29/04/2024

Procédure pfBlockerNG

Sommaire

Table des matières

Table des illustrations

1- Introduction

La sécurisation des réseaux informatiques est une préoccupation majeure pour les administrateurs système et les responsables de la sécurité. Les pares-feux jouent un rôle essentiel dans la protection des réseaux contre les menaces en ligne, en filtrant le trafic entrant et sortant selon des règles prédéfinies. pfSense est une solution de pare-feu open-source largement utilisée, offrant une gamme étendue de fonctionnalités pour renforcer la sécurité des réseaux.

Parmi les outils disponibles sur pfSense, pfBlockerNG se distingue comme un puissant package permettant d'ajouter des fonctionnalités de filtrage avancées basées sur des listes de blocage. Cette procédure détaillée vise à fournir aux administrateurs système les étapes nécessaires pour configurer et déployer pfBlockerNG sur pfSense, afin d'améliorer la protection contre les menaces en ligne telles que les logiciels malveillants, les publicités intrusives et les attaques provenant de certaines régions géographiques.

En suivant cette procédure, les utilisateurs seront en mesure de tirer pleinement parti des fonctionnalités de pfBlockerNG pour contrôler et filtrer le trafic réseau entrant et sortant, tout en bénéficiant d'une interface conviviale et de puissantes options de personnalisation. La mise en place de pfBlockerNG sur pfSense représente ainsi une étape importante dans la création d'un environnement réseau sécurisé et robuste, adapté aux besoins des entreprises et des utilisateurs individuels.

1.1– Schéma

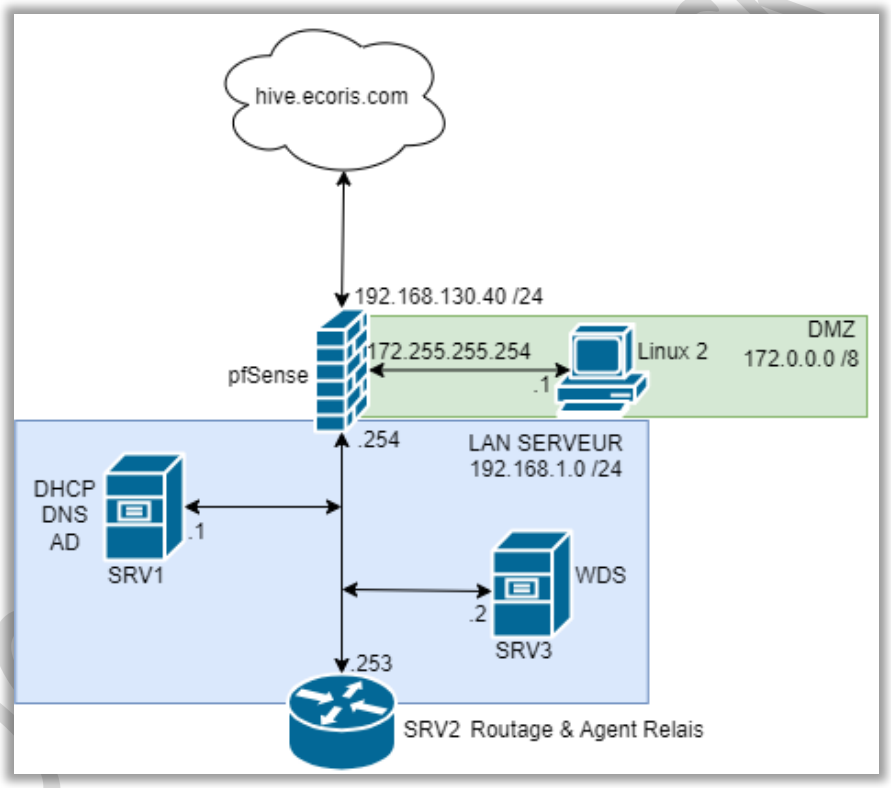


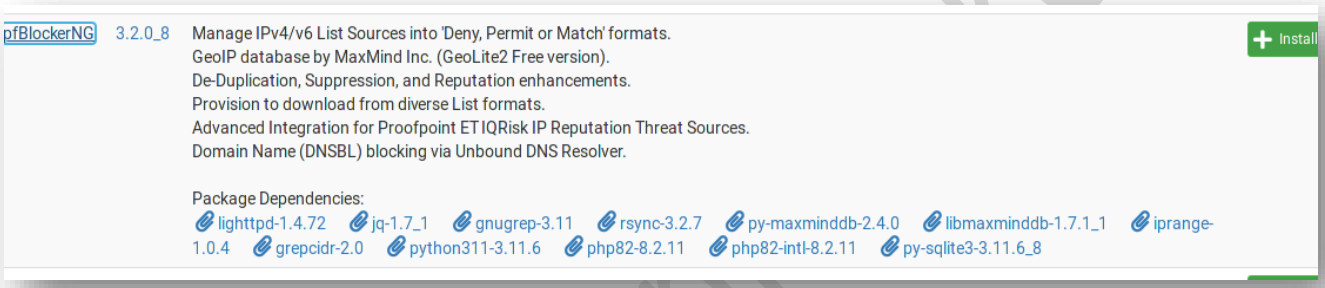
Figure 1 - Schéma réseau

1. Connexion à l'interface pfSense :

- Ouvrir un navigateur web.
- Accéder à l'adresse IP de l'interface de gestion de pfSense).

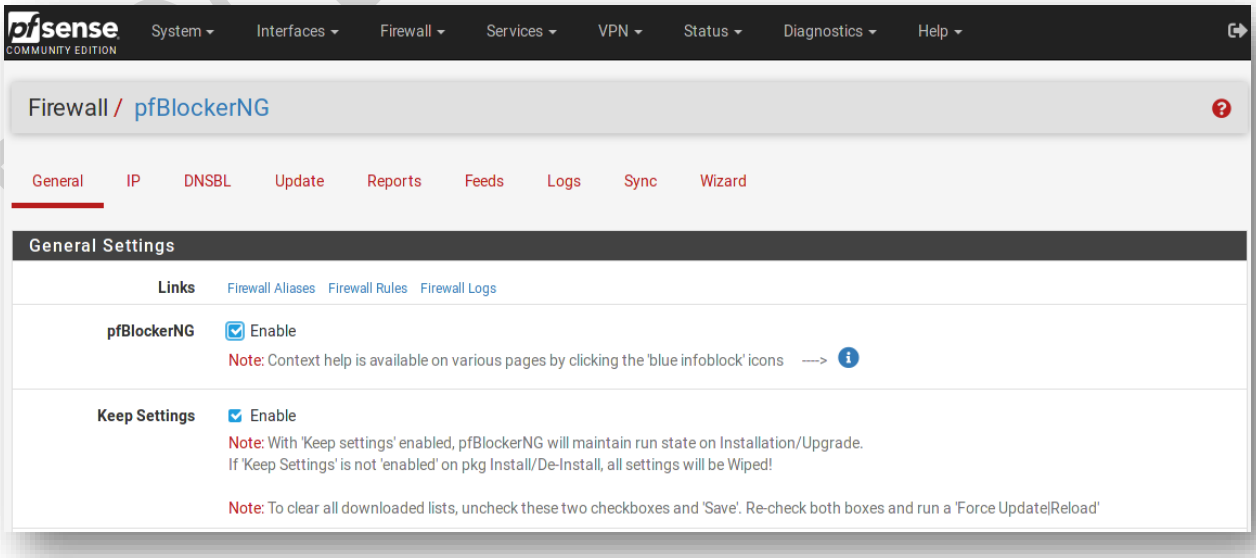
2. Installation de pfBlockerNG :

- Dans le menu de gauche, cliquer sur "System" puis "Package Manager".
- Aller dans l'onglet "Available Packages".
- Rechercher "pfBlockerNG" dans la barre de recherche.
- Cliquer sur "Install" pour installer le paquet.

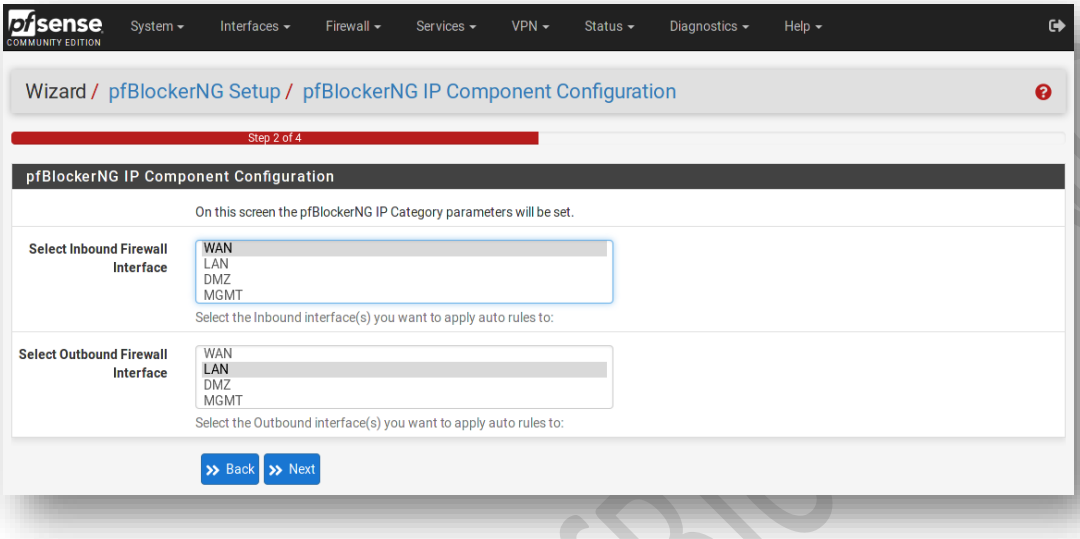


3. Configuration de pfBlockerNG :

- Une fois l'installation terminée, retourner dans le menu principal et cliquer sur "Firewall", puis "pfBlockerNG".
- Aller dans l'onglet "General".
- Activer pfBlockerNG en cochant la case "Enable".



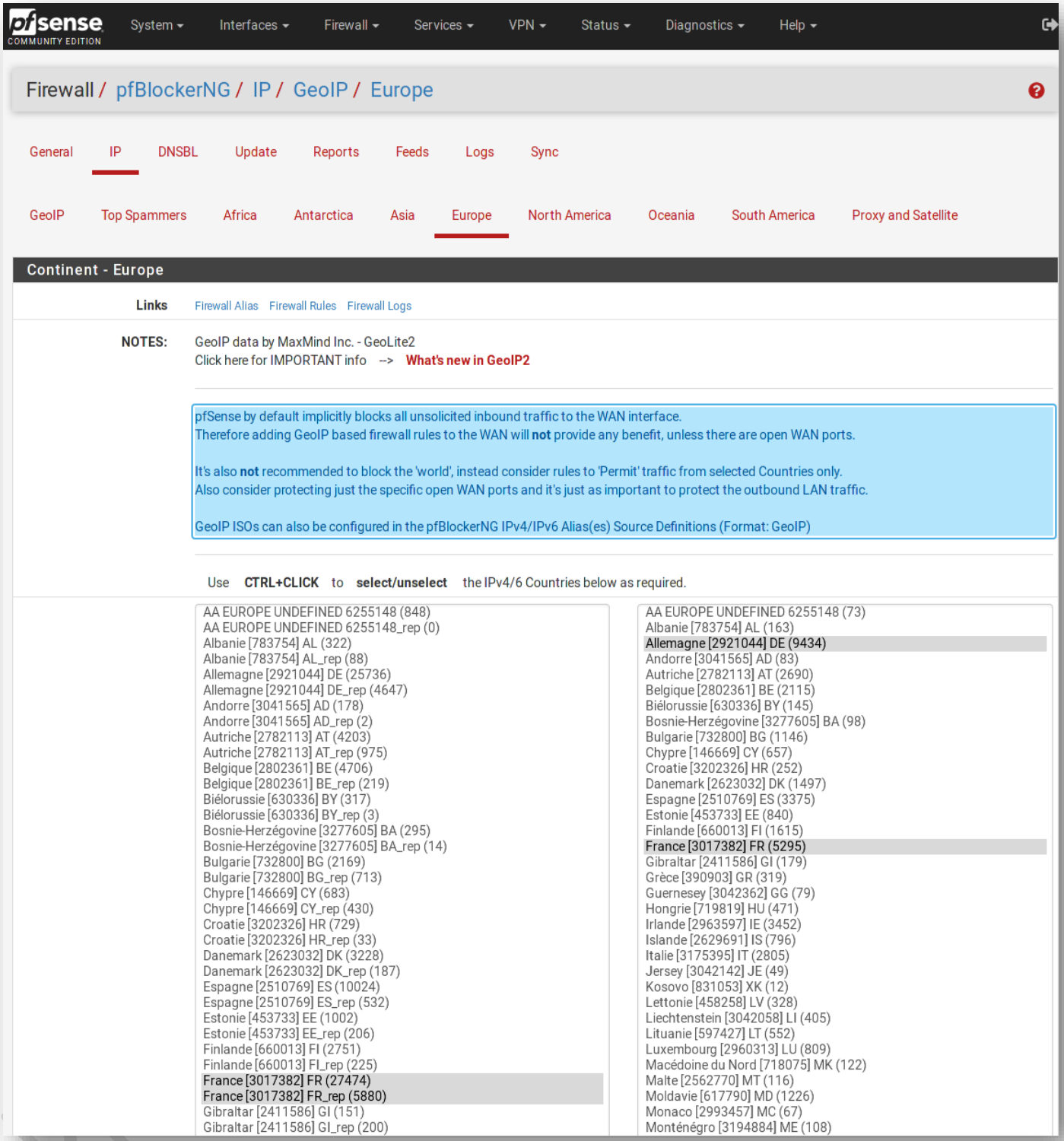
- Paramètres avancés :
    - Configuration des interfaces à surveiller : sélectionner les interfaces réseau à protéger avec pfBlockerNG.



    - Paramètres de blocage : définir le comportement des règles de blocage (par exemple, bloquer et loguer).
    - Mode de mise en liste blanche : configurer les adresses IP ou les plages à exclure des listes de blocage.
    - Options de journalisation : activer ou désactiver la journalisation des activités de pfBlockerNG.

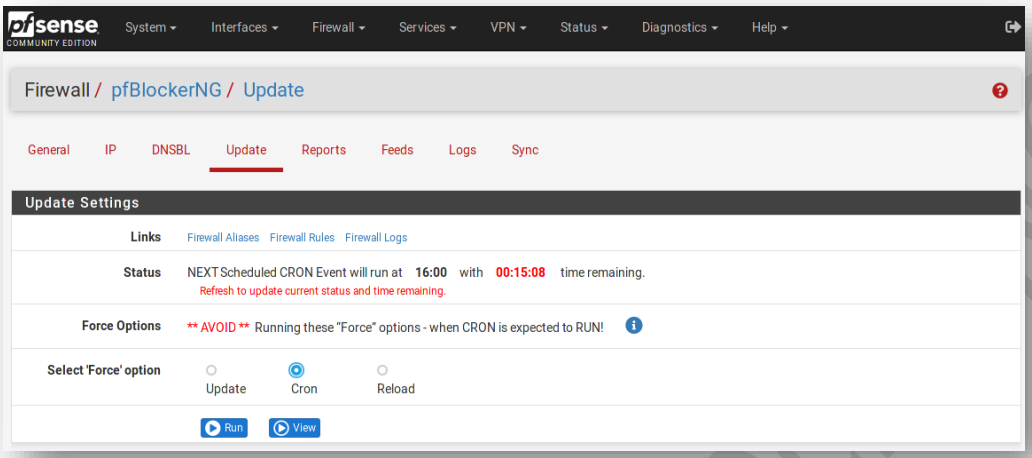
4. Configuration des listes de blocage :

- Aller dans l'onglet "IPv4" ou "IPv6" selon le type de trafic que tu souhaites filtrer.
- Ajouter des listes de blocage en cliquant sur "Add".
- Sélectionner le type de liste à utiliser :
    - DNSBL : pour bloquer les accès à des domaines malveillants.
    - GeoIP : pour bloquer les adresses IP en fonction de leur pays d'origine.
    - Liste d'adresses personnalisée : pour importer des listes externes de blocage.
- Configurer les sources de listes de blocage :
    - Pour DNSBL : ajouter des listes telles que "EasyList", "Malware Domains", etc.
    - Pour GeoIP : sélectionner les pays à bloquer.
- Configurer les options de mise à jour automatique selon tes préférences.


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / pfBlockerNG / IP / GeoIP / Europe
General
IP
DNSBL
Update
Reports
Feeds
Logs
Sync
GeoIP
Top Spammers
Africa
Antarctica
Asia
Europe
North America
Oceania
South America
Proxy and Satellite
Continent - Europe
Links
Firewall Alias
Firewall Rules
Firewall Logs
NOTES:
GeoIP data by MaxMind Inc. - GeoLite2
Click here for IMPORTANT info --> What's new in GeoIP2
pfSense by default implicitly blocks all unsolicited inbound traffic to the WAN interface.
Therefore adding GeoIP based firewall rules to the WAN will not provide any benefit, unless there are open WAN ports.
It's also not recommended to block the 'world', instead consider rules to 'Permit' traffic from selected Countries only.
Also consider protecting just the specific open WAN ports and it's just as important to protect the outbound LAN traffic.
GeoIP ISOs can also be configured in the pfBlockerNG IPv4/IPv6 Alias(es) Source Definitions (Format: GeoIP)
Use CTRL+CLICK to select/unselect the IPv4/6 Countries below as required.
AA EUROPE UNDEFINED 6255148 (848)
AA EUROPE UNDEFINED 6255148_rep (0)
Albanie [783754] AL (322)
Albanie [783754] AL_rep (88)
Allemagne [2921044] DE (25736)
Allemagne [2921044] DE_rep (4647)
Andorre [3041565] AD (178)
Andorre [3041565] AD_rep (2)
Autriche [2782113] AT (4203)
Autriche [2782113] AT_rep (975)
Belgique [2802361] BE (4706)
Belgique [2802361] BE_rep (219)
Biélorussie [630336] BY (317)
Biélorussie [630336] BY_rep (3)
Bosnie-Herzégovine [3277605] BA (295)
Bosnie-Herzégovine [3277605] BA_rep (14)
Bulgarie [732800] BG (2169)
Bulgarie [732800] BG_rep (713)
Chypre [146669] CY (683)
Chypre [146669] CY_rep (430)
Croatie [3202326] HR (729)
Croatie [3202326] HR_rep (33)
Danemark [2623032] DK (3228)
Danemark [2623032] DK_rep (187)
Espagne [2510769] ES (10024)
Espagne [2510769] ES_rep (532)
Estonie [453733] EE (1002)
Estonie [453733] EE_rep (206)
Finlande [660013] FI (2751)
Finlande [660013] FI_rep (225)
France [3017382] FR (27474)
France [3017382] FR_rep (5880)
Gibraltar [2411586] GI (151)
Gibraltar [2411586] GI_rep (200)
AA EUROPE UNDEFINED 6255148 (73)
Albanie [783754] AL (163)
Allemagne [2921044] DE (9434)
Andorre [3041565] AD (83)
Autriche [2782113] AT (2690)
Belgique [2802361] BE (2115)
Biélorussie [630336] BY (145)
Bosnie-Herzégovine [3277605] BA (98)
Bulgarie [732800] BG (1146)
Chypre [146669] CY (657)
Croatie [3202326] HR (252)
Danemark [2623032] DK (1497)
Espagne [2510769] ES (3375)
Estonie [453733] EE (840)
Finlande [660013] FI (1615)
France [3017382] FR (5295)
Gibraltar [2411586] GI (179)
Grèce [390903] GR (319)
Guernesey [3042362] GG (79)
Hongrie [719819] HU (471)
Irlande [2963597] IE (3452)
Islande [2629691] IS (796)
Italie [3175395] IT (2805)
Jersey [3042142] JE (49)
Kosovo [831053] XK (12)
Lettonie [458258] LV (328)
Liechtenstein [3042058] LI (405)
Lituanie [597427] LT (552)
Luxembourg [2960313] LU (809)
Macédoine du Nord [718075] MK (122)
Malte [2562770] MT (116)
Moldavie [617790] MD (1226)
Monaco [2993457] MC (67)
Monténégro [3194884] ME (108)

5. Appliquer les règles de filtrage :

- Une fois les listes de blocage configurées, cliquer sur "Update" pour télécharger les dernières données.
- Aller dans l'onglet "Update".
- Cliquer sur "Run" pour mettre à jour les listes de blocage.



6. Vérification du fonctionnement :

- Accéder à l'onglet "Alerts" pour surveiller les activités bloquées par pfBlockerNG.
- Tester le filtrage en tentant d'accéder à des ressources bloquées pour vérifier que pfBlockerNG fonctionne correctement.