Réglages permettant d'utiliser fail2ban derrière HAProxy

Difficulté

Moyen

Le service fail2ban d'une machine située derrière le HAProxy (càd un “real server”) ne peut fonctionner correctement car toutes les requêtes lui arrivent via le proxy ⇒ bannir l'IP d'origine de la requête ne sert à rien (car requête arrive du proxy) ⇒ la requête arrive tout de même ou alors c'est le proxy, donc tout communication, qui est banni.

Il faut donc que le “real server” demande à OPNSense de bannir les mauvaises IPs pour lui.

Créer un utilisateur

- sans aucun privilège.
- éditer son profil
  - lui donner uniquement les privilèges `Diagnostics: PF Table IP addresses`
  - créer la clé API et bien sauvegarder les informations de connexion

Créer un alias

`Firewall` ⇒ `Aliases` de type `Host(s)` sans renseigner d'ip.

Créer 2 règles de blocage dans le firewall

Une pour http, l'autre pour https. Dans le WAN:

```
 blocage   IPv4+6 TCP/UDP   alias_ci_dessus      *     alias-HAProxy     80
(HTTP)     *     *     blocage http fail2ban
 blocage   IPv4+6 TCP/UDP   alias_ci_dessus      *     alias-HAProxy     443
(HTTPS)     *     *     blocage http fail2ban
```

Communiquer l'ip à bannir

Il faut maintenant que le “real server” puisse se connecter à OPNSense via une ligne de commande “curl” pour indiquer la/les ip(s) à assigner à l'alias de blocage.
Cette communication s'effectue en https. Il faut donc:

1. Créer si nécessaire une règle de passage TCP dans le firewall:
   Source = le real server , destination = l'adresse de OPNsense située dans le réseau du real server , port = celui utilisé pour joindre l'interface web GUI.

2. Configurer si nécessaire l'interface web pour qu'elle soit joignable depuis le réseau du real server:
`System` ⇒ `Settings` ⇒ `Administration` ⇒ `Web GUI` ⇒ `Listen interfaces`

From:
https://wiki.guedel.eu/ - **Wiki-GuedeL**

Permanent link:
https://wiki.guedel.eu/doku.php?id=welcome:opnsense:haproxy_et_fail2ban&rev=1639514194

Last update: **2021/12/14 20:36**