MAÎTRISER PFSENSE

Généralités sur pfSense

Qu'est-ce que pfSense et quel est son rôle principal dans une infrastructure réseau ?

C’est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu
Il agit comme passerelle entre un réseau local et Internet, en filtrant le trafic, en assurant la protection contre les intrusions, et en gérant des services comme le VPN

Sur quel système d’exploitation est basé pfSense ?

Elle est basé sur le système d'exploitation FreeBSD
FreeBSD est un système d'exploitation open-source basé sur Unix

Quels sont les principaux avantages de pfSense par rapport à un pare-feu matériel propriétaire ?

Gratuit et **open source**

Flexible : personnalisation poussée selon les besoins.

Mises à jour régulières et large communauté de support.

Fonctionnalités avancées intégrées (VPN, IDS/IPS, QoS...).

Interface web intuitive pour la gestion et la configuration.

Installation et Configuration

Quelles sont les exigences minimales en termes de matériel pour installer pfSense ?

Processeur : 1 GHz (32 ou 64 bits)

RAM : 1 Go

Stockage : 4 Go (HDD ou SSD)

Réseau : 2 cartes réseau (une pour le WAN, une pour le LAN)

Quelle interface web est utilisée pour configurer et administrer pfSense après son installation ?

Accessible via : https://192.168.1.1 (par défaut depuis le réseau LAN)

Nom d'utilisateur par défaut : admin

Mot de passe par défaut : pfsense

Quels sont les trois types d'interfaces réseau typiques configurées lors de l’installation de pfSense ?

WAN – Pour la connexion à Internet

LAN – Pour le réseau local interne

OPT – Interface(s) optionnelle(s), utilisée(s) pour DMZ, VLAN, Wi-Fi, etc.

Règles et Filtrage de trafic

Quelle est la logique par défaut des règles de pare-feu sous pfSense pour les interfaces WAN et LAN ?

LAN

Tout le trafic sortant est **autorisé** par défaut : les appareils du réseau peuvent accéder librement à Internet.

WAN

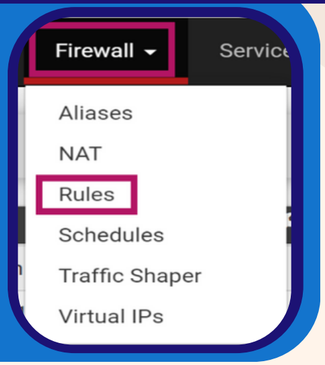
Tout le trafic entrant est **bloqué** par défaut : le réseau est protégé des accès externes non autorisés.

Installation et Configuration

Comment créer une règle de pare-feu pour bloquer l'accès à un site web spécifique sur pfSense ?

Pare-feu > Règles > LAN, ajoute une nouvelle règle :

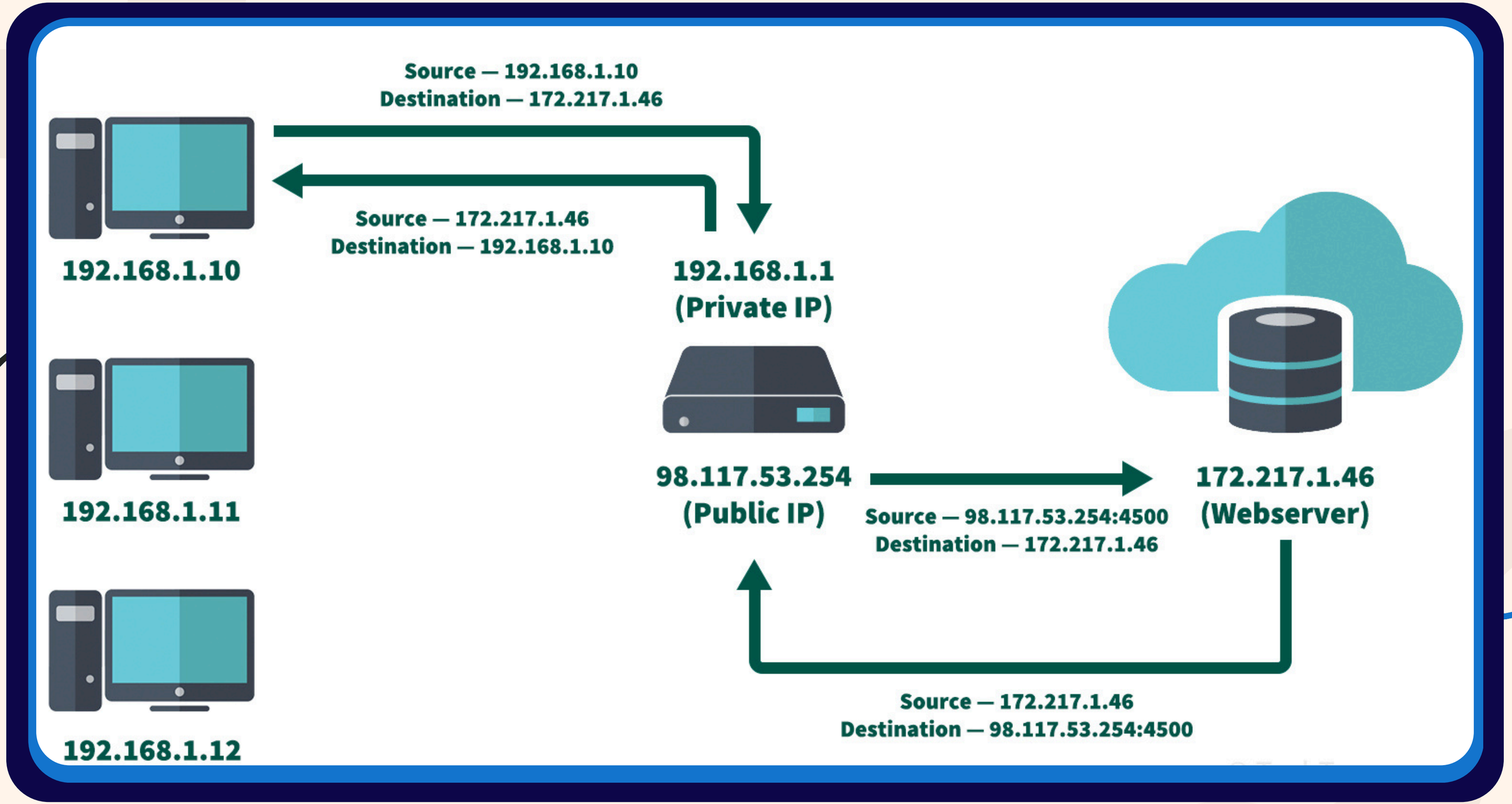
Action : Bloquer
Destination : l'alias créé
Protocole : TCP/UDP



Quelle est la différence entre une règle de pare-feu et une règle NAT (Network Address Translation) dans pfSense ?

Les règles de **pare-feu** autorisent ou rejettent le trafic entrant et sortant du réseau.

Les règles **NAT** traduisent les adresses IP du trafic autorisé par la règle de pare-feu.


Source — 192.168.1.10
Destination — 172.217.1.46
Source — 172.217.1.46
Destination — 192.168.1.10
192.168.1.10
192.168.1.11
192.168.1.12
192.168.1.1
(Private IP)
98.117.53.254
(Public IP)
Source — 98.117.53.254:4500
Destination — 172.217.1.46
172.217.1.46
(Webserver)
Source — 172.217.1.46
Destination — 98.117.53.254:4500

VPN et Sécurité

Quels sont les deux principaux types de VPN que pfSense prend en charge ?

IPsec : compatible avec de nombreux appareils et standards réseau.

OpenVPN : sécurisé, flexible, largement utilisé.

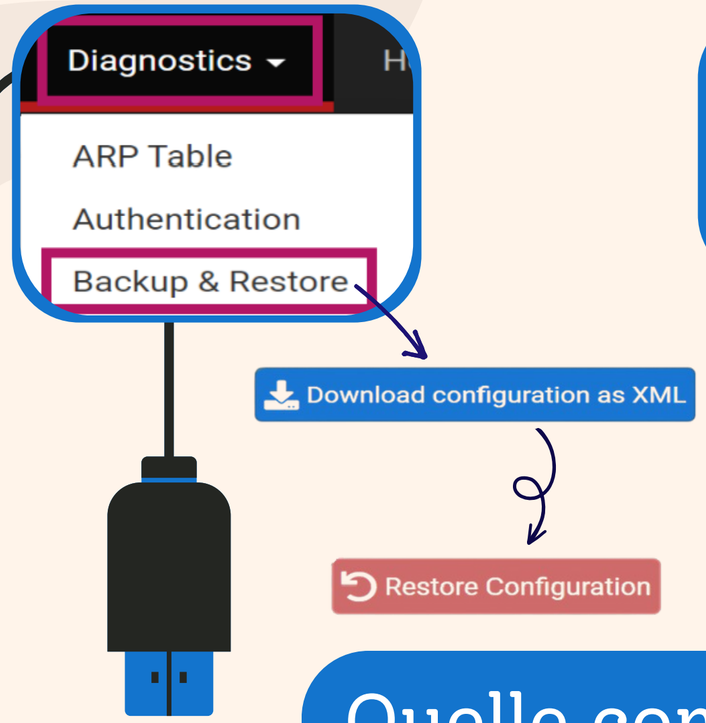
Quelle fonctionnalité de pfSense permet de détecter et prévenir les intrusions dans un réseau ?

les fonctionnalités qui permettent de détecter et de prévenir les intrusions est **Snort** (ou **Suricata**).
Ce sont des systèmes de détection/prévention d'intrusion (IDS/IPS) intégrables à pfSense.

Comment pfSense gère-t-il la journalisation et la surveillance du trafic réseau ?

pfSense gère la **journalisation** et la **surveillance du trafic** réseau via son **interface web**, où les administrateurs peuvent consulter les **logs** et utiliser des **outils de surveillance** intégrés pour **analyser le trafic**

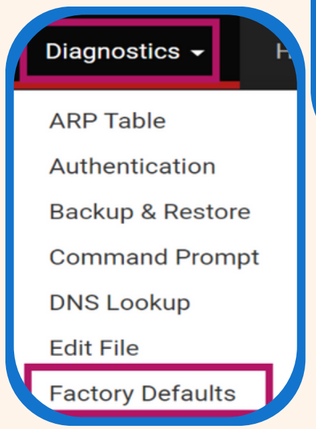
Fonctions avancées et administration



Comment sauvegarder et restaurer la configuration d'un pare-feu pfSense ?

Sauvegarde :
Accède à Diagnostics > Sauvegarde/ Restauration, puis clique sur Télécharger la configuration pour obtenir un fichier XML de sauvegarde.

Restauration :
Va dans le même menu, choisis le fichier XML sauvegardé, et clique sur Restaurer la configuration. Le système redémarrera automatiquement.



Quelle commande ou méthode permet de réinitialiser pfSense en cas de problème de configuration ?

Méthode via interface web :

Diagnostics > Factory Defaults, puis clique sur Restore Factory Defaults.

Commande en ligne de commande (console) :

```
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
```

MERCI !