineux

> 💡 ***Realtime*** *(HFSC) : Garantit une bande passante minimale pour la queue, même en cas de congestion. Idéal pour la VoIP.* ***Upperlimit*** *(HFSC) : Limite maximale de bande passante. Empêche le P2P de consommer tout le lien.*

8.5 Floating Rules pour le Traffic Shaping

Les **Floating Rules** avec direction **Out** sont utilisées pour assigner le trafic aux queues.

Firewall → Rules → Floating → Add :

Règle pour la VoIP (SIP + RTP)

Champ	Valeur
Action	Match
Interface	WAN
Direction	Out
Protocol	UDP
Source	Any
Destination	Any
Dest. Port	`5060-5061` (SIP), `10000-20000` (RTP)
Ackqueue/Queue	`qACK` / `qVoIP`
Description	VoIP → queue prioritaire

Règle pour le trafic web

Champ	Valeur
Action	Match
Interface	WAN
Direction	Out
Protocol	TCP
Dest. Port	`80, 443`
Ackqueue/Queue	`qACK` / `qWeb`
Description	HTTP/HTTPS → queue web

8.6 Limiters

Les **Limiters** offrent une alternative aux queues ALTQ pour limiter la bande passante par IP ou par flux.

Firewall → Traffic Shaper → Limiters → Add :

Créer un limiter de download

Champ	Valeur
Name	`Download_10Mbps`
Bandwidth	`10 Mbit/s`
Mask	Source addresses (limite par IP source)
Queue Size	`50`
Scheduler	FQ_CODEL (recommandé anti-bufferbloat)

Créer un limiter d'upload

Champ	Valeur
Name	`Upload_2Mbps`
Bandwidth	`2 Mbit/s`
Mask	Destination addresses
Scheduler	FQ_CODEL

Appliquer via une règle de firewall

Dans une règle LAN, section **Advanced** :

Champ	Valeur
In / Out pipe	`Download_10Mbps` / `Upload_2Mbps`

> ***Limiters vs Queues** :*
>
> - **Queues (ALTQ)** : Priorisation relative entre types de trafic
> - **Limiters** : Limitation absolue de bande passante (par IP, par subnet)
> - Les deux peuvent être combinés

8.7 Monitoring du Traffic Shaping

Status → Queues :

Colonne	Description
Queue	Nom de la file d'attente
Bandwidth	Bande passante allouée
Borrows	Bande passante empruntée aux autres queues
Suspends	Nombre de suspensions
Drops	Paquets supprimés (congestion)
Length	Nombre de paquets en attente

> ⚠ *Si **Drops** est élevé sur une queue, augmenter sa bande passante ou sa priorité.*

Status → Traffic Graph :

Graphique en temps réel du trafic par interface, utile pour visualiser l'effet du Traffic Shaping.

Chapitre 9 : Disponibilité élevée (High Availability)

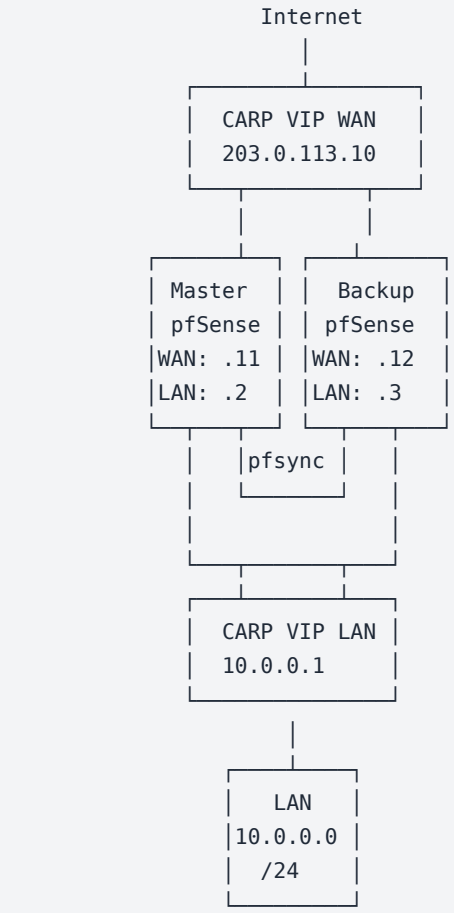
9.1 Concepts de haute disponibilité

La **haute disponibilité (HA)** garantit la continuité de service en cas de panne d'un firewall grâce à un **cluster actif/passif** de deux pfSense.

Composants du HA pfSense

Technologie	Rôle	Description
CARP	IP virtuelle partagée	Common Address Redundancy Protocol — IP flottante entre Master et Backup
pfsync	Synchronisation des états	Réplique la table d'états du firewall (connexions actives)
XMLRPC	Synchronisation de configuration	Réplique la configuration (règles, NAT, DHCP, etc.) du Master vers le Backup

Architecture HA




```
Adresses IP :
  Master WAN: 203.0.113.11    Backup WAN: 203.0.113.12
  Master LAN: 10.0.0.2        Backup LAN: 10.0.0.3
  CARP VIP WAN: 203.0.113.10  CARP VIP LAN: 10.0.0.1
```

Copier

> *Les **clients** utilisent les **IP CARP** (VIP) comme passerelle et non les IP réelles des pfSense. En cas de bascule, l'IP ne change pas.*

9.2 Prérequis

Élément	Exigence
Matériel	2 pfSense **identiques** (même version, même hardware recommandé)
Interfaces	Même nombre d'interfaces sur les deux
Réseau	Un lien dédié pour pfsync (recommandé)
IP	3 IP par segment : 1 Master + 1 Backup + 1 CARP VIP
Licences	pfSense Plus : licence HA incluse

9.3 Configuration du Master

Étape 1 : Adresses IP des interfaces

Interface	IP Master	Masque
WAN	`203.0.113.11`	`/24`
LAN	`10.0.0.2`	`/24`
SYNC (OPT1)	`172.16.0.1`	`/30`

Étape 2 : Configuration de pfsync

System → High Avail. Sync :

State Synchronization Settings (pfsync) :

Champ	Valeur
Synchronize States	☑
Synchronize Interface	SYNC (`172.16.0.1`)
pfsync Synchronize Peer IP	`172.16.0.2` (IP SYNC du Backup)

Configuration Synchronization Settings (XMLRPC Sync) :

Champ	Valeur
Synchronize Config to IP	`172.16.0.2`
Remote System Username	`admin`
Remote System Password	(mot de passe du Backup)

Éléments à synchroniser (cocher tout) :

Option	Description
☑ Toggle All	Tout sélectionner
☑ User Manager, Cert Manager	Utilisateurs et certificats
☑ Firewall Rules, NAT, Aliases	Règles de sécurité
☑ DHCP Server, DNS, NTP	Services réseau
☑ OpenVPN, IPsec	Configuration VPN
☑ Traffic Shaper, Limiters	QoS
☑ Virtual IPs	Adresses CARP
☑ Static Routes, Gateways	Routage
☑ Scheduled Tasks	Tâches planifiées

Étape 3 : Créer les VIP CARP

Firewall → Virtual IPs → Add :

VIP WAN :

Champ	Valeur
Type	CARP
Interface	WAN
Address	`203.0.113.10/24`
Virtual IP Password	`carpwan2024`
VHID Group	`1`
Advertising Frequency	Base: `1`, Skew: `0` (Master)
Description	`CARP VIP WAN`

VIP LAN :

Champ	Valeur
Type	CARP
Interface	LAN
Address	`10.0.0.1/24`
Virtual IP Password	`carplan2024`
VHID Group	`2`
Advertising Frequency	Base: `1`, Skew: `0` (Master)
Description	`CARP VIP LAN`

Étape 4 : Configurer le NAT et les services avec les VIP

Outbound NAT : Utiliser les **VIP CARP** comme adresse de traduction (pas l'adresse d'interface) :

Interface	Source	Translation
WAN	LAN net	`203.0.113.10` (CARP VIP WAN)

DHCP Server : Configurer la passerelle distribuée sur la **VIP LAN** :

Paramètre	Valeur
Gateway	`10.0.0.1` (CARP VIP)
DNS	`10.0.0.1` (CARP VIP)

9.4 Configuration du Backup

Étape 1 : Adresses IP

Interface	IP Backup	Masque
WAN	`203.0.113.12`	`/24`
LAN	`10.0.0.3`	`/24`
SYNC (OPT1)	`172.16.0.2`	`/30`

Étape 2 : Configuration de pfsync

System → High Avail. Sync :

Champ	Valeur
Synchronize States	☑
Synchronize Interface	SYNC (`172.16.0.2`)
pfsync Synchronize Peer IP	`172.16.0.1` (IP SYNC du Master)

> ⚠ ***Ne PAS configurer XMLRPC sur le Backup*** *— la synchronisation de configuration est* ***unidirectionnelle*** *(Master → Backup).*

Étape 3 : Vérification de la synchronisation

Après avoir configuré les deux pfSense :

1. Les **VIP CARP** apparaissent automatiquement sur le Backup (via XMLRPC)
2. Les **règles de firewall**, le **NAT**, le **DHCP**, etc. sont synchronisés
3. Vérifier dans **Status → CARP (failover)** :

Sur le Master	Sur le Backup
Status: **MASTER**	Status: **BACKUP**
VIP WAN: MASTER	VIP WAN: BACKUP
VIP LAN: MASTER	VIP LAN: BACKUP

9.5 Test du failover

Test 1 : Bascule manuelle

Status → CARP (failover) :

Action	Effet
Enter Persistent CARP Maintenance Mode	Force le Master en mode Backup
Leave Persistent CARP Maintenance Mode	Redevient Master

Test 2 : Simulation de panne

1. Depuis un client, lancer un `ping -t 10.0.0.1` (VIP LAN)
2. **Éteindre** le pfSense Master (ou débrancher le câble LAN)
3. Observer :
    - Coupure de 1-3 secondes maximum
    - Le Backup prend le rôle de Master
    - Le ping reprend
4. Rallumer le Master :
    - Il reprend automatiquement le rôle de Master (skew `0`)
    - Les connexions existantes sont maintenues grâce à **pfsync**

Test 3 : Vérification des états

1. Établir une connexion SSH ou télécharger un fichier volumineux
2. Forcer le failover pendant le transfert
3. Le transfert doit **continuer sans interruption** (grâce à pfsync)

9.6 Bonnes pratiques HA

Recommandation	Raison
Interface SYNC dédiée	Isoler le trafic pfsync du trafic de production
Câble croisé pour SYNC	Connexion directe entre les deux pfSense
Même version pfSense	Éviter les incompatibilités
VHID uniques	Éviter les conflits si plusieurs clusters CARP sur le même réseau
Tester régulièrement	Vérifier que le failover fonctionne (maintenance mensuelle)
Monitorer CARP	Alertes SNMP/syslog en cas de bascule
Sauvegardes régulières	Même avec HA, les backups restent essentiels

9.7 Dépannage HA

Problème	Cause probable	Solution
Les deux pfSense sont Master	Split-brain : pas de communication CARP	Vérifier le lien SYNC et les règles de firewall
XMLRPC ne synchronise pas	Mauvais identifiants ou IP	Vérifier l'IP SYNC et les credentials
Failover lent (>5 secondes)	Skew trop élevé ou réseau congestionné	Réduire le skew, dédier l'interface SYNC
Connexions perdues après failover	pfsync non configuré	Activer et configurer pfsync correctement
VIP non attribuées au Backup	XMLRPC non configuré	Vérifier la synchro des Virtual IPs

Règles de firewall pour SYNC

Firewall → Rules → SYNC :

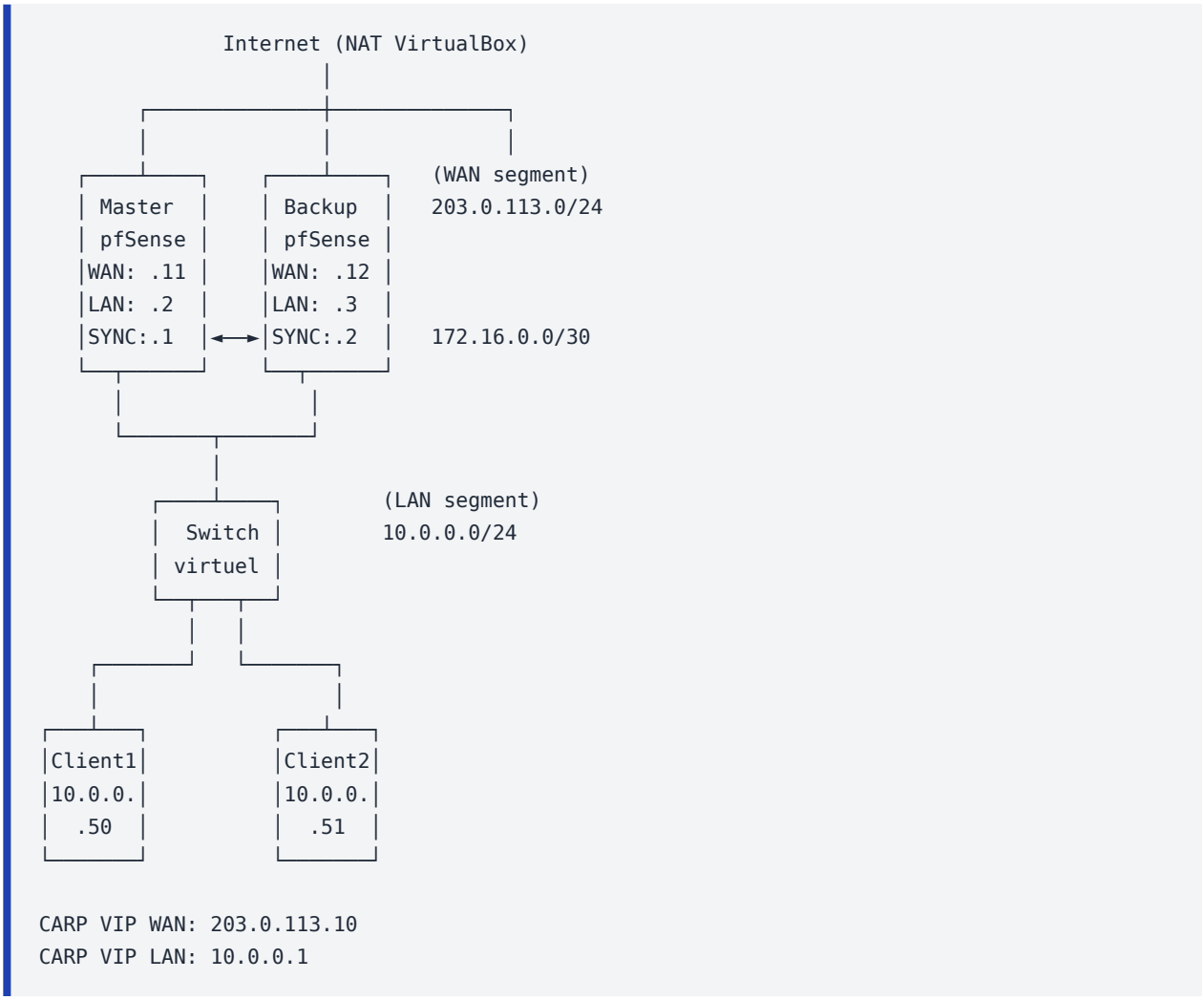
#	Action	Source	Destination	Port	Description
1	Pass	SYNC net	SYNC net	pfsync	Autoriser pfsync
2	Pass	SYNC net	SYNC net	443	Autoriser XMLRPC

TP 1 : Mise en place du HA avec pfSense

Objectifs

- Déployer un cluster HA avec deux pfSense
- Configurer CARP, pfsync et XMLRPC
- Tester le failover et valider la continuité de service

Topologie du lab



Copier

Étape 1 : Préparation des VMs

Créer 2 VMs pfSense avec 3 interfaces réseau chacune :

Interface	Réseau VirtualBox	Usage
Adapter 1 (em0)	NAT	WAN
Adapter 2 (em1)	Réseau interne « LAN »	LAN
Adapter 3 (em2)	Réseau interne « SYNC »	Synchronisation

Étape 2 : Configuration IP

Master :

Interface	IP	Masque
WAN	DHCP (NAT)	auto
LAN	`10.0.0.2`	`/24`
SYNC	`172.16.0.1`	`/30`

Backup :

Interface	IP	Masque
WAN	DHCP (NAT)	auto
LAN	`10.0.0.3`	`/24`
SYNC	`172.16.0.2`	`/30`

Étape 3 : Configuration CARP et pfsync (Master)

1. Créer les **VIP CARP** :
    - WAN : VIP appropriée, VHID 1, Skew 0
    - LAN : `10.0.0.1/24`, VHID 2, Skew 0
2. Configurer **pfsync** via l'interface SYNC
3. Configurer **XMLRPC** vers `172.16.0.2`
4. Cocher **tous les éléments à synchroniser**

Étape 4 : Configuration du Backup

1. Configurer **pfsync** via l'interface SYNC (peer: `172.16.0.1`)
2. **Ne pas** configurer XMLRPC sur le Backup
3. Vérifier que les VIP et les règles sont synchronisées automatiquement

Étape 5 : Configuration du DHCP et NAT

Sur le **Master** (synchronisé automatiquement vers le Backup) :

1. DHCP : Passerelle = `10.0.0.1` (VIP CARP LAN), DNS = `10.0.0.1`
2. Outbound NAT : Translation vers la VIP CARP WAN
3. Règles de firewall sur l'interface SYNC pour autoriser pfsync et XMLRPC

Étape 6 : Tests de validation

Test A : État du cluster

Vérification	Master	Backup
Status → CARP	MASTER pour toutes les VIP	BACKUP pour toutes les VIP
Status → System Logs → Firewall	Pas d'erreurs CARP	Pas d'erreurs CARP
Firewall → Rules	Règles synchronisées	Identiques au Master

Test B : Connectivité client

Test	Commande	Résultat
Ping VIP LAN	`ping 10.0.0.1`	□
Ping Master	`ping 10.0.0.2`	□
Ping Backup	`ping 10.0.0.3`	□
Accès Internet	`ping 8.8.8.8`	□
DNS	`nslookup google.com`	□

Test C : Failover

1. Depuis Client1 : `ping -t 10.0.0.1` (continu)
2. **Éteindre le Master** (ou `Enter Persistent CARP Maintenance Mode`)
3. Constater :
    - Interruption de 1-3 secondes
    - Le ping reprend □
    - Sur le Backup : Status → CARP affiche **MASTER**
4. **Rallumer le Master** :
    - Le Master reprend le rôle (preemption)
    - Le Backup redevient BACKUP
    - Pas d'interruption notable

Test D : Persistance des connexions

1. Démarrer un téléchargement volumineux depuis Client1
2. Forcer le failover (Maintenance Mode sur le Master)
3. Le téléchargement doit **continuer sans interruption** grâce à pfsync
4. Vérifier dans **Diagnostics → States** que les connexions sont présentes sur les deux pfSense

Livrables

- □ Cluster HA fonctionnel avec 2 pfSense

- □ VIP CARP correctement configurées (WAN + LAN)
- □ Synchronisation pfsync et XMLRPC validée
- □ Test de failover réussi avec continuité de service
- □ Captures d'écran : Status CARP (Master + Backup), test ping pendant failover
- □ Rapport documentant la configuration et les tests

Chapitre 10 : Accès Shell distant et déploiement de scripts SQL

10.1 Activer SSH sur pfSense

Par défaut, le service SSH est désactivé sur pfSense. Il faut l'activer avant de pouvoir se connecter à distance.

System → Advanced → Secure Shell :

Paramètre	Valeur
Enable Secure Shell	□ Cocher
SSHd Key Only	Password or Public Key (pour commencer)
SSH Port	22 (ou un port personnalisé comme 2222)
Listen Interfaces	Toutes (ou uniquement LAN/MGMT en production)

Sauvegarder et appliquer les changements. Le service SSH démarre immédiatement.

10.2 Créer la règle firewall WAN pour autoriser SSH

Pour accéder à pfSense en SSH **depuis le WAN**, il suffit de créer une règle de firewall autorisant le port 22 vers l'adresse WAN de pfSense. Pas besoin de NAT puisqu'on se connecte directement au firewall lui-même.

Firewall → Rules → WAN → Add ↑ :

Champ	Valeur
Action	**Pass**
Interface	WAN
Address Family	IPv4
Protocol	**TCP**
Source	Any
Destination	**WAN Address**
Destination Port Range	**22** (SSH)
Description	`Autoriser SSH vers pfSense`

Sauvegarder → **Apply Changes**.

> ⚠ ***En production*** *: restreindre le champ Source à votre IP publique uniquement, ou désactiver cette règle après la maintenance.*

10.3 Connexion SSH avec Termius

Termius est un client SSH/SFTP multiplateforme (Windows, macOS, Linux, iOS, Android) avec une interface moderne.

Étape 1 : Configurer l'hôte dans Termius

Ouvrir Termius → **New Host** :

Champ	Valeur
Label	`pfSense-FW01`
Address	IP WAN de pfSense (ou IP LAN si connexion locale)
Port	`22`
Username	`admin`
Password	Mot de passe admin de pfSense

Cliquer sur **Connect**.

Étape 2 : Le menu console pfSense

Une fois connecté en SSH, pfSense affiche son **menu console** :

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) ***

 WAN (wan)       -> em0        -> v4: DHCP
 LAN (lan)       -> em1        -> v4: 10.x.x.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator 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
```

Copier

Étape 3 : Accéder au Shell

Taper `8` puis **Entrée** pour accéder au shell FreeBSD :

```
Enter an option: 8

[2.7.2-RELEASE][admin@fw01.local.lan]/root:
```

Copier

Vous êtes maintenant dans un **shell root FreeBSD**. Vous avez accès à toutes les commandes système : `ls`, `cd`, `cat`, `mysql`, `pkg`, etc.

> ⚠ ***Attention** : Le shell root donne un accès complet au système. Une mauvaise commande peut casser la configuration de pfSense. Toujours savoir ce que vous faites avant d'exécuter une commande.*

10.4 Transférer le script PHP via SFTP avec Termius

Le protocole **SFTP** (SSH File Transfer Protocol) permet de transférer des fichiers de manière sécurisée via la connexion SSH existante.

Le script `pfsense_firewall.php` automatise les **exercices 2, 3 et 4** du TP 1 :

- Création des **aliases** (SERVEURS_WEB, PORTS_WEB, PORTS_VOIP, DNS_PUBLICS, VLAN_ALL)
- Création des **règles de firewall** (DATA, VOIX, MGMT)
- Création des **Port Forward** HTTP/HTTPS vers le serveur web
- Configuration du **DNS Resolver** (Host Overrides + DNSSEC)

> *Le script utilise l'API PHP interne de pfSense (`/etc/inc/*.inc`) pour modifier directement le `config.xml` et appliquer les changements. Pas besoin de MySQL — tout se fait via les fonctions natives de pfSense.*

Étape 1 : Ouvrir une session SFTP dans Termius

Dans Termius :

1. Cliquer sur l'hôte `pfSense-FW01` déjà configuré
2. Choisir **SFTP** au lieu de **Terminal** (ou utiliser l'icône de transfert de fichiers)
3. L'explorateur SFTP s'ouvre avec l'arborescence de pfSense

Étape 2 : Naviguer vers le dossier cible

Dans le panneau distant (pfSense), naviguer vers :

```
/root/
```

Copier

C'est le répertoire home de l'utilisateur admin (root) sur pfSense.

Étape 3 : Transférer le fichier PHP

1. Dans le panneau local (votre PC), naviguer vers le dossier contenant `pfsense_firewall.php`
2. **Glisser-déposer** le fichier du panneau local vers `/root/` sur pfSense
3. Attendre la fin du transfert (barre de progression)

```
Transfert : pfsense_firewall.php → /root/pfsense_firewall.php 
```

Copier

Étape 4 : Vérifier le fichier transféré

Revenir dans le **Terminal SSH** (option `8` du menu pfSense) :

```
ls -la /root/pfsense_firewall.php
```

Copier

Résultat attendu :

```
-rw-r--r--  1 root  wheel  12845 Mar  1 10:30 /root/pfsense_firewall.php
```

Copier

10.5 Adapter le script à votre groupe AVANT le transfert

> ⚠ ***IMPORTANT** : Modifier le script **sur votre PC** avec un éditeur comme **VSCode** avant de le transférer sur pfSense. Ne pas essayer de l'éditer directement sur pfSense.*

Étape 1 : Ouvrir le script dans VSCode

Sur votre poste de travail, ouvrir `pfsense_firewall.php` dans **Visual Studio Code** (ou tout autre éditeur de code).

Étape 2 : Localiser le bloc CONFIGURATION

Rechercher le bloc suivant (vers la ligne 70) avec `Ctrl+G` ou `Ctrl+F` :

```
// ============================================================
//  CONFIGURATION — Adapter à votre groupe
// ============================================================
```

Copier

Étape 3 : Modifier les variables selon votre groupe

Remplacer les valeurs par celles de votre groupe :

```
// Réseaux des VLANs (MODIFIER SELON VOTRE GROUPE)
$NET_DATA = '10.X.10.0/24';   // X = numéro de votre groupe
$NET_VOIX = '10.X.20.0/24';
$NET_MGMT = '10.X.30.0/24';

// Serveurs DATA
$SRV_WEB01 = '10.X.10.10';
$SRV_WEB02 = '10.X.10.11';

// Premier téléphone VOIX
$PHONE01 = '10.X.20.10';
```

Copier

Groupe	$NET_DATA	$NET_VOIX	$NET_MGMT	$SRV_WEB01
G1	10.1.10.0/24	10.1.20.0/24	10.1.30.0/24	10.1.10.10
G2	10.2.10.0/24	10.2.20.0/24	10.2.30.0/24	10.2.10.10
G3	10.3.10.0/24	10.3.20.0/24	10.3.30.0/24	10.3.10.10
G4	10.4.10.0/24	10.4.20.0/24	10.4.30.0/24	10.4.10.10
G5	10.5.10.0/24	10.5.20.0/24	10.5.30.0/24	10.5.10.10
G6	10.6.10.0/24	10.6.20.0/24	10.6.30.0/24	10.6.10.10
G7	10.7.10.0/24	10.7.20.0/24	10.7.30.0/24	10.7.10.10

> ⚠ ***Prérequis*** *: Les interfaces DATA, VOIX et MGMT doivent déjà être créées dans pfSense (Exercice 1 du TP) avec les bonnes descriptions (`DATA`, `VOIX`, `MGMT`). Le script les détecte automatiquement par leur nom.*

10.6 Exécuter le script

Depuis le shell pfSense (option **8**) :

```
php /root/pfsense_firewall.php
```

Copier

Sortie attendue

```
=== SCRIPT DEMARRE ===
[OK] Configuration chargee depuis /cf/conf/config.xml
[OK] Interface DATA => opt1
[OK] Interface VOIX => opt2
[OK] Interface MGMT => opt3
[10:30:01] Backup de la configuration en cours...
[10:30:01] Backup créé : config.xml.bak_20260301_103001
[10:30:01] === Création des aliases ===
[10:30:01]   Alias créé : SERVEURS_WEB
[10:30:01]   Alias créé : PORTS_WEB
[10:30:01]   Alias créé : PORTS_VOIP
[10:30:01]   Alias créé : DNS_PUBLICS
[10:30:01]   Alias créé : VLAN_ALL
[10:30:01] === Création des règles firewall ===
[10:30:01]   Création des règles VLAN DATA...
[10:30:01]   Création des règles VLAN VOIX...
[10:30:01]   Création des règles VLAN MGMT...
[10:30:01]   5 règles DATA créées
[10:30:01]   5 règles VOIX créées
[10:30:01]   5 règles MGMT créées
[10:30:01] === Création du Port Forward (NAT) ===
[10:30:01]   NAT créé : Port Forward HTTP vers srv-web01
[10:30:01]   NAT créé : Port Forward HTTPS vers srv-web01
[10:30:02] === Configuration DNS Resolver ===
[10:30:02]   DNSSEC activé
[10:30:02]   Host override : srv-web01.local.lan → 10.7.10.10
[10:30:02]   Host override : srv-web02.local.lan → 10.7.10.11
[10:30:02]   Host override : phone01.local.lan → 10.7.20.10
[10:30:02] === Sauvegarde de la configuration ===
[10:30:02]   config.xml mis à jour
[10:30:02] === Application des règles firewall ===
[10:30:05]   Règles firewall appliquées
[10:30:05] === Redémarrage du DNS Resolver ===
[10:30:07]   DNS Resolver redémarré
[10:30:07] === TERMINÉ - Configuration appliquée avec succès ===
```

Copier

> ⚠ *Si le script affiche `[ERREUR] Interface DATA introuvable`, vérifier que vos interfaces sont bien nommées **DATA**, **VOIX** et **MGMT** dans **Interfaces → Assignments** (la description doit correspondre exactement).*

10.7 Vérifier dans l'interface web

Après exécution du script, ouvrir le **webConfigurator** et vérifier chaque élément :

Vérification	Chemin dans pfSense	Résultat attendu
Aliases	Firewall → Aliases	5 aliases créés (SERVEURS_WEB, PORTS_WEB, PORTS_VOIP, DNS_PUBLICS, VLAN_ALL)
Règles DATA	Firewall → Rules → DATA	5 règles (DNS, Web, Block VOIX, Block MGMT, Block All)
Règles VOIX	Firewall → Rules → VOIX	5 règles (VoIP, DNS, Block DATA, Block MGMT, Block All)
Règles MGMT	Firewall → Rules → MGMT	5 règles (HTTPS, SSH, Web, DNS, Block All)
NAT	Firewall → NAT → Port Forward	2 règles (HTTP 80, HTTPS 443 → srv-web01)
DNS	Services → DNS Resolver → Host Overrides	3 entrées (srv-web01, srv-web02, phone01)
DNSSEC	Services → DNS Resolver	☑ DNSSEC coché

10.8 Ce que fait le script en détail

Le script utilise les **fonctions internes de pfSense** pour modifier la configuration :

Fonction	Rôle
`parse_config(true)`	Charge le `/cf/conf/config.xml` en tableau PHP
`write_config()`	Sauvegarde le tableau PHP dans `config.xml`
`filter_configure()`	Recharge le pare-feu (pf) avec les nouvelles règles
`services_unbound_configure()`	Redémarre le DNS Resolver (Unbound)

```
┌──────────────────────────────────────────────────────────┐
│           Fonctionnement du script                       │
│                                                          │
│  pfsense_firewall.php                                    │
│       │                                                  │
│       ├─ 1. parse_config() ──→ Lit config.xml            │
│       │                                                  │
│       ├─ 2. Modifie le tableau $config en mémoire        │
│       │     - $config['aliases']['alias'][]              │
│       │     - $config['filter']['rule'][]                │
│       │     - $config['nat']['rule'][]                   │
│       │     - $config['unbound']['hosts'][]              │
│       │                                                  │
│       ├─ 3. write_config() ──→ Écrit config.xml          │
│       │                                                  │
│       ├─ 4. filter_configure() ──→ Applique le firewall  │
│       │                                                  │
│       └─ 5. services_unbound_configure() ──→ Relance DNS │
└──────────────────────────────────────────────────────────┘
```

Copier

> ***Sécurité** : Le script crée automatiquement un **backup** du `config.xml` avant toute modification. En cas de problème, restaurer avec :*
>
> ```
> cp /cf/conf/config.xml.bak_XXXXXXXX_XXXXXX /cf/conf/config.xml
> rm /tmp/config.cache
> /etc/rc.reload_all
> ```
>
> Copier

10.9 Récapitulatif des étapes

Étape	Action	Outil
1	Activer SSH sur pfSense	WebGUI → System → Advanced
2	Créer la règle WAN → SSH (port 22)	WebGUI → Firewall → Rules → WAN
3	Adapter les variables du script à votre groupe	**VSCode** sur votre PC
4	Se connecter en SSH	Termius → Terminal → port 22
5	Accéder au shell	Menu pfSense → option **8**
6	Transférer `pfsense_firewall.php`	Termius → SFTP → glisser-déposer vers `/root/`
7	Exécuter le script	`php /root/pfsense_firewall.php`
8	Vérifier dans le webConfigurator	Aliases, Rules, NAT, DNS Resolver

> ***Astuce Termius*** *: Vous pouvez sauvegarder vos hôtes, identifiants et clés SSH dans Termius pour vous reconnecter rapidement sans retaper les informations à chaque fois.*

> ***Ré-exécution*** *: Le script est* ***idempotent*** *— il supprime les règles qu'il a créées avant de les recréer. Vous pouvez donc le relancer en toute sécurité après avoir modifié les variables.*

10.10 Où trouver le script ?

Télécharger le script : pfsense_firewall.php

Le script est servi depuis le wiki (dossier `public/`). Après téléchargement : ouvrez-le dans VSCode, **adaptez** les variables en tête (groupe G1 à G7, réseaux DATA/VOIX/MGMT), puis transférez-le sur pfSense via SFTP (voir § 10.4) et exécutez `php /root/pfsense_firewall.php` (voir § 10.6).