

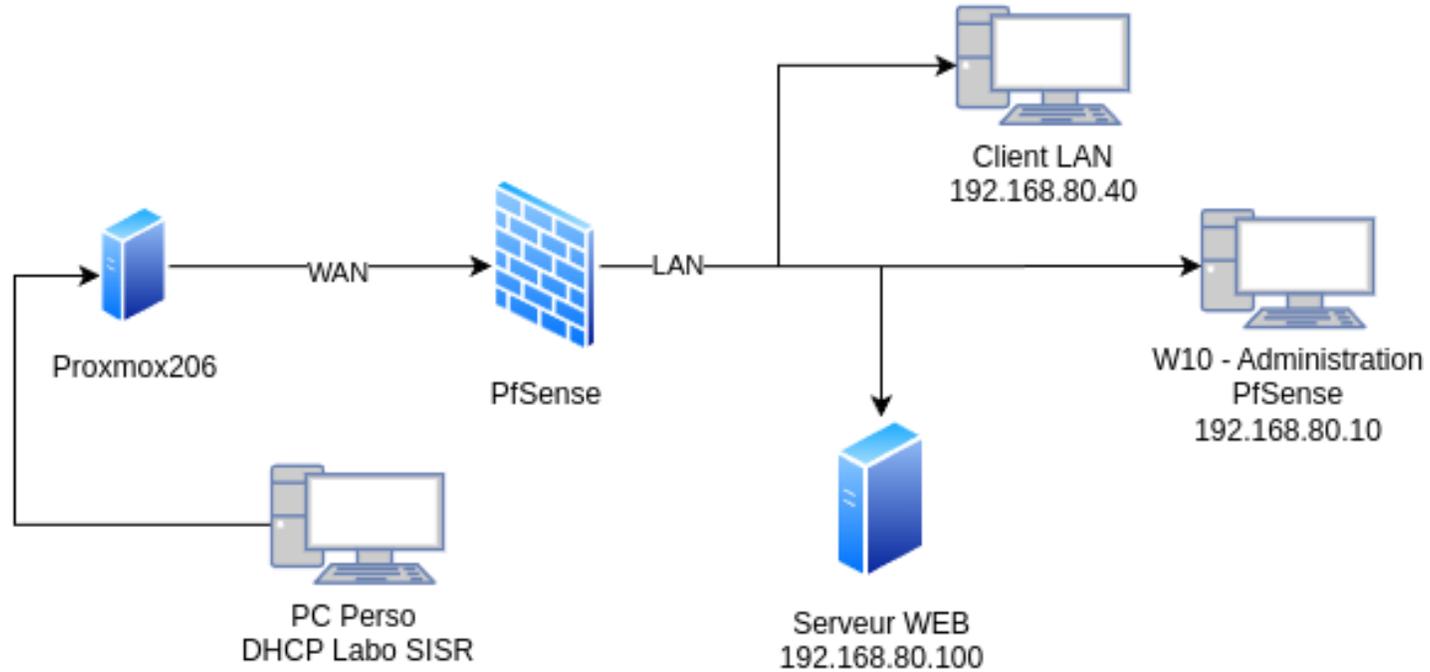
**TP – Proxy**



# A quoi sert Proxy Squid

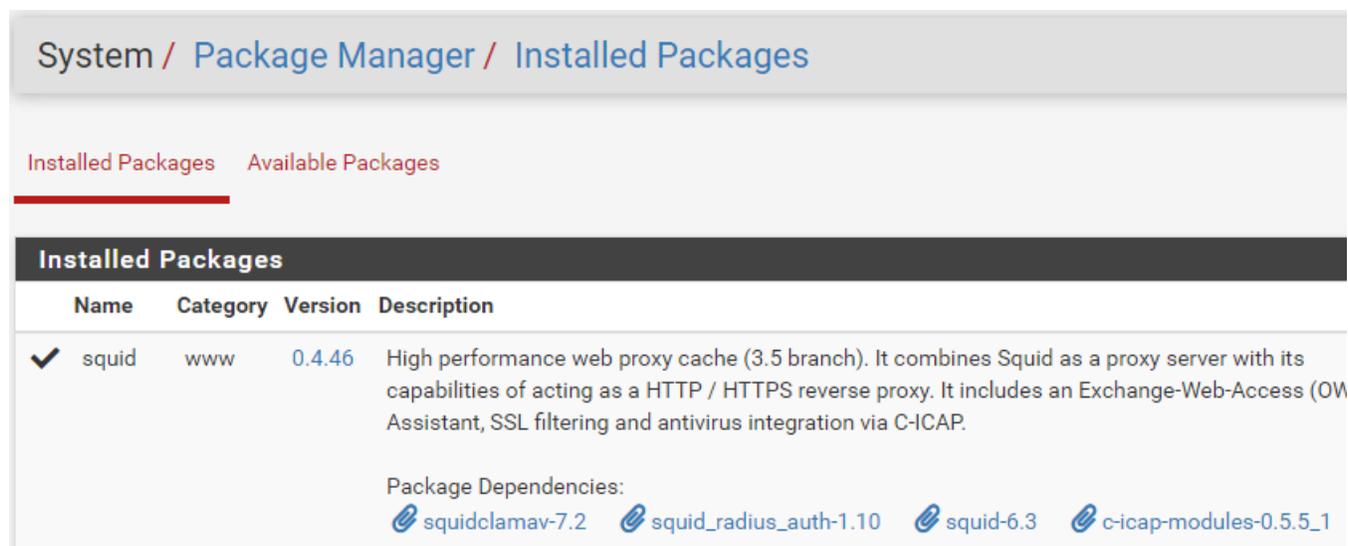
- Proxy Squid permet de :
  - Filtrer les accès et bloquer certains sites ou catégories de site grâce à des **Access Control Lists ( ACL )** .
  - Intercepter le trafic HTTP/HTTPS avec le mode proxy transparent sans de configuration manuelle sur les postes clients.
  - Surveille et journalise les requête web en temps réel et génère des journaux détaillés afin d'analyser le trafic réseau.
  - Contrôle d'accès avancé avec la possibilité de restreindre l'accès à internet selon des plages horaires, groupes d'utilisateurs ou adresses IP spécifiques, cela peut être utile pour encadré l'accès des employés.

# Présentation de l'infrastructure



# Installation de Proxy Squid

- Dans notre serveur PfSense en accès web, nous nous rendons dans **Systeme > Package Manager**, puis nous installons squid.
- Rendez vous dans l'onglet Services du PfSense pour la configuration de squid.
- Installation et configuration de PfSense : <https://baptiste-mathius.github.io/img/BTS2/TP-B2-Pfsense.pdf>



System / Package Manager / Installed Packages

Installed Packages Available Packages

Installed Packages			
Name	Category	Version	Description
✓ squid	www	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OW Assistant, SSL filtering and antivirus integration via C-ICAP.

Package Dependencies:

[squidclamav-7.2](#) [squid\\_radius\\_auth-1.10](#) [squid-6.3](#) [c-icap-modules-0.5.5\\_1](#)

# Configuration de Proxy Squid

- Pour la configuration, nous nous rendons dans l'onglet **Service > Squid proxy server > general**.
- On coche enable squid proxy afin de démarrer le service.
- On coche également **enable access logging**, pour avoir un retour sur les logs dans le but d'analyser la suite de nos règles que nous allons mettre en place.

**Logging Settings**

**Enable Access Logging** This will enable the access log.  
**Warning:** Do NOT enable if available disk space is low.

**Log Store Directory**   
The directory where the logs will be stored; also used for log rotation.  
**Important:** Do NOT include the trailing / when setting a custom directory.

**Rotate Logs**   
Defines how many days of logfiles will be kept. Rotation is disabled if set to 0.

**Log Pages Denied by SquidGuard**  Makes it possible for SquidGuard denied log to be included.  
[Click Info for detailed instructions.](#)

**Headers Handling, Language and Other Customizations**

**Visible Hostname**   
This is the hostname to be displayed in proxy server error messages.

**Administrator's Email**   
This is the email address displayed in error messages to the administrator.

**Error Language**   
Select the language in which the proxy server will display error messages.

**X-Forwarded Header**

**Transparent Proxy Settings**

**Transparent HTTP Proxy** Enable transparent mode to forward all requests for destination IP addresses.  
**Important:** Transparent proxy mode works without any additional configuration. **Important:** Transparent mode will filter SSL (port 443) if you enable it. **Hint:** In order to proxy both HTTP and HTTPS protocols **without** additional configuration, you need to enable the **Transparent Proxy** options on your DNS/DHCP servers.

**Transparent Proxy Interface(s)**   
The interface(s) the proxy server will transparently intercept requests on.

# Configuration de Proxy Squid

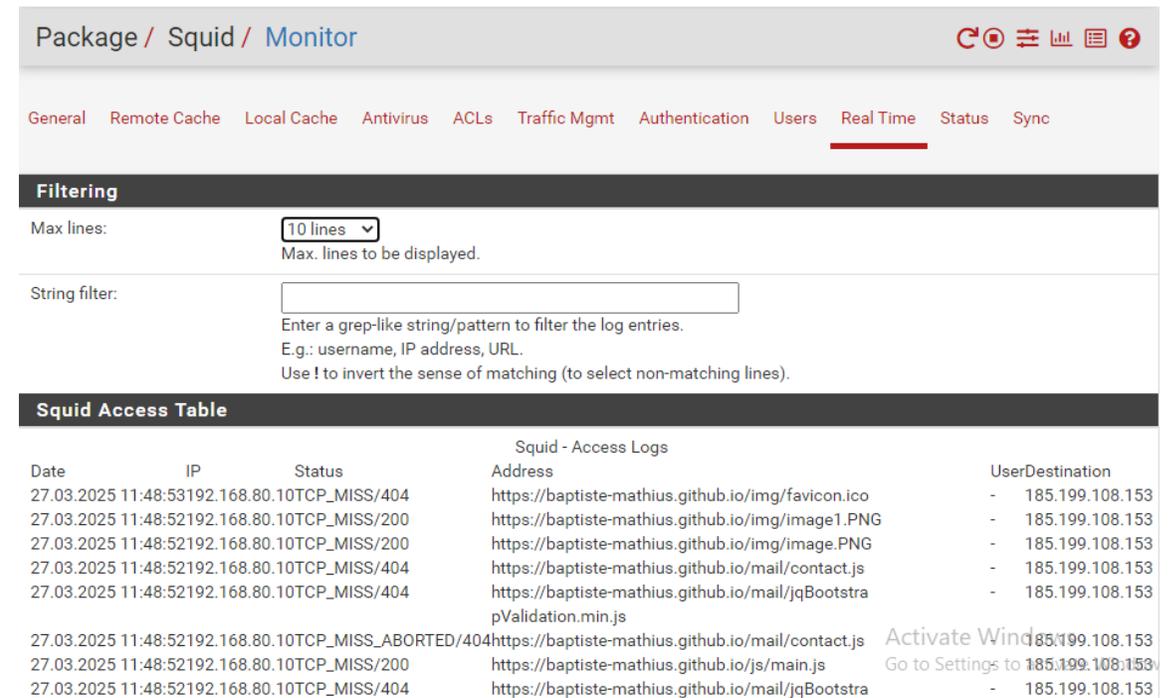
- Nous choisissons l'interface **LAN** pour le proxy puis les écoutes d'IP en IPv4 et nous mettons le **port 8088**.
- On active l'option HTTPS/SSL interception et nous ajoutons notre Certificat Autosigné sinon le service ne démarrera pas.
- On valide notre configuration en cliquant sur **save**.

The image shows a configuration page for Squid proxy with the following settings:

- SSL Man In the Middle Filtering**
  - HTTPS/SSL Interception**:  Enable SSL filtering.
  - SSL/MITM Mode**: Splice Whitelist, Bump Otherwise (dropdown). Description: The SSL/MITM mode determines how SSL interception is treated. Default: Splice Whitelist, Bump Otherwise. [Click Info for details](#).
  - SSL Intercept Interface(s)**: WAN, LAN (dropdown). Description: The interface(s) the proxy server will intercept SSL requests.
  - SSL Proxy Port**: (empty text input). Description: This is the port the proxy server will listen on to intercept SSL.
  - SSL Proxy Compatibility Mode**: Modern (dropdown). Description: The compatibility mode determines which cipher suites and details. [i](#)
  - DHParams Key Size**: 2048 (default) (dropdown). Description: DH parameters are used for temporary/ephemeral DH key exchanges.
  - CA**: CA (dropdown).
- Proxy Interface(s)**: WAN, LAN, loopback (dropdown). Description: The interface(s) the proxy server will bind to. Use CTRL + click to toggle.
- Outgoing Network Interface**: Default (auto) (dropdown). Description: The interface the proxy server will use for outgoing connections.
- Proxy Port**: 8088 (text input). Description: This is the port the proxy server will listen on. Default: 3128.

# Test du Proxy

- Ensuite nous allons consulter différents sites comme un Web héberger sur une VM avec un apache et mon portfolio.
- Nous pouvons voir que l'adresse de mon portfolio remonte, notre Proxy est donc actif.
- Passons maintenant à la suite avec la sécurisation.



The screenshot shows the Squid Monitor web interface. At the top, there is a breadcrumb trail: "Package / Squid / Monitor". Below this is a navigation menu with tabs: "General", "Remote Cache", "Local Cache", "Antivirus", "ACLs", "Traffic Mgmt", "Authentication", "Users", "Real Time", "Status", and "Sync". The "Real Time" tab is currently selected. Below the navigation menu is a "Filtering" section with a "Max lines:" dropdown set to "10 lines" and a "String filter:" input field. Below the filtering section is the "Squid Access Table" which displays a table of access logs.

Date	IP	Status	Squid - Access Logs Address	UserDestination
27.03.2025 11:48:53	192.168.80.10	TCP_MISS/404	https://baptiste-mathius.github.io/img/favicon.ico	- 185.199.108.153
27.03.2025 11:48:52	192.168.80.10	TCP_MISS/200	https://baptiste-mathius.github.io/img/image1.PNG	- 185.199.108.153
27.03.2025 11:48:52	192.168.80.10	TCP_MISS/200	https://baptiste-mathius.github.io/img/image.PNG	- 185.199.108.153
27.03.2025 11:48:52	192.168.80.10	TCP_MISS/404	https://baptiste-mathius.github.io/mail/contact.js	- 185.199.108.153
27.03.2025 11:48:52	192.168.80.10	TCP_MISS/404	https://baptiste-mathius.github.io/mail/jqBootstrapValidation.min.js	- 185.199.108.153
27.03.2025 11:48:52	192.168.80.10	TCP_MISS_ABORTED/404	https://baptiste-mathius.github.io/mail/contact.js	- 185.199.108.153
27.03.2025 11:48:52	192.168.80.10	TCP_MISS/200	https://baptiste-mathius.github.io/js/main.js	- 185.199.108.153
27.03.2025 11:48:52	192.168.80.10	TCP_MISS/404	https://baptiste-mathius.github.io/mail/jqBootstrap	- 185.199.108.153

# Blocage du Port 80

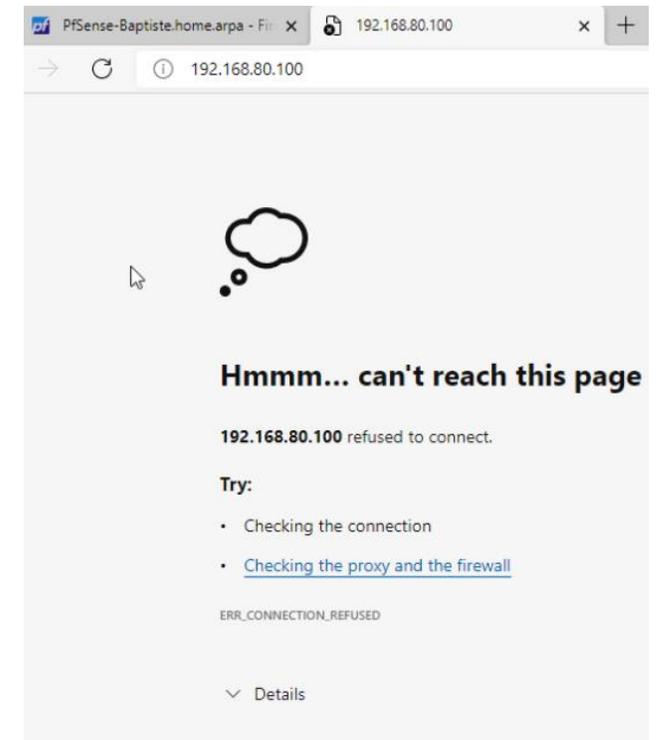
- On ajoute cette règle dans l'onglet Firewall / Rules / LAN, pour bloquer le port 80.
- Puis on test sur notre navigateur, nous voyons que la page est inaccessible.

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	0/21.78 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	0/82 KiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Block HTTP



# Redirection du client vers le proxy

- Nous allons maintenant rediriger notre machine cliente directement sur notre proxy.
- Il faut donc se rendre dans **settings, network & internet** puis on ajoute le proxy.

Proxy

Use a proxy server for Ethernet or Wi-Fi connections. Proxy settings don't apply to VPN connections.

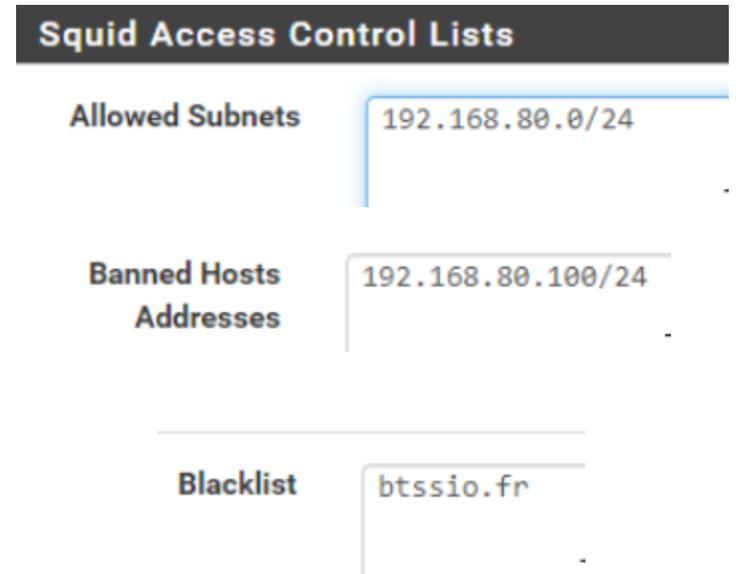
Use a proxy server

On

Address  Port

# Restriction sur le proxy

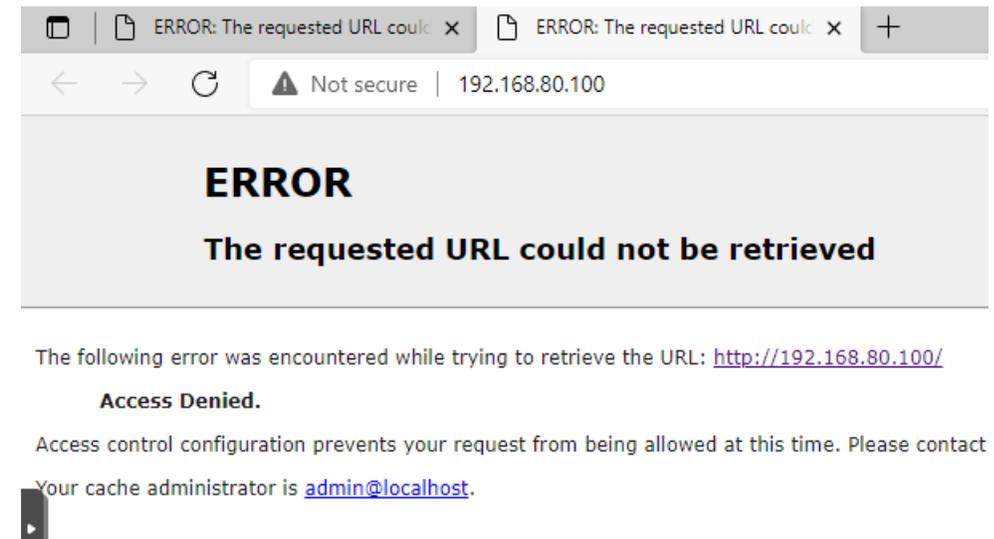
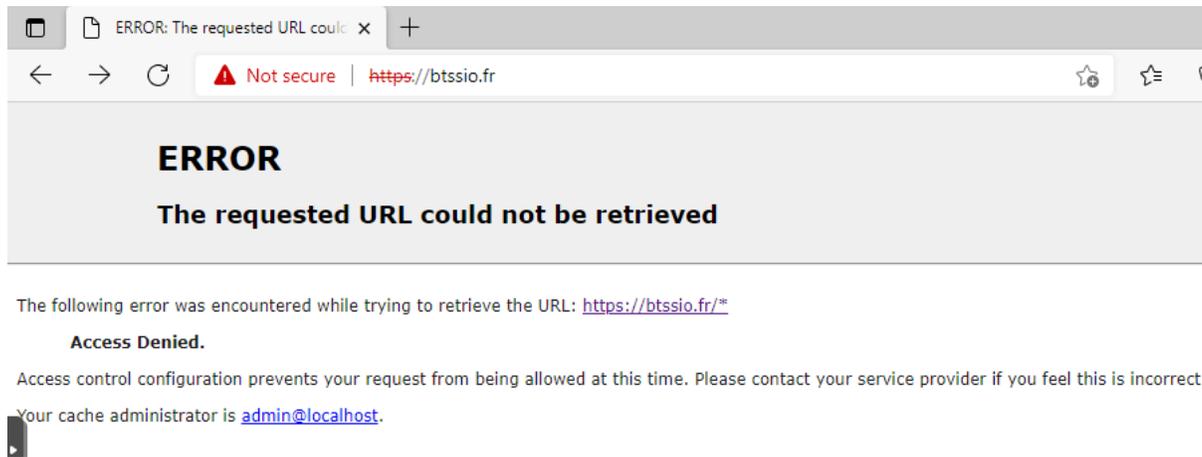
- Avec Proxy Squid, nous avons plusieurs possibilités :
- Nous allons donc autoriser nos adresses LAN et nous allons blacklist le moodle et notre serveur Web.
- Pour cela on se rend dans **Services -> Squid Proxy Server -> ACLs**



Allow subnets	adresses autorisées sur le proxy
Unrestricted IPs	accès non restreints
Banned hosts addresses	bannir des adresses
Whitelist	liste blanche des IP/sites web consultables
Blacklist	liste noire des IP/Sites non consultables

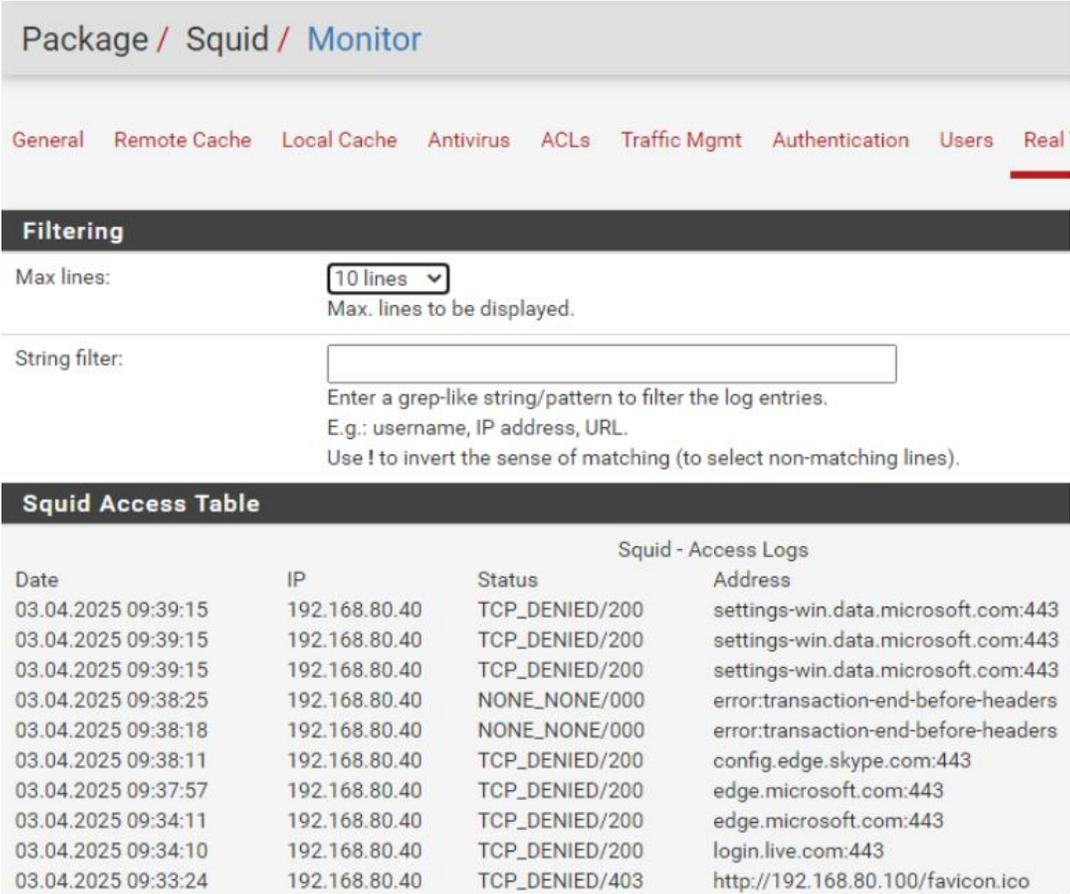
# Test et vérifications

- Passons sur notre client LAN et testons cela :



# Analyse des logs proxy

- Dans le Real Time, nous voyons les log d'accès Squid, avec les status et les adresses consultées.
- Tout ce qui est consulté et qui n'est pas du réseau 192.168.80.0 ne peut pas être consulté.
- Nous pouvons voir que notre serveur web est blacklist donc il est inaccessible



Package / Squid / Monitor

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real

### Filtering

Max lines:  Max. lines to be displayed.

String filter:

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).

### Squid Access Table

Date	IP	Status	Squid - Access Logs Address
03.04.2025 09:39:15	192.168.80.40	TCP_DENIED/200	settings-win.data.microsoft.com:443
03.04.2025 09:39:15	192.168.80.40	TCP_DENIED/200	settings-win.data.microsoft.com:443
03.04.2025 09:39:15	192.168.80.40	TCP_DENIED/200	settings-win.data.microsoft.com:443
03.04.2025 09:38:25	192.168.80.40	NONE_NONE/000	error:transaction-end-before-headers
03.04.2025 09:38:18	192.168.80.40	NONE_NONE/000	error:transaction-end-before-headers
03.04.2025 09:38:11	192.168.80.40	TCP_DENIED/200	config.edge.skype.com:443
03.04.2025 09:37:57	192.168.80.40	TCP_DENIED/200	edge.microsoft.com:443
03.04.2025 09:34:11	192.168.80.40	TCP_DENIED/200	edge.microsoft.com:443
03.04.2025 09:34:10	192.168.80.40	TCP_DENIED/200	login.live.com:443
03.04.2025 09:33:24	192.168.80.40	TCP_DENIED/403	http://192.168.80.100/favicon.ico