## Suivi des modifications

| *Version* | *Référence* | *Auteur* | *Date* | *Commentaires* |
|---|---|---|---|---|
| A | TP_Abo | Alexandre | 29/01/2025 | Création |
| | | | | |
| | | | | |

## Objet :

Mise en place d'un serveur Docker et Portainer sous Debian 12

## Diffusion :

BTS SIO – Étudiants BTS SIO.

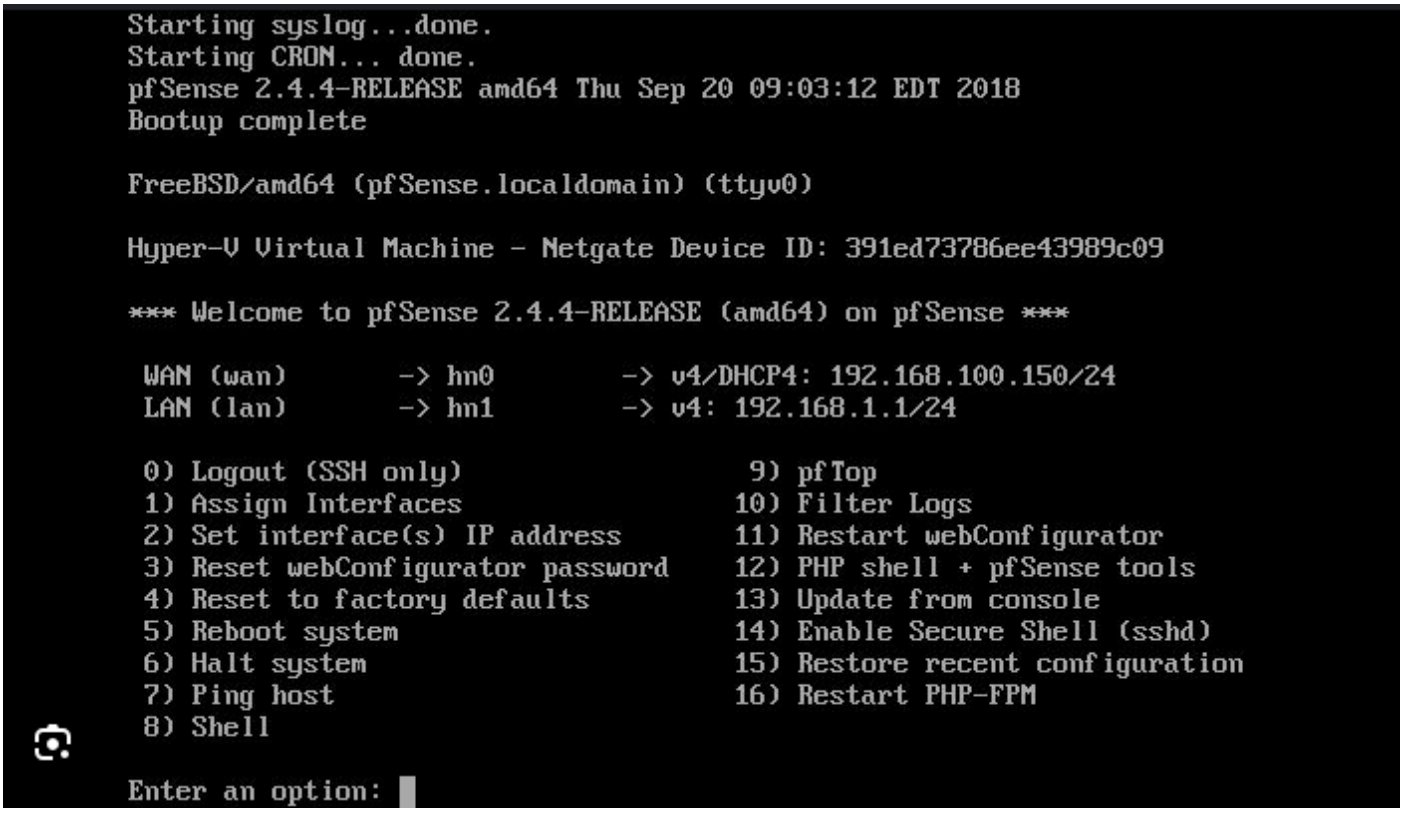
---

## Développement :

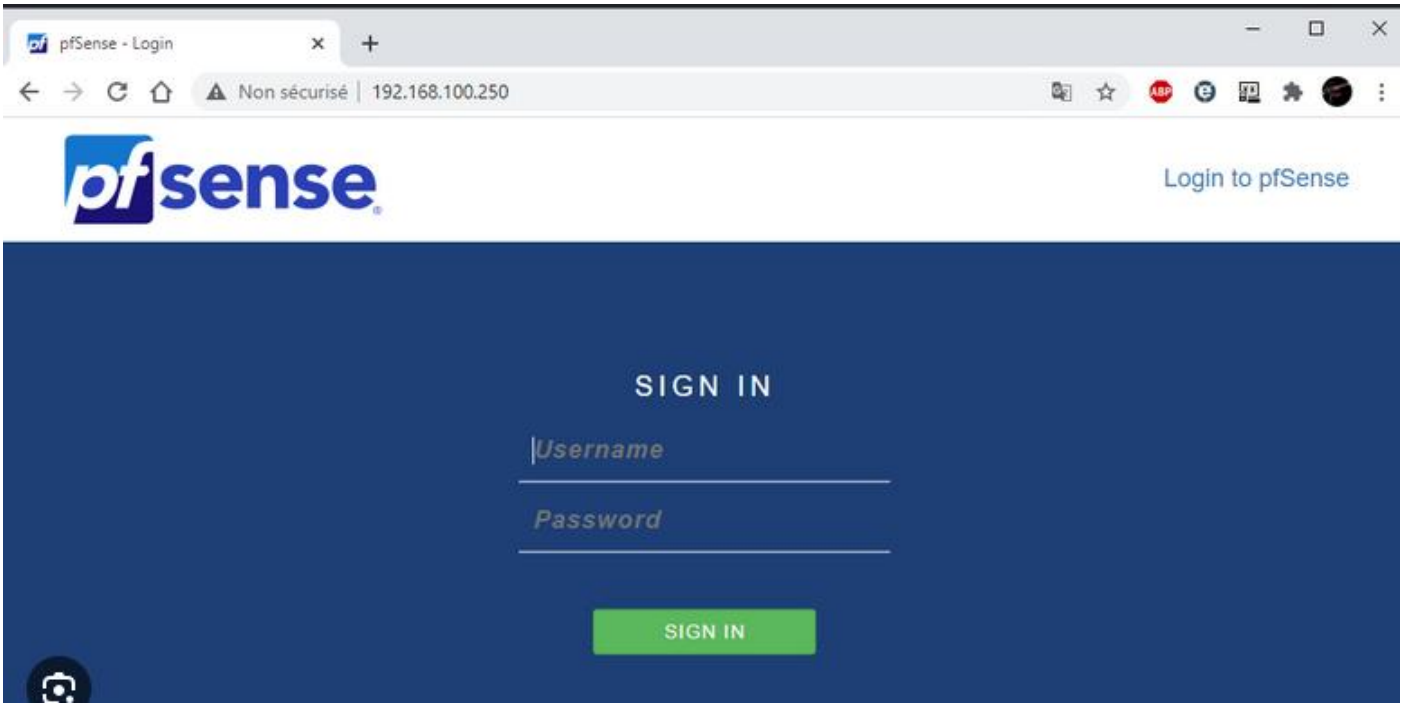
# Table des matières

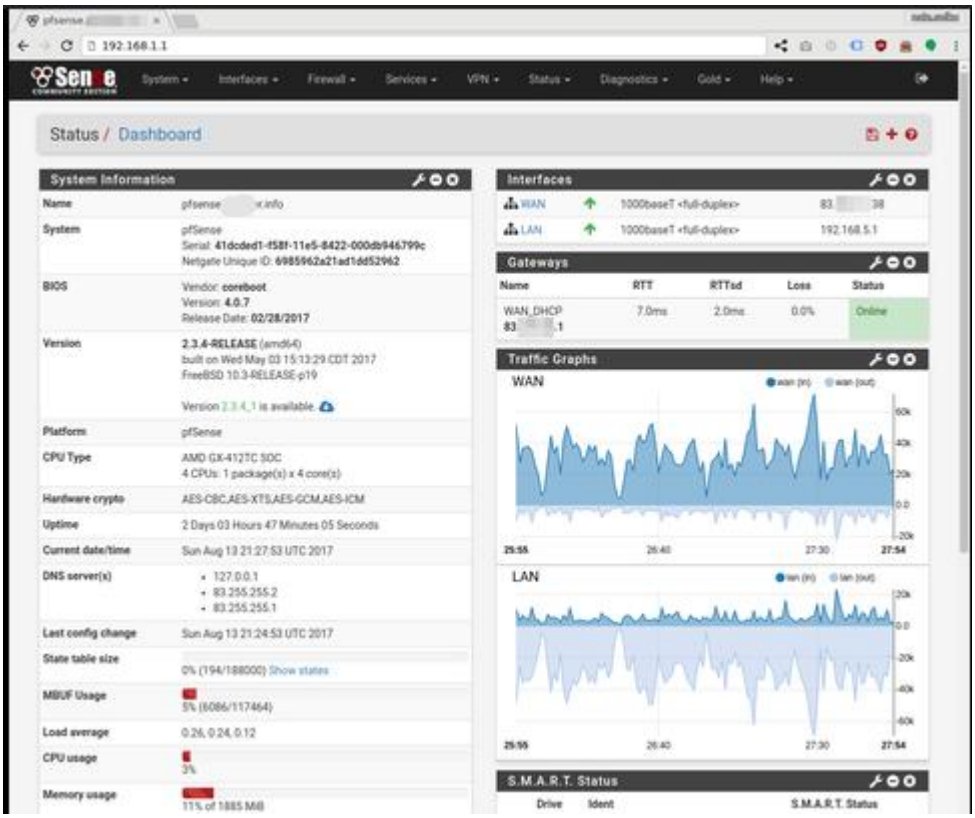
# Installation pfSense

L'installation de pfSense ce fait assez simplement. Nous devons juste définir son adresse IP coté WAN, celle qui nous donnera internet, et son adresse IP coté LAN, ça sera notre passerelle pour notre réseau local. pfSense sera notre routeur mais également notre pare-feu (firewall) pour notre réseau LAN, il peut également faire office de proxy transparent, afin de bloquer certains site.




Une fois l'installation faite tout ce passera sur l'interface web de pfSense.

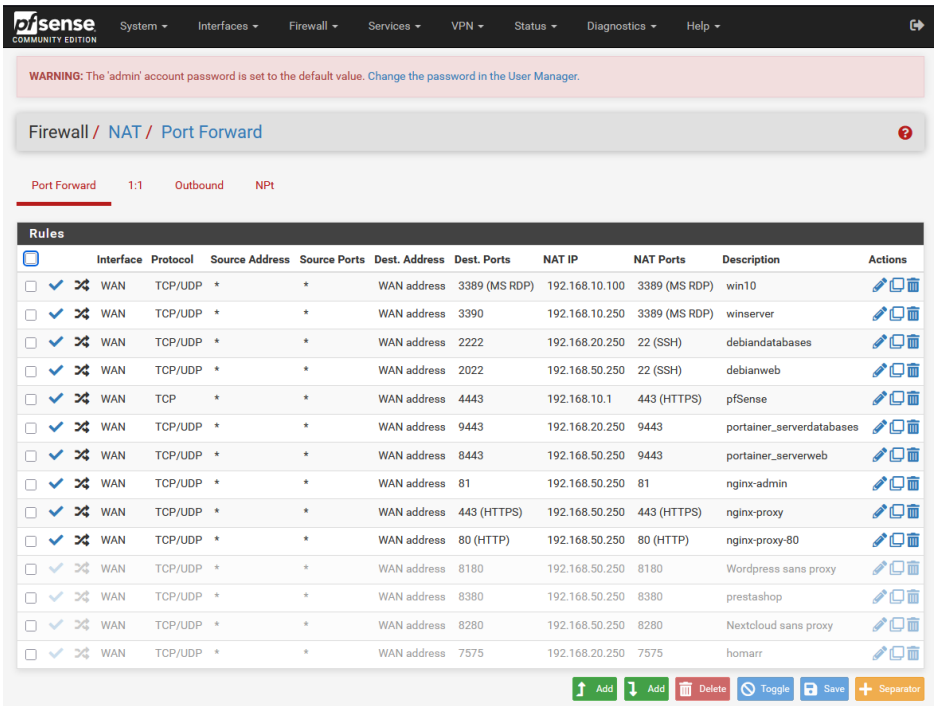




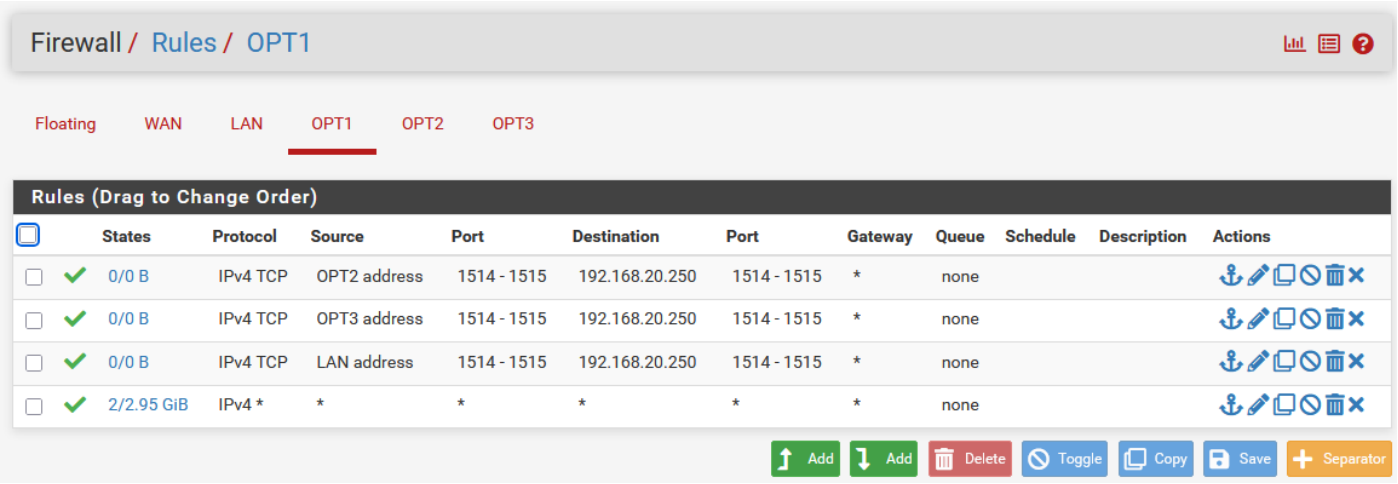

# Configuration du Pare-Feu pfSense

Le pare-feu de pfSense permet de bloquer des ports, ou de faire des redirections de ports si nécessaire.

Exemple de règles de redirection de ports.




Règles de pare-feu.



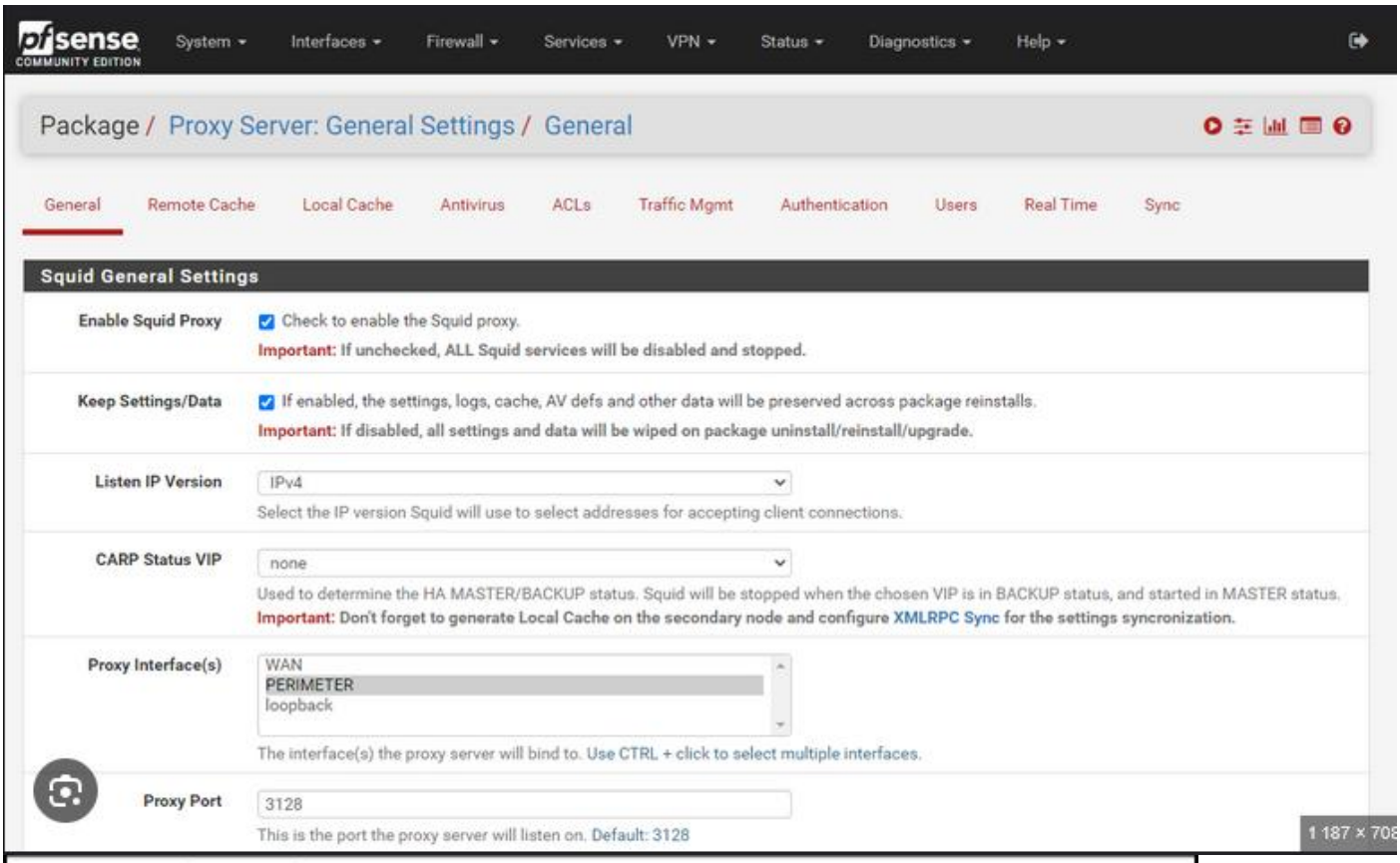

Ces règles permettent le bon fonctionnement de l'agent Wazuh, ainsi l'agent peut communiquer avec son serveur même si celui-ci est dans un VLAN différent que celui du serveur.

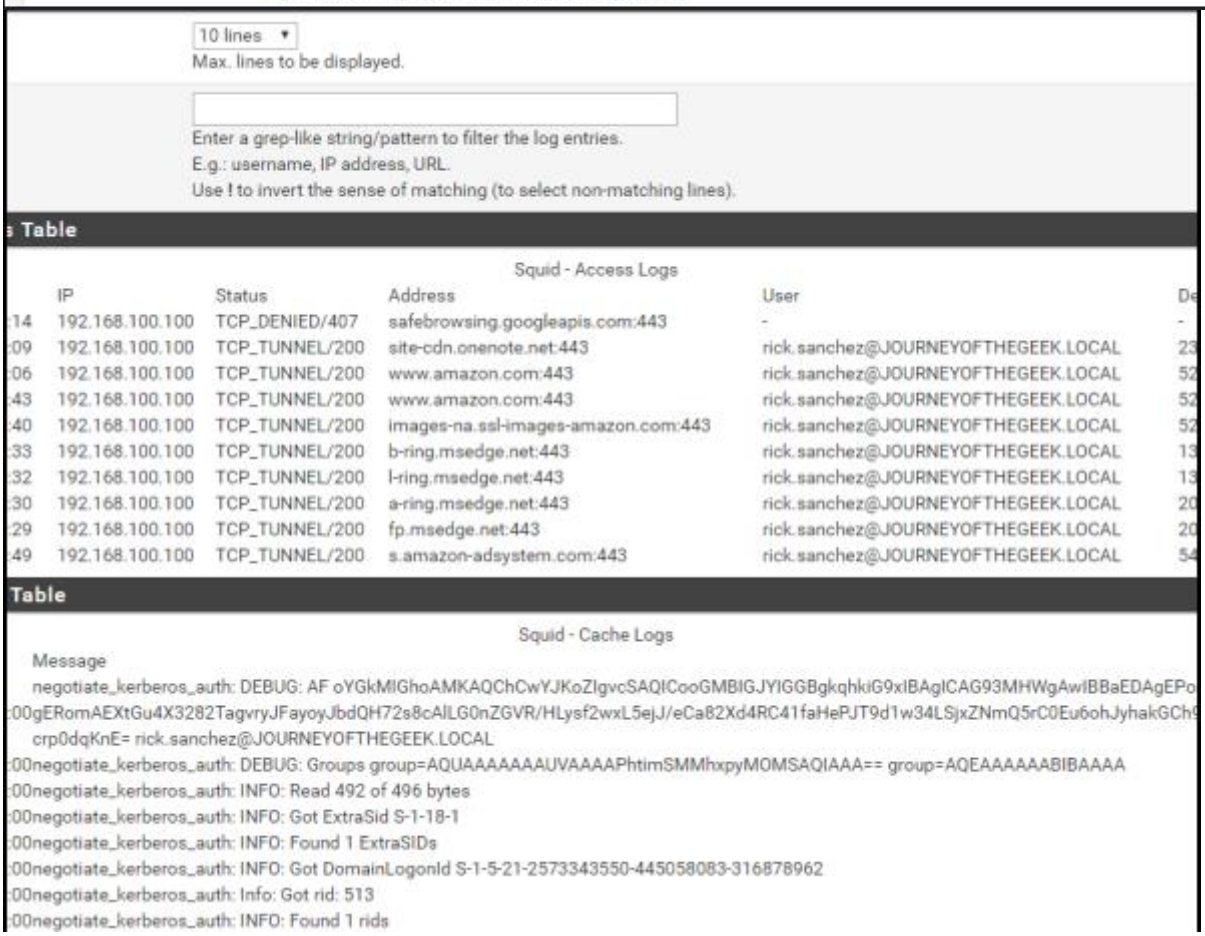
## Configuration du proxy squid

Nous allons utiliser Squid en mode proxy transparent. Cela signifie que le trafic web des utilisateurs sera redirigé automatiquement vers le proxy, sans configuration manuelle sur les postes clients.

Dans ce mode, Squid ne déchiffre pas le contenu des paquets HTTPS, mais se limite à lire le nom de domaine (SNI - Server Name Indication) contenu dans la requête TLS. Grâce à cette information, Squid peut appliquer des règles de filtrage pour autoriser ou bloquer l'accès à certains sites en fonction de leur fiabilité ou de leur catégorie.

Ce fonctionnement permet de filtrer efficacement le trafic HTTPS sans inspection approfondie du contenu, ce qui évite des problèmes de certificats ou de confidentialité, mais limite aussi la finesse du contrôle (pas de filtrage par URL ou contenu précis en HTTPS).


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Proxy Server: General Settings / General
General
Remote Cache
Local Cache
Antivirus
ACLs
Traffic Mgmt
Authentication
Users
Real Time
Sync
Squid General Settings
Enable Squid Proxy
Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data
If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version
IPv4
Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP
none
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.
Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings syncronization.
Proxy Interface(s)
WAN
PERIMETER
loopback
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Proxy Port
3128
This is the port the proxy server will listen on. Default: 3128
1 187 × 708


10 lines
Max. lines to be displayed.
Enter a grep-like string/pattern to filter the log entries.
E.g.: username, IP address, URL.
Use ! to invert the sense of matching (to select non-matching lines).
Table
Squid - Access Logs
IP Status Address User
14 192.168.100.100 TCP_DENIED/407 safebrowsing.googleapis.com:443 -
09 192.168.100.100 TCP_TUNNEL/200 site-cdn.onenote.net:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
06 192.168.100.100 TCP_TUNNEL/200 www.amazon.com:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
43 192.168.100.100 TCP_TUNNEL/200 www.amazon.com:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
40 192.168.100.100 TCP_TUNNEL/200 images-na.ssl-images-amazon.com:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
33 192.168.100.100 TCP_TUNNEL/200 b-ring.msedge.net:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
32 192.168.100.100 TCP_TUNNEL/200 l-ring.msedge.net:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
30 192.168.100.100 TCP_TUNNEL/200 a-ring.msedge.net:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
29 192.168.100.100 TCP_TUNNEL/200 fp.msedge.net:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
49 192.168.100.100 TCP_TUNNEL/200 s.amazon-adsystem.com:443 rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
Table
Squid - Cache Logs
Message
negotiate_kerberos_auth: DEBUG: AF oYGkMIGhoAMKAQChCwYJKoZIgvcSAQICooGMBIGJYIGGBgkqhkiG9xIBAgICAG93MHWgAwIBBaEDAgEPo
00gERomAEXtGu4X3282TagvryJFayoyJbdQH72s8cAlLG0nZGVR/HLysf2wxL5ejJ/eCa82Xd4RC41faHePJT9d1w34LSjxZNmQ5rC0Eu6ohJyhakGCh9
crp0dqKnE= rick.sanchez@JOURNEYOFTHEGEEK.LOCAL
00negotiate_kerberos_auth: DEBUG: Groups group=AQUAAAAAAAUVAAAAPhtimSMMhxpyMOMSAQIAAA== group=AQEAAAAAABIBAAAA
00negotiate_kerberos_auth: INFO: Read 492 of 496 bytes
00negotiate_kerberos_auth: INFO: Got ExtraSid S-1-18-1
00negotiate_kerberos_auth: INFO: Found 1 ExtraSIDs
00negotiate_kerberos_auth: INFO: Got DomainLogonId S-1-5-21-2573343550-445058083-316878962
00negotiate_kerberos_auth: Info: Got rid: 513
00negotiate_kerberos_auth: INFO: Found 1 rids

# Configuration VPN

Nous allons utiliser pfSense pour mettre en place un VPN (réseau privé virtuel), ce qui permettra aux utilisateurs d'accéder à distance au réseau local de manière sécurisée, comme s'ils étaient physiquement connectés à celui-ci.

Le VPN créé avec pfSense établit un tunnel chiffré entre le poste client et le routeur pfSense, garantissant la confidentialité et l'intégrité des données qui transitent. Cela est particulièrement utile pour le télétravail, l'accès à des serveurs internes ou encore pour connecter plusieurs sites distants entre eux.

Avec pfSense, il est possible de configurer différents types de VPN, comme OpenVPN, IPSec ou WireGuard, chacun ayant ses avantages. OpenVPN est souvent privilégié pour sa compatibilité et sa simplicité de mise en œuvre. Une fois configuré, le VPN ne nécessite qu'un petit client sur l'ordinateur distant, et les règles de pare-feu permettent de contrôler précisément ce à quoi l'utilisateur a accès à travers le tunnel VPN.