

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 ⇒ banir 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 toute communication, qui est banni.

Il faut donc que le "real server" demande à OPNSense de banir 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 une règle de blocage dans le firewall

From:
<https://wiki.guedel.eu/> - Wiki-GuedeL

Permanent link:
https://wiki.guedel.eu/doku.php?id=welcome:opnsense:haproxy_et_fail2ban&rev=1639513006

Last update: 2021/12/14 20:16

