CONTEXTE ENTREPRISE CPACCARD IT

BTS – SIO 2022/2024

GeoIP

AUTO GEO LOCATION

Clément PACCARD

TABLE DES MATIERES

PRESENTATION ENTREPRISE

L’entreprise CPACCARD IT, située à Annecy, comporte actuellement un employé, Clément PACCARD. Elle souhaite augmenter la sécurité de son accès à internet.

La société souhaite interdire l’accès aux sites web hébergés dans des pays dit à risques.

Pour répondre aux exigences de la société, la solution retenue a été une sécurisation par Géolocalisation IP avec pfBlocker NG.

Le pare-feu de l’entreprise est un PfSense, il s’agit d’une distribution open source de firewall et de routeur basée sur le système d'exploitation FreeBSD.

1- PFBLOCKER NG

La première étape a été d'installer le plugin pfBlocker NG sur le pare-feu de l'entreprise. Pour ce faire :

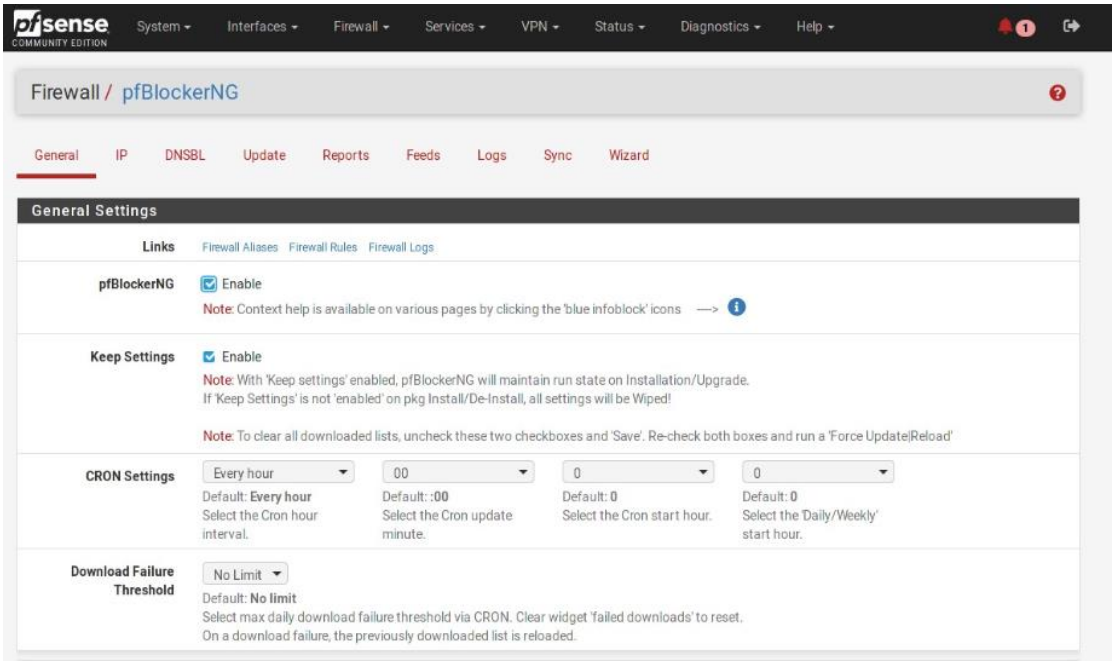
- Aller dans le menu System > Package Manager > Available Packages.

- Chercher le paquet pfBlockerNG et cliquer sur le bouton Install à droite.

- Confirmer l'installation en cliquant sur Confirm.

- Aller dans le menu Firewall > pfBlockerNG et cliquer sur l'onglet General.

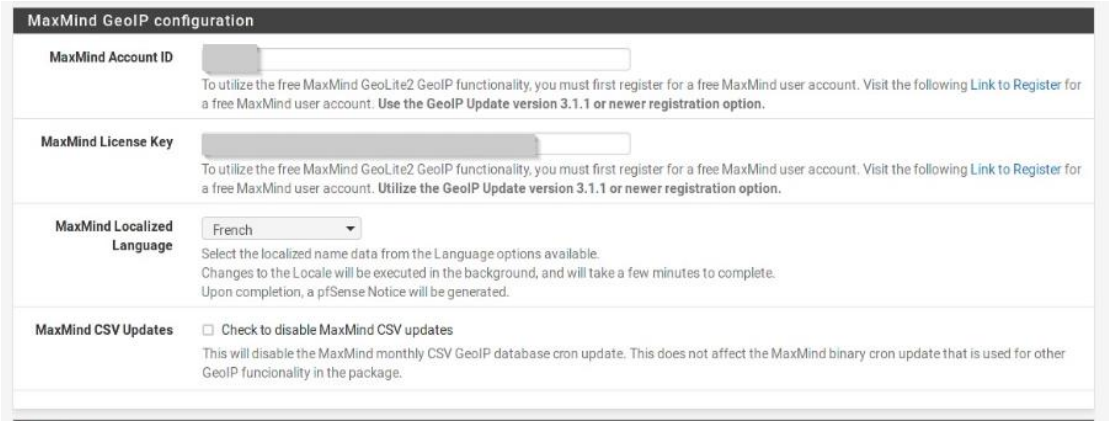
- Activer le service pfBlockerNG en cochant la case Enable pfBlockerNG.



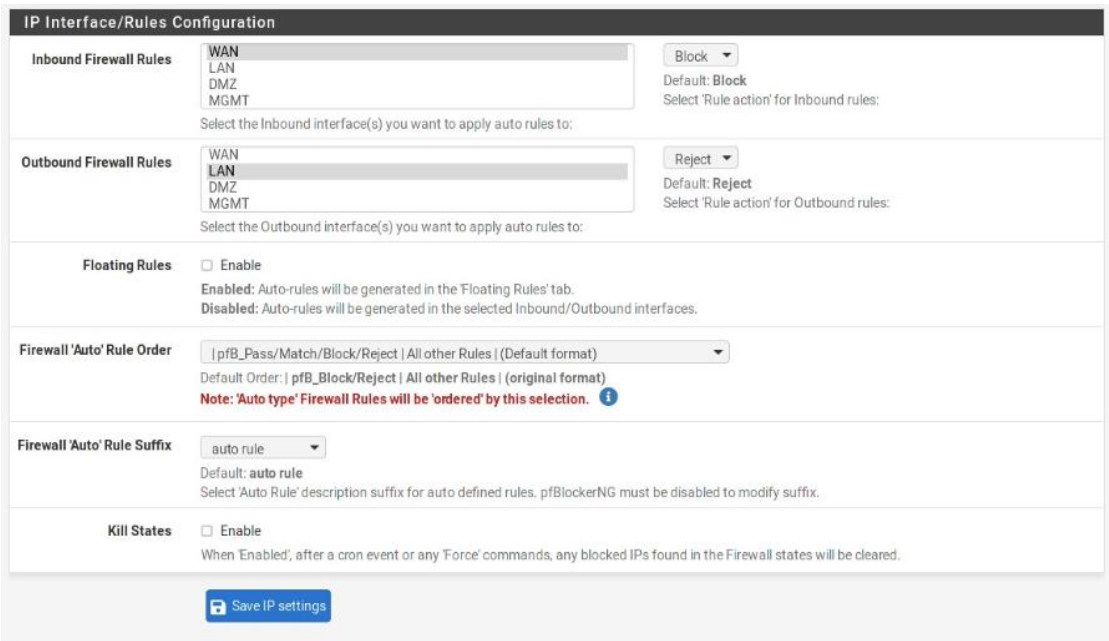
La deuxième étape a été de configurer les réglages de bases. Il faut au préalable créer un compte MaxMind et obtenir une clé de licence pour utiliser le service (dans mon cas la clé et le numéro de compte m'ont été fourni).

- Cliquer sur l'onglet IP.

- Entrer le MaxMind Account ID et la clé de licence.



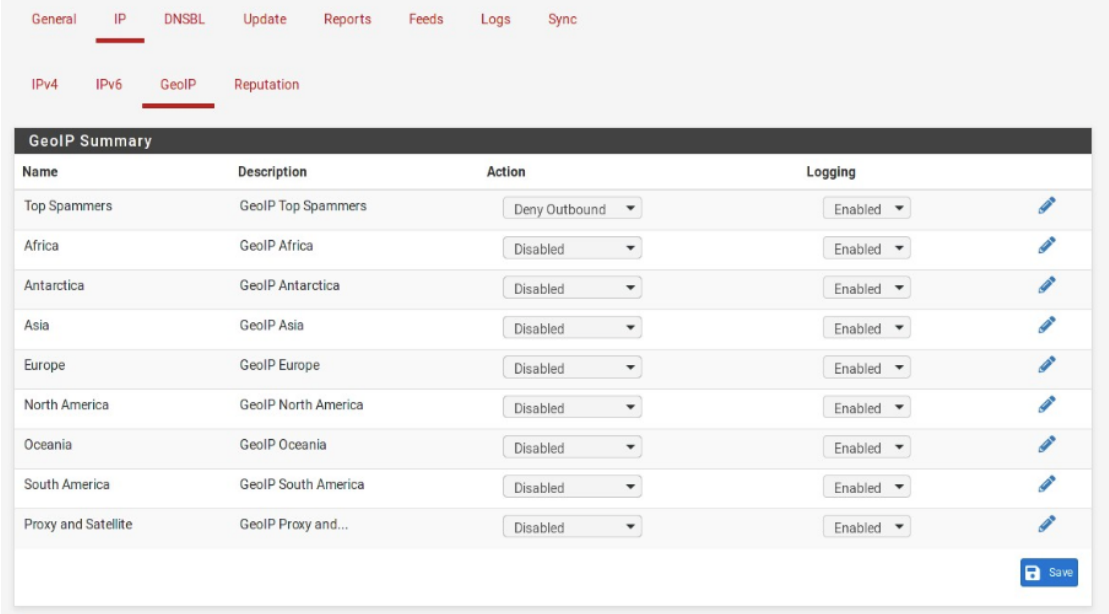
- Par défaut les réglages IP Interfaces sont corrects. Il faut qu'il soit dans la configuration suivante :



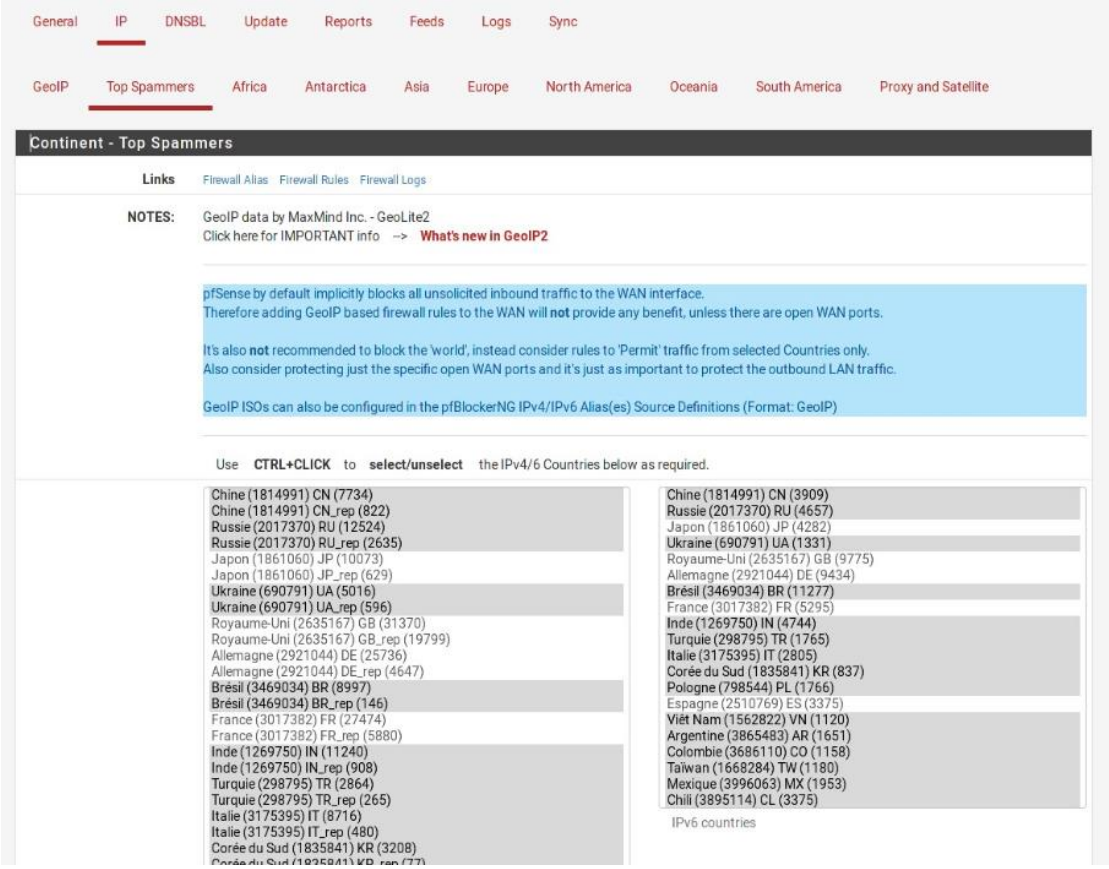
La troisième étape a été de configurer les pays dit à risques pour bloquer l'accès à leurs sites web. Pour ce faire :

- Cliquer sur l'onglet IP > GeoIP.

- Dans Top Spammers, définir l'action sur Deny Outbound puis cliquer sur le crayon pour modifier la liste.

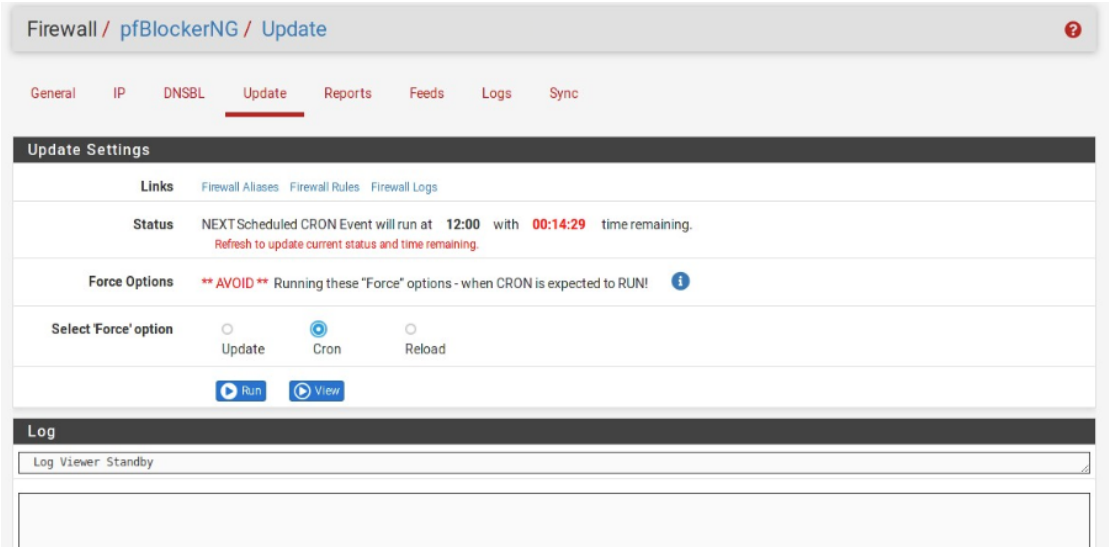


- On peut ici sélectionner les pays que l'on souhaite interdire et bloquer. Par défaut on a la liste des plus réputés mais il est possible de sélectionner des pays plus spécifiques dans les continents (Onglets dans la partie supérieur).



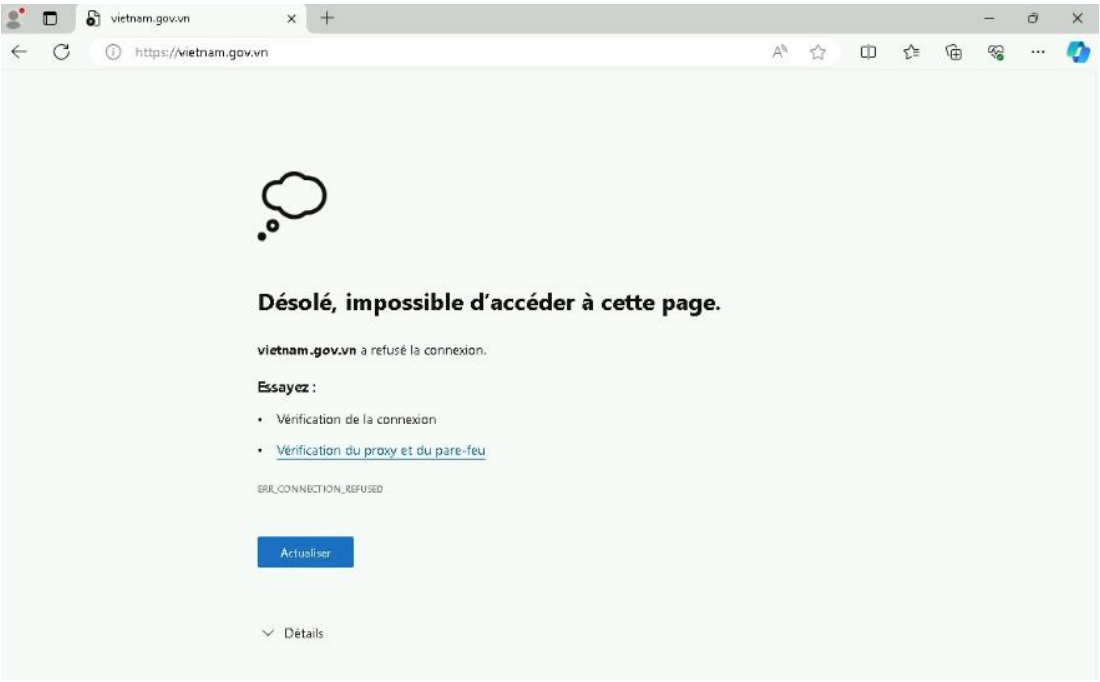
- Cliquer sur Save en bas de la page pour valider les changements et appliquer le blocage.

ATTENTION pour chaque modification il faut faire un Cron Update. Pour ce faire il faut se rendre dans l'onglet update et sélectionner Cron puis Run.



Enfin la dernière étape à été de tester ces blocages. Le plus simple dans ce cas est de prendre un site internet, de vérifier qu'il est bien hébergé dans l'un des pays bloqué (ex. //vietnam.gov.vn hébergé au Vietnam, source : https://my-ip-finder.fr). On va ensuite tenter de joindre ce site web depuis un poste dans le LAN 1 (ex. Serveur 1).

On a bien le message suivant :



Le blocage est donc fonctionnel.

2- EVOLUTIONS POSSIBLES

Voici une liste d’évolutions possibles :

- Configurer des règles de pare-feu plus granulaires en fonction du protocole ou du port.

- Créer des listes blanches de pays autorisés à accéder aux services critiques de l'entreprise.

- Activer des rapports sur les tentatives de connexion suspectes ou inhabituelles depuis des pays étrangers.

- Tester régulièrement la fiabilité et la performance des services de géolocalisation utilisés.

3- LIMITATIONS

Le téléchargement des listes DNSBL est impossible car certains ports sont bloqués par le réseau de l’école. Ainsi le pare-feu ne peut joindre les serveurs concernés.