Procédure de configuration

Pfsense

2023 - 2024

Une image contenant dessin humoristique, capture d’écran, mammifère, Graphique

Description générée automatiquement

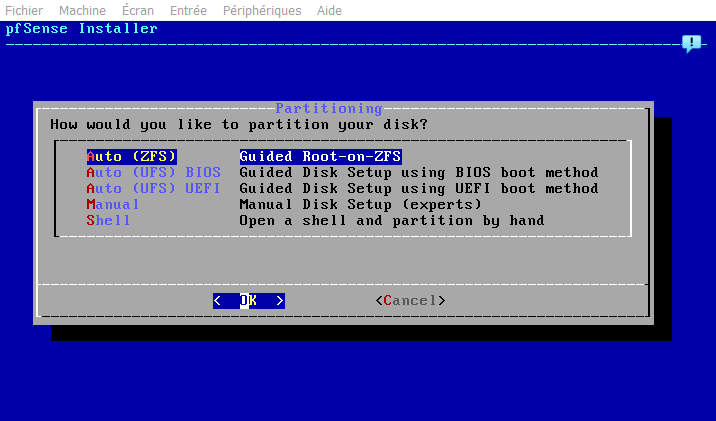
PfSense est un système d'exploitation open-source basé sur FreeBSD, spécialement conçu pour fonctionner comme un pare-feu et un routeur. pfSense offre des fonctionnalités de pare-feu avancées pour filtrer et surveiller le trafic réseau entrant et sortant. Il peut également être utilisé comme un routeur pour diriger le trafic entre différents réseaux. PfSense prend en charge les protocoles VPN pour sécuriser les communications sur Internet. Il offre des outils de surveillance et de reporting pour analyser le trafic réseau en temps réel.

PfSense peut être installé sur du matériel dédié, tel que des serveurs, des PC ou des appliances spécialement conçues pour pfSense.

En résumé, pfSense est un système d'exploitation puissant et polyvalent qui peut être installé sur une variété d'équipements, du matériel dédié aux machines virtuelles, offrant une solution de pare-feu et de routage flexible pour les réseaux de toutes tailles.

**1 – Téléchargement et installation de pfSense :**

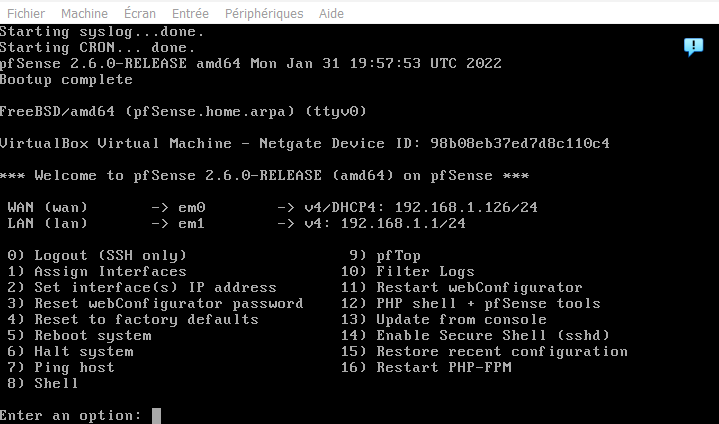
* Téléchargez la dernière version de pfSense depuis le site officiel.
* Installez pfSense sur un matériel approprié ou sur une machine virtuelle.

****

* Installer en auto (ZFS).
* Laisser par défaut jusqu’à l’installation.
* Avant de redémarrer, veuillez éjecter le disque ou l’image ISO de l’équipement.

**2 – Configuration des interfaces**

Lorsque pfsense a redémarré, on accède à un menu de configuration.



* Option 2 pour changer l’adresse IP des interfaces :

IP LAN : 192.168.201.253

CIDR : 30

* On peut maintenant accéder à l’interface web de configuration via une machine du réseau LAN avec l’URL suivant : https://192.168.201.253

**3 - Connexion à l'interface Web de pfSense :**

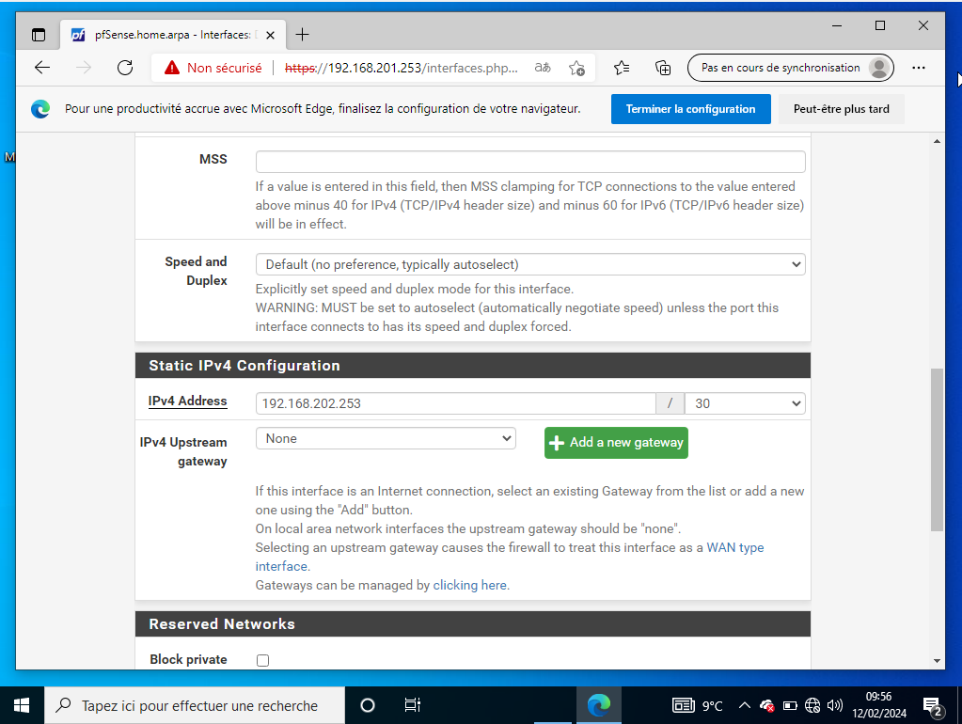
* Connectez-vous à l'interface Web de pfSense en utilisant un navigateur Web.
* Identifiez-vous avec les informations d'identification par défaut (admin/pfsense).

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**

**4 - Configuration de l'interface WAN :**

* Allez dans "Interfaces" > "WAN".
* Configurez les paramètres de l'interface WAN.

****

* Désactivez les options « Block private network ».

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

**5 - Configuration de l'interface DMZ :**

* Allez dans "Interfaces" > "Assignements".
* Cliquez sur l'onglet "Interfaces".
* Sélectionnez l'interface DMZ.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

* Configurez-la avec les paramètres appropriés :

Description : DMZ

IP adresse : 192.168.204.253

CIDR : 30

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**

**6 - Règles de pare-feu :**

* Allez dans "Firewall" > "Rules".
* Configurez les règles de pare-feu pour chaque interface (WAN, LAN, DMZ).

**Exemple de configuration de règle LAN :**

* Allez dans "Firewall" > "Rules".
* Assurez-vous d'être sur l'onglet "LAN".
* Créez une nouvelle règle qui permet le trafic sortant (sortant vers l'Internet) et bloque le trafic entrant.

**Configurez la règle comme suit :**

* Action : Pass
* Interface : LAN
* Adresse source : any
* Adresse de destination : any
* Protocole : any (ou spécifiez les protocoles autorisés)
* État : Actif
* Description : (facultatif, mais utile pour identifier la règle)

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

**Règle basique du pare-feu :**

* De préférence, sur la LAN doit pouvoir communiquer avec la WAN.
* La WAN doit pouvoir communiquer avec la DMZ sur les ports nécessaires et être autorisé à répondre uniquement aux requêtes de la LAN.
* La DMZ doit pouvoir communiquer uniquement avec la WAN.

**7 - Test et vérification :**

* Testez votre configuration en essayant d'accéder à Internet à partir des différentes interfaces et en vérifiant que le trafic est autorisé conformément à vos règles.