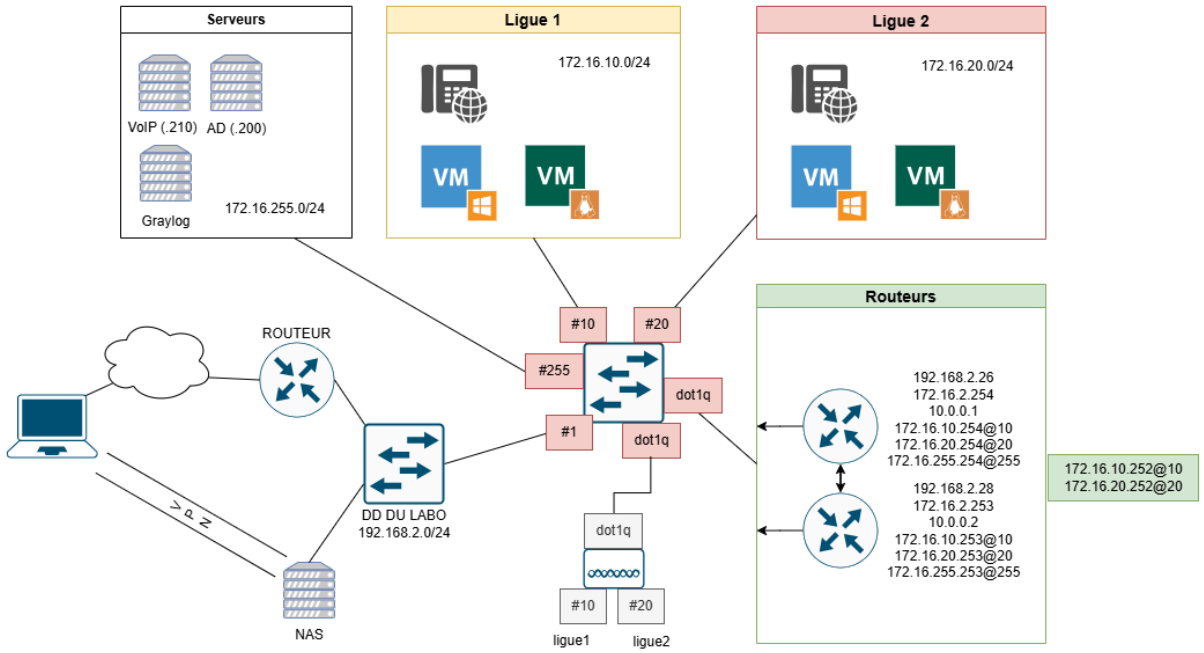
AP3-M4 SPorTif

* vert: tâche effectuée et présentée lors de la disposition fonctionnelle
* orange: tâche en cours de finalisation, non présentée lors de la disposition fonctionnelle

Contexte :

Mettre en conformité avec la loi, le contrôle des accès Internet réalisé pour les utilisateurs de la M2L.

Schéma Réseau :



pfS1

```
WAN (wan)       -> em2        -> v4: 192.168.2.26/24
LAN (lan)       -> em1        -> v4: 172.16.2.254/24
PFSYNC (opt1)   -> em0        -> v4: 10.0.0.1/30
L1 (opt2)       -> em1.10     -> v4: 172.16.10.254/24
L2 (opt3)       -> em1.20     -> v4: 172.16.20.254/24
SERV (opt4)     -> em1.255    -> v4: 172.16.255.254/24
```

pfS2

```
WAN (wan)       -> em2        -> v4: 192.168.2.28/24
LAN (lan)       -> em1        -> v4: 172.16.2.253/24
PFSYNC (opt1)   -> em0        -> v4: 10.0.0.2/30
L1 (opt2)       -> em1.10     -> v4: 172.16.10.253/24
L2 (opt3)       -> em1.20     -> v4: 172.16.20.253/24
SERV (opt4)     -> em1.255    -> v4: 172.16.255.253/24
```

VLAN Interfaces

Interface	VLAN tag	Priority	Description
em1 (lan)	10		Ligue 1
em1 (lan)	20		Ligue 2
em1 (lan)	255		Serveurs

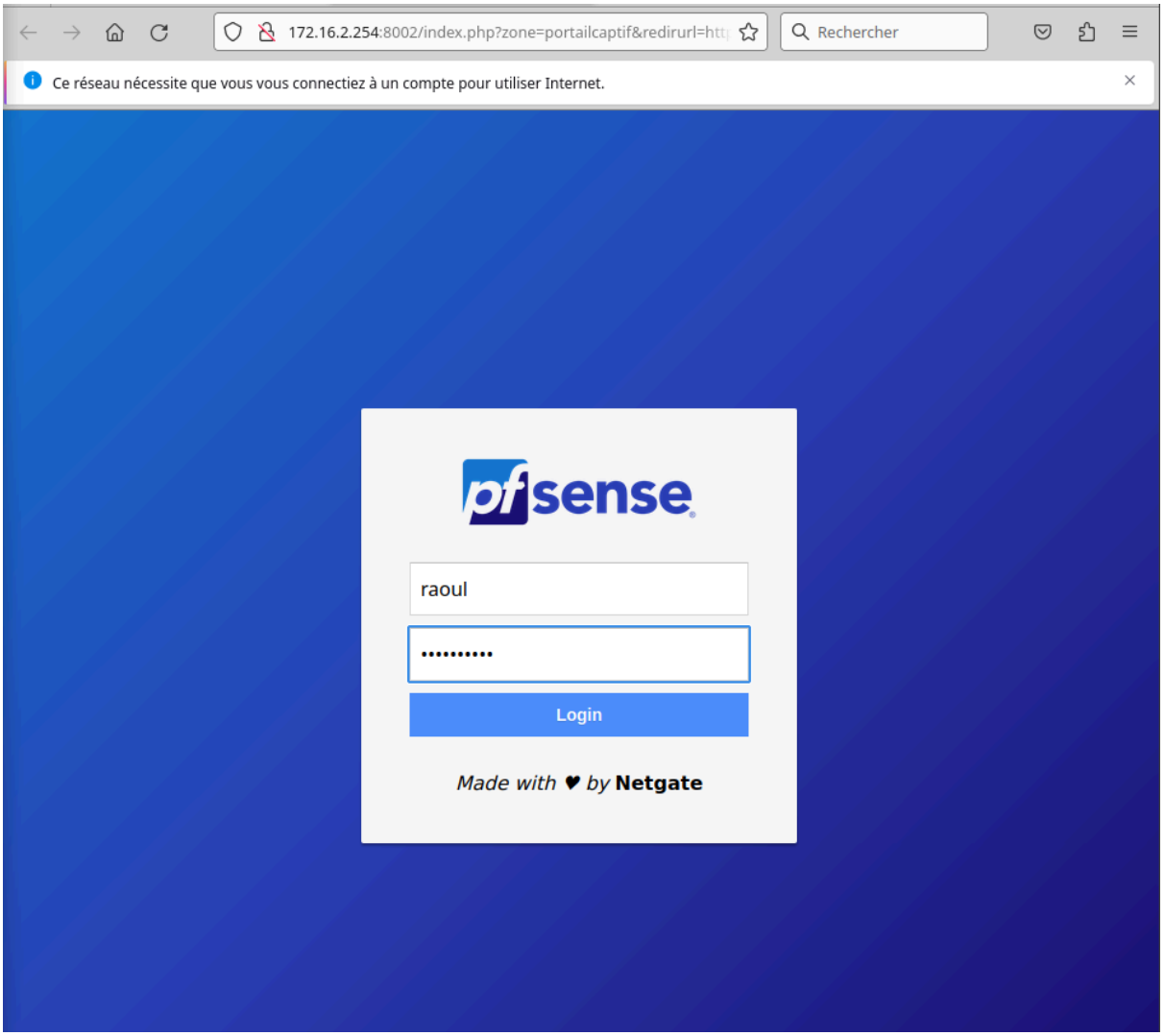
Interface	Network port
WAN	em2 (08:00:27:1d:ce:87)
LAN	em1 (08:00:27:9c:30:bf)
PFSYNC	em0 (08:00:27:4d:3c:04)
L1	VLAN 10 on em1 - lan (Ligue 1)
L2	VLAN 20 on em1 - lan (Ligue 2)
SERV	VLAN 255 on em1 - lan (Serveurs)

Save

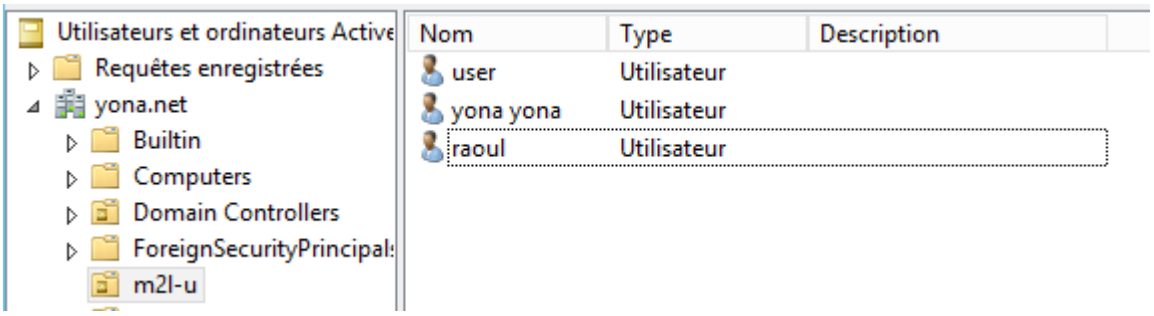
Virtual IP Address

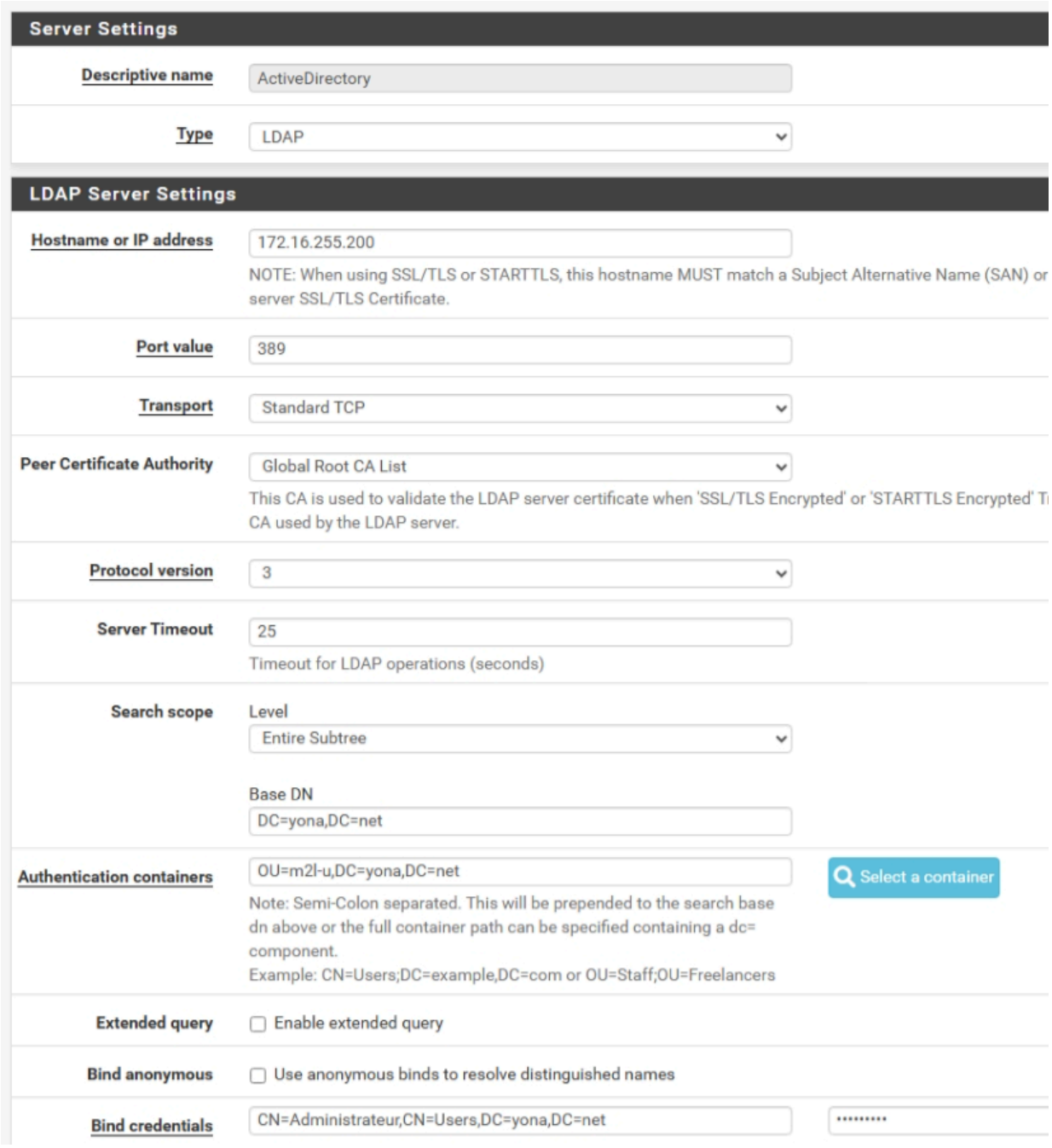
Virtual IP address	Interface	Type	Description
172.16.10.252/24 (vhid: 26)	L1	CARP	IP VIR LIGUE1
172.16.20.252/24 (vhid: 27)	L1	CARP	IP VIR LIGUE2
172.16.255.252/32 (vhid: 28)	WAN	CARP	IP V SERVEURS

Tentative de connexion à internet à partir d'un navigateur

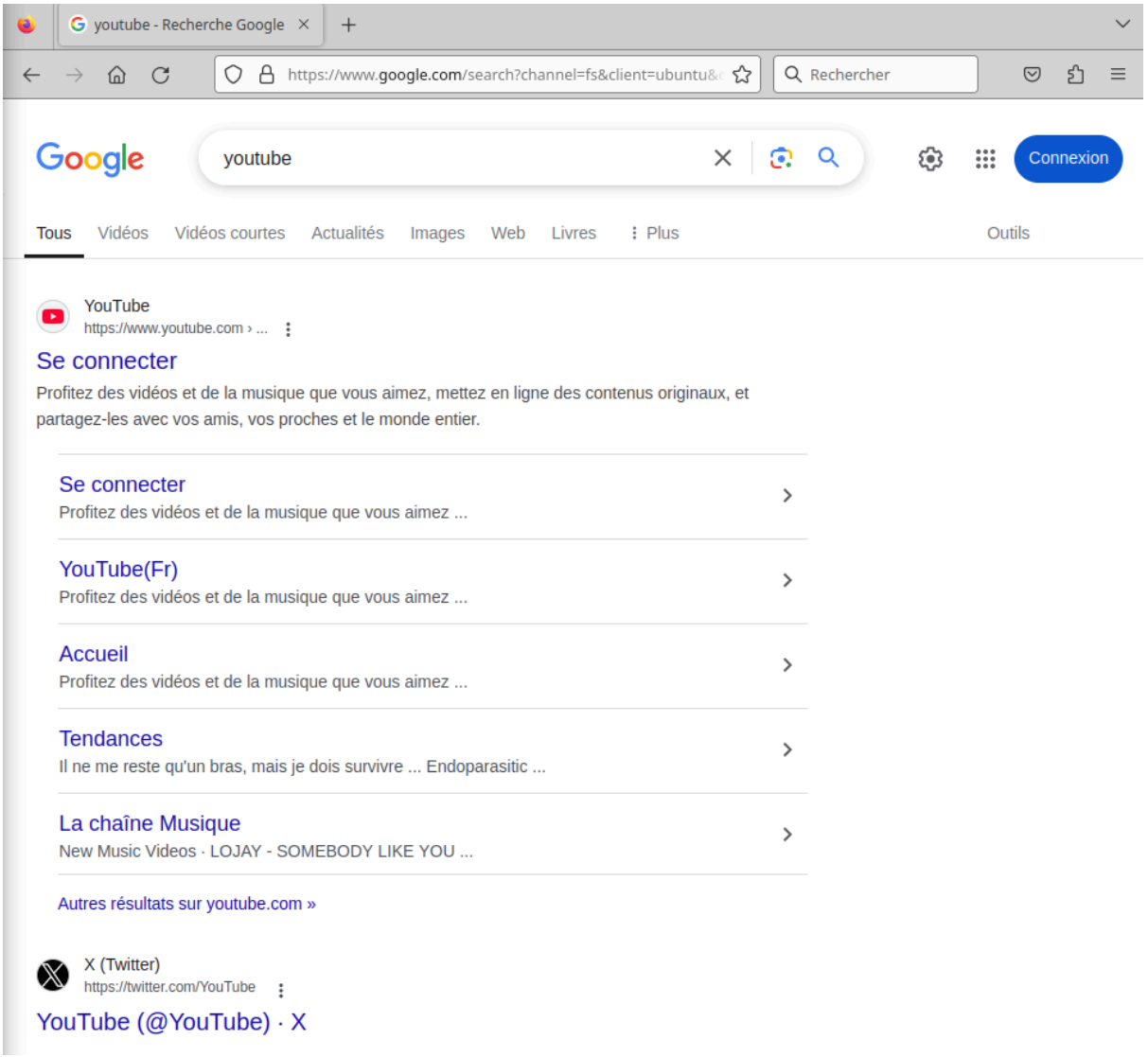


Le client en question se situe au niveau de l'OU "m2l-u".

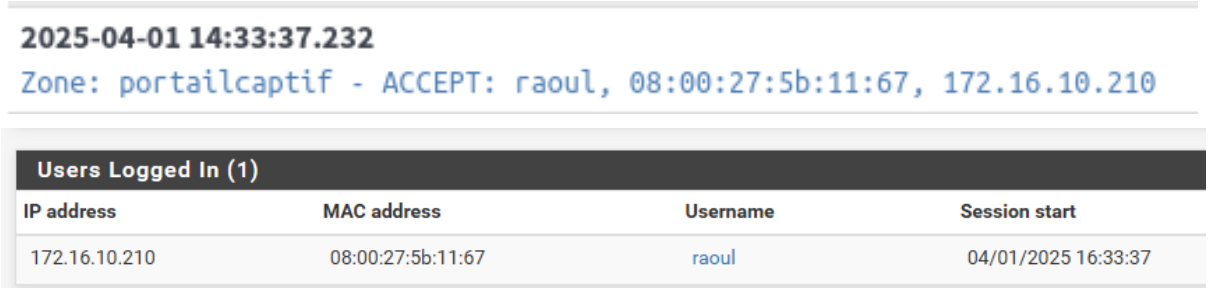


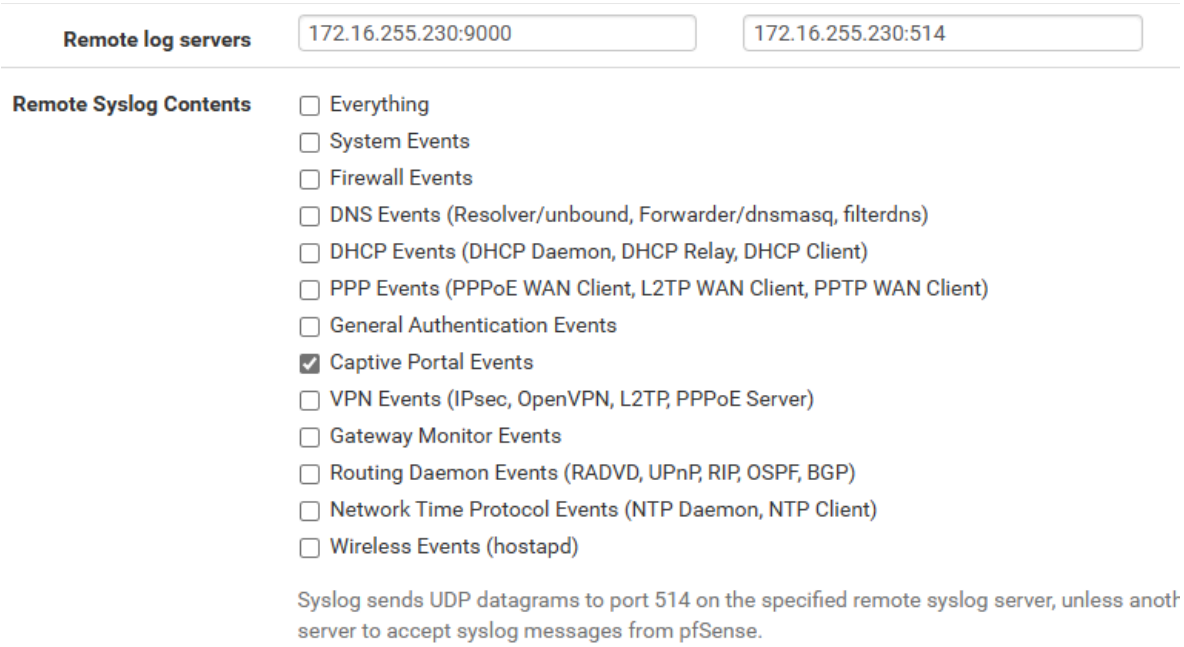


Le client est maintenant en mesure de se rendre sur internet



On retrouve en simultané sur graylog, que raoul s'est bien authentifié au portail captif.



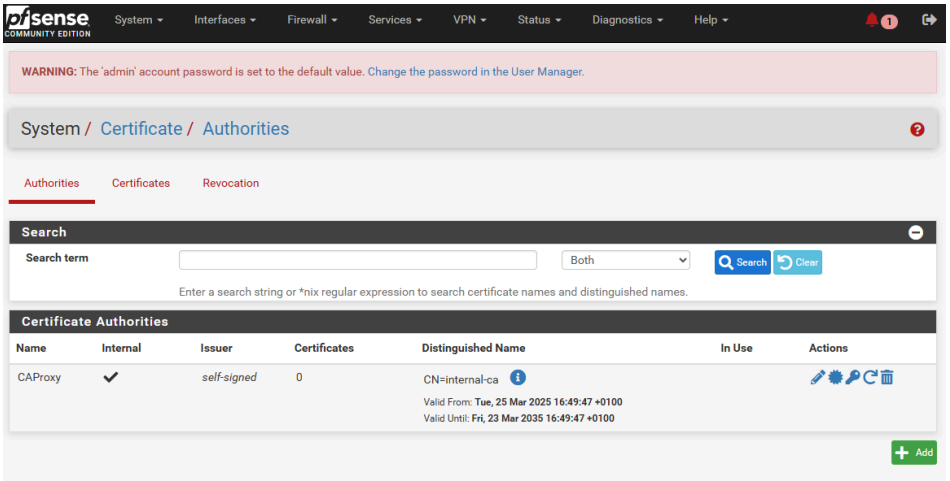

Remote log servers
172.16.255.230:9000
172.16.255.230:514
Remote Syslog Contents
Everything
System Events
Firewall Events
DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
General Authentication Events
Captive Portal Events
VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
Gateway Monitor Events
Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
Network Time Protocol Events (NTP Daemon, NTP Client)
Wireless Events (hostapd)
Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless anoth
server to accept syslog messages from pfSense.

Filtrage web d'URL via le proxy Squid sur pfsense :

Objectif : Bloquer les accès aux sites internet non conforme pour tout utilisateurs de chaques ligues

Outils utilisés :
- Squid (Proxy)
- SquidGuard (Contrôle les contenus des sites webs accessibles par les utilisateurs)
- LightSquid (Journalise les sites webs consultés par les utilisateurs)

Création d'un certificat nommé "CAProxy"pour permettre le filtrage https



Concernant la configuration de **Squid**, en sachant que les clients proviennent de deux ligues différentes, le proxy sera activé sur les interfaces L1 et L2.

Pour la configuration de **SquidGuard**, nous avons utilisé une liste publique contenant un ensemble de sites webs placés en liste noire Blacklists UT1
Il est possible d'autoriser ou de bloquer une ou plusieurs catégories souhaités (sites pour adultes, jeux…)

Target Rules List

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories		
[blk_blacklists_adult]	access	deny
[blk_blacklists_agressif]	access	deny
[blk_blacklists_arjel]	access	---
[blk_blacklists_associations_religieuses]	access	---
[blk_blacklists_astrology]	access	---
[blk_blacklists_audio-video]	access	---
[blk_blacklists_bank]	access	---
[blk_blacklists_bitcoin]	access	---
[blk_blacklists_blog]	access	---
[blk_blacklists_celebrity]	access	---
[blk_blacklists_chat]	access	allow
[blk_blacklists_child]	access	---
[blk_blacklists_cleaning]	access	---
[blk_blacklists_cooking]	access	---
[blk_blacklists_cryptojacking]	access	---
[blk_blacklists_dangerous_material]	access	---
[blk_blacklists_dating]	access	---
[blk_blacklists_ddos]	access	---
[blk_blacklists_dialer]	access	---
[blk_blacklists_doh]	access	---
[blk_blacklists_download]	access	---
[blk_blacklists_drogue]	access	---
[blk_blacklists_dynamic-dns]	access	---
[blk_blacklists_educational_games]	access	---
[blk_blacklists_examen_pix]	access	---
[blk_blacklists_exceptions_liste_bu]	access	---
[blk_blacklists_fakenews]	access	deny
[blk_blacklists_filehosting]	access	---
[blk_blacklists_financial]	access	---
[blk_blacklists_forums]	access	---
[blk_blacklists_gambling]	access	---
[blk_blacklists_games]	access	---
[blk_blacklists_hacking]	access	---
[blk_blacklists_jobsearch]	access	---
[blk_blacklists_lingerie]	access	---
[blk_blacklists_liste_blanche]	access	---

Lightsquid :

Test : En allant sur la page web de lightsquid, on retrouve l'utilisateur raoul qui a consulté le site web x.com le 5 Avril 2025
(Le résultat ci-dessous est une représentation de la fonctionnalité réelle)

Squid rapport d'accès utilisateur

Utilisateur	raoul
Groupe	**L1**
Date:	**05 Avr 2025**

#	Site(s) Accédé(s)	Connexion(s)	Octets	Somme	%
1	x.com	1	100 000	100 000	100 %

Install graylog :

Installer les dépendances
sudo apt install -y apt-transport-https gnupg2 uuid-runtime pwgen curl

Installer Java (OpenJDK 11)
sudo apt install -y openjdk-11-jdk

Installer MongoDB
MongoDB est utilisé par Graylog pour stocker les données.

wget -qO - https://www.mongodb.org/static/pgp/server-6.0.asc | sudo apt-key add -
echo "deb [arch=amd64] https://repo.mongodb.org/apt/debian buster/mongodb-org/6.0 main" | sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list
sudo apt update
sudo apt install -y mongodb-org
sudo systemctl enable --now mongod

Installer Elasticsearch:

Graylog utilise **OpenSearch ou Elasticsearch** pour l'indexation des logs.

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
sudo apt update
sudo apt install -y elasticsearch

Modifier le fichier de configuration
sudo nano /etc/elasticsearch/elasticsearch.yml

Ajoutet :

cluster.name: graylog

action.auto_create_index: false

Puis redémarrer Elasticsearch :

sudo systemctl enable --now elasticsearch

6. Installer Graylog

wget https://packages.graylog2.org/repo/packages/graylog-5.0-repository_latest.deb
sudo dpkg -i graylog-5.0-repository_latest.deb
sudo apt update
sudo apt install -y graylog-server

7. Configurer Graylog

Générez un secret et un mot de passe pour l'admin :

pwgen -N 1 -s 96

Ajoutez ce secret dans /etc/graylog/server/server.conf :

sudo nano /etc/graylog/server/server.conf

Modifiez les lignes suivantes :

password_secret = mdp
root_password_sha2 = HASH_MOT_DE_PASSE
http_bind_address = 0.0.0.0:9000

Générez le mot de passe en SHA-256 :

echo -n "monmotdepasse" | sha256

8. Démarrer et activer Graylog

sudo systemctl daemon-reload
sudo systemctl enable --now graylog-server

9. Accéder à l'interface Web

Ouvrez votre navigateur et accédez à :

http://172.16.255.210:9000

Annexes :

Planification de projet → https://redmine.0x01.ovh/

Plans de tests :

Test	Attendu	Résultat
Tentative de connection à Internet via un navigateur	Le client doit s'authentifier auprès d'un portail captif avec ses identifiants stockés sur un Active Directory pour obtenir l'accès Internet	OK
Tentative de connexion au Serveur WEB intranet depuis un client	Le client doit pouvoir consulter le WEB intranet	OK
Identifier l'utilisateur qui se connecte au portail captif par son IP et son adresse MAC	Depuis l'interface Graylog on peut identifier qui s'est au portail captif	OK

Schémas: V1 / v2 / v3