

# CONTEXTE ENTREPRISE CPACCARD IT

**BTS – SIO 2022/2024**



**AUTO GEO LOCATION**

**Clément PACCARD**

# TABLE DES MATIERES

|                     |                      |               |
|---------------------|----------------------|---------------|
| <b>PRESENTATION</b> | <b>ENTREPRISE</b>    | <b>.....1</b> |
| 1-                  | pfBlocker NG         | .....2        |
| 2-                  | Evolutions possibles | .....7        |
| 3-                  | Limitations          | .....7        |

# 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.

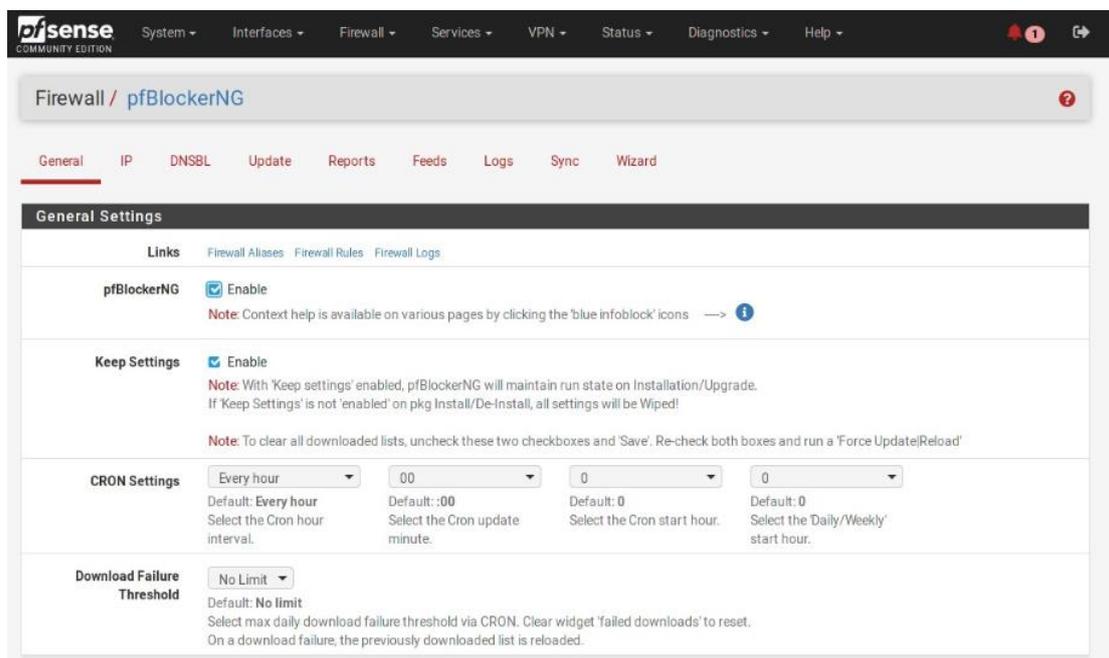
Pour répondre aux exigences de la société, la solution retenue a été une sécurisation par Géolocalisation IP avec pfBlocker NG.

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

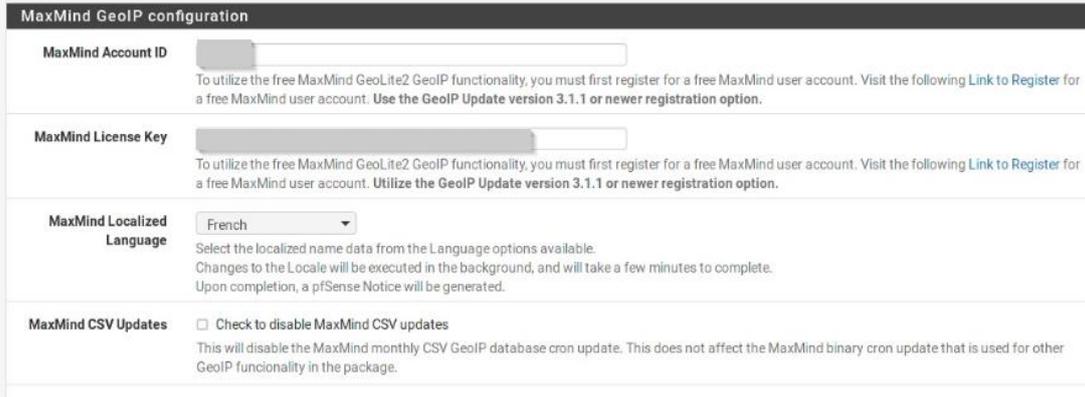
La première étape a été d'installer le plugin pfBlocker NG sur le pare-feu de l'entreprise. Pour ce faire :

- 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).

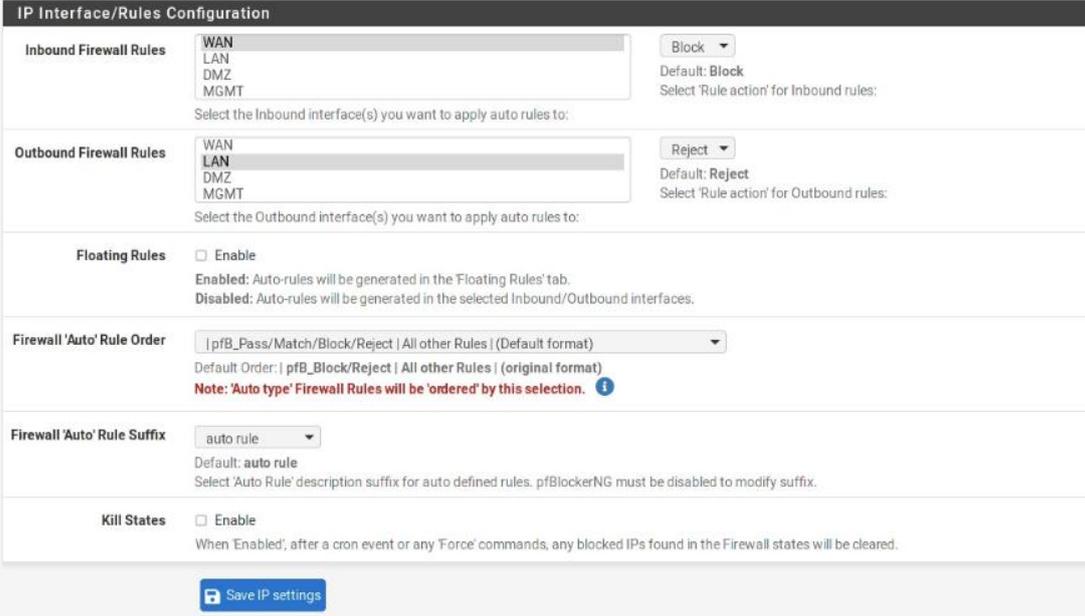
- Cliquer sur l'onglet IP.
- Entrer le MaxMind Account ID et la clé de licence.



The screenshot shows the 'MaxMind GeoIP configuration' page. It contains four main sections:

- MaxMind Account ID:** A text input field with a greyed-out value. Below it, a note states: 'To utilize the free MaxMind GeoLite2 GeoIP functionality, you must first register for a free MaxMind user account. Visit the following [Link to Register](#) for a free MaxMind user account. Use the **GeoIP Update version 3.1.1 or newer registration option**.'
- MaxMind License Key:** A text input field with a greyed-out value. Below it, a note states: 'To utilize the free MaxMind GeoLite2 GeoIP functionality, you must first register for a free MaxMind user account. Visit the following [Link to Register](#) for a free MaxMind user account. Utilize the **GeoIP Update version 3.1.1 or newer registration option**.'
- MaxMind Localized Language:** A dropdown menu set to 'French'. Below it, a note states: 'Select the localized name data from the Language options available. Changes to the Locale will be executed in the background, and will take a few minutes to complete. Upon completion, a pfSense Notice will be generated.'
- MaxMind CSV Updates:** A checkbox labeled 'Check to disable MaxMind CSV updates' which is currently unchecked. Below it, a note states: 'This will disable the MaxMind monthly CSV GeoIP database cron update. This does not affect the MaxMind binary cron update that is used for other GeoIP functionality in the package.'

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



The screenshot shows the 'IP Interface/Rules Configuration' page. It contains several sections:

- Inbound Firewall Rules:** A dropdown menu with 'WAN' selected. To the right, a 'Block' dropdown menu is set to 'Block'. Below it, a note states: 'Default: Block. Select 'Rule action' for Inbound rules:'. Below the dropdowns, a note states: 'Select the Inbound interface(s) you want to apply auto rules to:'.
- Outbound Firewall Rules:** A dropdown menu with 'WAN' selected. To the right, a 'Reject' dropdown menu is set to 'Reject'. Below it, a note states: 'Default: Reject. Select 'Rule action' for Outbound rules:'. Below the dropdowns, a note states: 'Select the Outbound interface(s) you want to apply auto rules to:'.
- Floating Rules:** A checkbox labeled 'Enable' which is currently unchecked. Below it, a note states: 'Enabled: Auto-rules will be generated in the 'Floating Rules' tab. Disabled: Auto-rules will be generated in the selected Inbound/Outbound interfaces.'
- Firewall 'Auto' Rule Order:** A dropdown menu with '| pfB\_Pass/Match/Block/Reject | All other Rules | (Default format)' selected. Below it, a note states: 'Default Order: | pfB\_Block/Reject | All other Rules | (original format)'. Below that, a note states: 'Note: 'Auto type' Firewall Rules will be 'ordered' by this selection. ⓘ'.
- Firewall 'Auto' Rule Suffix:** A dropdown menu with 'auto rule' selected. Below it, a note states: 'Default: auto rule. Select 'Auto Rule' description suffix for auto defined rules. pfBlockerNG must be disabled to modify suffix.'
- Kill States:** A checkbox labeled 'Enable' which is currently unchecked. Below it, a note states: 'When 'Enabled', after a cron event or any 'Force' commands, any blocked IPs found in the Firewall states will be cleared.'

At the bottom of the page, there is a blue button labeled 'Save IP settings'.

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.

The screenshot shows a web application interface for configuring GeoIP. The navigation menu includes 'General', 'IP', 'DNSBL', 'Update', 'Reports', 'Feeds', 'Logs', and 'Sync'. Under 'IP', there are sub-menus for 'IPv4', 'IPv6', 'GeoIP', and 'Reputation'. The 'GeoIP Summary' table is displayed below, with columns for Name, Description, Action, and Logging. The 'Top Spammers' row is highlighted, showing 'Deny Outbound' as the action and 'Enabled' as the logging status. A 'Save' button is located at the bottom right of the table.

| Name                | Description         | Action        | Logging |
|---------------------|---------------------|---------------|---------|
| Top Spammers        | GeoIP Top Spammers  | Deny Outbound | Enabled |
| Africa              | GeoIP Africa        | Disabled      | Enabled |
| Antarctica          | GeoIP Antarctica    | Disabled      | Enabled |
| Asia                | GeoIP Asia          | Disabled      | Enabled |
| Europe              | GeoIP Europe        | Disabled      | Enabled |
| North America       | GeoIP North America | Disabled      | Enabled |
| Oceania             | GeoIP Oceania       | Disabled      | Enabled |
| South America       | GeoIP South America | Disabled      | Enabled |
| Proxy and Satellite | GeoIP Proxy and...  | Disabled      | Enabled |

- 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).

The screenshot shows the 'Continent - Top Spammers' configuration page. At the top, there are navigation tabs: General, IP (selected), DNSBL, Update, Reports, Feeds, Logs, Sync. Below these are continent-specific tabs: GeolIP, Top Spammers (selected), Africa, Antarctica, Asia, Europe, North America, Oceania, South America, Proxy and Satellite.

The main content area is titled 'Continent - Top Spammers' and includes a 'Links' section with 'Firewall Alias', 'Firewall Rules', and 'Firewall Logs'. A 'NOTES' section contains the following text:

GeolIP data by MaxMind Inc. - GeoLite2  
 Click here for IMPORTANT info -> [What's new in GeolIP2](#)

pfSense by default implicitly blocks all unsolicited inbound traffic to the WAN interface. Therefore adding GeolIP 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.

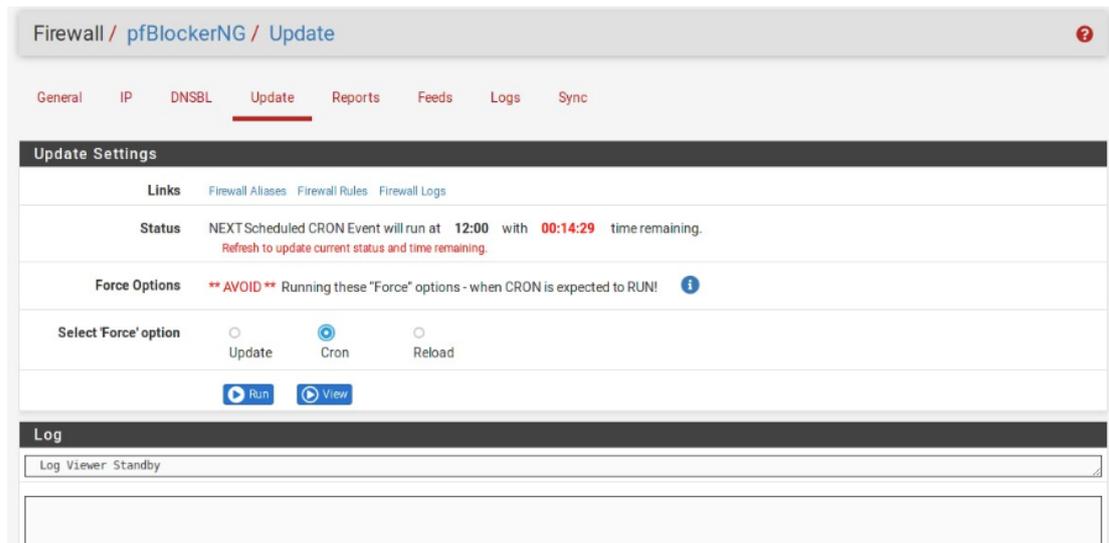
GeolIP ISOs can also be configured in the pfBlockerNG IPv4/IPv6 Alias(es) Source Definitions (Format: GeolIP)

Use **CTRL+CLICK** to **select/unselect** the IPv4/6 Countries below as required.

The interface displays two columns of country lists. The left column lists IPv4 countries, and the right column lists IPv6 countries. Each entry includes the country name, its ISO code, and the number of IP addresses. For example, in the IPv4 list, 'Chine (1814991) CN (7734)' is highlighted. In the IPv6 list, 'Russie (2017370) RU (4657)' is highlighted.

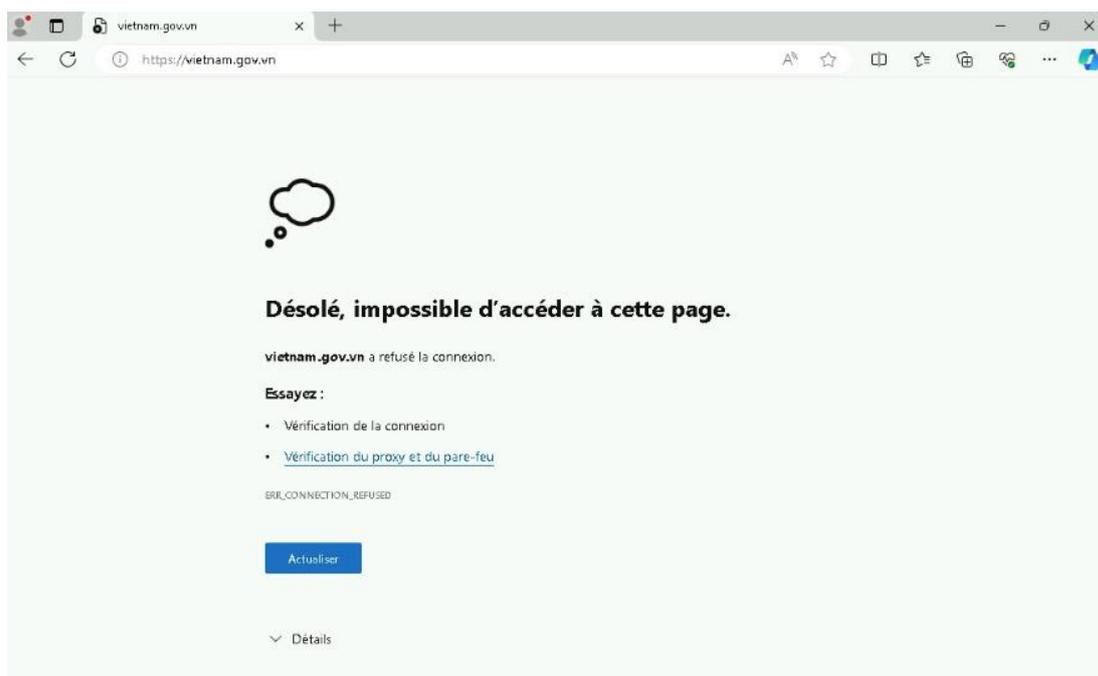
- Cliquer sur Save en bas de la page pour valider les changements et appliquer le blocage.

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.