

ADRAR FORMATION

Mis en place d'un Proxy



MARAVAL Liam
07/10/2024

Ce document sera décomposé en plusieurs chapitres :

1. Contexte : Définition des besoins ainsi que le choix des solutions en réponse à la demande client.
2. Configuration technique : Procédure technique de mise en place des solutions
3. Conclusion
4. Annexes

Table des matières

1.	Contexte	2
1.1	Demandes du client.....	2
1.2	Evolution de l'infrastructure	3
1.3	Choix de la solution	5
1.4	Sécurisation des accès.....	5
2.	Configuration technique.....	6
2.1	Configuration de Squid.....	6
2.2	Configuration du SquidGuard.....	10
2.3	Test client du Proxy	14
2.4	Configuration du filtrage Web par compte AD	16
2.5	Configuration de LightSquid	22
2.6	Déploiement des configuration Proxy par GPO	25
2.7	Configuration du portail captif pour les Guest.....	32
3.	Conclusion	37
4.	Annexes	38

1. Contexte

1.1 Demandes du client

Nous avons été sollicités par l'ADRAR pour concevoir et déployer une solution de Proxy destinée à sécuriser les accès Internet sur leur site.

La gestion des droits d'accès à certains sites se fera en fonction du groupe LDAP auquel appartient l'utilisateur pour le personnel du centre de formation et des stagiaires.

En plus de la gestion des droits, nous sommes chargés de mettre en place une solution de conservation des accès Internet comme le prévoit la loi pour tout organisme fournissant un accès Internet public.

Les utilisateurs seront répartis dans 3 groupes :

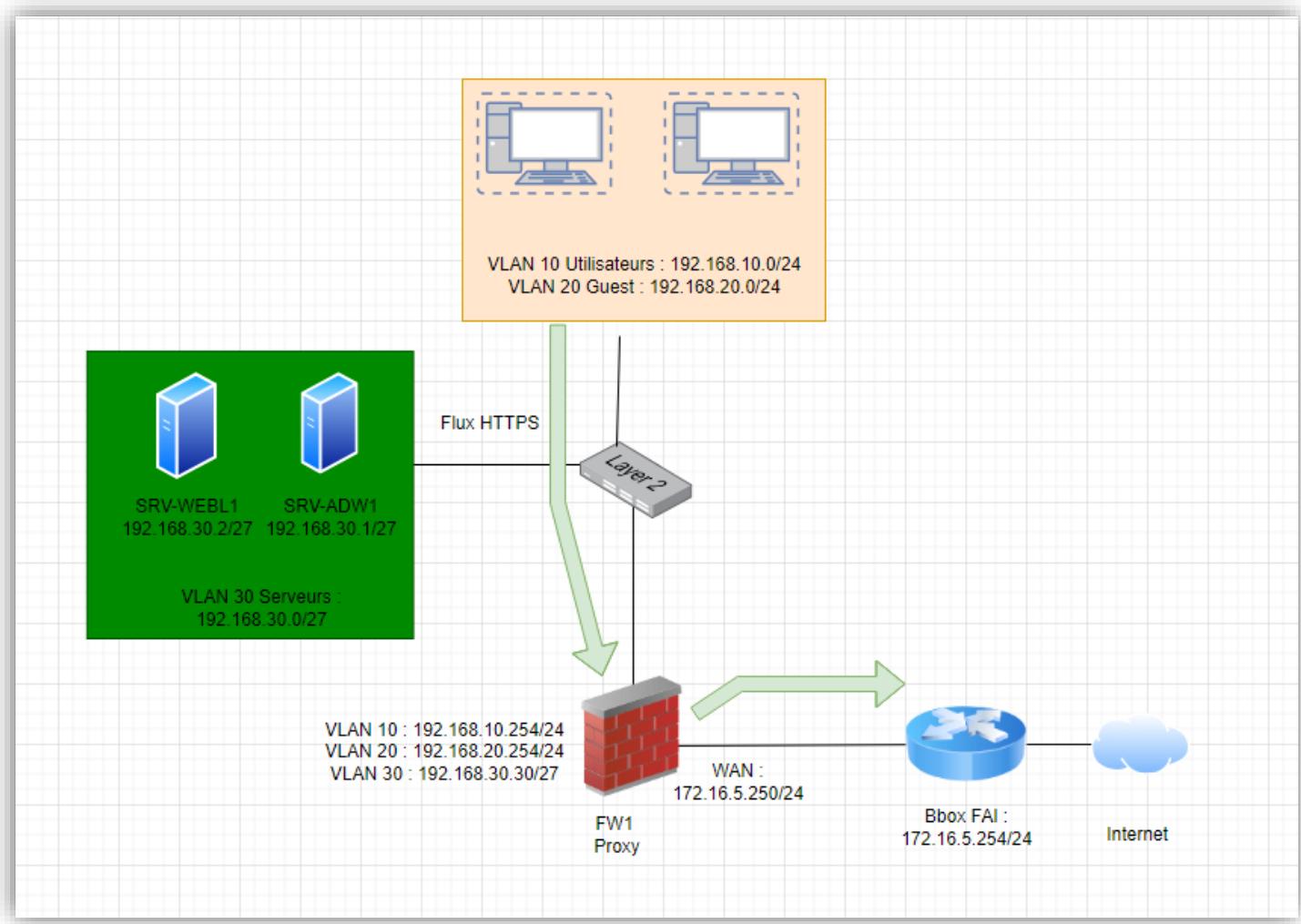
- Administration : pour les employés de l'ADRAR
- Formation : pour les stagiaires
- Guest : pour des utilisateurs externes
 - Le personnel administratif aura accès à tous les sites internet, sauf ceux inclus dans la blacklist « Adultes » ainsi que « Shopping » de UT1.
 - Les stagiaires n'auront pas accès aux sites : réseaux sociaux + jeux + sites pour adultes de la blacklist UT1.
 - Les Guest devront passer par un portail captif en se connectant à un navigateur Web, et n'auront accès qu'à un nombre de sites limités

Voici l'infrastructure en place actuellement :

- 3 Réseaux distincts :
 - Un réseau « **Utilisateurs** »
 - Un réseau « **Guest** »
 - Un réseau « **Serveurs** »
- Un serveur AD avec un domaine adrар.local
- Un serveur DHCP
- Un pare feu PfSense

1.2 Evolution de l'infrastructure

Pour mieux comprendre la mise en place de la nouvelle infrastructure, veuillez-vous référer au nouveau schéma effectué :



Afin de répondre à la demande de l'ADRAR, nous allons déployer un Proxy sur le PfSense déjà en place.

Ce service remplira plusieurs fonctions essentielles :

- Agir en tant qu'intermédiaire entre les requêtes Web clientes et les serveurs Web externes
- Anonymiser les IP clientes
- Effectuer un filtrage des flux Web
- Mettre en cache les données afin d'améliorer les performances
- Journaliser les activités via des fichiers de logs.

Pour répondre aux exigences de sécurité et de protection des données des utilisateurs conformément au RGPD, le proxy sera configuré de manière stricte et explicite.

De plus, nous souhaitons améliorer la sécurité en mettant en place du filtrage Web via des groupes AD, ce qui peut être implémenté uniquement via un Proxy explicite.

Afin de déployer notre configuration, une GPO sera mise en place sur notre Active Directory pour forcer l'utilisation du Proxy dans le navigateur Firefox, celui-ci étant imposé sur les postes utilisateurs.

Nous avons choisi cette solution car le déploiement des configurations via DHCP/DNS et WPAD n'est pas envisageable car proscrit par l'ANSSI (lien du document en Annexes).



Attention

Le protocole *Web Proxy Autodiscovery Protocol* (WPAD) est une alternative au fichier .PAC ; il s'appuie sur DHCP et DNS pour la récupération d'un fichier de configuration wpad.dat. Même s'il est relativement simple à mettre en œuvre pour le déploiement d'une configuration automatique de serveur mandataire, plusieurs vulnérabilités affectent ce protocole. Son utilisation est donc à proscrire *absolument*.

Pour rappel, une charte informatique devra être à faire signer pour les utilisateurs avec une rubrique les informant de l'utilisation du proxy.

Concernant les filtrages web, celui-ci va s'effectuer en fonction des groupes d'appartenance des utilisateurs.

Pour ce faire, nous allons configurer une liaison avec l'AD.

Squid effectuera des requêtes LDAP afin de vérifier l'appartenance au groupe de l'utilisateur et lui appliquer les règles de filtrage via des ACLs définies le service.

En ce qui concerne la gestion des utilisateurs Guest, nous avons opté pour la mise en place d'un portail captif.

L'authentification se fera par vouchers et les utilisateurs seront placés dans un VLAN isolé et sécurisé. Cependant ils ne passeront pas par le Proxy pour des raisons techniques, de réglementation et de sécurité (plus de détails dans la partie **1.4 Sécurisation des accès**)

1.3 Choix de la solution

Concernant le choix de la solution, nous avons opté pour « **Squid** ».

Plus précisément 3 plugins seront installés sur Pfsense :

- **Squid Proxy Filter** : Qui servira à configurer le proxy dans ces paramètres générales (Port du proxy, définition du cache ect...)
- **SquidGuard** : qui servira pour mettre en place le filtrage d'URL via la blacklist ainsi qu'à configurer les ACLs pour les filtrages en fonction du groupe Active Directory
- **LightSquid** : Qui va servir comme outil d'analyse de notre Proxy afin de voir les logs par utilisateur, l'utilisation du cache, les sites les plus visités ect...

Nous avons retenu cette solution pour plusieurs raisons :

- Intégration complète dans Pfsense via les plugins
- Solution éprouvée et fiable
- Documentation et communauté très présentes
- Solution complète permettant un paramétrage poussé de notre proxy
- Solution offrant de bonnes performances

1.4 Sécurisation des accès

A des fins de sécurité, le port par défaut du Proxy sera modifié.

Concernant les filtrages des flux Web nous allons télécharger une blacklist « **UT1** » qui regroupe des sites Web par catégorie.

Celle-ci va nous permettre de rejeter tout trafic inapproprié ou présentant un risque pour SI.

Afin de répondre aux normes de la législation, nous allons aussi mettre en place une conservation des logs utilisateurs pour une durée de 180 jours.

Concernant la demande de l'ADRAR pour le filtrage des Guest via le proxy, celle-ci est difficilement applicable.

L'architecture et les contraintes de Pfsense nous obligeraient à ajouter un deuxième pare feu et à configurer un proxy en mode transparent avec le SSL Bump activé.

En effet, les postes des utilisateurs externes ne faisant pas partie du domaine, nous ne pouvons pas pousser notre GPO sur leurs postes.

Comme mentionné en début de document, le fonctionnement en mode transparent avec le SSL Bump pose problème si l'on veut respecter la confidentialité des données et notamment le RGPD. Voici les points essentiels bloquants :

- Capture non approuvé de données personnelles des utilisateurs (articles 5 et 6 du RGPD).
- Absence de consentement explicite (article 7 RGPD).
- Non-respect de la confidentialité des communications chiffrées.
- Amendes RGPD en cas de non-conformité
- Surveillance pouvant être perçue comme intrusive par les visiteurs et donc nuire à l'image de l'entreprise.

La solution serait d'intégrer des CGU au portail captif pour informer les utilisateurs externes de l'utilisation d'un proxy mais Pfsense ne le permet pas.

C'est donc pour ces raisons que nous avons opté pour la solution d'un portail captif avec authentification via vouchers (avec rétention des logs pendant 180 jours également) et du VLAN isolé.

Cependant, si un souhait est formulé par l'ADRAR d'imposer un proxy transparent pour les Guest, nous pourrons l'ajouter.

Un document officiel informant de l'utilisation du Proxy devra être à faire signer pour chaque utilisateur nécessitant d'une connexion « Guest ».

La partie configuration technique sera identique à celle dans le chapitre **2.Configuration technique** pour le deuxième pare-feu, il suffira de cocher deux cases supplémentaires pour activer le mode transparent et le SSL Bump.

2. Configuration technique

2.1 Configuration de Squid

Dans un 1^{er} temps, nous allons installer les différents plugins Squid :

Nom	Version	Description	
Lightsquid	3.0.6_6	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	+ Install
squid	0.4.44_24	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 (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	+ Install
squidGuard	1.16.18_5	High performance web proxy URL filter.	+ Install

Nous allons maintenant configurer le cache de notre Proxy que nous mettrons à 600Mo (la taille du cache sera revue à la hausse celle-ci étant configurée à 600 Mo à des fins de tests, il sera recommandé de l'augmenter entre 20Go et 50Go en fonction de son utilisation) :

The screenshot shows the configuration interface for a Squid proxy. The top navigation bar includes tabs for General, Remote Cache, Local Cache (which is currently selected), Antivirus, ACLs, Traffic Mgmt, Authentication, Users, Real Time, Status, and Sync.

Squid Cache General Settings

- Disable Caching**: Disable caching completely. This may be required if Squid is only used as a proxy to audit website access.
- Cache Replacement Policy**: Set to "Heap LFUDA". A note states: "The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. Default: heap LFUDA".
- Low-Water Mark in %**: Set to 90. A note states: "The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm." with an info icon.
- High-Water Mark in %**: Set to 95. A note states: "The high-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm." with an info icon.
- Do Not Cache**: A text area for entering domain(s) or IP address(es) that should never be cached. A note says: "Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line."
- Enable Offline Mode**: Enable this option and the proxy server will never try to validate cached objects. A note states: "Offline mode gives access to more cached information than normally allowed (e.g., expired cached versions where the origin server should have been contacted otherwise)."
- External Cache Managers**: A text area for entering IPs for external Cache Managers. A note says: "Enter the IPs for the external Cache Managers to be granted access to this proxy. Separate entries by semi-colons (;)".

Squid Hard Disk Cache Settings

Hard Disk Cache Size: Set to 600. A note states: "Amount of disk space (in megabytes) to use for cached objects." This field is highlighted with a yellow box.

Nous pouvons maintenant continuer les configurations générales de notre proxy dans la rubrique « Services » puis « Squid Proxy Server » :

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

Squid General Settings

Enable Squid Proxy Check to enable the Squid proxy. **1**
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 **2**
Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP

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 synchronization.

Proxy Interface(s)

 3
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Outgoing Network Interface **4**
The interface the proxy server will use for outgoing connections.

Proxy Port **4**
This is the port the proxy server will listen on. Default: 3128

ICP Port

This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.

Patch Captive Portal **This feature was removed - see Bug #5594 for details!**

Resolve DNS IPv4 First **5**
Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.

1. Activer le Proxy Squid
2. Version IPV4 pour l'écoute de notre Proxy
3. Interfaces d'utilisation de notre Proxy
4. Port du Proxy
5. Activer la résolution IPv4 en premier

Nous continuons ensuite la configuration en descendant sur la page :

Logging Settings

- Enable Access Logging** This will enable the access log. **1**
Warning: Do NOT enable if available disk space is low.
- Log Store Directory** **2**
The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.
- Rotate Logs** **3**
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
- Log Pages Denied by SquidGuard** Makes it possible for SquidGuard denied log to be included on Squid logs.
[Click Info for detailed instructions.](#) **i**

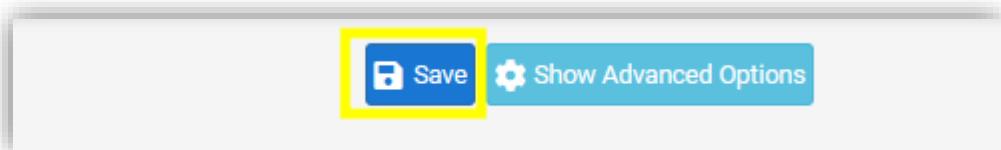
1. Activer les logs sur le proxy
2. Répertoire de stockage des logs
3. Durée de conservation des logs

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 users.
- Error Language** **1**
Select the language in which the proxy server will display error messages to users.
- X-Forwarded Header Mode**
Choose how to handle X-Forwarded-For headers. Default: on **i**
- Disable VIA Header** If not set, Squid will include a Via header in requests and replies as required by RFC2616.
- URI Whitespace Characters Handling**
Choose how to handle whitespace characters in URL. Default: strip **i**
- Suppress Squid Version** Suppresses Squid version string info in HTTP headers and HTML error pages if enabled. **2**

1. Langue affichée pour les erreurs
2. Masque les informations de la version du serveur Squid dans les en tête HTTP

Puis nous sauvegardons la configuration :



2.2 Configuration du SquidGuard

Nous commençons par activer « **SquidGuard Proxy Filter** » :

The screenshot shows the pfSense web interface with the following details:

- Header:** Shows the pfSense logo and navigation links: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.
- Warning Bar:** A red bar at the top left says "WARNING: The 'admin' account password is set to the default value".
- Page Title:** Package / Proxy filter SquidGuard: General
- Submenu:** General settings, Common ACL, Groups ACL, Targets.
- General Options:**
 - Enable:** A checkbox labeled "Check this option to enable squidguard" is checked and highlighted with a yellow box.
 - Important:** Text: "Please set up at least one category before enabling. See this link for details." and "To activate squidGuard configuration, click the Save button at the bottom of the page." Below this is a green "Apply" button.
 - SquidGuard service state:** STA (Stable)
- LDAP Options:**
 - Enable LDAP Filter:** A checkbox is present but not checked.
 - SquidGuard Proxy Filter:** A checkbox is highlighted with a yellow box.
 - LDAP DN:** Input field for LDAP DN.
 - LDAP DN Password:** Input field for LDAP DN password.
 - LDAP Cache Time:** Input field set to 0.
 - Strip NT domain name:** A checkbox.
 - Strip Kerberos Realm:** A checkbox.
 - LDAP Version:** A dropdown menu set to Version 3.
- Right Panel:** Shows a sidebar with links: Auto Config Backup, Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP Proxy, NTP, PPPoE Server, Router Advertisement, SNMP, Squid Proxy Server, Squid Reverse Proxy. Below this is a "Rewrites" section with tabs: Blacklist, Log, XMLRPC Sync.

Maintenant, nous activons les logs dans **SquidGuard** et renseignons notre blacklist :

Logging options

- Enable GUI log** Check this option to log the access to the Proxy Filter GUI.
- Enable log** Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings. **1**
- Enable log rotation** Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

Miscellaneous

- Clean Advertising** Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

Blacklist options

- Blacklist** Check this option to enable blacklist **2**
- Blacklist proxy**

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

- Blacklist URL** **3**
Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

Save

1. Activer les logs
2. Activer la blacklist
3. URL de la blacklist

Il faut désormais se rendre dans le menu Blacklist, et allons renseigner l'URL de notre UT1 et ensuite cliquer sur Download pour charger toutes les catégories définies dans celles-ci :

The screenshot shows the 'Blacklist Update' interface. At the top, there is a navigation bar with tabs: General settings, Common ACL, Groups ACL, Target categories, Times, Rewrites, Blacklist (which is highlighted with a yellow box), Log, and XMLRPC Sync. Below the navigation bar is a progress bar indicating '0 %' download of 'http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz'. There are three buttons below the progress bar: 'Download' (green), 'Cancel' (orange), and 'Restore Default' (blue). A text input field below the progress bar says 'Enter FTP or HTTP path to the blacklist archive here.' At the bottom of the page is a 'Blacklist update Log' section containing the following text:

```
Begin blacklist update
Start download.
Download archive http://dsi.ut-
capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 66 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.
```

Nous allons maintenant dans le menu Common ACL, cliquons sur le + pour déplier les catégories.

The screenshot shows the 'Common ACL' interface. At the top, there is a navigation bar with tabs: General settings, Common ACL (which is highlighted with a yellow box), Groups ACL, Target categories, Times, Rewrites, Blacklist, Log, and XMLRPC Sync. Below the navigation bar is a 'General Options' section with a 'Target Rules' input field containing 'lblk_blacklists_social_networks all'. Below this is a 'Target Rules List' section with a '+' button. A note below the list says: 'ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.'

Nous accédons à toutes les catégories téléchargées dans la blacklist.

Nous autorisons le « **Default access** » pour que toutes les catégories soient autorisées par défaut.

Ensuite, nous affinons la sécurité en interdisant chaque catégorie voulu. (Voici un exemple pour les réseaux sociaux) :

[blk_blacklists_social_networks]	access	deny	<input type="button" value="▼"/>
[blk_blacklists_special]	access	—	<input type="button" value="▼"/>
[blk_blacklists_sports]	access	—	<input type="button" value="▼"/>
[blk_blacklists_stalkerware]	access	—	<input type="button" value="▼"/>
[blk_blacklists_strict_redirector]	access	—	<input type="button" value="▼"/>
[blk_blacklists_strong_redirector]	access	—	<input type="button" value="▼"/>
[blk_blacklists_translation]	access	—	<input type="button" value="▼"/>
[blk_blacklists_tricheur]	access	—	<input type="button" value="▼"/>
[blk_blacklists_tricheur_pix]	access	—	<input type="button" value="▼"/>
[blk_blacklists_update]	access	—	<input type="button" value="▼"/>
[blk_blacklists_vpn]	access	—	<input type="button" value="▼"/>
[blk_blacklists_warez]	access	—	<input type="button" value="▼"/>
[blk_blacklists_webmail]	access	—	<input type="button" value="▼"/>
Default access [all]	access	allow	<input type="button" value="▼"/>

Nous continuons maintenant la configuration de notre ACL par défaut :

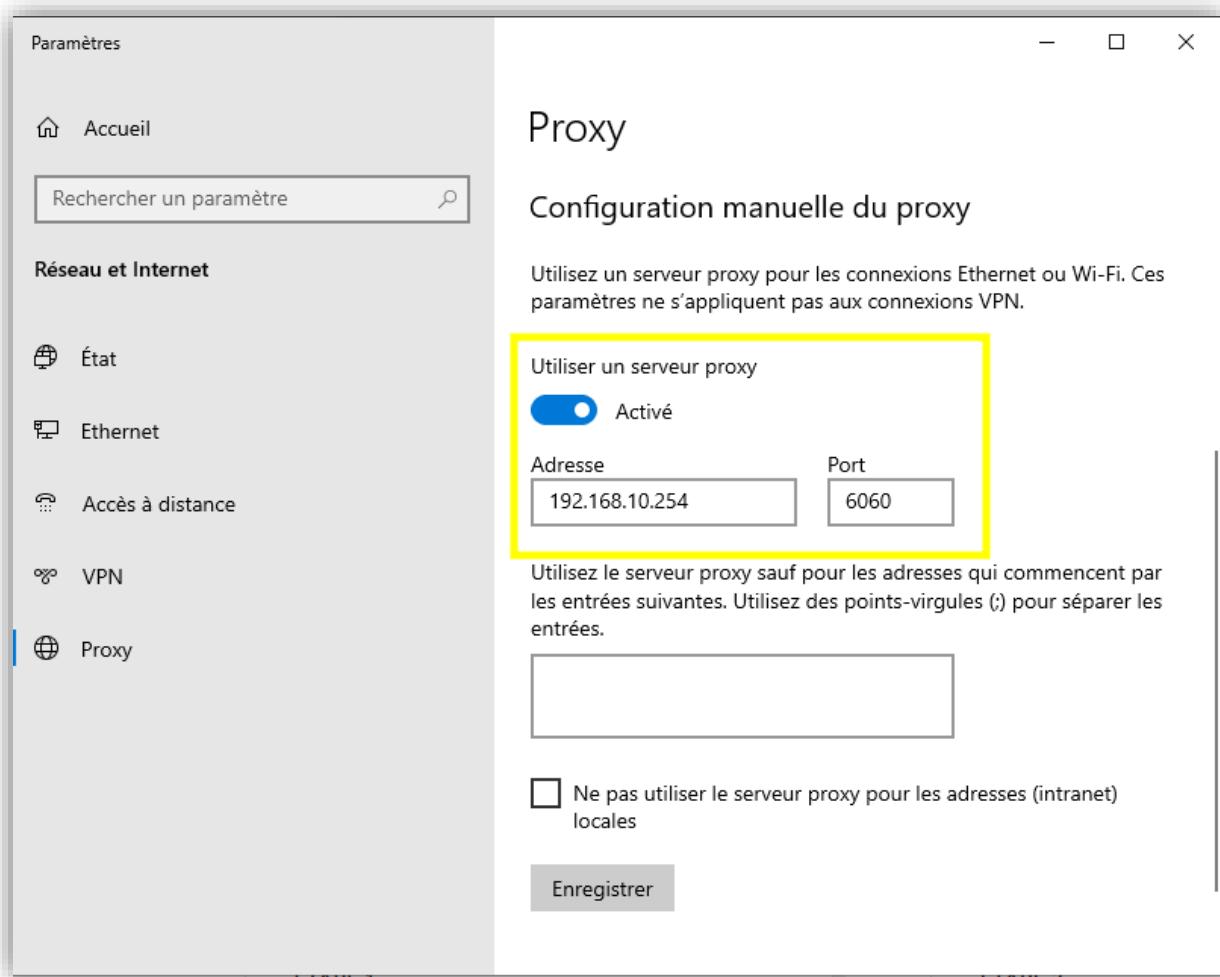
Do not allow IP-Addresses in URL	<input checked="" type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.	1	
Proxy Denied Error	<input type="text"/>		
The first part of the error message displayed to clients when access was denied. Defaults to Request denied by g_get('product_name') proxy.			
Redirect mode	<input type="button" value="int blank page"/>	2	
Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible. Options: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'			
Redirect info	<input type="text"/>		
Enter external redirection URL, error message or size (bytes) here.			
Use SafeSearch engine	<input checked="" type="checkbox"/> Enable the protected mode of search engines to limit access to mature content. At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. Note: This option overrides 'Rewrite' setting.		
Rewrite	<input type="button" value="none (rewrite not defined)"/>		
Enter the rewrite condition name for this rule or leave it blank.			
Log	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.		3
<input type="button" value="Save"/>			

1. Ne pas autoriser l'accès au site via l'IP
2. Message d'erreur affiché lors d'une connexion refusée
3. Active les logs pour cette ACL

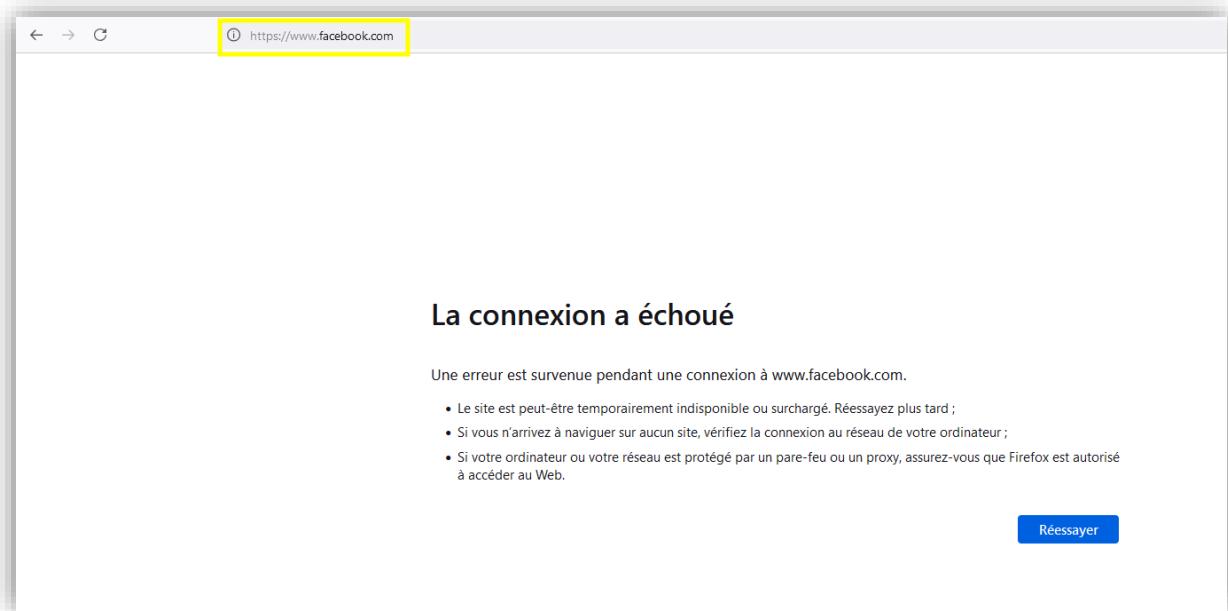
2.3 Test client du Proxy

Nous effectuons maintenant notre test sur une machine cliente.

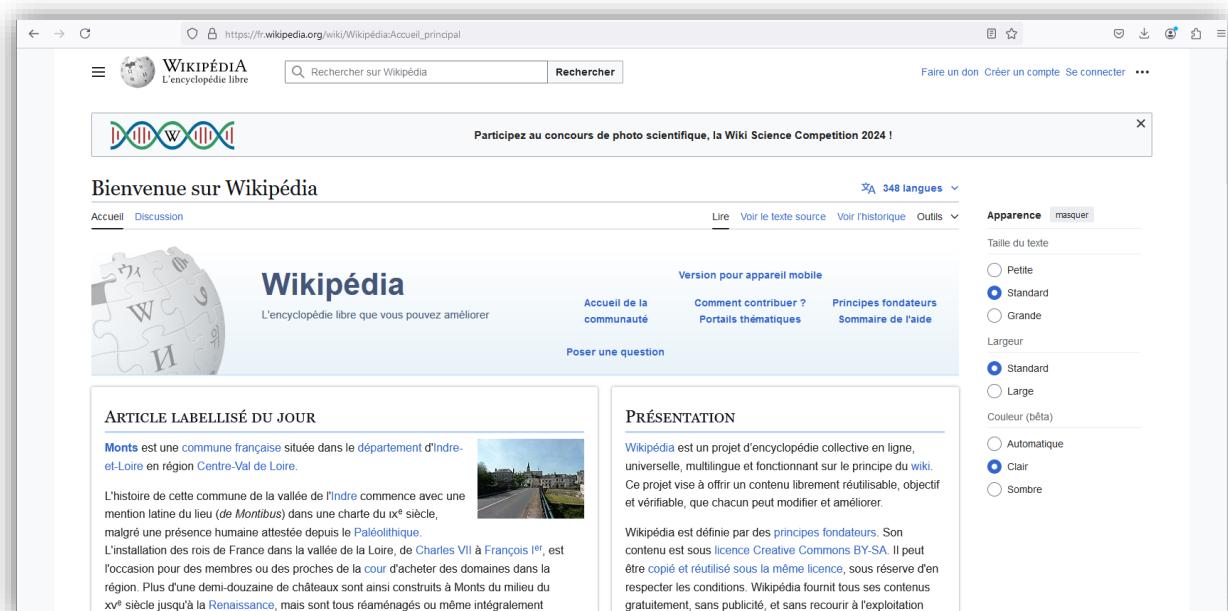
Nous allons dans le menu de configuration de proxy de Windows et renseignons les paramètres suivant :



Nous essayons maintenant d'accéder à « Facebook » qui fais partie de la catégorie « réseaux sociaux » bloquée dans notre ACL par default :



Nous essayons avec Wikipédia qui fais partie des sites autorisés :



Nous vérifions également les logs dans notre service « SquidGuard » :

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist **Log** XMLRPC Sync

Blacklist Update

Show 50 entries starting at << 0 >>

23.11.2024 18:46:55 192.168.10.100/192.168.100 www.facebook.com:443 .100 Request(default/blk_blacklists_social_networks/-) - CONNECT REDIRECT

2.4 Configuration du filtrage Web par compte AD

Maintenant, nous allons pouvoir mettre en place le filtrage par groupe AD.

Nous allons donc dans le menu « **Authentification** » de notre « **Squid Proxy Server** » et renseignons les éléments suivants :

Squid Authentication General Settings

Authentication Method	LDAP 1	Select an authentication method. This will allow users to be authenticated by local or external services.
Authentication Server	192.168.30.1 2	Enter the IP or hostname of the server that will perform the authentication here.
Authentication server port	389 3	Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.
Authentication Prompt	Merci de vous connecter avec votre compte utilisateur 4	This string will be displayed at the top of the authentication request window.
Authentication Processes	5 5	The number of authenticator processes to spawn. If many authentications are expected within a short timeframe, increase this number accordingly.
Authentication TTL	180 6	This specifies for how long (in minutes) the proxy server assumes an externally validated username and password combination to be valid. When the Time To Live expires, the user will be prompted for credentials again. Default: 5
Authentication Max User IP Addresses	<input type="text"/>	Enforces a limit to the number of unique IP addresses from which a single user can login. Attempts to login from additional IP addresses are denied until the Authentication TTL has expired. Default: none ?
Require Authentication for Unrestricted IPs	<input type="checkbox"/> If enabled, even 'Unrestricted IPs' configured on the ACLs tab are required to authenticate to use the proxy.	
Subnets That Don't Need Authentication	<input type="text"/>	Enter subnet(s) or IP address(es) (in CIDR format) that should NOT be asked for authentication to access the proxy. Put each entry on a separate line. ?

1. Méthode d'authentification au proxy via le LDAP
2. IP de notre contrôleur de domaine
3. Port d'écoute de notre LDAP
4. Message à afficher aux utilisateurs pour l'authentification
5. Nombre de processus d'authentification simultanés autorisés
6. Durée de validité de l'authentification (en minutes)

Nous continuons en renseignant les paramètres LDAP :

Squid Authentication LDAP Settings

LDAP version	3	1
Transport	TCP - Standard	2
LDAP Server User DN	CN=SVC_Pfsense,CN=Users,DC=adrar,DC=local	3
LDAP Password	4
LDAP Base Domain	DC=adrar,DC=local	5
LDAP Username DN Attribute	uid	6
LDAP Search Filter	(&(objectCategory=person)(objectClass=user)(sAMAccountName=%s))	7
LDAP not follow referrals	<input type="checkbox"/> Do not follow referrals.	

Squid Authentication RADIUS Settings

RADIUS Secret	Enter the RADIUS secret for RADIUS authentication here.
Save	

1. Version de LDAP utilisée
2. Protocole de transport utilisé TCP
3. DN de notre compte de service pour la lecture LDAP
4. Mot de passe associé au compte
5. Base DN du domaine
6. Attribut DN des utilisateurs
7. Filtre de recherche LDAP pour trouver des utilisateurs

Une fois nos configurations effectuées nous cliquons sur « **Save** » pour enregistrer.

Dans la rubrique « **General Settings** » de « **SquidGuard** » nous allons renseigner les éléments suivants :

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Enable Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link](#) for details.
 The Save button at the bottom of this page must be clicked to save configuration changes.
 To activate squidGuard configuration changes, **the Apply button must be clicked.**

Apply

SquidGuard service state: **STARTED**

LDAP Options

Enable LDAP Filter	<input checked="" type="checkbox"/> Enable options for setup ldap connection to create filters with ldap search	1
LDAP DN	CN=SVC_Pfsense,CN=Users,DC=adrar,DC=local	2
LDAP DN Password	3
LDAP Cache Time	300	4
Strip NT domain name	<input checked="" type="checkbox"/> Strip NT domain name component from user names (/ or \ separated).	5
Strip Kerberos Realm	<input checked="" type="checkbox"/> Strip Kerberos Realm component from user names (@ separated).	6
LDAP Version	Version 3	7

1. Activer le filtrage via LDAP
2. DN du compte de service
3. Mot de passe associé au compte
4. Durée de la mise en cache
5. Supprime le / ou \ des noms d'utilisateur pour l'authentification
6. Supprime le @NomDeDomaine pour l'authentification utilisateurs
7. Version de LDAP utilisée

Nous allons maintenant effectuer nos règles de filtrage par groupe LDAP.
Pour cela, nous allons dans le menu « **Groups ACL** » :

Proxy filter SquidGuard: Groups Access Control List (ACL) / Edit / Groups ACL

General settings Common ACL **Groups ACL** Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Disabled Check this to disable this ACL rule.

Name **1**
Enter a unique name of this rule here.
The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

Order **2**
Select the new position for this ACL item. ACLs are evaluated on a first-match source basis.
Note: Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list.
Example: ACL with single (or short range) source ip 10.0.0.15 must be placed before ACL with more large ip range 10.0.0.0/24.

Client (source) **3**
Enter client's IP address or domain or "username" here. To separate them use space.
Example:
IP: 192.168.0.1 - Subnet: 192.168.0.0/24 or 192.168.1.0/255.255.255.0 - IP-Range: 192.168.1.1-192.168.1.10
Domain: foo.bar matches foo.bar or *.foo.bar
Username: 'user1'
Ldap search (Ldap filter must be enabled in General Settings):
ldapusersearch ldap://192.168.0.100/DC=domain,DC=com?sAMAccountName?sub?(&(sAMAccountName=%s)(memberOf=CN=it%2cCN=Users%2cDC=domain%2cDC=com))
Attention: these line don't have break line, all on one line

Time
Select the time in which 'Target Rules' will operate or leave 'none' for rules without time restriction. If this option is set then in off-time the second ruleset will operate.

Target Rules

1. Nom de note ACL
2. Ordre d'exécutions de l'ACL
3. Requêtes afin de filtrer l'ACL sur le groupe LDAP nommé « **GG_Formateurs** »

Une fois cela fait, nous allons définir les filtrages web à effectuer.

Nous cliquons sur le « + » dans « **Target Rules List** » de la même façon que précédemment afin d'autoriser ou non certaines catégories. Voici un exemple :

Target Categories	Target Categories for off-time
[blk_blacklists_adult]	access deny [blk_blacklists_adult]

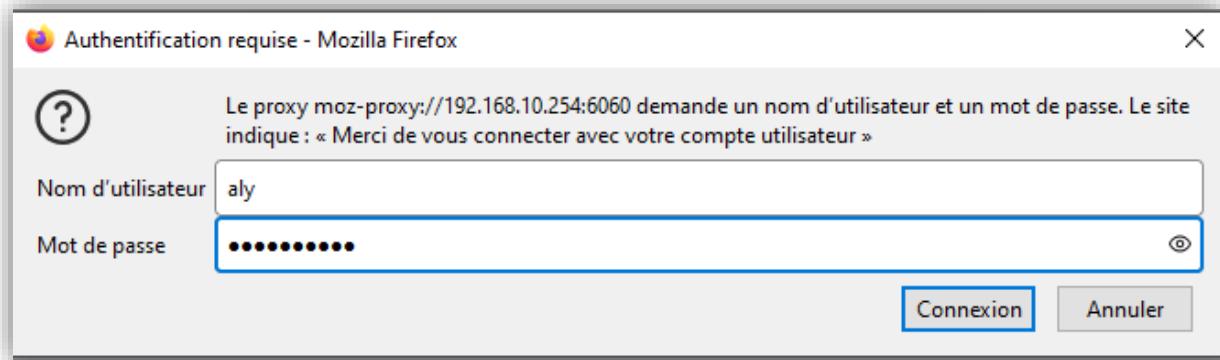
Nous continuons ensuite la configuration :

Do not allow IP-Addresses in URL	<input checked="" type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist. 1
Redirect mode	int error page (enter error message) 2 Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible. Options: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'
Redirect	Enter the external redirection URL, error message or size (bytes) here.
Use SafeSearch engine	<input checked="" type="checkbox"/> To protect your children from adult content you can use the protected mode of search engines. At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. 3 Note: This option overrides 'Rewrite' setting.
Rewrite	none (rewrite not defined) Enter the rewrite condition name for this rule or leave it blank.
Rewrite for off-time	none (rewrite not defined) Enter the rewrite condition name for this rule or leave it blank.
Description	ACL pour le groupe Formateurs 4 You may enter any description here for your reference.
Log	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.
Save	

1. Ne pas autoriser l'accès au site via des IP
2. Message affiché lors d'une connexion refusée
3. Utiliser SafeSearch pour les recherches sur les navigateurs
4. Description de l'ACL

Nous sauvegardons la configuration et effectuons un test via un poste client.

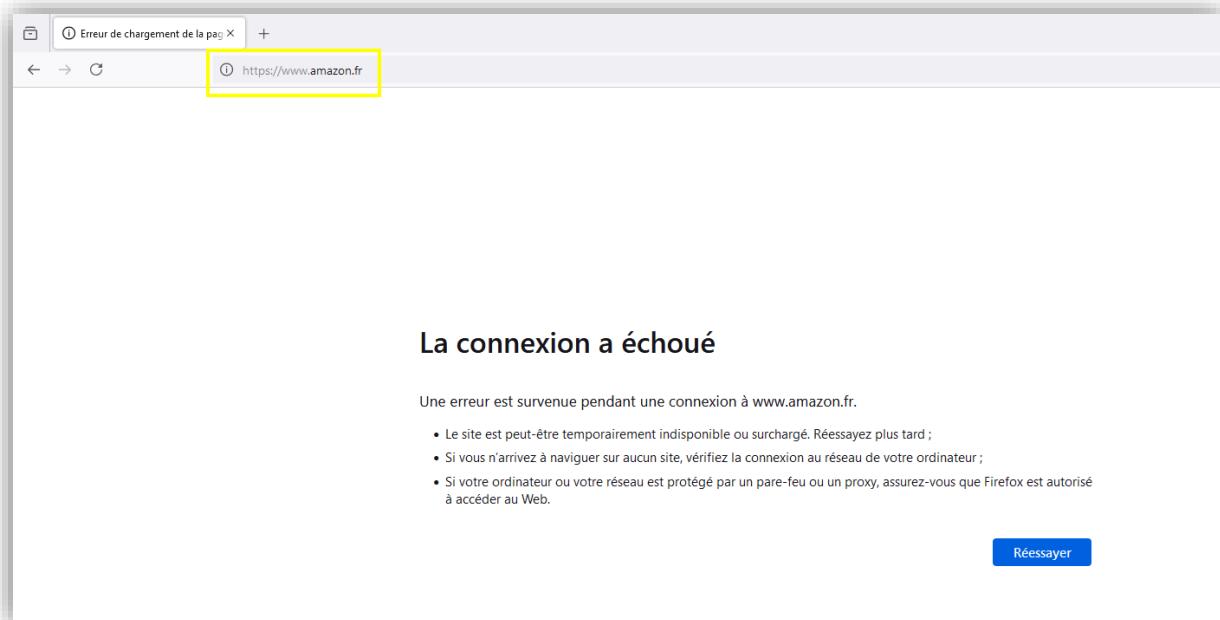
Dès l'ouverture du navigateur, un message apparaît demandant les identifiants d'accès au proxy.



Nous regardons les logs et voyons l'utilisateur authentifié

29.11.2024 16:00:29	192.168.10.80	TCP_TUNNEL/503	https:443	aly	-
29.11.2024 16:00:28	192.168.10.80	TCP_MISS/200	http://detectportal.firefox.com/success.txt?	aly	34.107.221.82
29.11.2024 16:00:28	192.168.10.80	TCP_MISS/200	http://detectportal.firefox.com/success.txt?	aly	34.107.221.82
29.11.2024 16:00:28	192.168.10.80	TCP_MISS/200	http://detectportal.firefox.comcanonical.html	aly	34.107.221.82
29.11.2024 16:00:28	192.168.10.80	TCP_TUNNEL/200	www.googleadservices.com:443	aly	216.58.215.34

Une fois renseigné, nous essayons d'accéder à la Amazon qui fait partie de la rubrique Shopping qui est interdite pour ce groupe.



Le site est bien bloqué par le proxy.

Nous vérifions dans les logs en regardant le nom de l'ACL qui bloque le trafic Web :

The screenshot shows the 'Logs' tab of the SquidGuard configuration interface. It displays a list of log entries under the 'Blacklist Update' section. Two entries are highlighted with yellow boxes:

- 24.11.2024 20:01:59 192.168.10.100/192.168.10 play.google.com:443 .100 Request(ACL_Formateurs/blk_blacklists_games/-) aly CONNECT REDIRECT
- 24.11.2024 20:01:59 192.168.10.100/192.168.10 www.amazon.fr:443 .100 Request(ACL_Formateurs/blk_blacklists_shopping/-) aly CONNECT REDIRECT

Nous allons effectuer les mêmes configurations pour créer les ACLs pour le filtrage des groupes « **GG_Stagiaires** » et « **GG_Guest** »

2.5 Configuration de LightSquid

Maintenant nous allons pouvoir configurer LightSquid qui nous servira principalement afin d'avoir des statistiques sur l'utilisation de notre Proxy

Pour le configurer nous allons dans le menu suivant :

The screenshot shows the pfSense web interface with the 'Squid Proxy Reports: Settings' page selected. The 'Status' menu is open, showing various system status options. The 'Squid Proxy Reports' option is highlighted with a yellow box.

Instructions

Perform these steps after install **IMPORTANT:** Click Info and follow the instructions below if this

Web Service Settings

Lightsquid Web Port	7445	Port the lighttpd web server for Lightsquid will listen on. (Default: 7445)
Lightsquid Web SSL	<input checked="" type="checkbox"/> Use SSL for Lightsquid Web Access	This option configures the Lightsquid web server to use SSL and
Lightsquid Web User	admin	Username used to access lighttpd. (Default: admin)
Lightsquid Web Password	*****	Password used to access lighttpd. (Default: pfsense)

Links

[Open Lightsquid](#) [Open sqstat](#)

Nous renseignons les paramètres suivants pour accéder à la page de LightSquid :

Instructions

Perform these steps after install **IMPORTANT:** Click Info and follow the instructions below if this is initial install! [i](#)

Web Service Settings

Lightsquid Web Port	7445	1
Port the lighttpd web server for Lightsquid will listen on. (Default: 7445)		
Lightsquid Web SSL	<input checked="" type="checkbox"/> Use SSL for Lightsquid Web Access	
This option configures the Lightsquid web server to use SSL and uses the WebGUI HTTPS certificate.		
Lightsquid Web User	admin	2
Username used to access lighttpd. (Default: admin)		
Lightsquid Web Password	*****	3
Password used to access lighttpd. (Default: pfsense)		
Links	Open Lightsquid	Open sqstat

Report Template Settings

Language	French	
Select report language.		
Report Template	Base	
Select report template.		
Bar Color	Orange	
Select bar color.		

Reporting Settings and Scheduler

IP Resolve Method	Squidauth	4
Select which method(s) should be attempted (in the order listed below) to resolve IPs to hostnames.		
Click Info for details. (Default: DNS) i		
Skip URL(s)		

1. Port d'écoute
2. Utilisateur pour se connecter
3. Mot de passe du compte
4. Méthode de résolution des noms via Squid

Nous accédons à la page via l'IP de notre Firewall et le port défini précédemment.

Pour se connecter, nous utilisons le login défini précédemment.

Sur cette page, nous pouvons avoir un détail des connexions selon la date et la machine, des graphiques, des tops sites, du temps passé etc...

Date	Group	Users	Oversize	Bytes	Average	Hit %
28 Nov 2024	gr	1	0	7.5M	7.5M	6.02%
Total/Average:		1	0	7.5M	7.5M	6.02%

[LightSquid v1.8](#) (c) Sergey Erokhin AKA ESL

Squid user access report

Whole MONTH

Work Period: Nov 2024

#	Time	Graph	MONTH	User	Real Name	Connect	Bytes	%	Cumulative
1				192.168.10.80	?	67	7.5 M	100.0%	7.5 M

[LightSquid v1.8](#) (c) Sergey Erokhin AKA ESL

Squid user access report						
		User: 192.168.10.80 (?)	Connect	Bytes	Cumulative	%
Total	#	Accessed site			7.5 M	
	1	safebrowsing.googleapis.com:443	1	6.9 M	6.9 M	92.8%
	2	ciscobinary.openh264.org	1	472 947	7.4 M	6.0%
	3	img-getpocket.cdn.mozilla.net:443	6	26 457	7.4 M	0.3%
	4	incoming.telemetry.mozilla.org:443	3	13 680	7.4 M	0.1%
	5	aus5.mozilla.org:443	3	13 516	7.4 M	0.1%
	6	content-signature-2.cdn.mozilla.net:443	1	9 274	7.5 M	0.1%
	7	www.gstatic.com:443	1	7 639	7.5 M	0.0%
	8	o.pki.goog	8	6 761	7.5 M	0.0%
	9	r11.o.lencr.org	5	4 792	7.5 M	0.0%
	10	ocsp.digicert.com	5	4 148	7.5 M	0.0%
	11	r10.o.lencr.org	3	2 874	7.5 M	0.0%
	12	detectportal.firefox.com	9	2 593	7.5 M	0.0%
	13	push.services.mozilla.com:443	1	39	7.5 M	0.0%
	14	https:443	10	0	7.5 M	0.0%
	15	err:443	10	0	7.5 M	0.0%
	Total			7.5 M		
LightSquid v1.8 (c) Sergey Erokhin AKA ESL						

2.6 Déploiement des configuration Proxy par GPO

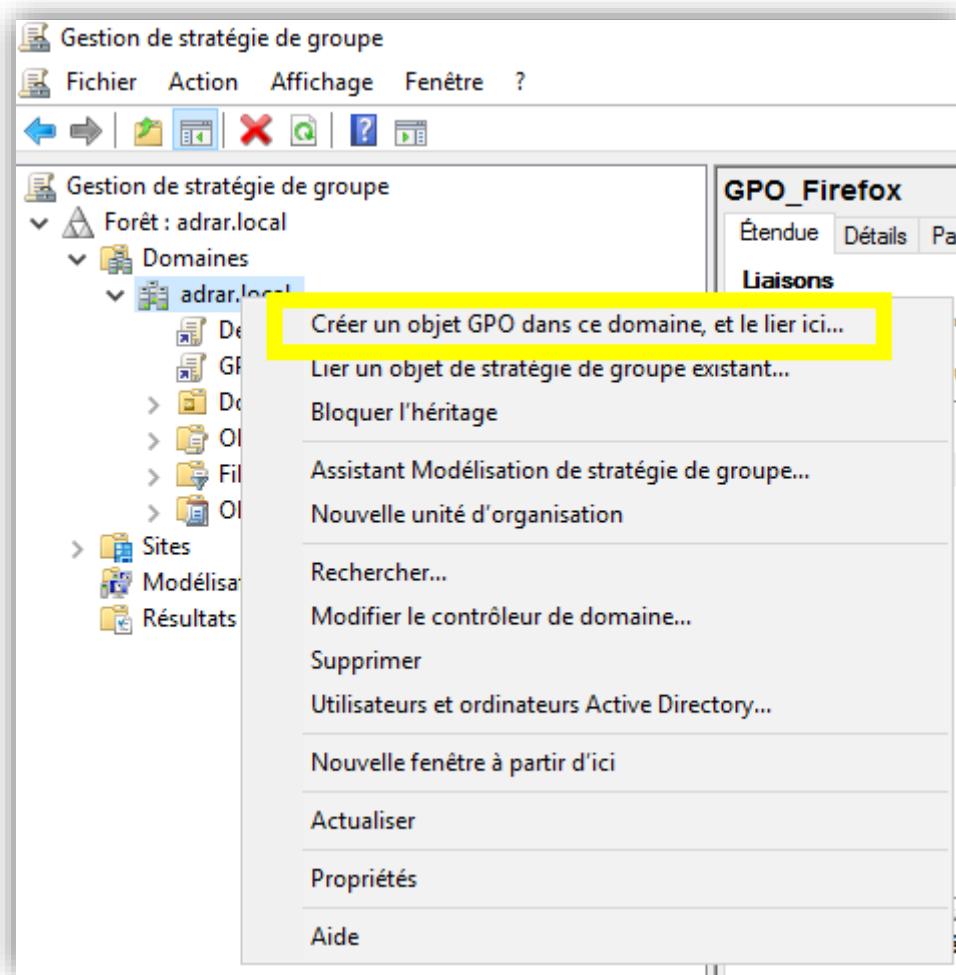
Pour déployer nos configurations Proxy sur nos machines clientes, nous allons mettre en place une GPO.

Nous commençons par télécharger les fichiers « **admx** » pour Firefox car c'est ce navigateur utilisé sur nos postes clients.

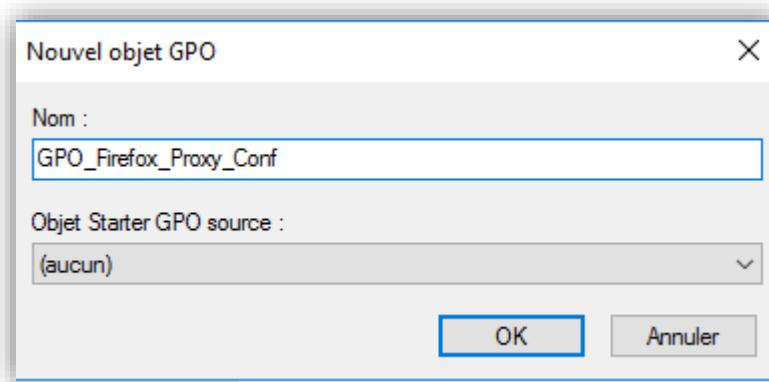
Une fois cela fait nous copions les fichiers et dossiers dans « **C:\Windows\PolicyDefinitions** » sur le contrôleur de domaine :

 de-DE	28/11/2024 13:29	Dossier de fichiers
 en-US	28/11/2024 13:29	Dossier de fichiers
 ru-RU	28/11/2024 13:29	Dossier de fichiers
 firefox.admx	26/11/2024 15:54	Fichier ADMX
 mozilla.admx	05/07/2023 14:28	Fichier ADMX

Nous ouvrons la console GPO et créons une nouvelle règle :



Nous nommons notre GPO



Nous allons dans la rubrique suivante et allons configurer différentes options :

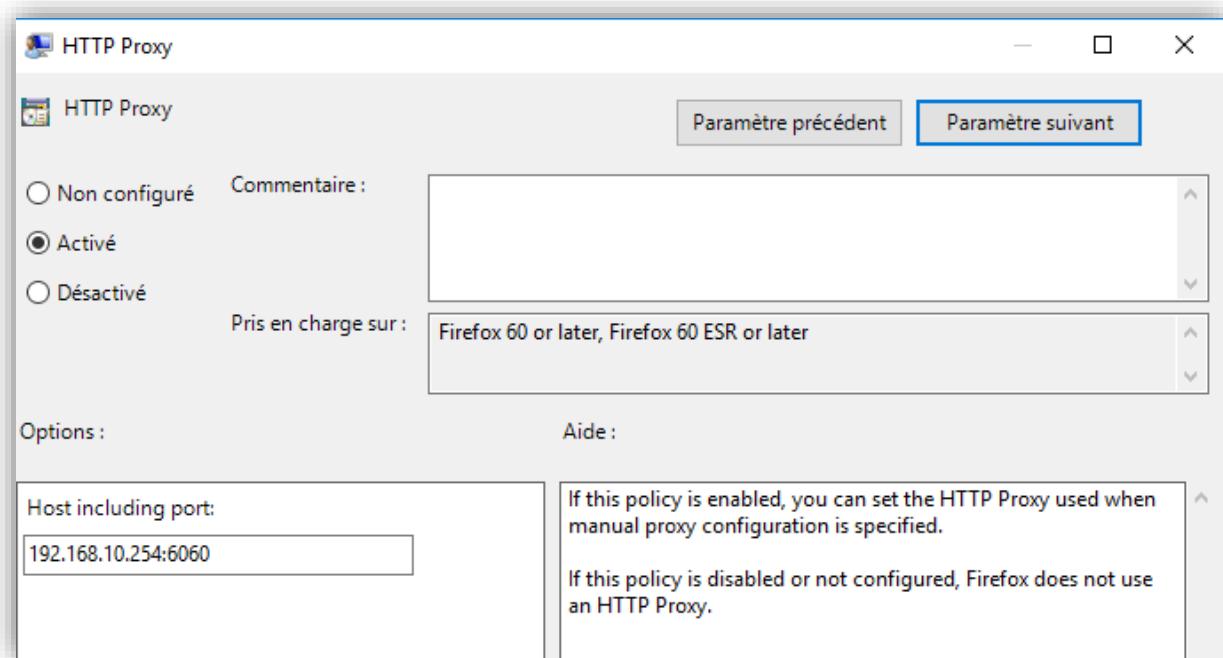
The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays a GPO structure under 'Stratégie GPO: Firefox [SRV-ADW1].ADRAR.LOCAL'. The path selected is 'Configuration ordinateur > Stratégies > Mozilla > Firefox > Proxy Settings'. The right pane is titled 'Proxy Settings' and contains a table of proxy configuration parameters:

Paramètre	Etat	Commentaire
Automatic proxy configuration URL	Non configuré	Non
Do not prompt for authentication if password is saved	Non configuré	Non
Connection Type	Activé	Non
HTTP Proxy	Activé	Non
Do not allow proxy settings to be changed	Activé	Non
Proxy Passthrough	Non configuré	Non
SOCKS Host	Non configuré	Non
HTTPS Proxy	Non configuré	Non
Use HTTP proxy for HTTPS	Activé	Non
Proxy DNS when using SOCKS	Non configuré	Non

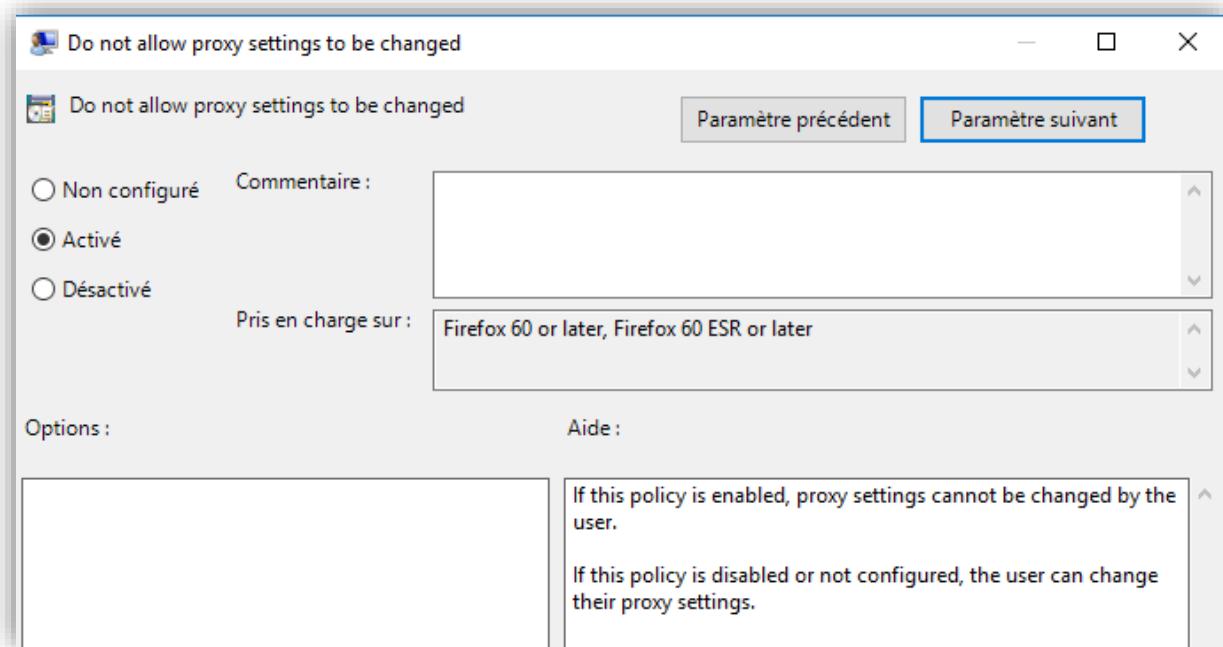
Dans « **Connection Type** » nous allons définir « **Manual Proxy configuration** » pour pousser la configuration de notre proxy sur le navigateur manuellement :

The screenshot shows the 'Connection Type' policy editor window. At the top, there are buttons for 'Paramètre précédent' and 'Paramètre suivant'. The main area has three radio button options: 'Non configuré' (unchecked), 'Activé' (checked), and 'Désactivé' (unchecked). To the right of 'Activé' is a 'Commentaire:' field and a note about supported versions: 'Pris en charge sur : Firefox 60 or later, Firefox 60 ESR or later'. Below this is an 'Options:' section containing a dropdown menu with 'Manual proxy configuration' selected. To the right of the dropdown is an 'Aide:' section with two paragraphs explaining the policy.

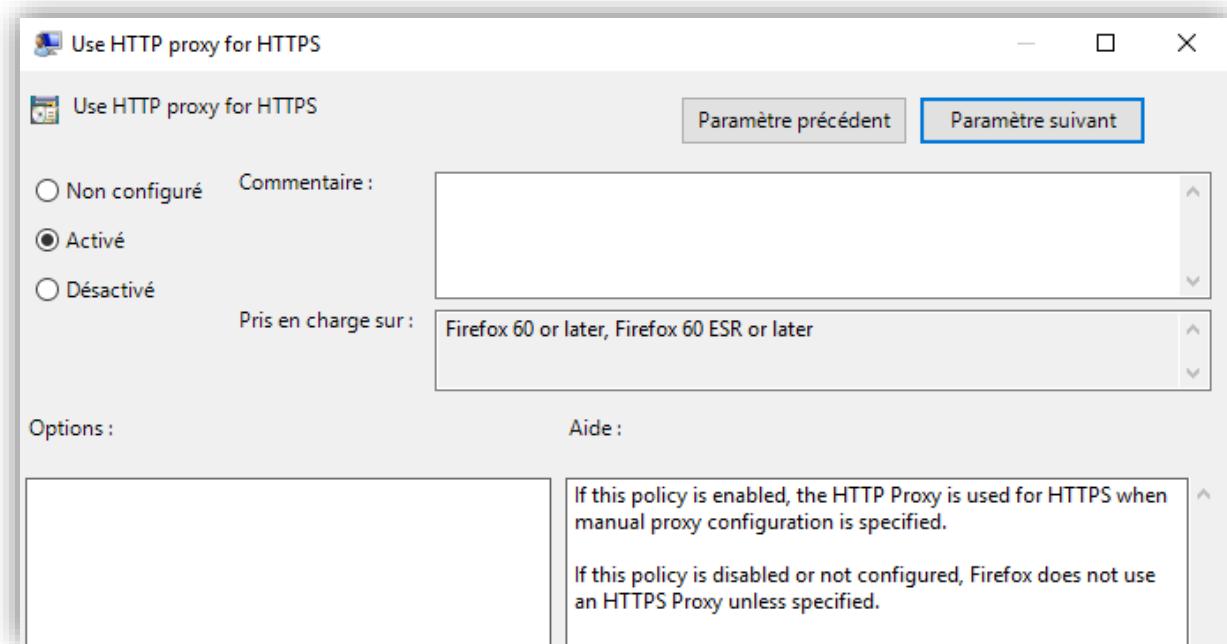
Dans ce paramètre, nous définissons l'IP et le port de notre Proxy :



Ici nous interdisons la modification des paramètres de Proxy

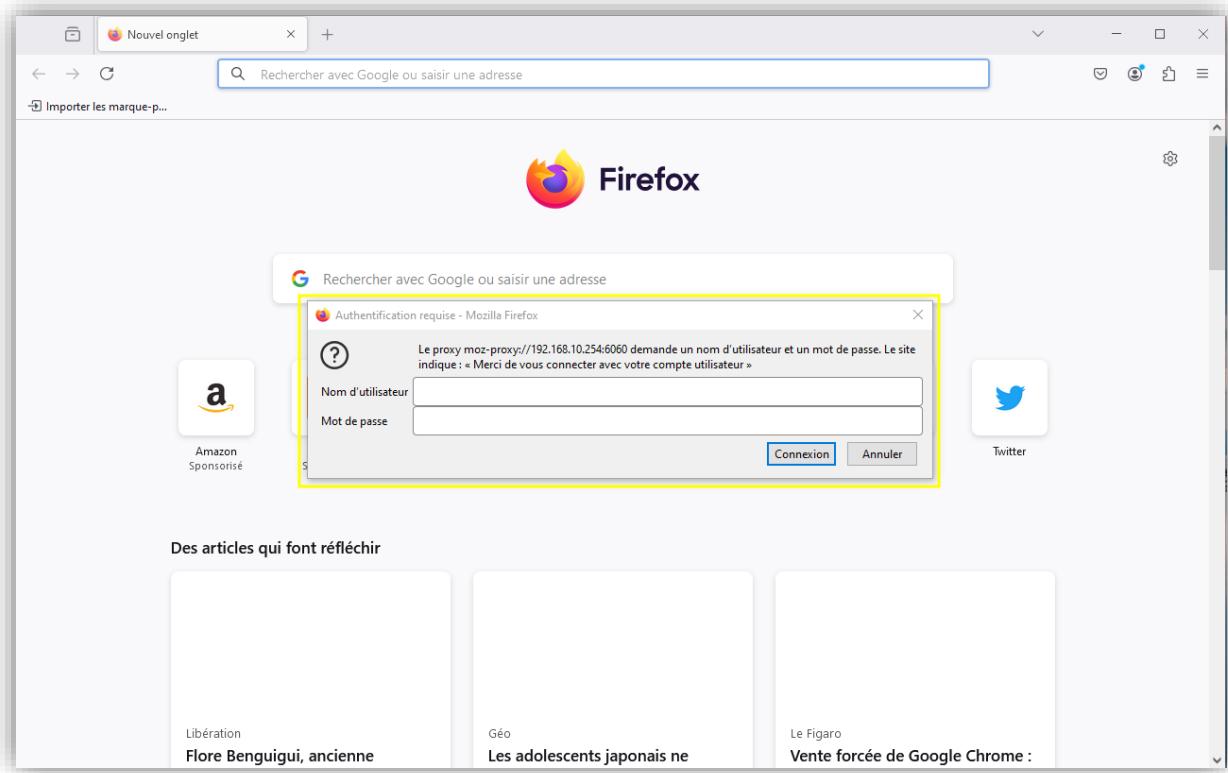


Ici, nous indiquons d'utiliser les mêmes configurations Proxy pour HTTP et HTTPS

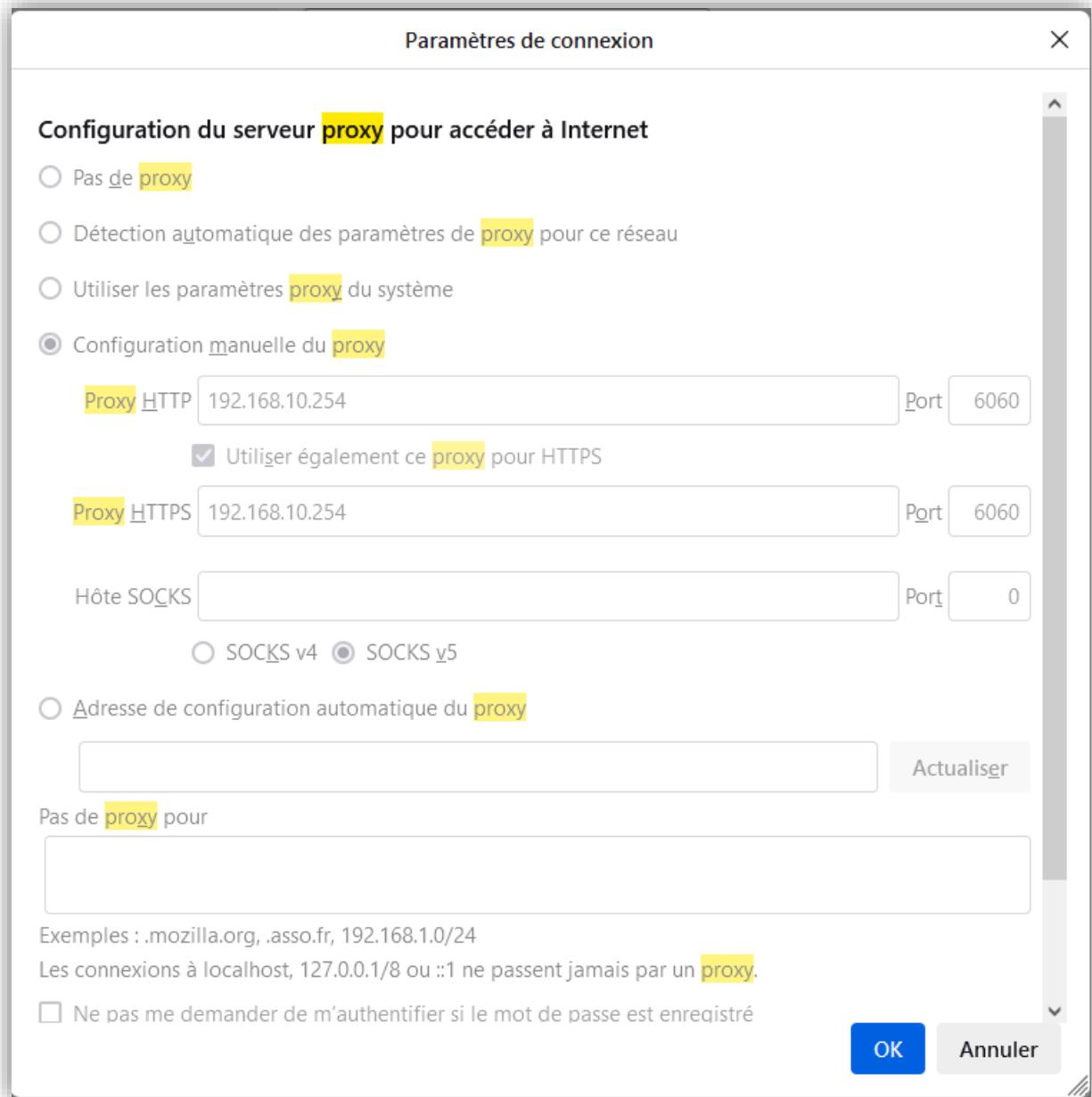


Nous pouvons maintenant effectuer notre test de validation de la GPO.

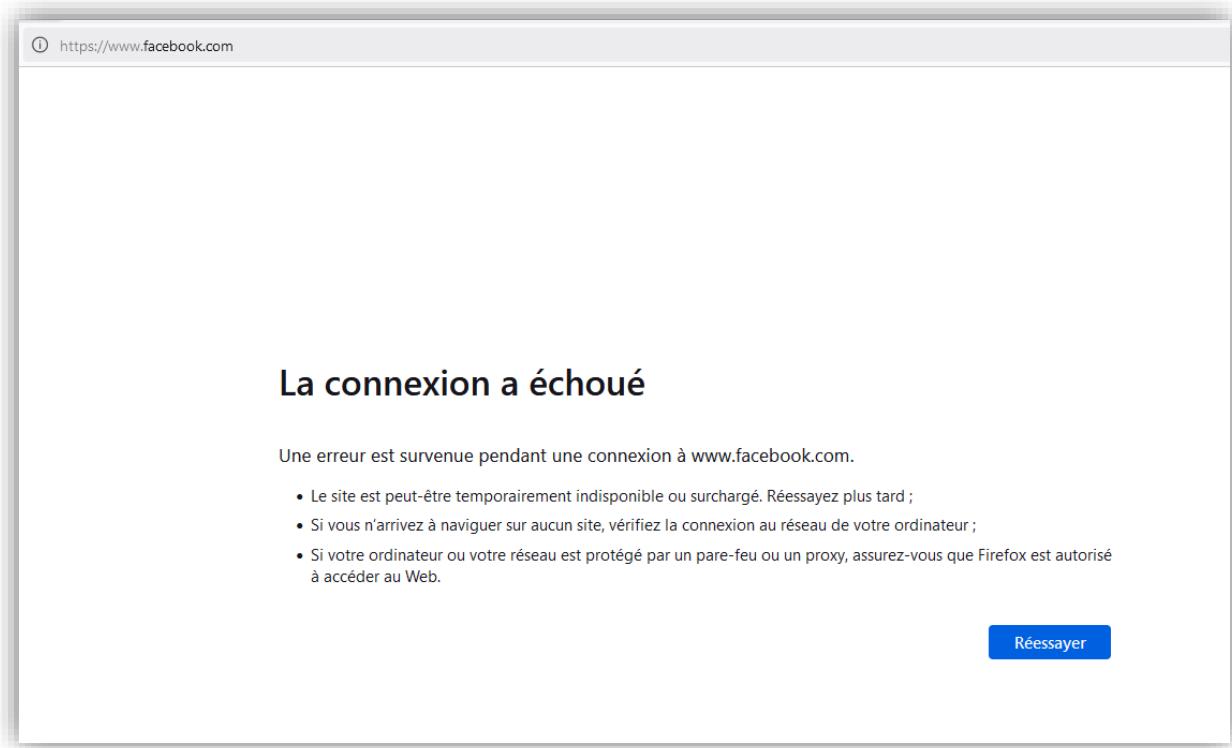
La page de connexion apparaît sur le navigateur dès l'ouverture du navigateur sur le poste utilisateur :



Dans les paramètres de Proxy de Firefox, nous voyons la configuration que nous ne pouvons modifier :



Puis nous validons le bon fonctionnement du filtrage Web :

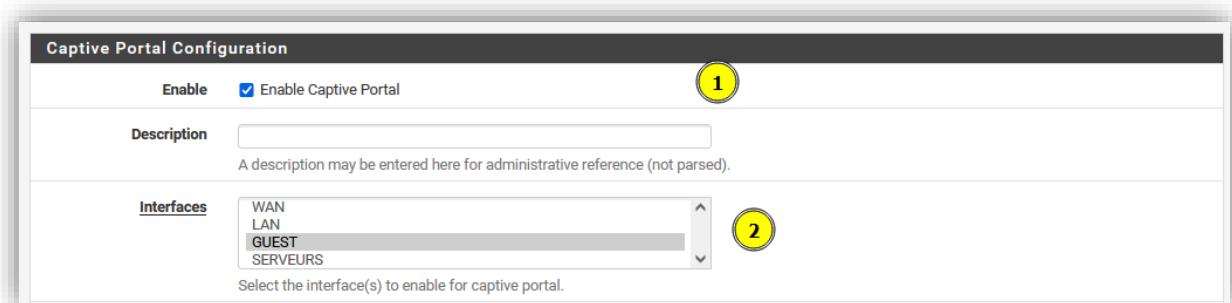


Dans nos logs, nous voyons bien le refus par « **ACL_Stagiaires** » :

```
28.11.2024 14:06:45 192.168.10.150/192.168.10.150 www.facebook.com:443 Request(ACL_Stagiaires/blk_blacklists_social_networks/-) lmaraval CONNECT REDIRECT
```

2.7 Configuration du portail captif pour les Guest

Nous commençons la configuration du portail captif dans le menu « **Services** » puis « **Captive Portal** » :



1. Activer le portail captif
2. Interface d'assignation du portail captif à l'interface Guest

Plus bas dans la page nous renseignons les paramètres suivants :

The screenshot shows the 'Authentication' configuration page. It includes sections for 'Authentication Method', 'Authentication Server', 'Secondary authentication Server', 'Reauthenticate Users', and 'Local Authentication Privileges'. Below this is the 'HTTPS Options' section, which contains a 'Login' configuration. A yellow circle labeled '1' highlights the dropdown menu for 'Authentication Method'. A yellow circle labeled '2' highlights the dropdown menu for 'Authentication Server'.

Authentication

Authentication Method Use an Authentication backend 1
 Select an Authentication Method to use for this zone. One method must be selected.
 - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
 - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
 - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server Local Database 2
 You can add a remote authentication server in the [User Manager](#).
 Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

Secondary authentication Server Local Database

You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

Reauthenticate Users Reauthenticate connected users every minute
 If reauthentication is enabled, requests are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in. The cached credentials are necessary for the portal to perform automatic reauthentication requests.

Local Authentication Privileges Allow only users/groups with "Captive portal login" privilege set

HTTPS Options

Login Enable HTTPS login
 When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

Save

1. Authentification via une page demandant un login ou voucher
2. Authentification via la base locale (le serveur voucher étant le pare feu)

Nous pouvons désormais configurer le serveur vouchers :

Create, Generate and Activate Rolls with Vouchers

Enable Enable the creation, generation and activation of rolls with vouchers 1

Create, Generate and Activate Rolls with Vouchers

Voucher Public Key

```
-----BEGIN PUBLIC KEY-----
MCQwDQYJKoZIhvCNQEBBQADEwAwEAIJAMXBEFe59829AgMBAAE=
-----END PUBLIC KEY-----
```

Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers. [Generate new keys](#) 2

Voucher Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MD4CAQACQDFwRBXuffNvQIDAQABAggHUmMi87YcQQIFAOejg2ECBQDa
jUPdAgQs
OvrBAgQn08yFAgUAhxaVdQ==
-----END RSA PRIVATE KEY-----
```

Paste an RSA private key (64 Bit or smaller) in PEM format here. This key is only used to generate encrypted vouchers and doesn't need to be available if the vouchers have been generated offline. 3

Character set 2345678abcdefghijklmnopqrstuvwxyzABCDEF GHJKLMNOPQRSTUVWXYZ

Tickets are generated with the specified character set. It should contain printable characters (numbers, lower case and upper case letters) that are hard to confuse with others. Avoid e.g. 0/O and l/1.

of Roll bits 16

Reserves a range in each voucher to store the Roll # it belongs to. Allowed range: 1..31. Sum of Roll+Ticket+Checksum bits must be one Bit less than the RSA key size.

of Ticket bits 10

Reserves a range in each voucher to store the Ticket# it belongs to. Allowed range: 1..16. Using 16 bits allows a roll to have up to 65535 vouchers. A bit array, stored in RAM and in the config, is used to mark if a voucher has been used. A bit array for 65535 vouchers requires 8 KB of storage.

of Checksum bits 5

Reserves a range in each voucher to store a simple checksum over Roll # and Ticket#. Allowed range is 0..31.

Magic number 79897728

Magic number stored in every voucher. Verified during voucher check. Size depends on how many bits are left by Roll+Ticket+Checksum bits. If all bits are used, no magic number will be used and checked.

Invalid voucher message Voucher invalid

Error message displayed for invalid vouchers on captive portal error page (\$PORTAL_MESSAGES\$).

Expired voucher message Voucher expired

Error message displayed for expired vouchers on captive portal error page (\$PORTAL_MESSAGES\$).

Save

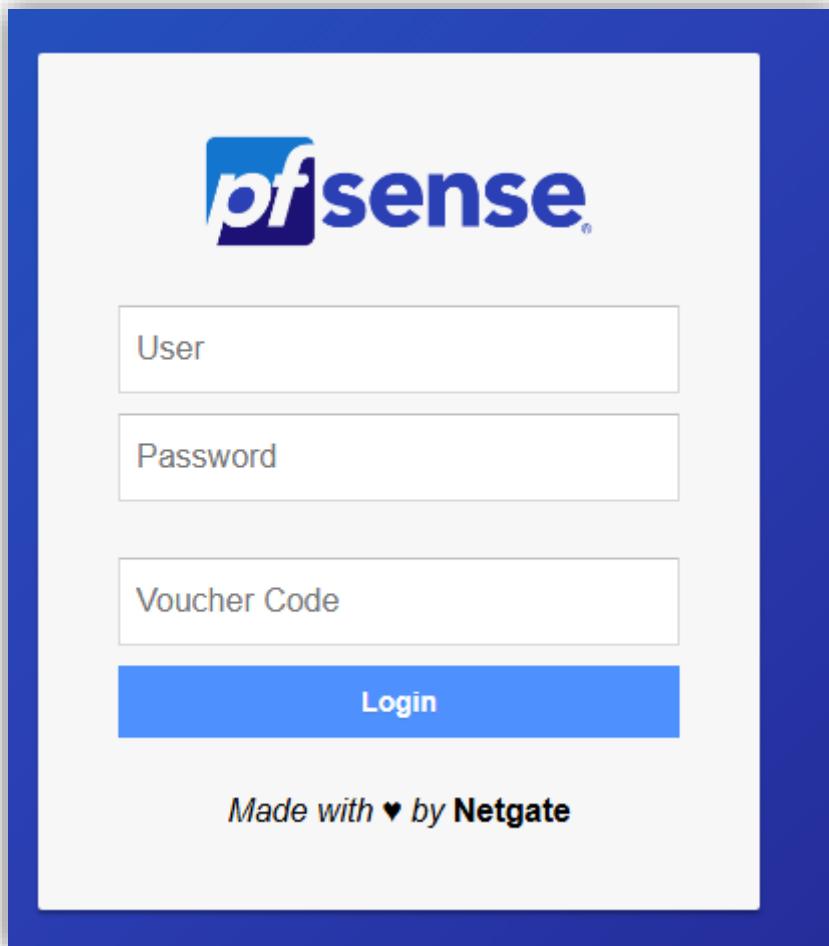
1. Activer le serveur vouchers
2. Clé privée pour déchiffrer les vouchers
3. Clé publique pour chiffrer les vouchers

Nous générerons un voucher via le bouton « Add » et l'exportons en CSV pour récupérer le login

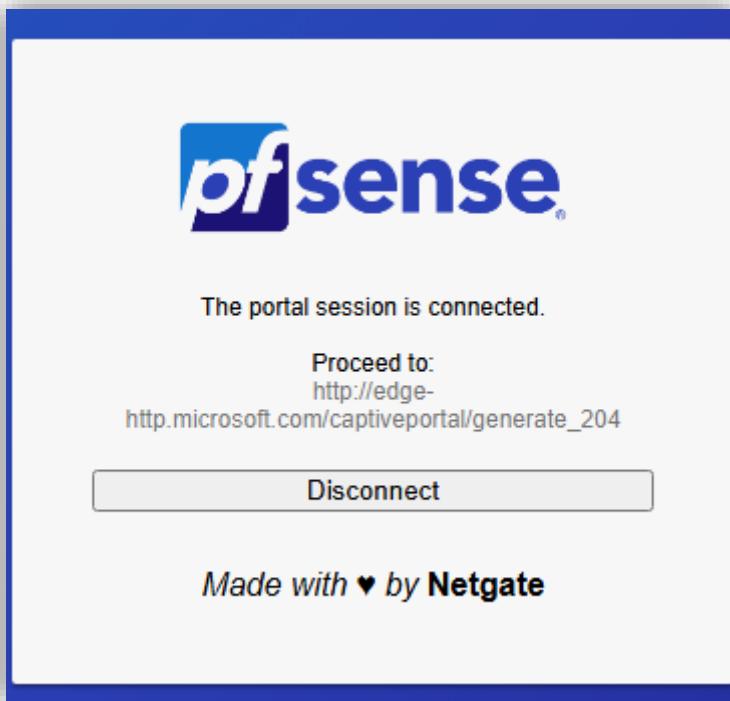
Voucher Rolls				
Roll #	Minutes/Ticket	# of Tickets	Comment	Actions
0	60	1		
+ Add				

Nous allons tester maintenant notre solution.

Une fois connecté au réseau « **Guest** », nous lançons le navigateur Firefox et voyons cette page :



Nous renseignons les codes vouchers générés précédemment et nous constatons l'authentification acceptée :



Nous retrouvons les logs de connexion dans notre pare feu afin d'avoir les détails de la session en cours :

```
Dec 6 09:42:42 logportalauth 99651 Zone: portail_captif - FAILURE: 2345678abcdefghijklmnqrstuvwxyzABCDEFGHIJKLMNPQRSTUVWXYZ, 00:0c:29:1d:a2:e1, 192.168.20.101
Dec 6 09:42:49 logportalauth 99651 Zone: portail_captif - CONCURRENT LOGIN - REUSING OLD SESSION: a5iW6d2JFA7, 00:0c:29:1d:a2:e1, 192.168.20.101
Dec 6 09:42:49 logportalauth 99651 Zone: portail_captif - Voucher login good for 60 min.: a5iW6d2JFA7, 00:0c:29:1d:a2:e1, 192.168.20.101
```

Users Logged In (1)				
IP address	MAC address	Username	Session start	Actions
192.168.20.101	00:0c:29:1d:a2:e1	a5iW6d2JFA7	12/06/2024 09:42:49	

3. Conclusion

En réponse aux besoins d'ADRAR, nous avons conçu et mis en place une solution de Proxy basée sur PfSense avec Squid et ses extensions, permettant de sécuriser et de contrôler efficacement les accès Internet. Cette infrastructure offre :

- Filtrage Web avancé : Une gestion personnalisée des accès basée sur les groupes LDAP (Formateurs, Stagiaires) pour une navigation adaptée et sécurisée.
- Portail captif : authentification via vouchers pour les visiteurs et limitation des accès via un VLAN Guest étanche et sécurisé.
- Journalisation conforme : Conservation des logs utilisateurs pour une durée de 180 jours, respectant les obligations légales.
- Sécurité renforcée : Proxy explicite sans SSL bump pour une meilleure conformité RGPD.

Cette solution fiable, évolutive et intégrée garantit la sécurité et l'efficacité des flux Internet tout en répondant aux exigences réglementaires.

4. Annexes

Documentation ANSSI sur la mise en place d'un Proxy :

https://cyber.gouv.fr/sites/default/files/2012/01/ansi-guide-passarelle_internet_securisee-v2.pdf

Documentation RGPD : <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

Installation et paramétrage de Pfsense : <https://www.it-connect.fr/installation-de-pfsense%EF%BB%BF/>

Configuration de Squid et Squid Guard sur Pfsense : <https://www.it-connect.fr/pfsense-et-squid-ajouter-le-filtrage-par-categories-avec-squid-guard/>

Configuration de LightSquid : <https://www.pc2s.fr/pfsense-proxy-transparent-filtrage-web-url-squid-squidguard/>

Configuration du portail captif Pfsense : <https://www.comparitech.com/blog/vpn-privacy/captive-portal-pfsense/>

Configuration des vouchers sur Pfsense :

<https://docs.netgate.com/pfsense/en/latest/captiveportal/vouchers.html>