Pare-feu pfSense CE 2.9 : VLAN, NAT et filtrage pour martinscie.lan

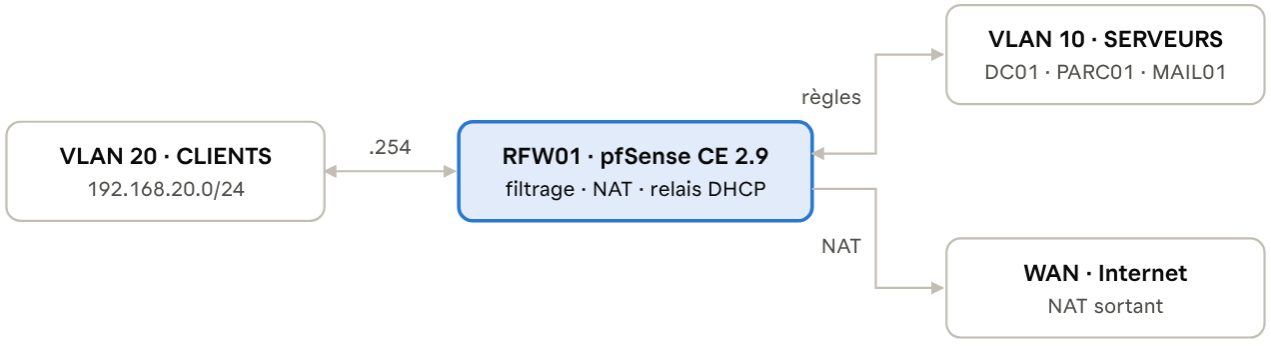
Nov 27, 2026 · @Serge Martins

Objectif

Installer le pare-feu **RFW01** sous **pfSense CE 2.9** en machine virtuelle et le configurer comme routeur inter-VLAN et passerelle Internet de **martinscie.lan** : VLAN 10 Serveurs, VLAN 20 Clients, NAT sortant, relais DHCP vers le serveur DHCP du VLAN 10 et règles de filtrage minimales.

Interface	Rôle	Adresse
WAN (vtnet0 / em0)	Accès Internet (box ou réseau de l'école)	DHCP
LAN parent (vtnet1)	Trunk 802.1Q vers le commutateur	sans adresse
VLAN 10 · SERVEURS	DC01, PARC01, MAIL01…	192.168.10.254/24
VLAN 20 · CLIENTS	Postes Windows 11 et Debian 13	192.168.20.254/24

RFW01 relie et filtre les deux VLAN et Internet



RFW01 · routage inter-VLAN et Internet

RFW01 est la passerelle .254 de chaque VLAN : il n'autorise des clients vers les serveurs que les services nécessaires et traduit les deux réseaux vers Internet.

Ressources de la VM : 2 vCPU, 2 Go RAM, 16 Go disque, deux cartes réseau (WAN et trunk).

Étape 1 – Installation

1. Télécharger le **Netgate Installer** (image d'installation en ligne de pfSense CE) depuis le site Netgate et démarrer la VM dessus.
2. L'installeur demande la configuration de la carte WAN (DHCP) pour télécharger pfSense : choisir **pfSense CE** → version **2.9.0**.
3. Système de fichiers **ZFS**, disque unique (stripe), puis redémarrer sans le média.
4. Sur la console : **1) Assign Interfaces** → ne pas créer de VLAN à ce stade, WAN = `vtnet0`, LAN = `vtnet1`.
5. **2) Set interface IP address** → LAN provisoire 192.168.1.1/24 pour atteindre l'interface web depuis une VM d'administration.

Étape 2 – Assistant de configuration

Ouvrir `https://192.168.1.1` (admin / pfsense) :

- Nom d'hôte `rfw01`, domaine `martinscie.lan`, serveur DNS `192.168.10.10` (DC01) puis 1.1.1.1 en secours.
- Fuseau horaire Europe/Paris, serveur NTP `fr.pool.ntp.org`.
- WAN en DHCP ; décocher *Block private networks* si la box est en 192.168.x.x (lab).
- **Changer le mot de passe admin.**

Étape 3 – VLAN et interfaces

1. **Interfaces → Assignments → VLANs → Add** : parent `vtnet1`, tag **10**, description SERVEURS ; puis tag **20**, CLIENTS.
2. **Interface Assignments** : ajouter `VLAN 10 on vtnet1` (OPT1) et `VLAN 20 on vtnet1` (OPT2).
3. Renommer et activer : OPT1 → **SERVEURS**, IPv4 statique 192.168.10.254/24 ; OPT2 → **CLIENTS**, 192.168.20.254/24.
4. Désactiver l'ancien LAN provisoire une fois l'administration accessible depuis le VLAN 10.

Côté hyperviseur, la carte trunk doit transporter les VLAN 10 et 20 (Proxmox : pont *VLAN aware* ; Hyper-V : `Set-VMNetworkAdapterVlan -Trunk` ; VMware : groupe de ports VLAN 4095).

Étape 4 – Relais DHCP pour le VLAN 20

Le DHCP des clients est assuré par le serveur DHCP du VLAN 10 (Windows Server 2025 ou Kea). Dans **Services → DHCP Relay** : activer, interface **CLIENTS**, serveur de destination **192.168.10.12**, cocher *Append circuit ID and agent ID*. Le service DHCP de pfSense doit être désactivé sur CLIENTS.

Étape 5 – Alias et règles de pare-feu

Créer des **alias** (*Firewall → Aliases*) :

Alias	Contenu
SRV_AD	192.168.10.10 (DC01)
PORTS_AD	53, 88, 123, 135, 389, 445, 464, 636, 3268, 49152:65535
SRV_WEB	192.168.10.20 (PARC01), 192.168.10.25 (MAIL01)
PORTS_WEB	80, 443, 587, 993

Règles sur l'interface **CLIENTS** (l'ordre compte, première règle qui correspond appliquée) :

#	Action	Source	Destination	Port	Description
1	Pass	CLIENTS net	SRV_AD	PORTS_AD (TCP/UDP)	Services Active Directory
2	Pass	CLIENTS net	SRV_WEB	PORTS_WEB	GLPI, messagerie
3	Block	CLIENTS net	SERVEURS net	*	Reste du VLAN serveurs interdit
4	Pass	CLIENTS net	*	80, 443	Accès Internet web

Sur **SERVEURS** : autoriser *SERVEURS net → any* (mises à jour, résolution DNS externe de DC01). Le NAT sortant **automatique** traduit les deux VLAN vers l'adresse WAN.

Étape 6 – Durcissement

- **System → Advanced → Admin Access** : interface web en HTTPS uniquement, accessible seulement depuis le VLAN 10 (règle d'anti-verrouillage désactivée après création d'une règle d'administration explicite).
- SSH désactivé, ou par clé uniquement.

- Comptes nominatifs avec droits limités ; authentification LDAP sur DC01 possible (*System → User Manager → Authentication Servers*).
- Sauvegarde : **Diagnostics → Backup & Restore** (et AutoConfigBackup chiffré).
- Mises à jour : **System → Update**, et paquet *System Patches* pour les correctifs recommandés.

Étape 7 – Tests

- Depuis un poste du VLAN 20 : bail DHCP reçu en 192.168.20.x avec passerelle .254 et DNS DC01.
- `nslookup dc01.martinscie.lan`, jonction au domaine, accès à GLPI : OK.
- `ping 192.168.10.41` (OCS01) : bloqué par la règle 3.
- **Status → System Logs → Firewall** : vérifier les blocages ; **Diagnostics → States** pour les connexions actives.

Dépannage

Symptôme	Piste
Pas d'adresse DHCP sur le VLAN 20	Relais non activé, port 67 bloqué, étendue absente sur le serveur DHCP
VLAN injoignables	Trunk non configuré dans l'hyperviseur ou le commutateur
Interface web inaccessible	Règle d'administration manquante : console → option 8 et `pfctl -d` temporairement
Pas d'Internet	Passerelle WAN, NAT sortant, DNS de DC01 sans redirecteurs