LYCÉE ROBERT SCHUMAN METZ

Projet SISR5-4 : Pare-feu et VPN.

VEYNAND SAINT FIACRE Lucille

16/03/2021

Table des matières

1 Introduction

Comment mettre en place un pare-feux logiciel ainsi qu'un VPN.

2 Contexte de travail et gestion des configurations

Voir contexte.doc

3 Gestion du travail en équipe et gestion du projet

	Date	Activité
VEYNAND SAINT FIACRE Lucille	16/03/2021 22/03/2021 23/03/2021	-Introduction -Étape 1 à 4 étape 2 (problème de proxy) -Beaucoup de difficulté à faire l'étape 4-5-6 -Le travail est maintenant centralisé sur la VM du P14 car il faut la centraliser

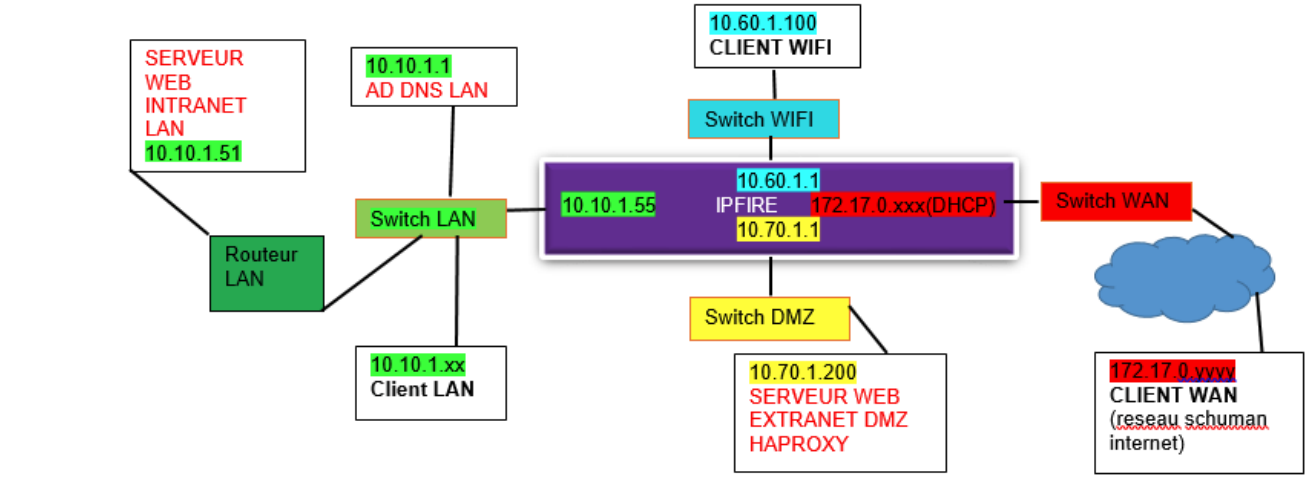
4 Activités compétences du référentiel du BTSSIO (reseaucerta.org)

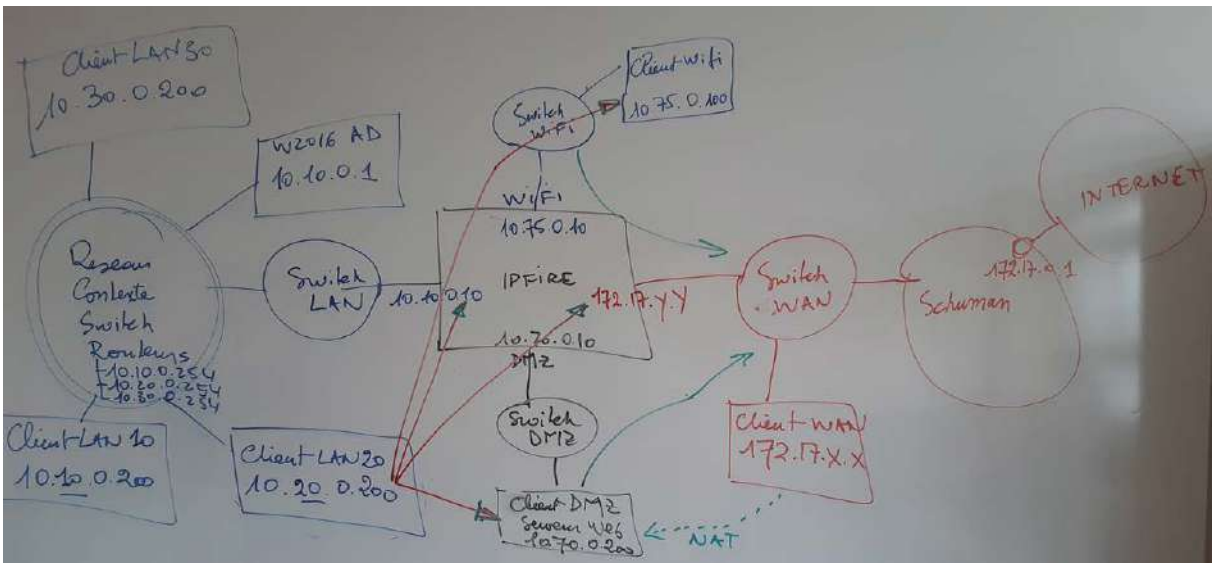
A1.1.2 , Étude de l'impact de l'intégration d'un service sur le système informatique
A1.1.3 , Étude des exigences liées à la qualité attendue d'un service
A1.2.4 , Détermination des tests nécessaires à la validation d'un service
A1.3.1 , Test d'intégration et d'acceptation d'un service
A1.3.3 , Accompagnement de la mise en place d'un nouveau service
A1.3.4 , Déploiement d'un service
A1.4.1 , Participation à un projet
A1.4.2 , Évaluation des indicateurs de suivi d'un projet et justification des écarts
A2.2.1 , Suivi et résolution d'incidents
A3.1.2 , Maquettage et prototypage d'une solution d'infrastructure
A3.1.3 , Prise en compte du niveau de sécurité nécessaire à une infrastructure
A3.3.1 , Administration sur site ou à distance des éléments d'un réseau, de serveurs, …
A5.2.2 , Veille technologique
A5.2.3 , Repérage des compléments de formation ou d'auto-formation ...
A5.2.4 , Étude d'une technologie, d'un composant, d'un outil ou d'une méthode

5 La documentation.

https://wiki.ipfire.org/configuration/network/dnsforward

6 Le Maquettage





7 Incident problème et assistance

Des problèmes avec le forward de DNS, résolu avec: https://wiki.ipfire.org/configuration/network/dnsforward

https://www.ipfire.org/
http://reseaux85.fr/index.php?title=IPFire_-_Firewall/Proxy/Filtrage/Addons
https://drive.google.com/file/d/0BwtfbS0twOeXaDFWay1xbUdCd00/view
https://wiki.ipfire.org/start
https://www.commentcamarche.net/contents/992-firewall-pare-feu
http://cerig.pagora.grenoble-inp.fr/Note/1999/Proxy_26-07-99.htm
https://www.memoireonline.com/07/11/4611/m_Mise-en-place-dun-proxy-Squid-securise-avec-authentification-LDAP3.html

Définir un pare-feu ?
Un pare-feu est un appareil de protection du réseau qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

IPFire : Type de logiciel ? OS ? Licence ?
IPFire est une distribution Linux, il suit une license libre, la GPL,

Fonctionnalité d'IPFire ?
IPFire a diverses fonctionnalités:
-Gestion de paquets : système léger pour un pare-feux, et modulable, il peut être mise à jour rapidement
-Parefeux
-Intrusion Detection System (Snort) de prévention des intrusions
-Serveur proxy avec filtrage de contenu et les fonctions de mise en cache des mises à jour (par exemple mises à jour Microsoft Windows, antivirus, et bien d'autres)
-Mise en cache
-Serveur de temps
-WOL (Wake up on LAN)
-VPN pour IPSec et serveur OpenVPN
-Serveur DHCP
-Dynamic DNS (DynDNS, No-IP)
-Analyse fonctions de surveillance du système et analyse des logs
-Qualité de service (QoS)

Définition de la sécurité garantie par IPFire ?
L'objectif principal d'IPFire est la sécurité. Son moteur de pare-feu et son système de détection d'intrusion, faciles à configurer, empêchent tout attaquant de pénétrer dans votre réseau. Dans la configuration par défaut, le réseau est divisé en différentes zones avec différentes stratégies de sécurité, telles qu'un réseau local et une zone démilitarisée, pour gérer les risques sur le réseau et disposer d'une configuration personnalisée pour les besoins spécifiques de chaque segment du réseau.
Mais même le pare-feu doit se protéger. IPFire est construit à partir de zéro et n'est basé sur aucune autre distribution. Cela permet aux développeurs de renforcer IPFire mieux que tout autre système d'exploitation serveur et de construire tous les composants spécifiquement pour une utilisation en tant que pare-feu.
Les mises à jour fréquentes maintiennent IPFire fort contre les vulnérabilités de sécurité et les nouveaux vecteurs d'attaque.

Quel type de pare-feu est IPFire ?
C'est un pare-feux logiciel cela veut dire qu'il n'est pas installé sur un matériel d'infrastructure dédié au pare-feux

Qu'est-ce que le système de détection et de prévention des intrusions
L'Intrusion Detection System est un système analysant le trafic réseau et détecte les exploits, s'il y'a détection, des alertes sont faites et l'attaqueur est immédiatement bloqué

Comment utiliser un VPN avec IPFire ?
Il est utilisé en concordance avec OpenVPN ou IPSec.
Pour IPSec: https://wiki.ipfire.org/configuration/services/ipsec
Pour OpenVPN: https://wiki.ipfire.org/configuration/services/openvpn/config

Définir le filtrage simple de paquets
Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall:

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

-Tout ce qui n'est pas explicitement interdit est autorisé
-Tout ce qui n'est pas explicitement autorisé est interdit

Définir le filtrage dynamique
Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP
Pour remédier à l'absence d'autorisation des ports on se sert d'un système « stateful inspection » c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Définir le filtrage applicatif
Le filtrage applicatif permet de filtrer les communications application par application.
Il permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau

Qu'est-ce qu'un serveur proxy
Un serveur proxy est un ordinateur connecté à Internet et dont votre ordinateur connaît l'adresse IP unique. Lorsque vous envoyez une requête Web, celle-ci est d'abord dirigée vers le serveur proxy

Partie 1 : **INSTALLATION de l'IPFire**

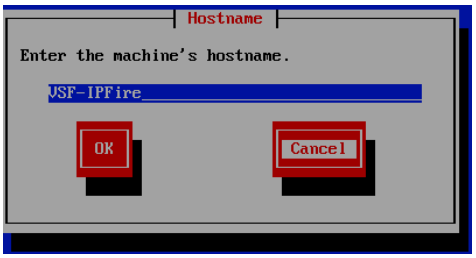
Préparer votre machine virtuelle avec 4 cartes réseau (LAN, WAN, DMZ, WIFI).
Télécharger iso IPFire 2.15
Lancer l'installation de IPFire à partir de l'iso (IPFire 2.15).

Choisir la langue pour utiliser IPfire.
Lire et accepter la licence.
Préparer le disque dure pour être partitionner en autorisant la suppression des données du disque et l'installation des systèmes de fichiers.
Choisir le système de fichier "ext4". Le disque va ensuite être partitionné et redémarré.
Appuyer sur OK pour redémarrer.

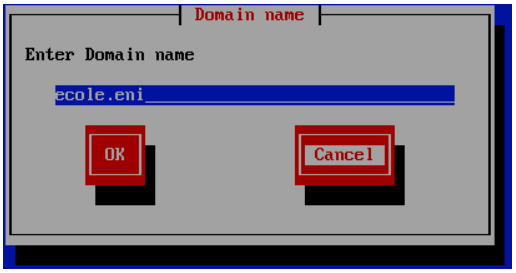
Partie 2 : **Paramétrage d'IPFIRE**

Après redémarrage choisir la langue du clavier et le fuseau horaire.

Donner le nom d'hôte de notre IPFire.

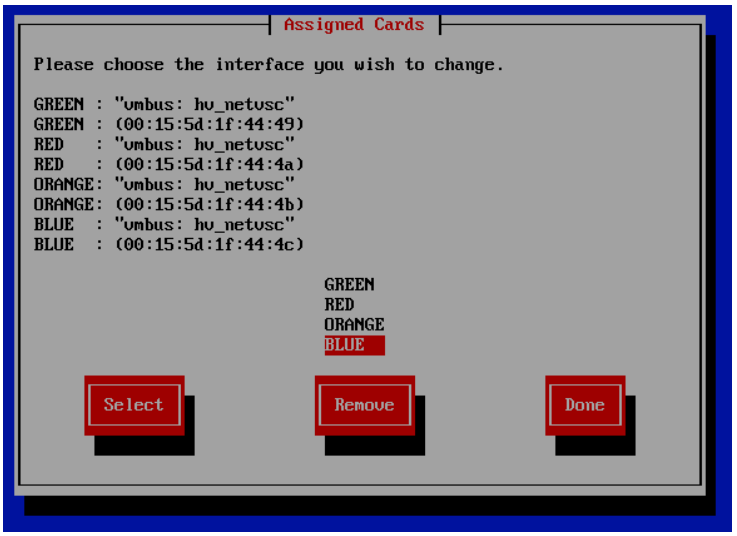


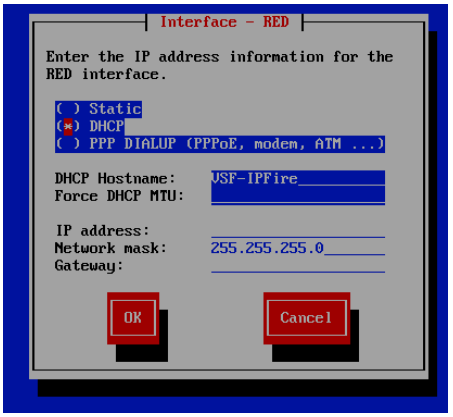
Rentrer le nom de domaine.

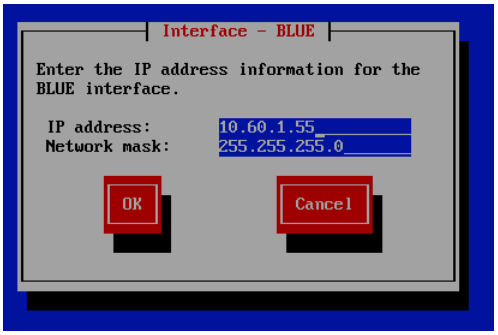


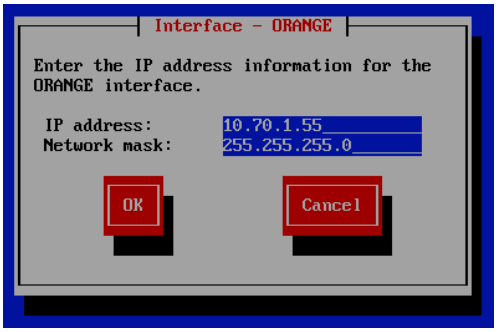
Saisir les mots de passe pour l'utilisateur "root" et pour l'administrateur "admin"
le mdp de root est root et d'amin azerty
Mot de passe : azerty

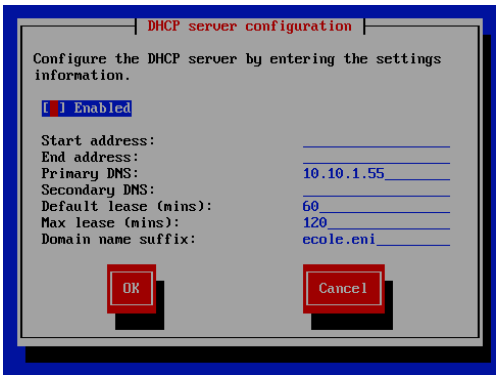
Configurer le réseau.









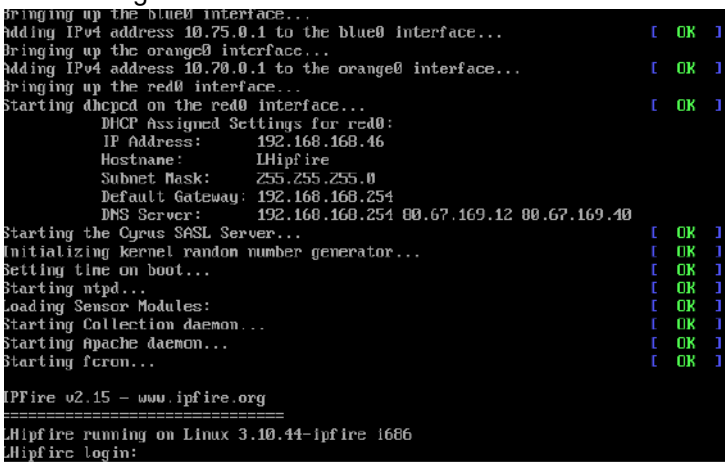


Attribuer une adresse IP (10.10.1.55/24 par exemple) à l'interface GREEN (LAN)
Configurer l'interface RED en DHCP (WAN).
Attribuer une adresse IP (10.70.1.55/24 par exemple) à l'interface ORANGE (DMZ).
Attribuer une adresse IP (10.75.1.55/24 par exemple) à l'interface BLUE (WIFI).

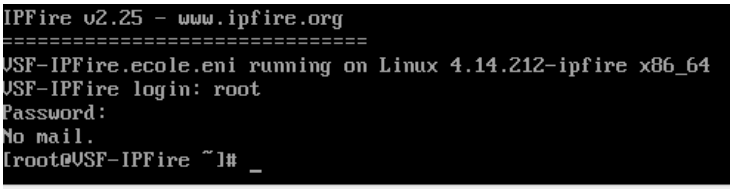
Paramétrer le DNS ainsi que la passerelle.
Terminer l'installation

Partie 3 : **Test de connexion**

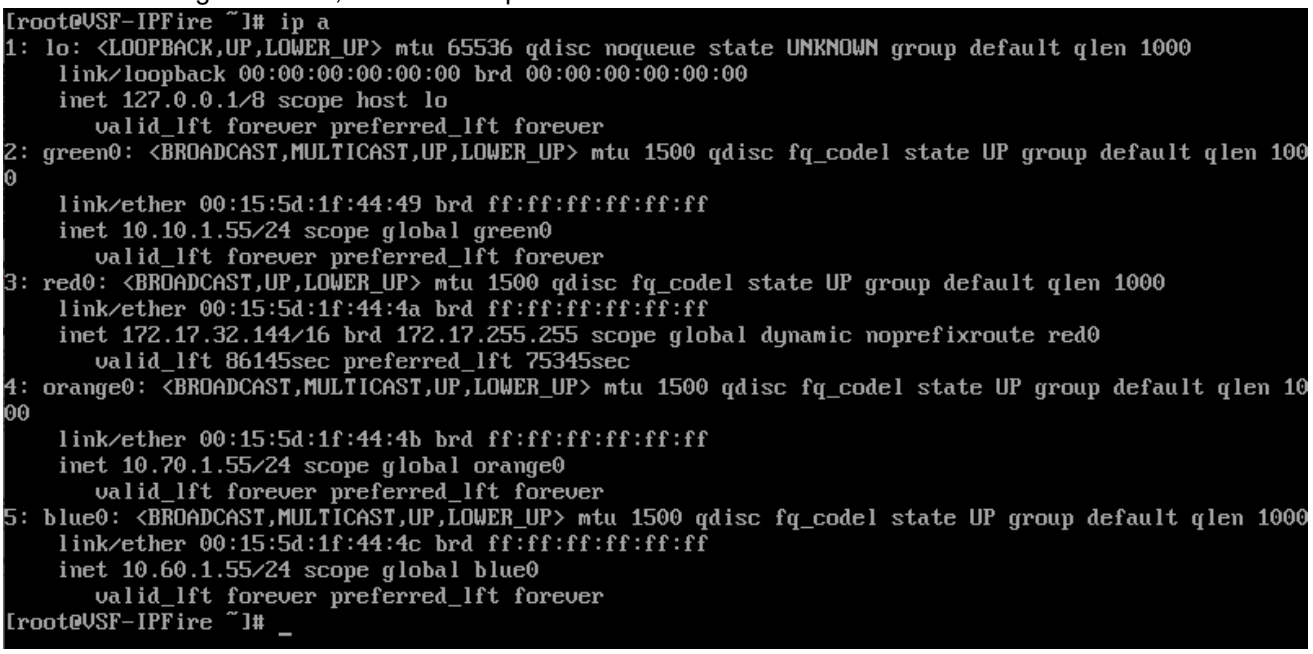
Redémarrage d'IPfire.



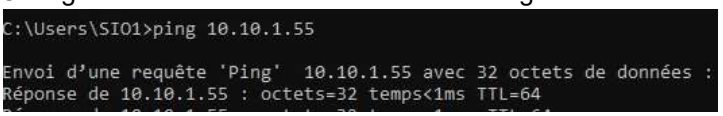
Connexion avec root



Vériffier les configurations IP, MAC de chaques interfaces.



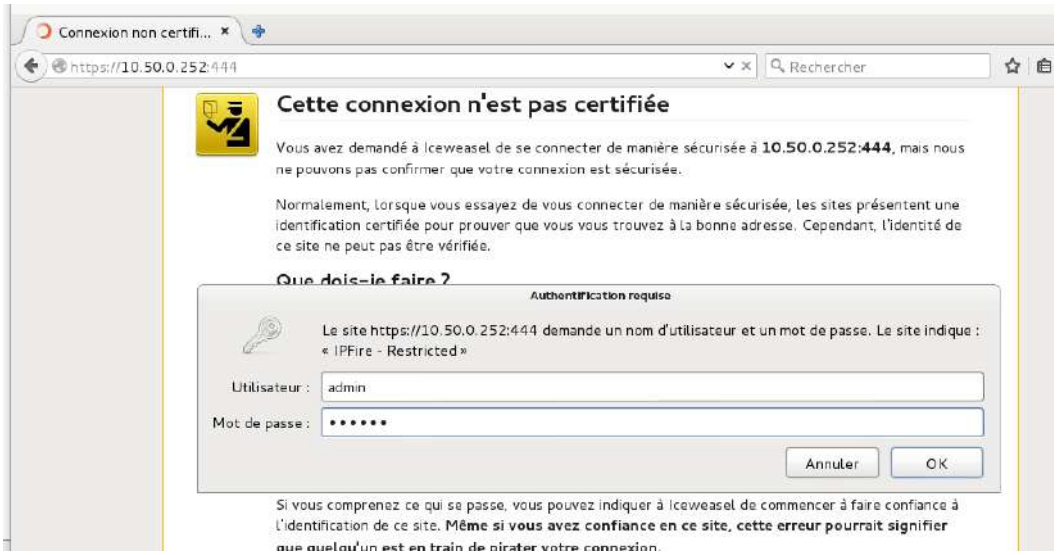
Configuration du client : vérifier son adressage IP. Et tester la communication entre le client et IPFire.



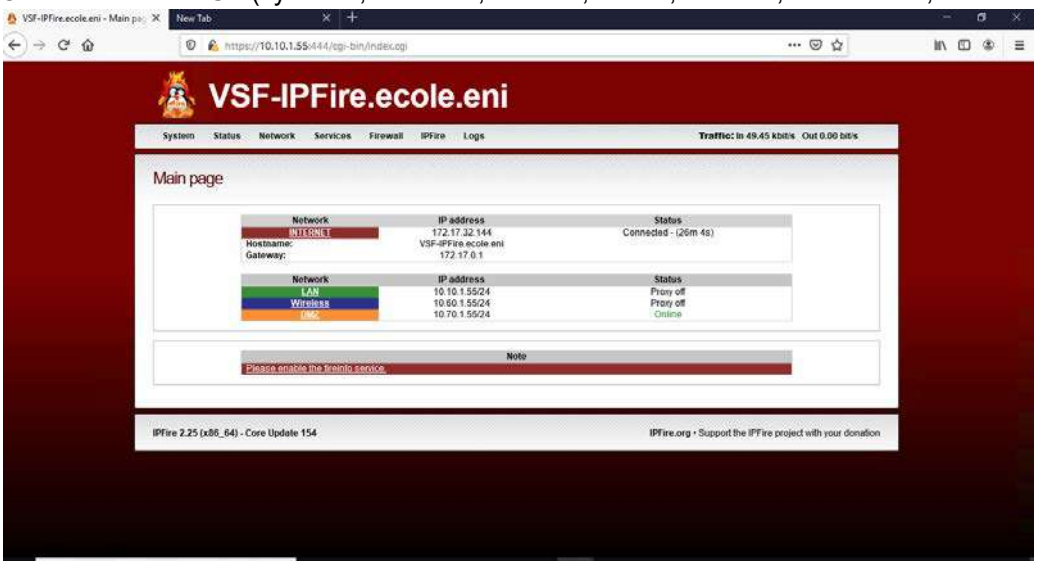
Vérifier la configuration du serveur proxy pour accéder à internet sur le navigateur du client.

Pour nous connecter sur le navigateur, il faut bien penser à désactiver le proxy (ou il faut le mettre dans les exceptions).
On se connecte avec l'adresse de Ipfire https://10.10.1.55:444. Et accepter le certificat SSL.

Connexion sécurisée à distance à Ipfire avec admin.



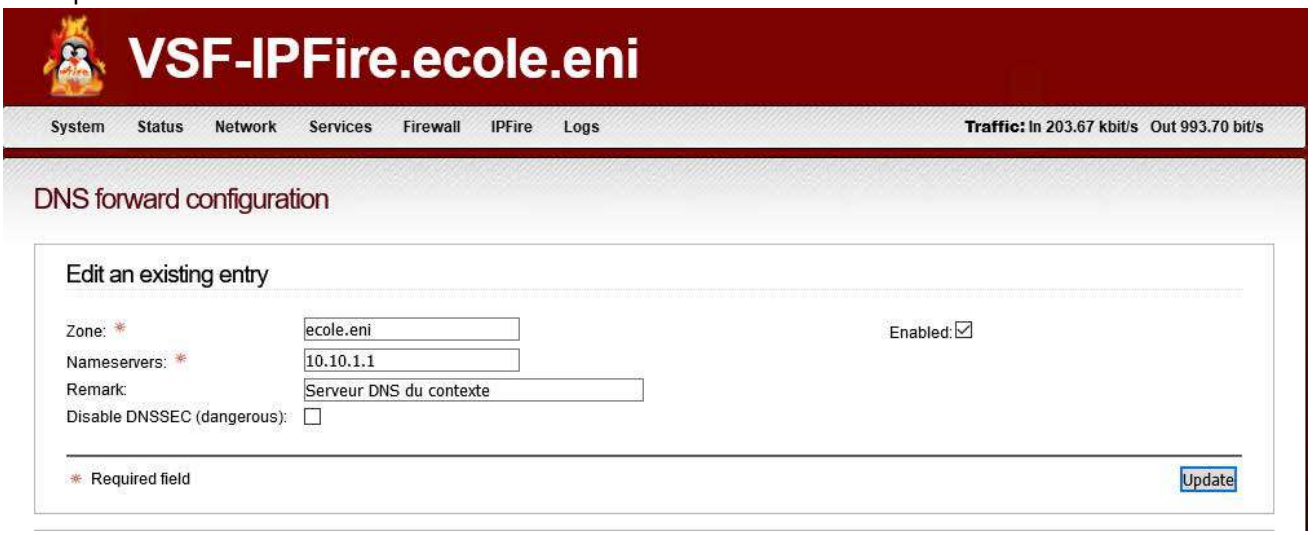
Vérifier la bonne configuration des interfaces sur la page principale de l'interface graphique d'IPFire.
Observer le STATUT (système, mémoire, Service, Média, Réseau, connexions, trafic réseau)



Partie 4 : **Configuration d'IP FIRE**

Étape 1 : Joindre le domaine ecole.eni

Afin d'ajouter la machine IPFire au domaine, il faut configurer le **DNS Forwarding** en ajoutant l'entrée correspondant à la zone DNS **ecole.eni** avec l'adresse IP du serveur.



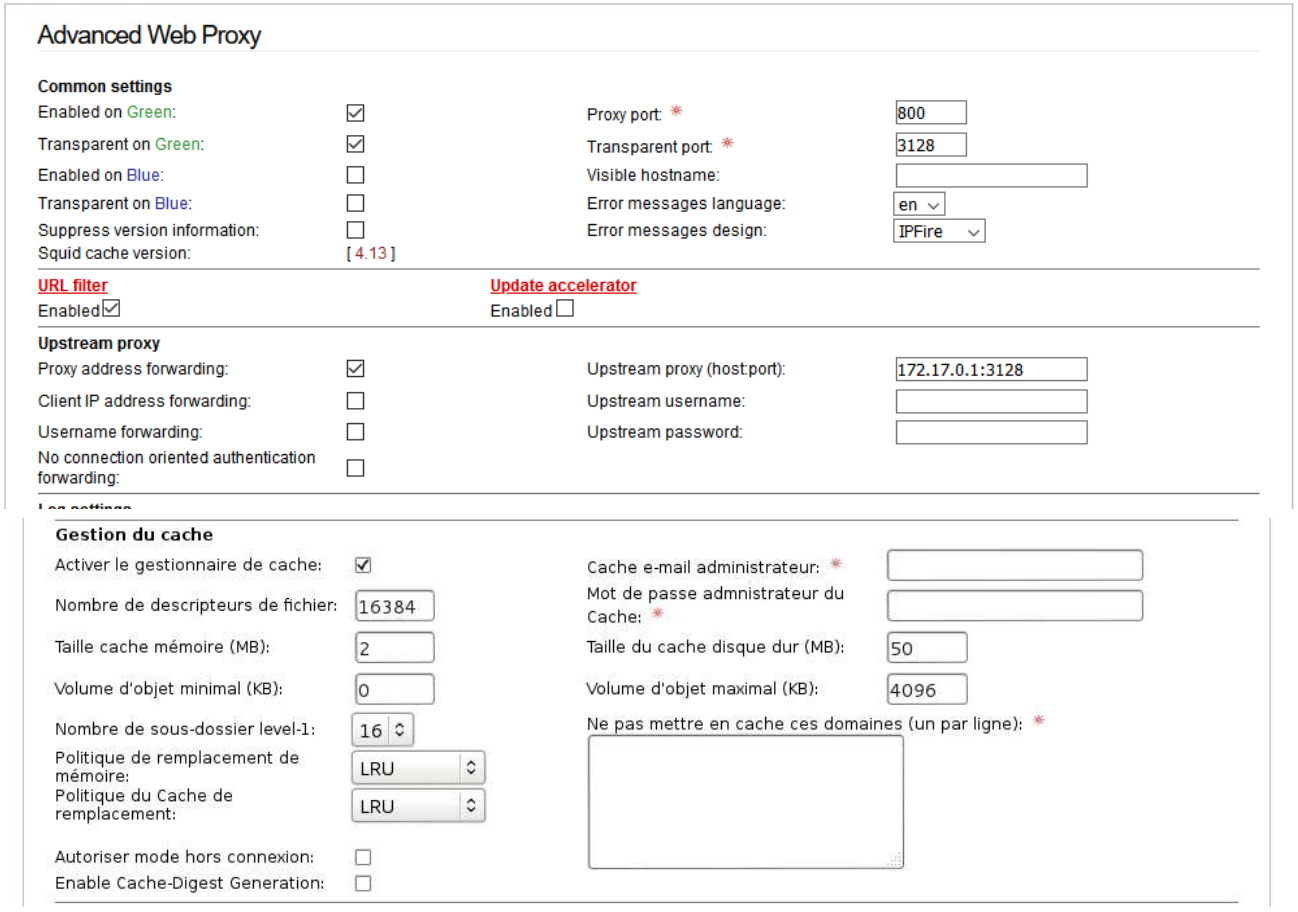
Afin que la redirection fonctionne, il a fallu suivre ces étapes:
https://wiki.ipfire.org/configuration/network/dhcp

Pour tester le **DNS Forwarding** il faut que **NSLOOKUP** sur le serveur IPFire de ecole.eni renvoie l'IP du serveur DNS du contexte.

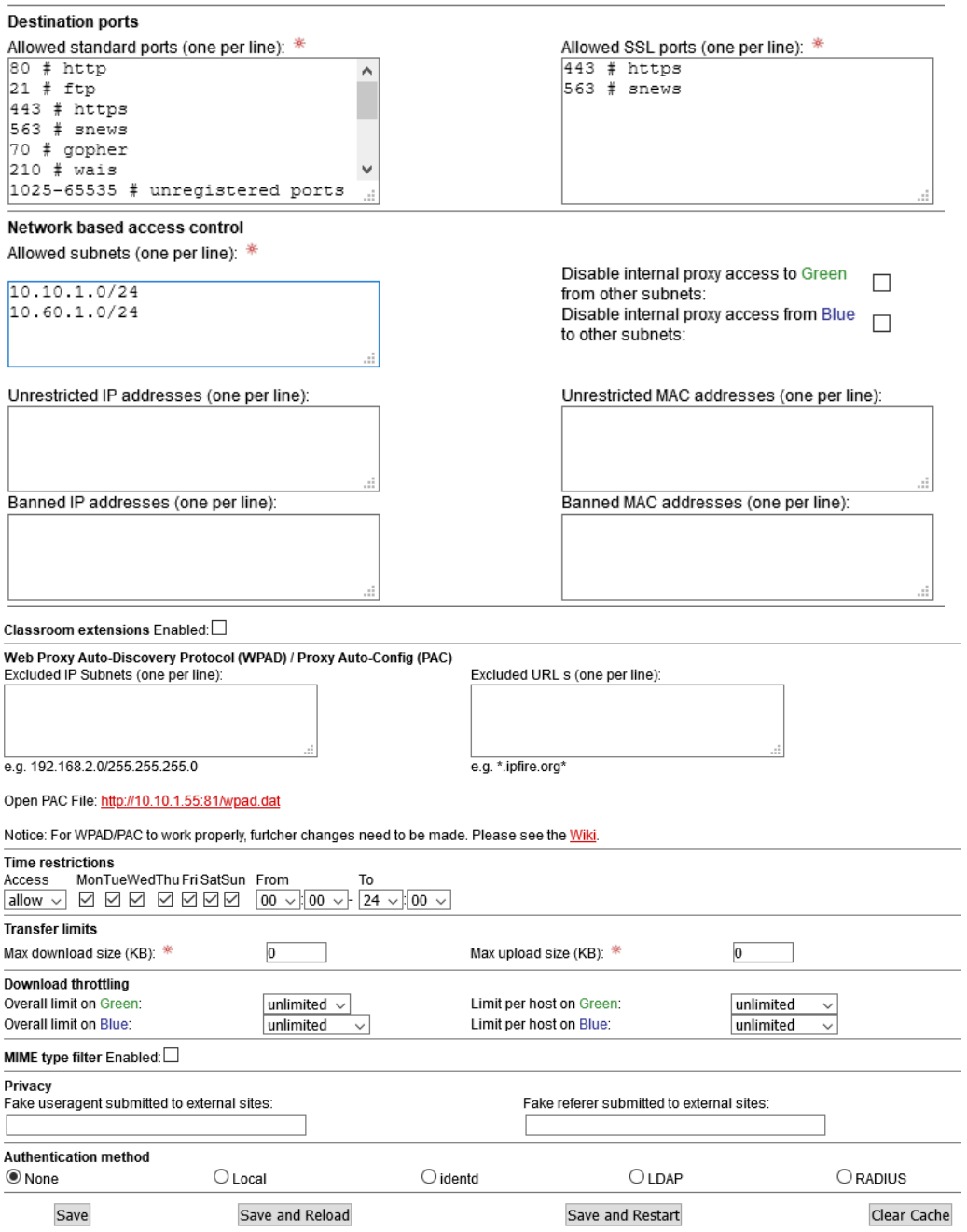
```
[root@VSF-IPFire ~]# nslookup slam.ecole.eni
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   slam.ecole.eni
Address: 10.10.1.51

[root@VSF-IPFire ~]#
```

Étape 2 : Fonction PROXY

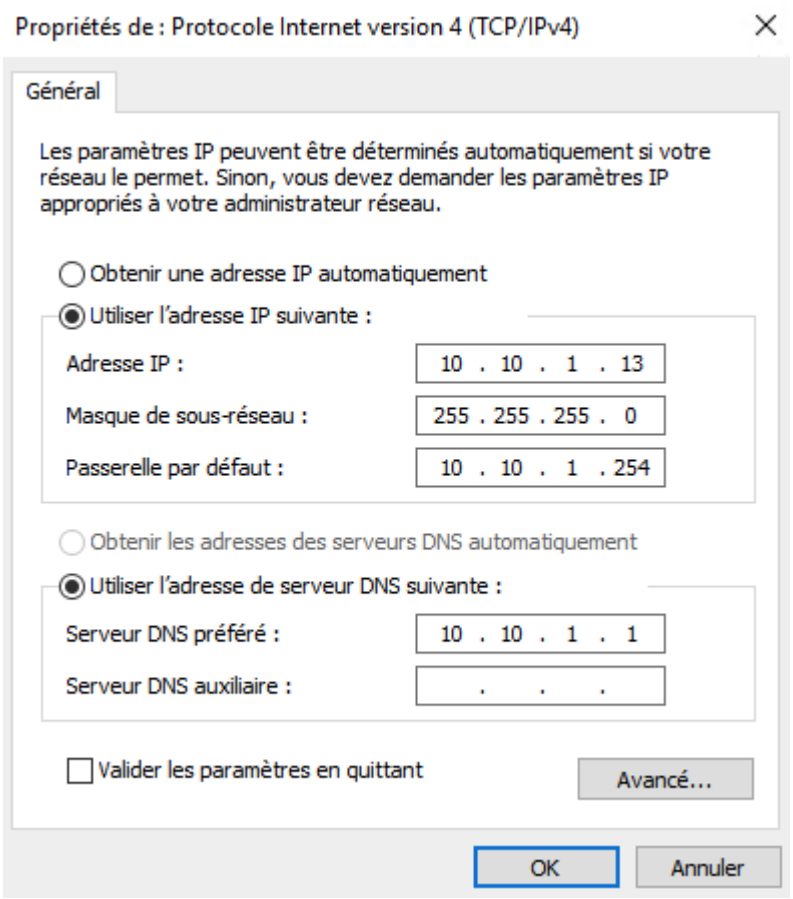
Une fois IPFire dans le domaine et donc les zones directes et indirectes de la zone DNS, le proxy web sans authentification AD/LDAP peut être configuré dans Réseau/Webproxy.
Dans Paramètres communs, cocher **Actif sur Green** et choisir le port 800.
Configurer le proxy avec les identifiants pour accéder à internet.


Advanced Web Proxy
Common settings
Enabled on Green:
Transparent on Green:
Enabled on Blue:
Transparent on Blue:
Suppress version information:
Squid cache version: [4.13]
Proxy port: 800
Transparent port: 3128
Visible hostname:
Error messages language: en
Error messages design: IPFire
URL filter
Enabled
Update accelerator
Enabled
Upstream proxy
Proxy address forwarding:
Client IP address forwarding:
Username forwarding:
No connection oriented authentication forwarding:
Upstream proxy (host:port): 172.17.0.1:3128
Upstream username:
Upstream password:

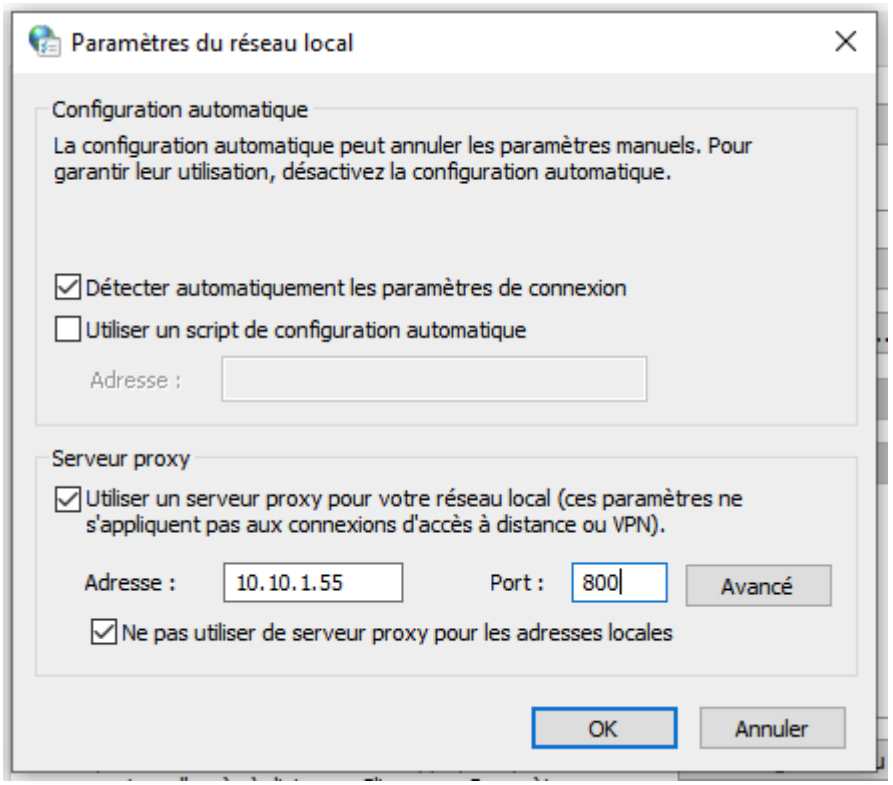
Gestion du cache
Activer le gestionnaire de cache:
Nombre de descripteurs de fichier: 16384
Taille cache mémoire (MB): 2
Volume d'objet minimal (KB): 0
Nombre de sous-dossier level-1: 16
Politique de remplacement de mémoire: LRU
Politique du Cache de remplacement: LRU
Autoriser mode hors connexion:
Enable Cache-Digest Generation:
Cache e-mail administrateur:
Mot de passe admnistrateur du Cache:
Taille du cache disque dur (MB): 50
Volume d'objet maximal (KB): 4096
Ne pas mettre en cache ces domaines (un par ligne):



Tester si un client du réseau LAN accède à internet (WAN) à travers IPFire. (Vérifier la configuration du proxy dans le navigateur du client).
Configuration client :



Configuration du proxy



Étape 3 : Configuration du filtrage URL

Définir les éléments à filtrer :

URL filter configuration

URL filter settings

Block categories

ads:	☐	aggressive:	☐	audio-video:	☐	drugs:	☐
gambling:	☐	hacking:	☐	mail:	☐	porn:	☐
proxy:	☐	violence:	☐	warez:	☐		

Custom blacklist

Blocked domains (one per line)
Example: www.domain.com

```
https://www.youtube.com/
```

Blocked URLs (one per line)
Example: www.domain.com/ads/

Enable custom blacklist: ☑

Custom whitelist

Allowed domains (one per line)
Example: www.domain.com

```
https://www.metz.fr
```

Allowed URLs (one per line)
Example: www.domain.com/ads/

Enable custom whitelist: ☑

Custom expression list

Blocked expressions (as regular expressions)

```
video
```

Enable custom expression list: ☑

File extension blocking

Block executable files: ☐
Block audio/video files: ☐
Block compressed archive files: ☐

Local file redirection

Enable local file redirection: ☐

Manage repository

Network based access control

Unfiltered IP addresses

```
10.10.1.55
```

Banned IP addresses

```
10.10.1.51
```

Time based access control

Set time constraints Set user quota

Block page settings

Redirect page template: legacy

Show category on block page:	☐	Redirect to this URL:	
Show URL on block page:	☐	Message line 1:	
Show IP on block page:	☐	Message line 2:	
Use "DNS error" to block URLs:	☐	Message line 3:	

Advanced settings

Enable expression lists: ☐ Enable log: ☐
Block "ads" with empty window: ☐ Log username: ☐
Block sites accessed by it's IP address: ☐ Split log by categories: ☐
Block all URLs not explicitly allowed: ☐ Allow custom whitelist for banned clients: ☐

* Required field

Save Save and Restart

URL filter maintenance

Blacklist update
The new blacklist will be automatically compiled to prebuilt databases. Depending on the size of the blacklist, this may take several minutes. Please wait for this task to be finished before restarting the URL filter.
To install an updated blacklist upload the .tar.gz file below:

Browse... No file selected. Upload blacklist

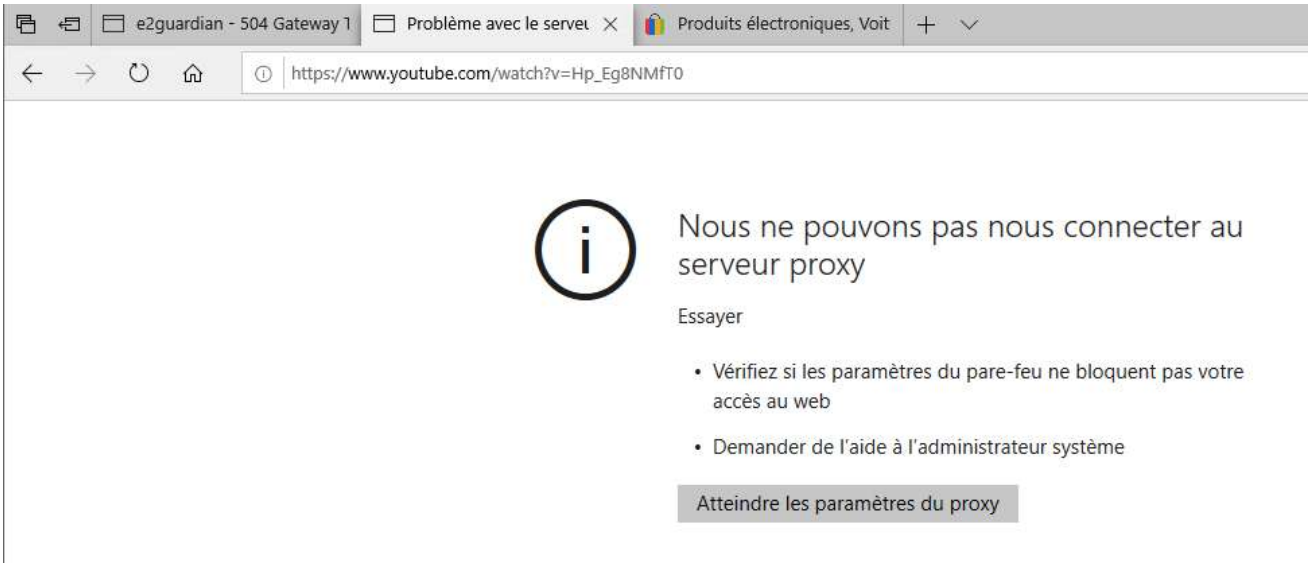
Automatic blacklist update
Enable automatic update: ☐
Automatic update schedule: monthly
Select download source: Shalla Secure Services
Custom source URL:
Save update settings Update now

Blacklist editor
Create and edit your own blacklist files
Blacklist editor

Backup URL filter settings
Include complete blacklist: ☐
Create backup file

Restore URL filter settings
To restore a previously saved configuration upload the .tar.gz backup file below:

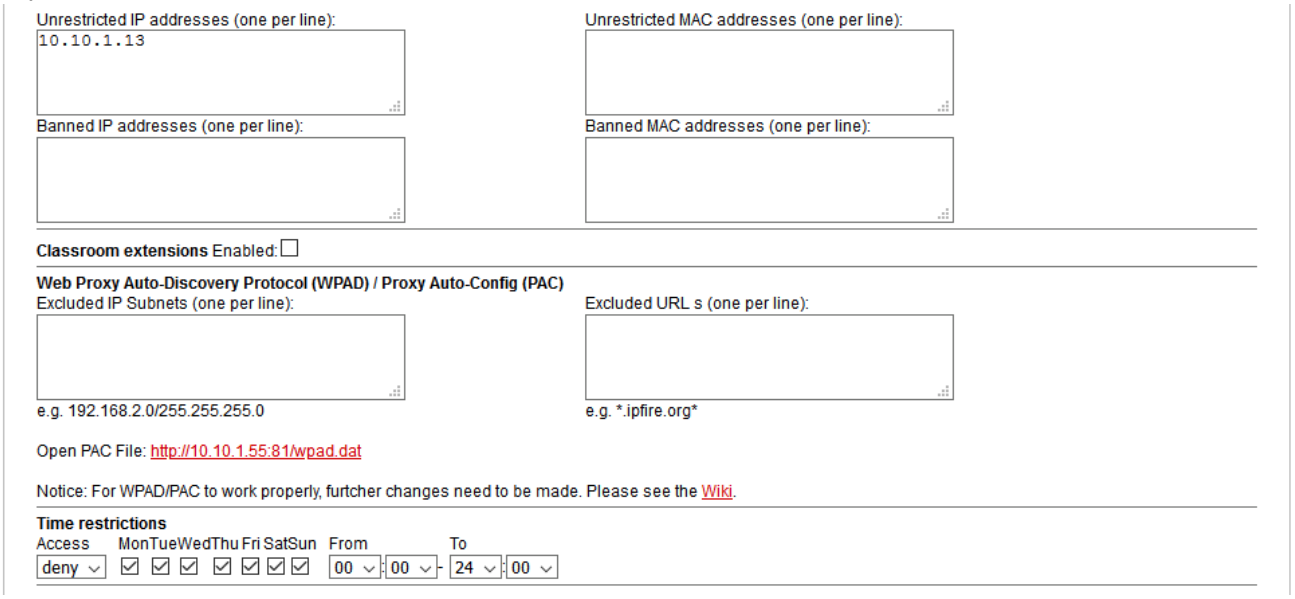
Valider le filtre et tester son application.



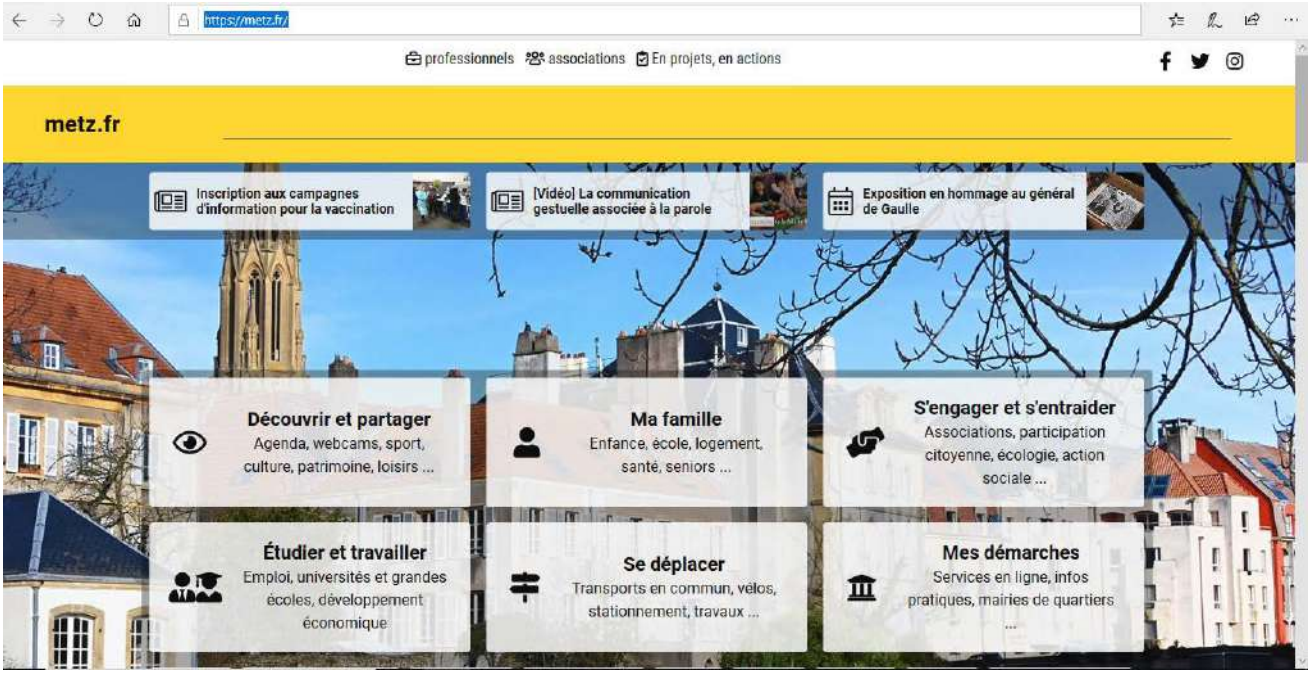
EXERCICE :

Filtrer ou interdire l'accès (totalement ou partiellement à des plages horaires) à des utilisateurs suivant leurs identification ou adresse IP ou adresse MAC.

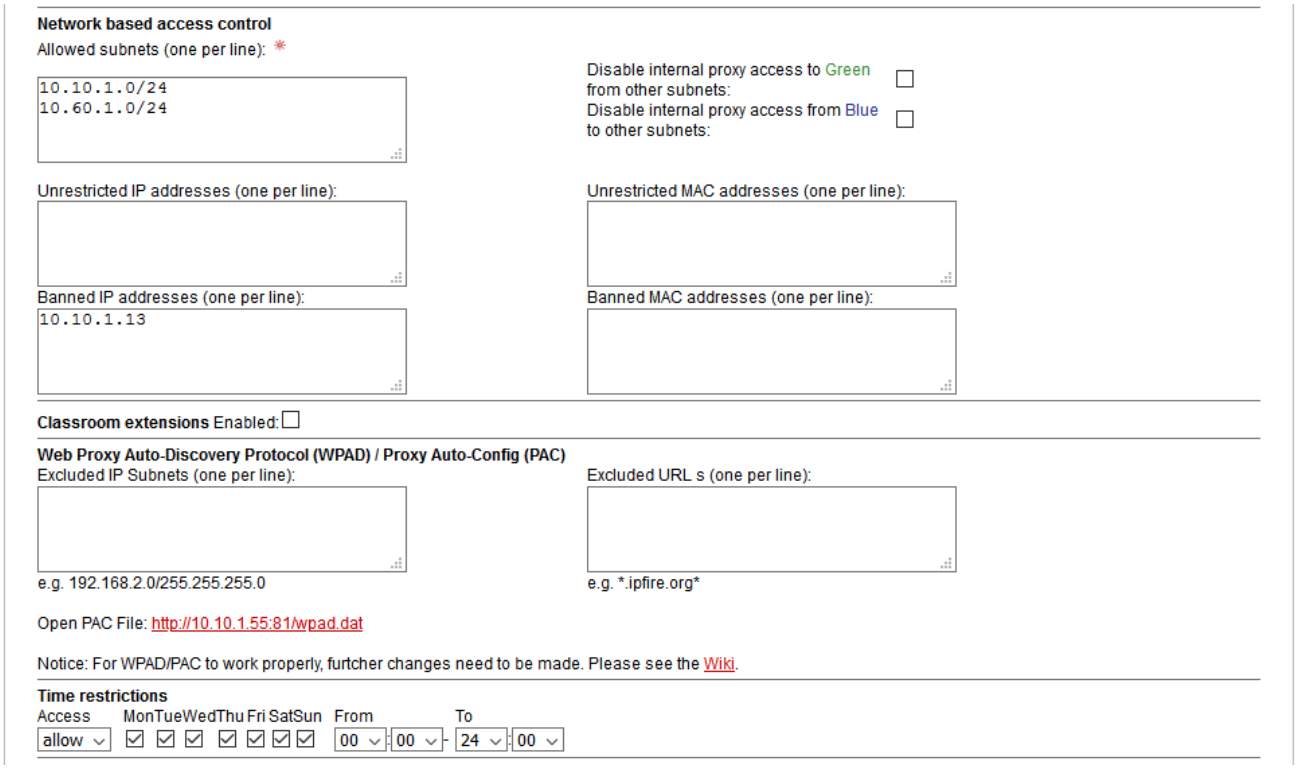
La procédure



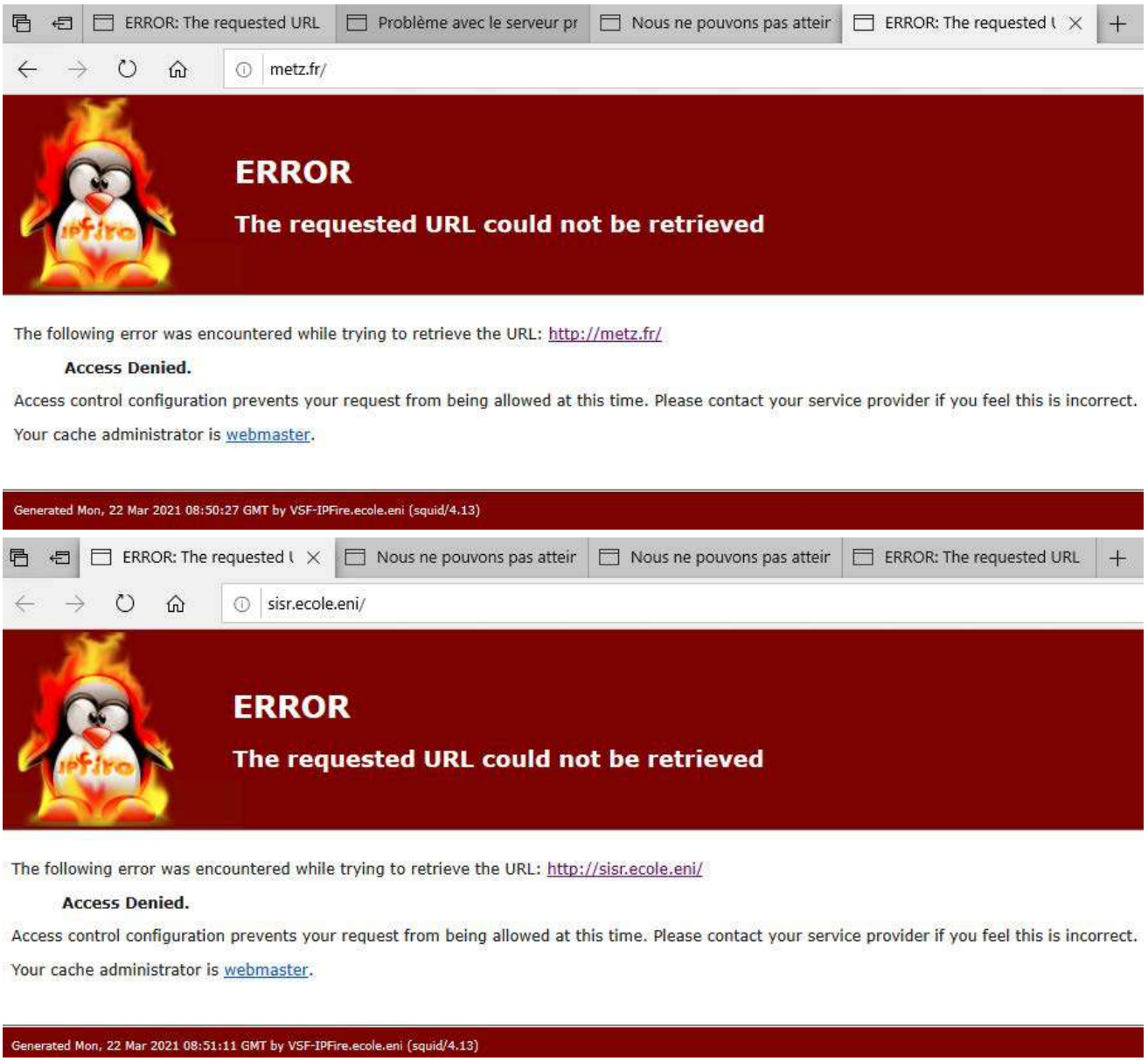
Le résultat:



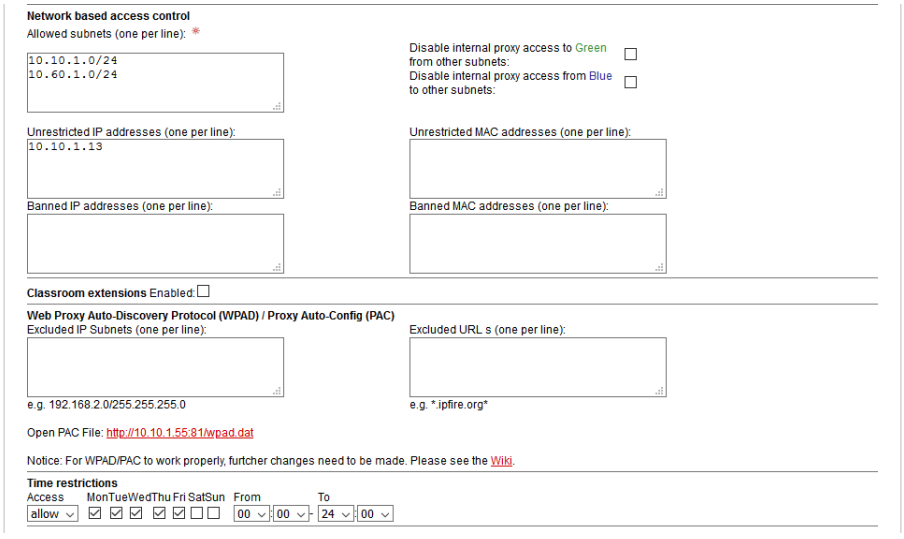
La procédure



Le résultat:

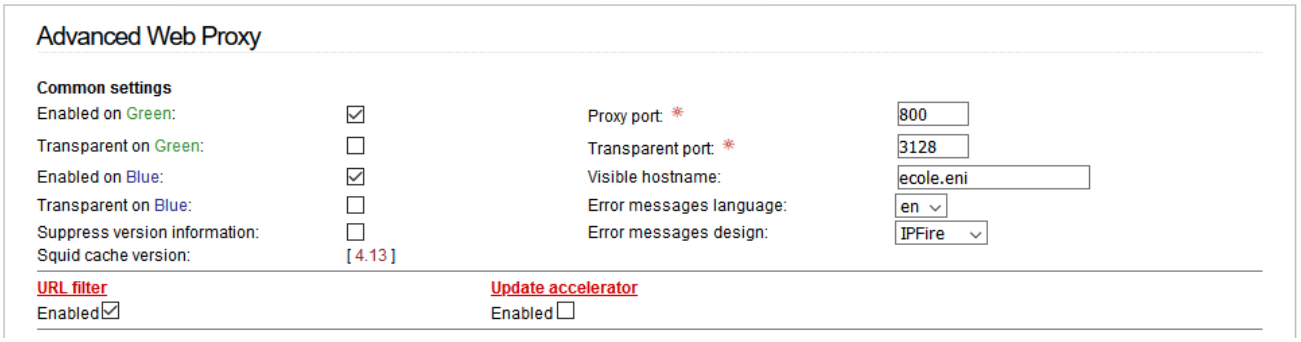


On a mit à la fin:

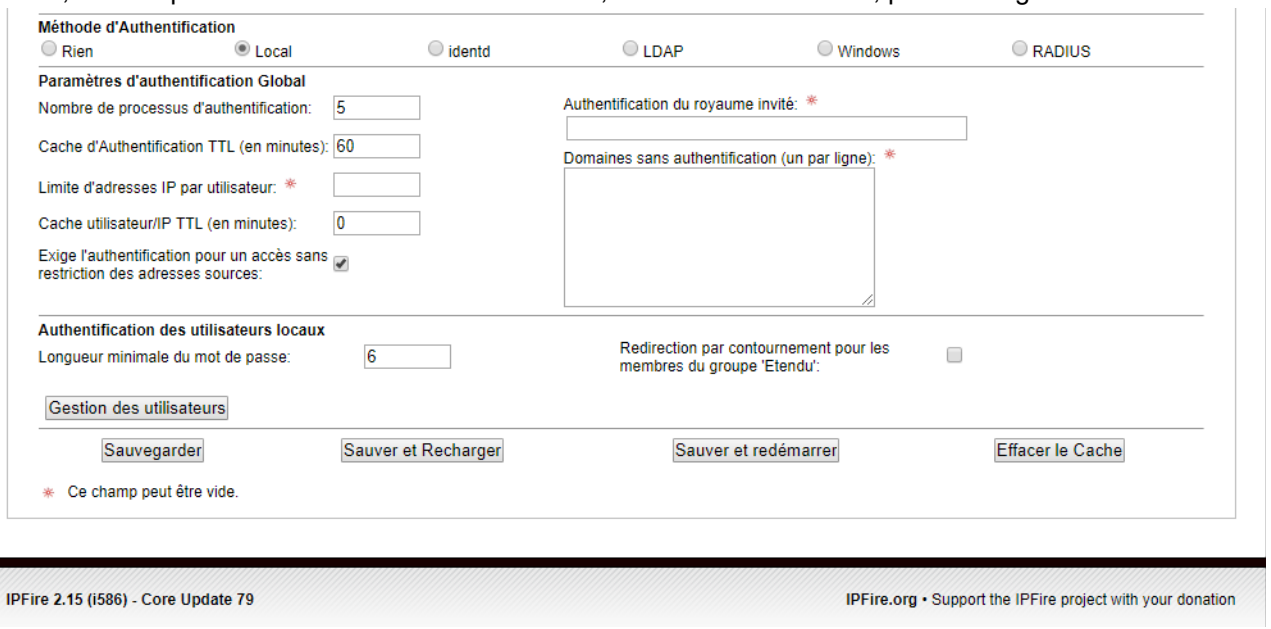


Étape 4 : Authentification Locale.

Pour mettre en place un proxy qui permet l'authentification des utilisateurs :
Il faut d'abord que la case « transparent » ne soit pas cochée :



Ensuite, dans la partie « Méthode d'authentification », il faut cocher « local », puis sauvegarder :



En local, il faut ajouter un utilisateur local :

Transfer limits

Max download size (KB): * 0 Max upload size (KB): * 0

Download throttling

Overall limit on Green: unlimited Limit per host on Green: unlimited
Overall limit on Blue: unlimited Limit per host on Blue: unlimited

MIME type filter Enabled: ☐

Privacy

Fake useragent submitted to external sites:

Fake referer submitted to external sites:

Authentication method

○ None ◉ Local ○ identd ○ LDAP ○ RADIUS

Global authentication settings

Number of authentication processes: 5
Authentication cache TTL (in minutes): 60
Limit of IP addresses per user:
User/IP cache TTL (in minutes): 0
Require authentication for unrestricted source addresses: ☑

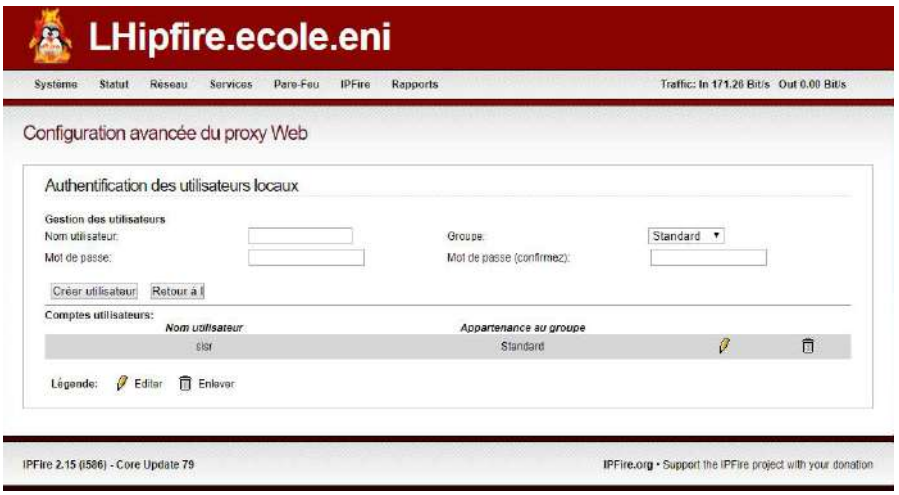
Authentication realm prompt:
Domains without authentication (one per line):

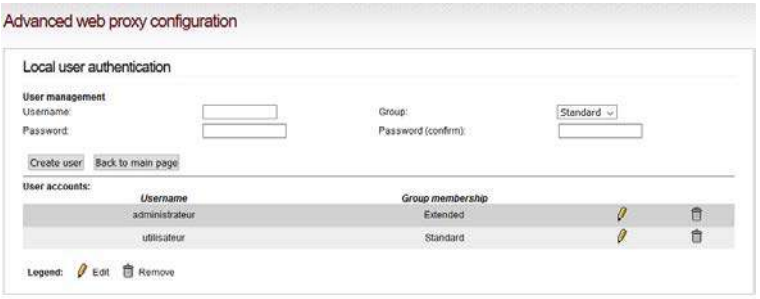
Local user authentication

Minimum password length: 6
Bypass redirection for members of the group 'Extended': ☐

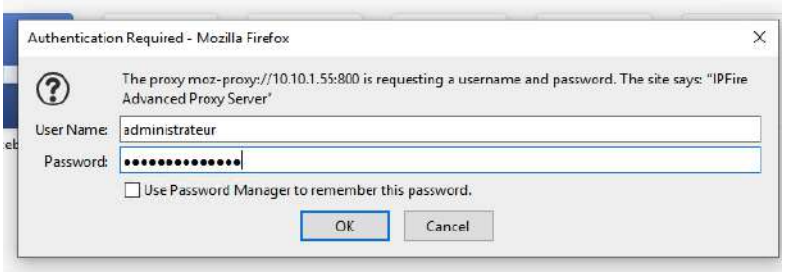
User management

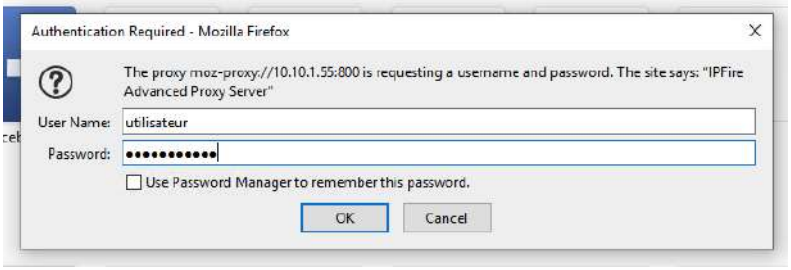
Save | Save and Reload | Save and Restart | Clear Cache





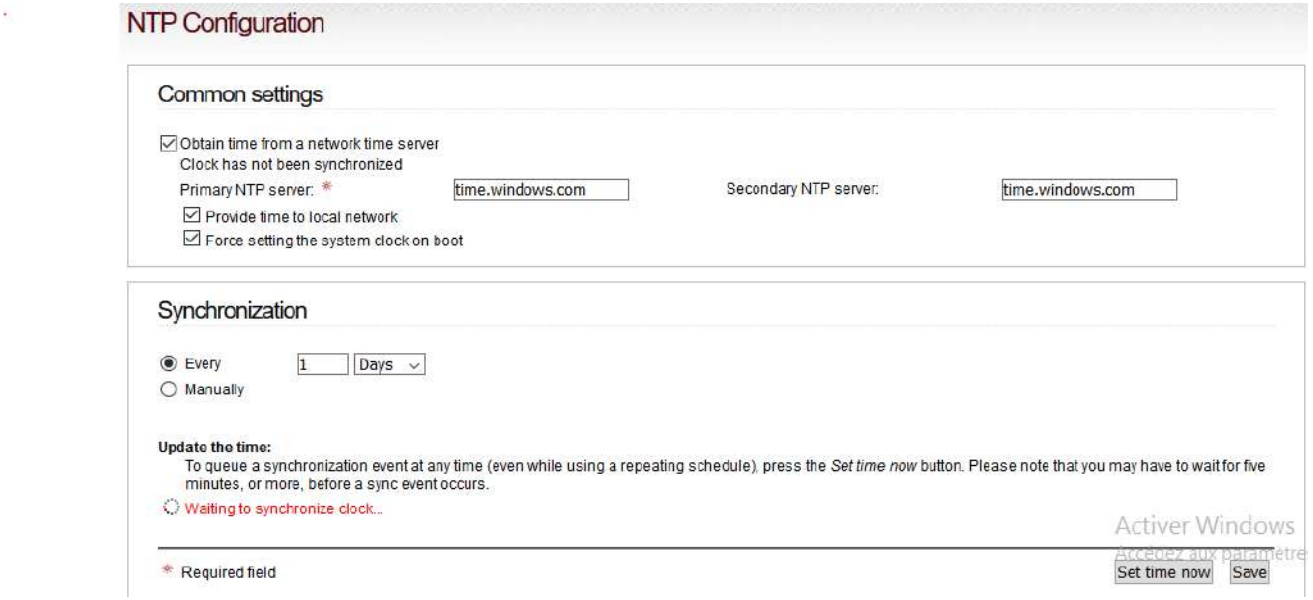
Cette fois-ci, il faut entrer le proxy dans le navigateur. Soit il faut le faire en local, soit il faut créer une GPO pour tous mes utilisateurs.
Tester l'authentification local d'un client.





Étape 5 : Méthode d'Authentification LDAP

Il reste à synchroniser l'heure de l'AD et d'IPFIRE :

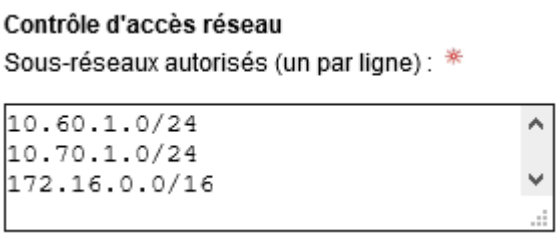


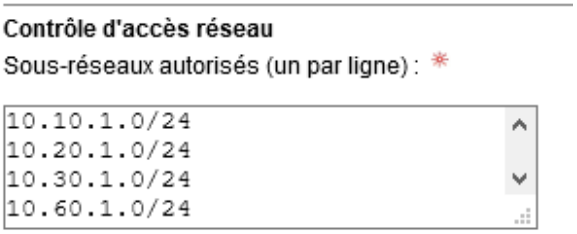
Test de connexion à internet du client à travers IPFIRE :

Étape 6 : Paramétrage des règles de connexion (routes statiques)

Il faut d'abord, pour que le réseau LOCAL puisse communiquer via IPFIRE. Pour cela, j'ai défini des routes statiques par VLAN, ayant pour passerelle le réseau 10 (celui des administrateurs). Dans « Réseau / Routes statiques » :

Dans « Réseau / Proxy Web » :





Sur les routeurs :

```
R12-CISCO1760(config)#ip route 10.60.1.0 255.255.255.0 10.10.1.76
R12-CISCO1760(config)#ip route 10.70.1.0 255.255.255.0 10.10.1.76
R12-CISCO1760(config)#ip route 172.17.0.0 255.255.0.0 10.10.1.76
R11-CISCO1760(config)#ip route 10.60.1.0 255.255.255.0 10.10.1.76
R11-CISCO1760(config)#ip route 10.70.1.0 255.255.255.0 10.10.1.76
R11-CISCO1760(config)#ip route 172.17.0.0 255.255.0.0 10.10.1.76
```

Résultat des tests ping d'un client du VLAN 10 à un autre du VLAN 60 :

```
C:\Users\SIO1>ping 10.60.1.176

Envoi d'une requête 'Ping'  10.60.1.176 avec 32 octets de données :
Réponse de 10.60.1.176 : octets=32 temps=2 ms TTL=127
Réponse de 10.60.1.176 : octets=32 temps=2 ms TTL=127
Réponse de 10.60.1.176 : octets=32 temps=1 ms TTL=127
Réponse de 10.60.1.176 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 10.60.1.176:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms
```

Résultat des tests ping d'un client du VLAN 10 à l'interface locale de l'IPFire (dans VLAN 10) :

```
C:\Users\SIO1>ping 10.10.1.76

Envoi d'une requête 'Ping'  10.10.1.76 avec 32 octets de données :
Réponse de 10.10.1.76 : octets=32 temps<1ms TTL=64
Réponse de 10.10.1.76 : octets=32 temps<1ms TTL=64
Réponse de 10.10.1.76 : octets=32 temps=1 ms TTL=64
Réponse de 10.10.1.76 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.10.1.76:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Résultat des tests ping d'un client du VLAN 10 à un autre du VLAN 70 :

```
C:\Users\SIO1>ping 10.70.1.176

Envoi d'une requête 'Ping'  10.70.1.176 avec 32 octets de données :
Réponse de 10.70.1.176 : octets=32 temps=2 ms TTL=127
Réponse de 10.70.1.176 : octets=32 temps=1 ms TTL=127
Réponse de 10.70.1.176 : octets=32 temps=1 ms TTL=127
Réponse de 10.70.1.176 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 10.70.1.176:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

Remarque : Sachant que le Proxy du lycée a des règles strictes (dû à une politique stricte du lycée), les pings ne marchent pas sur le réseau 172.17.0.0/16.

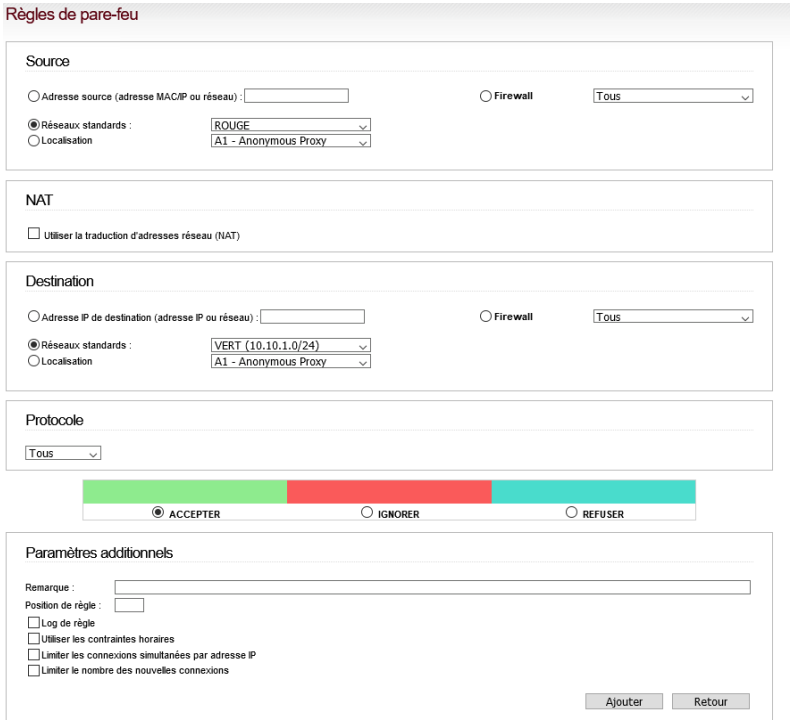
Étape 7 : Pare-feu

Pour établir les règles, j'ai procédé par une matrice des droits :

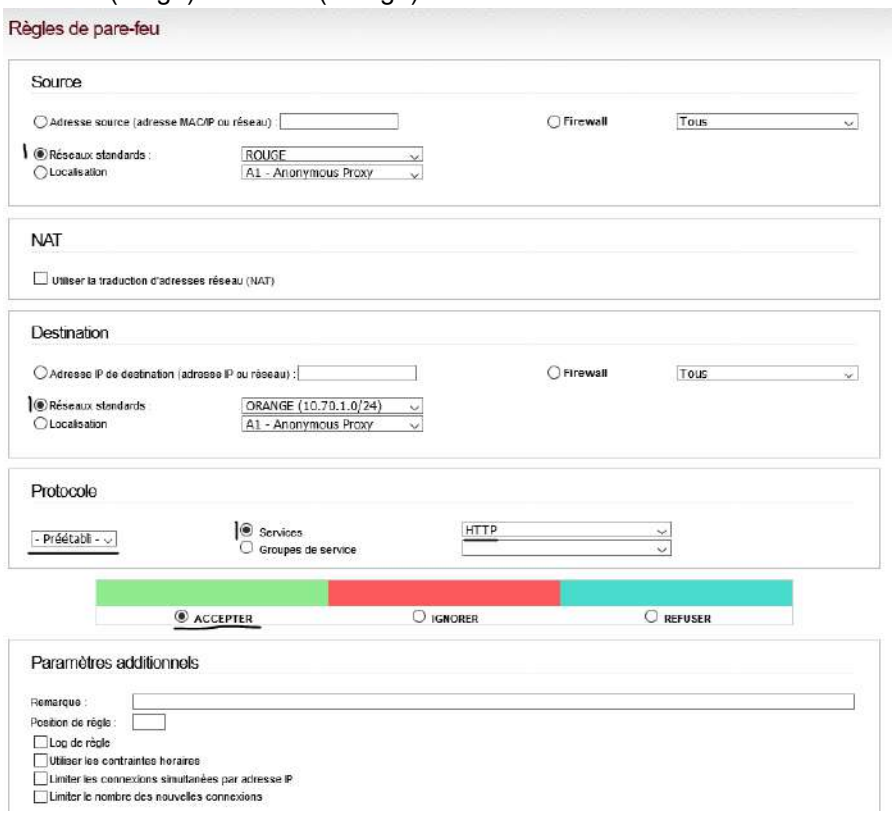
	RED	GREEN	ORANGE
RED		Autorisé	Autorisé NAT/PAT : 80
GREEN	Autorisé		Autorisé
ORANGE	Autorisé	Interdit	

1) J'ai, tout d'abord, mis en place les règles de filtrages, paramétrable dans "**Pare-feu / Règles de pare-feu**" :

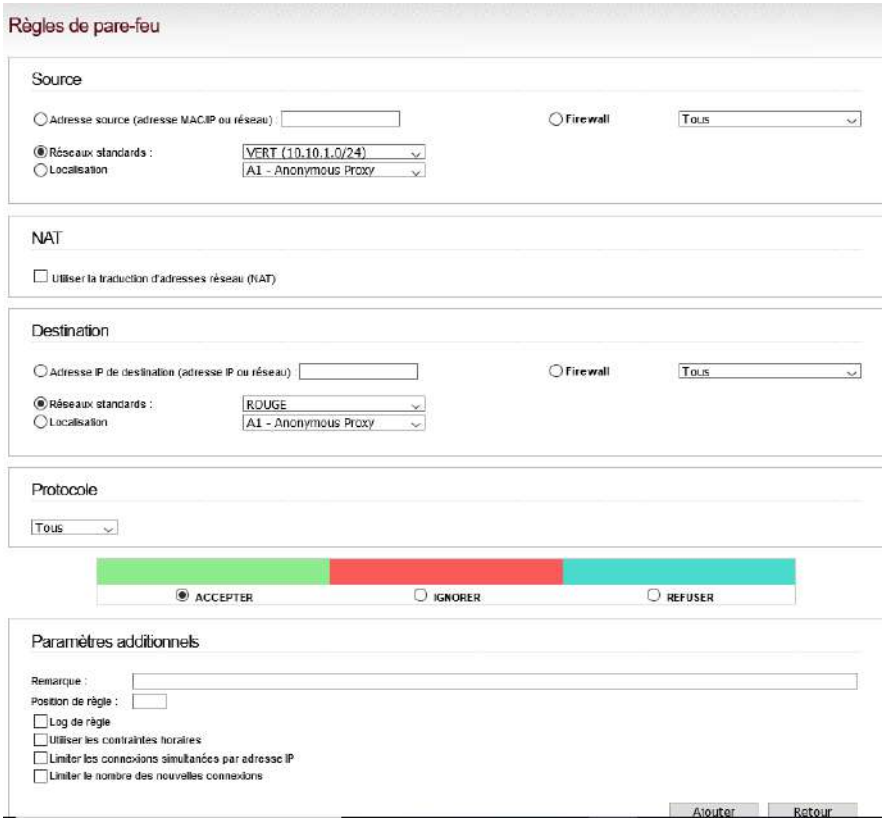
Du WAN (rouge) au LAN (vert) :



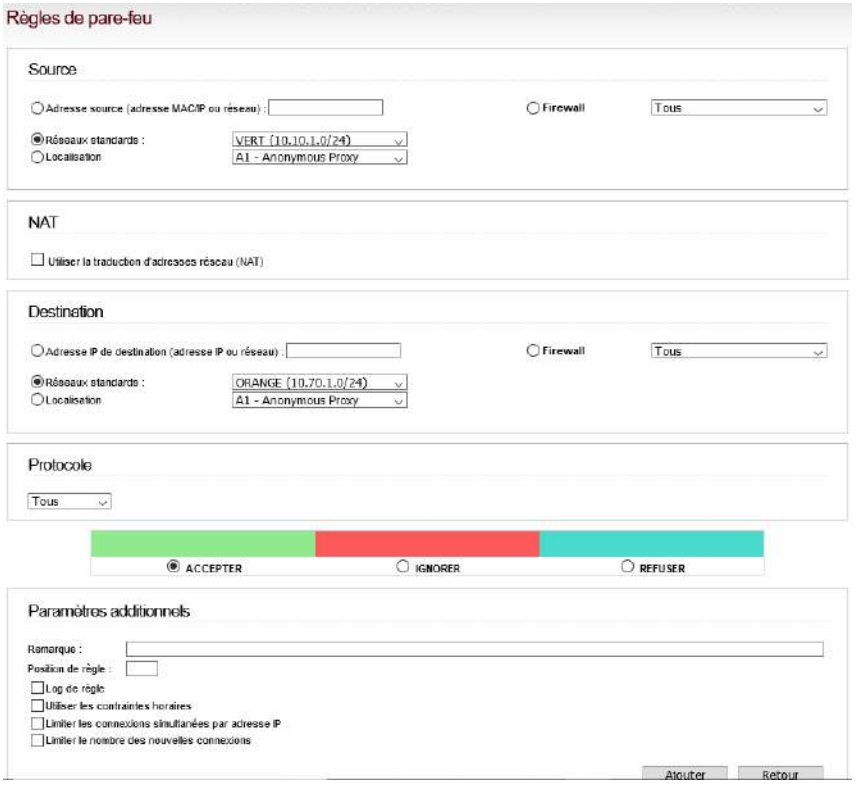
Du WAN (rouge) à la DMZ (orange) :



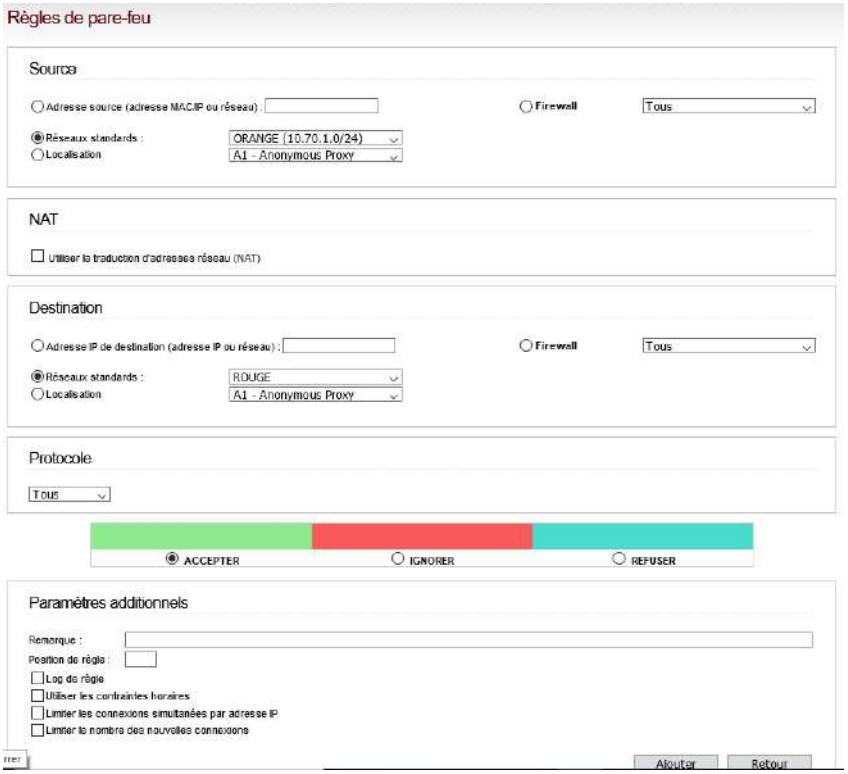
Du LAN (vert) au WAN (rouge) :



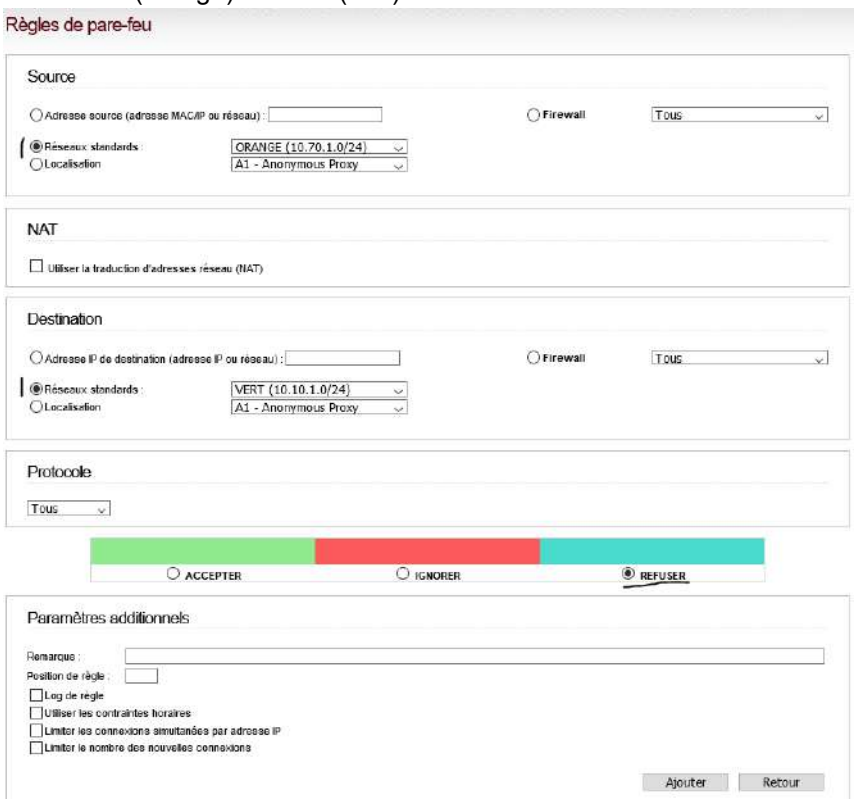
Du LAN (vert) à la DMZ (orange) :



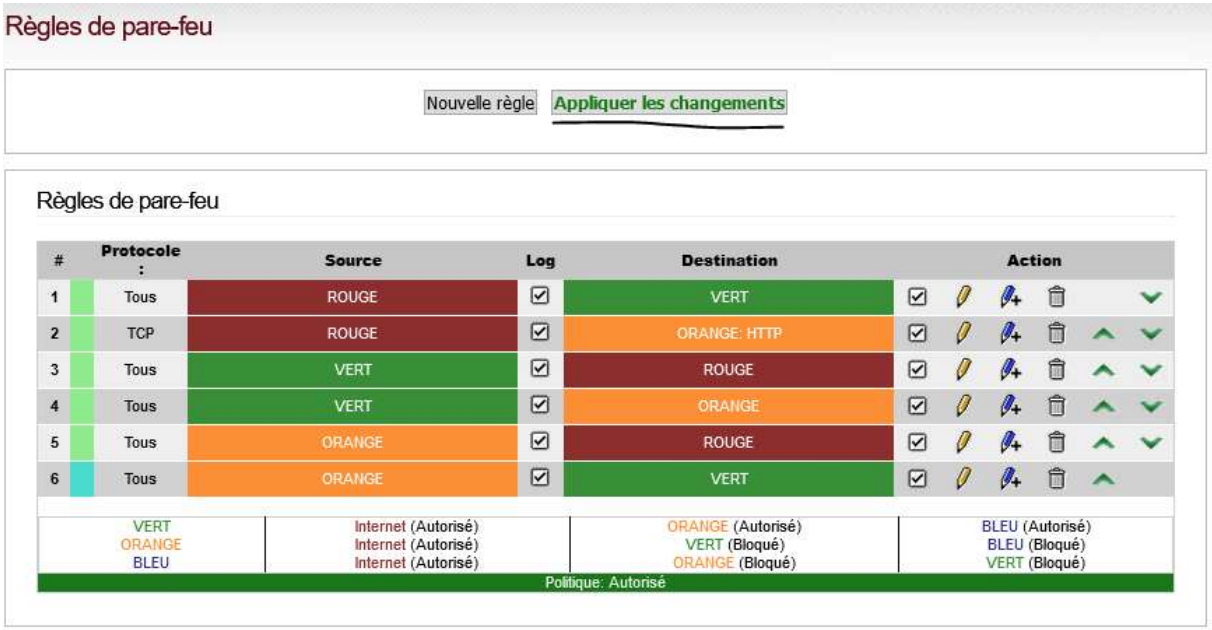
De la DMZ (orange) au WAN (rouge) :



De la DMZ (orange) au LAN (vert) :



Voici un résumé des règles de pare-feu appliquées :



2) Ensuite, j'ai vérifié les règles de connexions et de filtrage avec ***IPTABLES*** (dans "Pare-feu / Tables IP") :

Tables IP

Tables IP :

INPUT Mettre à jour

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
35181	22M	BADTCP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	CUSTOMINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	P2PBLOCK	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	GUARDIAN	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	OVPNBLOCK	all	--	tun+	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	IPS_INPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	IPTVINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	ICMPINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	LOOPBACK	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
72409	25M	CAPTIVE_PORTAL	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
72409	25M	CONNTRACK	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
524	43060	DHCPGREENINPUT	all	--	green0	*	0.0.0.0/0	0.0.0.0/0	
0	0	DHCPBLUEINPUT	all	--	blue0	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	LOCATIONBLOCK	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	IPSECINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	GUIINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	WIRELESSINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate NEW
53831	7361K	OVPNINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	TOR_INPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	INPUTFW	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53816	7360K	REDINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
51938	6736K	POLICYIN	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Table IP Mangle :

PREROUTING Mettre à jour

pkts	bytes	target	prot	opt	in	out	source	destination
392K	63M	NAT_DESTINATION	all	--	*	*	0.0.0.0/0	0.0.0.0/0

Traduction d'adresses réseaux table IP :

PREROUTING Mettre à jour

Chain PREROUTING (policy ACCEPT 15167 packets, 1726K bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
352K	40M	CUSTOMPREROUTING	all	--	*	*	0.0.0.0/0	0.0.0.0/0
352K	40M	CAPTIVE_PORTAL	all	--	*	*	0.0.0.0/0	0.0.0.0/0
352K	40M	SQUID	all	--	*	*	0.0.0.0/0	0.0.0.0/0
352K	40M	NAT_DESTINATION	all	--	*	*	0.0.0.0/0	0.0.0.0/0
352K	40M	UPNPFW	all	--	*	*	0.0.0.0/0	0.0.0.0/0

1. NAT / PAT

Définir un reverse-proxy.

Un **proxy** inverse (**reverse proxy**) est un type de serveur, habituellement placé en frontal de serveurs web. Contrairement au serveur **proxy** qui permet à un utilisateur d'accéder au réseau Internet, le **proxy** inverse permet à un utilisateur d'Internet d'accéder à des serveurs internes.

Exercice : Exonet Routeur NAT/PAT

L'entreprise SAGI externalisait ses serveurs HTTP, NNTP et SMTP pour l'Internet et l'extranet. Elle a décidé d'accueillir dans une zone démilitarisée ces serveurs. Ceci l'a conduit à revoir son architecture réseau et sa politique de sécurité.

Après avoir décidé dans un premier temps de créer une DMZ avec une adresse publique, l'administrateur décide d'utiliser aujourd'hui une adresse privée pour renforcer la sécurité.

Le routeur d'accès distant (R1) est un routeur filtrant, il permet d'interdire certains flux et en autoriser d'autres. Ce routeur prend aussi en charge la traduction d'adresses (NAT/PAT).

Les clients du réseau local ont un accès à Internet.

Vous trouverez en annexe 1 la structure schématique du nouveau réseau de l'entreprise.
Vous trouverez en annexe 2, des exemples de règles NAT/PAT appliquées par le routeur R1.
Vous trouverez en annexe 3 des exemples de règles de redirection appliquées par le routeur R1.

Première partie

1. Pourquoi le routeur R1 masque-t-il les adresses du réseau 192.168.50.0/24 ?

Le routeur masque les adresses du réseau 192.168.50.0/24 car il utilise le protocole NAT/PAT qui traduit des adresses IP privées en une adresse publique associé à un port pour chaque demande.

2. Expliquer le rôle des règles de l'annexe 3.

Ces règles permettent la communication des serveurs de la DMZ avec Internet, lors de demandes http sur l'adresse IP publique du routeur.

3. Le routage porte-t-il sur les adresses substituées ou sur les adresses réelles ?

Le routage porte sur les adresses substituées. (Traduction des adresses et ports par d'autres)

Deuxième partie

1. Pourquoi n'utilise-t-on pas le port standard 80 pour rediriger vers le serveur http partenaire de nom prive.sagi.fr ?

On n'utilise pas le port standard 80 pour rediriger vers le serveur HTTP partenaire de nom « prive.sagi.fr » car la communication n'est pas sécurisée. (Échanges non-cryptés par moyens de cryptage)

2. Comment les clients http des partenaires doivent-ils adresser leur requête pour accéder au serveur http partenaire prive.sagi.fr ?

Les clients HTTP des partenaires devraient adresser leur requête pour accéder au serveur HTTP partenaire « prive.sagi.fr » en utilisant un VPN et/ou un moyen de cryptage des échanges (TLS/SSL/cryptage asymétrique)

Troisième partie

L'administrateur décide d'appliquer une politique de sécurité plus restrictive. Il veut empêcher tout trafic entre l'Internet et l'Intranet. Pour cela, il va mettre en place un Proxy HTTP sur un serveur d'adresse 192.168.100.4 dans la DMZ qui écoutera sur le port 8080. Tous les utilisateurs devront passer par ce Proxy.

1. Comment fonctionne un Proxy-HTTP et quel est son intérêt ?

Un proxy est un dispositif informatique qui sert d'intermédiaire pour accéder à Internet (ou d'autres réseaux). De plus, il peut gérer le trafic venant de l'extérieur en l'autorisant ou l'interdisant selon la source du trafic, le type de trafic, la politique mise en place dans l'entreprise… mais aussi de l'intérieur en empêchant les fuites de données ou intrusions de logiciels malveillants.
Son intérêt est varié. Il peut permettre :

- L'accélération de l'affichage des pages web, grâce à son cache ;
- Bloquer l'accès à certains sites WEB ;
- Masquer son adresse IP ;
- Contourner la censure WEB…

2. Proposer une solution pour permettre aux postes de l'Intranet d'utiliser le Proxy-HTTP de façon transparente.

Pour permettre aux postes de l'Intranet d'utiliser le Proxy-HTTP de façon transparente, il faudrait :

- Régler l'option de serveur proxy sur son adresse IP (192.168.100.4) et un/des port(s) d'écoute ;
- Autoriser le trafic WEB entre le serveur Proxy http et les clients de l'Intranet en configurant des règles de filtrages sur le routeur ;
- Configurer une redirection de port entre l'interface du routeur ayant pour adresse IP publique 213.152.47.9 et le serveur Proxy.

3. Rédiger le(s) règle(s) permettant cette solution.

NAT/PAT

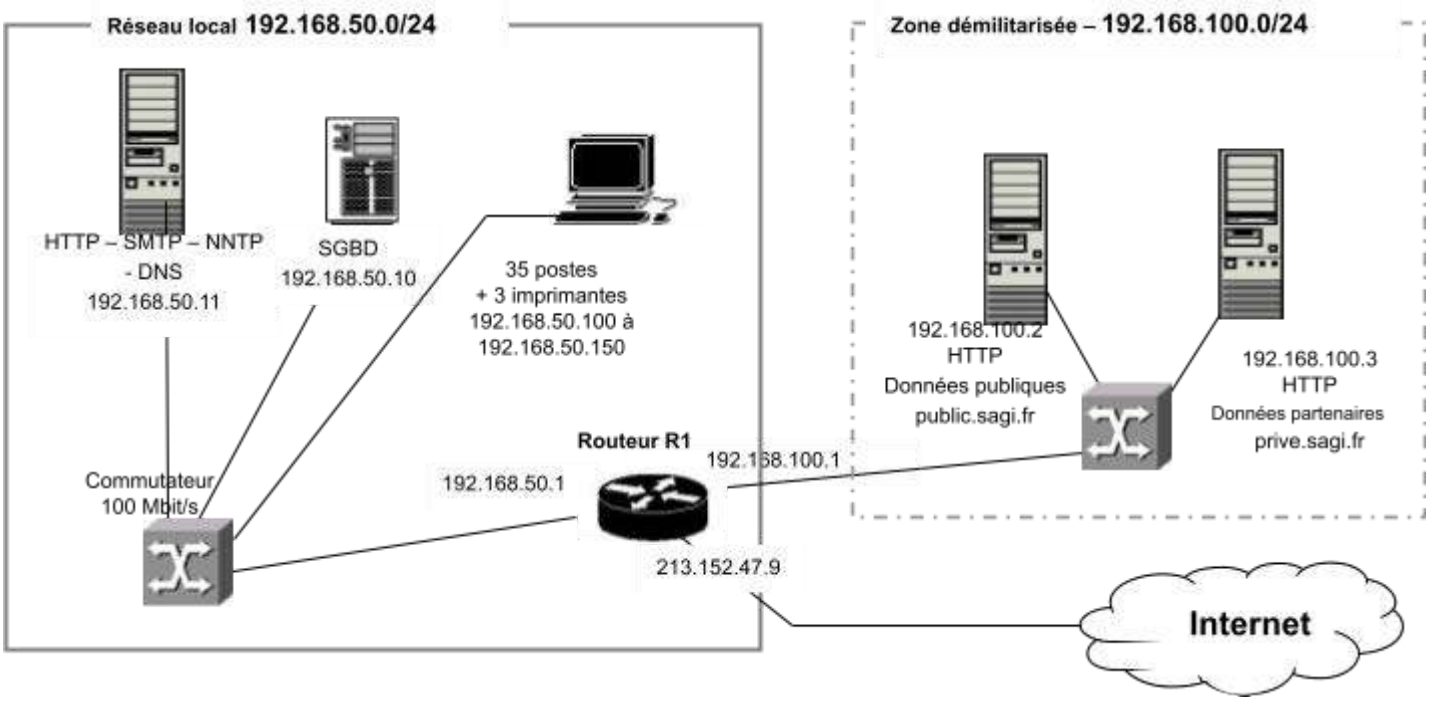
Numéro	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
1	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.100.0/24	*

Redirection de ports

Numéro	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
2	213.152.47.9	R	TCP	213.152.47.9	*	192.168.100.4/32	8080

Annexes

Annexe 1 : Structure schématique du réseau d'une entreprise



Annexe 2 : exemples de règles NAT/PAT

Le type NP (NAT/PAT) s'applique en sortie de l'interface et substitue l'adresse IP source et le port source privés par une adresse IP publique et un port public. Cette règle génère une entrée dans une table interne du routeur qui permettra de gérer la substitution inverse.

Numéro	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
1	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.50.0/24	*
2	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.100.0/24	*

Annexe 3 : exemples de règles de redirection

Le Type R (Redirection) s'applique en entrée de l'interface et substitue l'adresse IP destination et le port de destination publics par une adresse IP privée et un port privé. Cette règle génère une entrée dans une table interne du routeur qui permettra de gérer la substitution inverse.

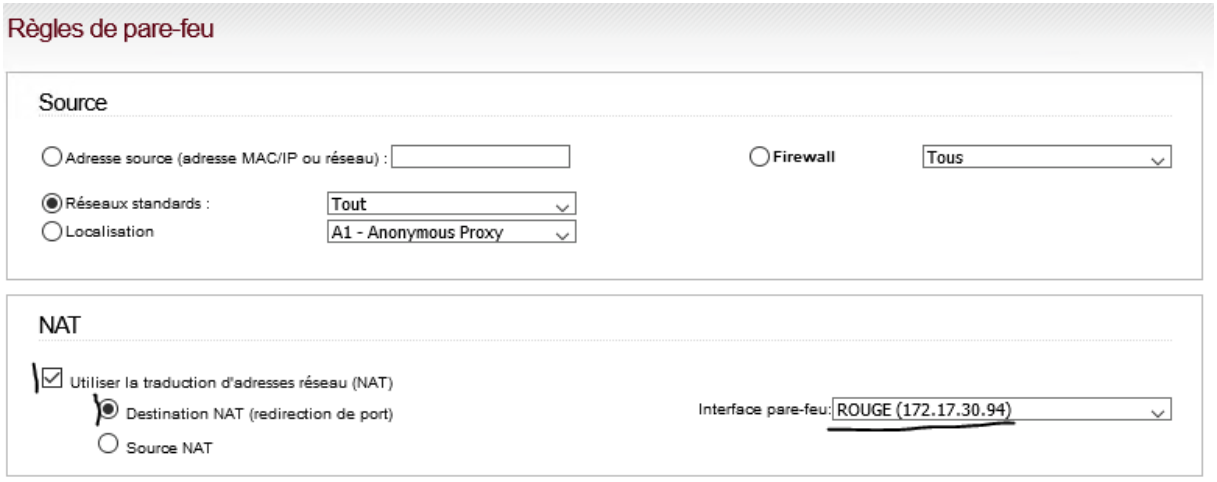
Numéro	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
3	213.152.47.9	R	TCP	213.152.47.9	80	192.168.100.2	80
4	213.152.47.9	R	TCP	213.152.47.9	4500	192.168.100.3	80

Le serveur HAProxy de la DMZ équilibre la charge entre les serveurs web qui constituent l'extranet.

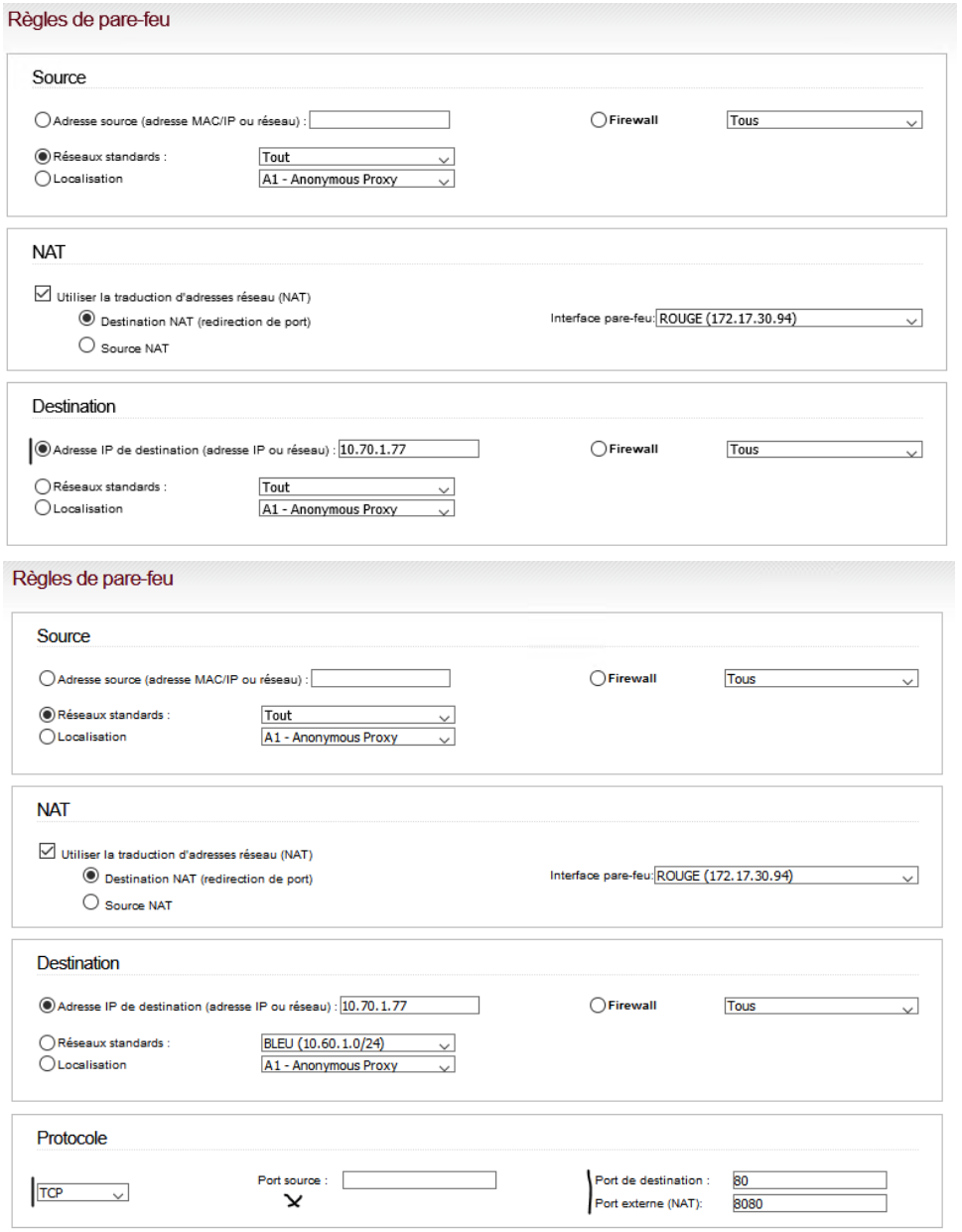
L'objectif est de rediriger les requêtes HTTP à destination de l'interface RED (**172.17.X.X donnée par DHCP**), GREEN et BLUE vers ***P14_SerwebTest*** **(qui sera changer par la suite par le serveur HAProxy et Serwebsecu1 et Serwebsecu2)** dans la DMZ (**10.70.1.77**).

1) Pour cela, j'ai été dans "Pare-Feu / Règles de pare-feu" et j'ai créé une nouvelle règle. J'ai mis l'option "**Réseaux standards : Tous**" comme source.

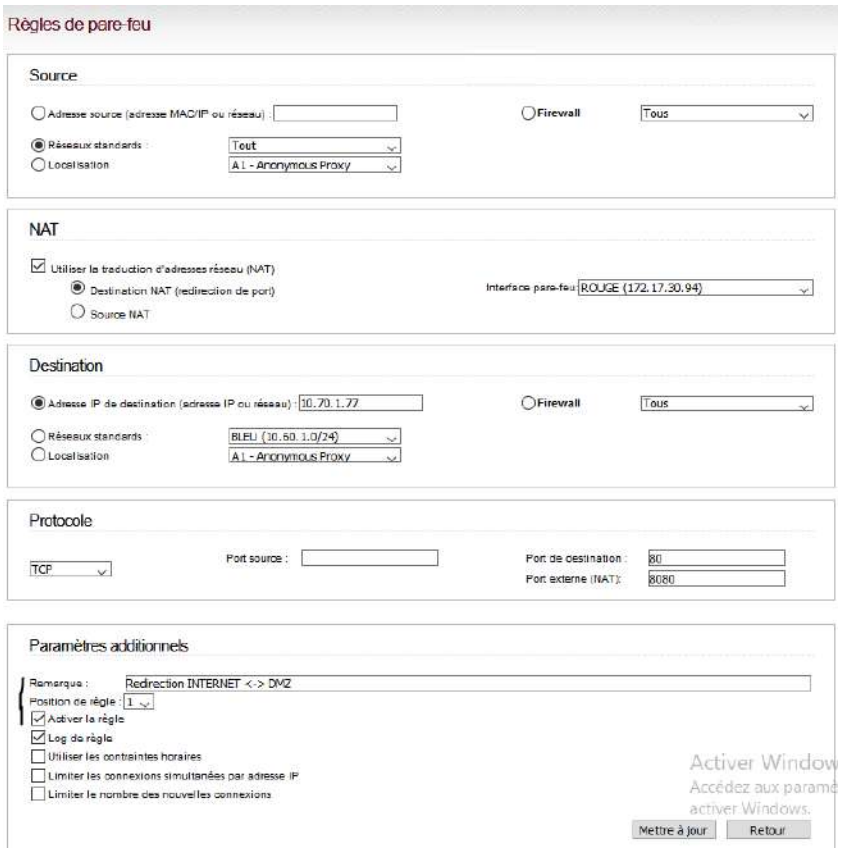
2) J'ai, ensuite, activé le NAT (en cochant la case) et j'ai sélectionné "**Destination NAT**" ,avec l'option "**Rouge**" comme "**Interface de pare-feu**".

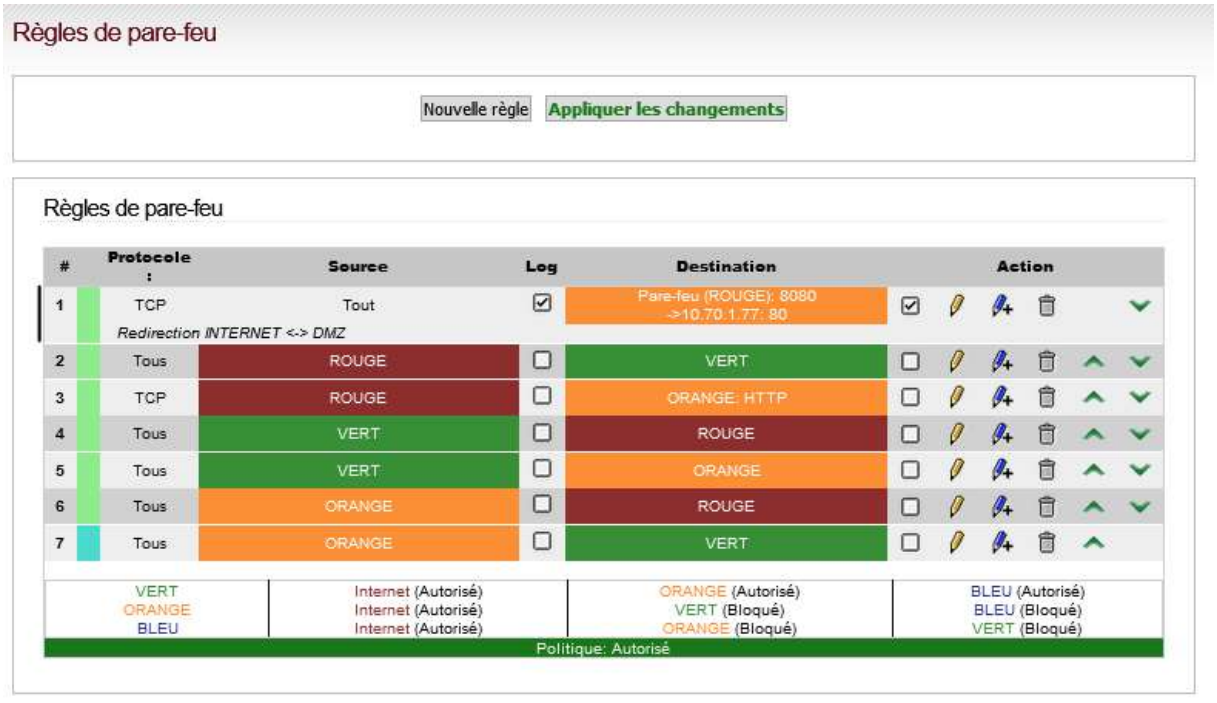


3) Dans la catégorie "**Destination**", j'ai saisi l'adresse IP **10.70.1.77** de protocole TCP avec 80 (HTTP) comme "**Port de destination**" et 8080 comme "**Port externe (NAT)**" qui est accessible par les membres en dehors de la DMZ (ici, en WAN, LAN et WIFI). Le port source correspond au port sur lequel le client veut te parler.

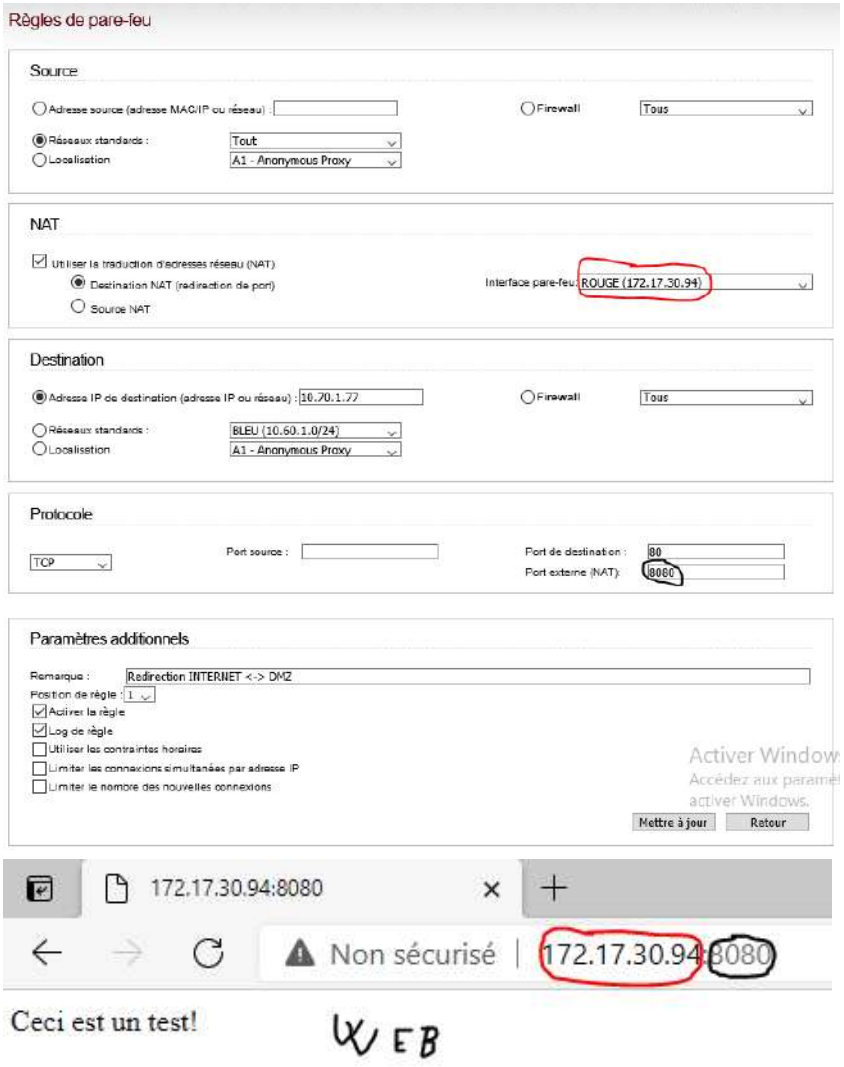


4) J'ai donné un nom à la règle et je l'ai placé en première position.





Après l'avoir ajouté comme exception, nous pouvons atteindre l'Extranet en attaquant l'adresse IP de l'interface RED (depuis n'importe quel réseau dans notre cas).



Remarque : Il ne faut pas oublier d'effacer l'historique des navigateurs WEB, entre les tests.

Partie 5 :	**VPN**

Étape 1 : Principe

Les applications et les systèmes distribués font de plus en plus partie intégrante du paysage d'un grand nombre d'entreprises. Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux.
Mais le succès de ces applications a fait aussi apparaître un de leur écueil. En effet si les applications distribuées deviennent le principal outil du système d'information de l'entreprise, comment assurer leur accès sécurisé au sein de structures parfois réparties sur de grandes distances géographiques ?
Afin d'assurer la confidentialité et l'intégrité des échanges, un VPN (Virtual Private Network) ou réseau privé virtuel met en place un système d'**authentification** et repose sur un **protocole d'encapsulation** (en anglais **tunneling**) permettant de sécuriser la transmission des données en les **chiffrant** (algorithmes de cryptographie).
Un système de Vpn doit pouvoir mettre en œuvre les fonctionnalités suivantes :

- **Authentification d'utilisateur**. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
- **Gestion d'adresses**. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.
- **Cryptage des données**. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- **Gestion de clés**. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- **Prise en charge multiprotocole**. La solution Vpn doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier Ip.

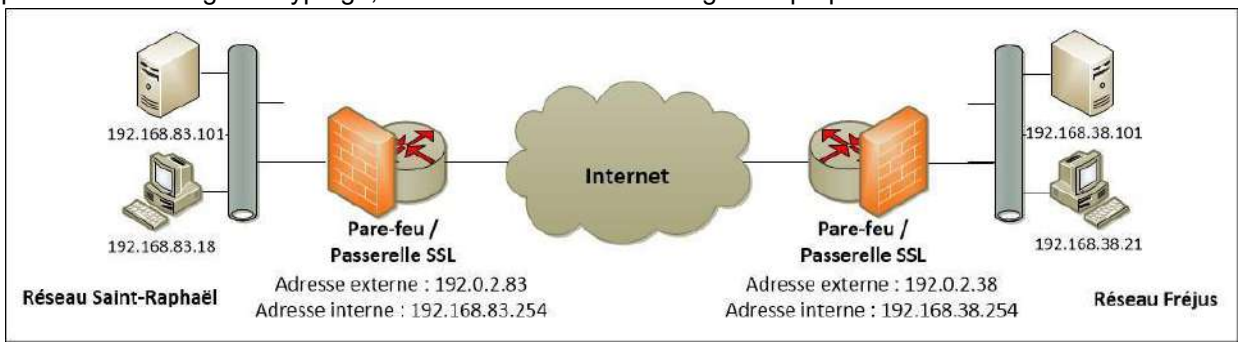
1 Typologie des VPN.

1.1 VPN d'entreprise

Dans ce cas, l'entreprise garde le contrôle de l'établissement des VPN.

VPN site à ite

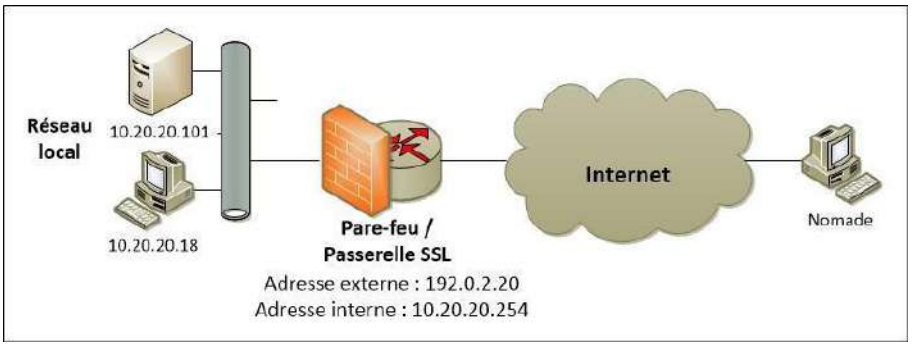
C'est un des cas les plus fréquents. Il s'agit de relier deux sites d'une même entreprise ou bien le site d'une entreprise et celui d'un fournisseur, d'un prestataire ou d'un client. Mais il faut également que tout ou partie des machines des deux réseaux puissent communiquer avec celles du réseau distant en utilisant les adresses privées de chaque réseau.
Généralement ce type de VPN est mis en place par l'interconnexion de deux éléments matériels (routeur/pare-feu) situés à la frontière entre le réseau interne et le réseau public de chaque site. Ces matériels prennent en charge le cryptage, l'authentification et le routage des paquets.



Cette solution n'assure aucune protection des données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux firewalls.

VPN poste à site

C'est également une utilisation très fréquente des VPN que celle consistant à permettre à des utilisateurs distants (nomades, travailleurs à domicile, commerciaux...) d'accéder aux ressources de l'entreprise via un VPN.



Pour construire cette solution, il faut sur le site central un matériel (firewall, routeur) constituant le point de terminaison de tous les VPN côté entreprise. Du côté des postes de travail distants, il faut un logiciel gérant le type de protocole choisi et compatible avec le matériel du site central.
Dans certains cas ce logiciel est déjà présent dans le système d'exploitation de ces postes. Dans d'autres cas, il est nécessaire d'installer ce composant logiciel.

- La protection est totale du poste distant au site central.
- Le cryptage impose une charge non négligeable au poste distant, ce qui peut en dégrader les performances.
- Les protocoles utilisés pour le VPN doivent pouvoir traverser le firewall du réseau sur lequel est branché le poste distant. En effet, à l'exception des VPN SSL, les tunnels sont généralement établis à l'aide de ports ou de protocoles différents des ports classiquement autorisés (80, 21, 443...) et ces ports spécifiques sont souvent interdits par l'administrateur réseau.
- Le cryptage n'est pas assuré au-delà du firewall du site central.

VPN poste à poste

Dans ce cas, l'objectif est d'établir un canal sécurisé de bout en bout entre deux postes ou, plus couramment, entre un poste et un serveur. Le poste et le serveur peuvent être situés sur le même réseau ou sur deux réseaux distants reliés eux-mêmes par un VPN site à site.
Ici n'interviennent que des composants logiciels : un logiciel client sur le poste "demandeur" et un logiciel utilisé en serveur sur le poste "destinataire".
Quand les postes se situent sur des réseaux locaux séparés par Internet, il est nécessaire que les deux extrémités puissent échanger leurs messages sur des protocoles et des ports qui doivent être autorisés par les firewalls situés sur chaque site. Cela nécessite également des translations d'adresses puisque les machines concernées sont rarement dotées d'adresses IP publiques.

1.2. VPN opérateur

Lorsqu'il s'agit d'interconnecter plusieurs sites d'une même entreprise avec des besoins de performances et de disponibilité, il est plus judicieux, mais aussi plus coûteux, de faire appel à un opérateur qui va donc mettre en place un réseau privatif entre tous les sites. Ce réseau tient plus d'un réseau de tunnels que d'un véritable réseau VPN.

2. Principaux protocoles.

2.1. Niveau 2

Ces VPN encapsulent les données dans des trames et ce sont ces trames que va véhiculer le tunnel dans une communication point à point. Nous sommes ici au niveau 2 du modèle OSI. La plupart de ces protocoles sont progressivement délaissés au profit de protocoles plus souples comme peuvent l'être ceux des niveaux 3 à 7.

- **PPTP (Point to Point Tunneling Protocol)**

Ce protocole soutenu par Microsoft est très simple mais assez limité. Il est en fort déclin maintenant.

- **L2F (Layer 2 Forwarding)**

Cisco a développé ce protocole autour des années 1996. L'IETF en a fait un standard en 1998 avec la RFC 2341. Son fonctionnement est assez voisin de PPTP.

- **L2TP (Layer 2 Tunneling Protocol)**

Dérivé de PPTP et de L2F ce protocole est maintenant un des protocoles VPN implantés nativement sur les machines Windows, ce qui explique son succès.

2.2. Niveau 3 et +

IPsec

Ce protocole très populaire est un des plus robustes mais il est aussi un des plus complexes.

SSL/TLS

Ce protocole en plein essor est simple de mise en œuvre.

3. Mise en œuvre d'un VPN SSL.

3.1. Les types de VPN SSL/TLS

D'une façon générale, le VPN SSL est destiné principalement à interconnecter un poste à un site central. Il fonctionne donc essentiellement en mode client-serveur même s'il est parfois possible de trouver des VPN SSL site à site.
Il est classique de classer arbitrairement les VPN SSL dans trois grandes catégories :

- Le portail web pour accès à des sites web, utilisable avec un navigateur simple il est limité à des applications/sites accessibles en http ou https.
- Le portail applicatif qui permet, toujours à partir d'un navigateur, d'accéder à quelques types d'applications supplémentaires (ssh, rdp, ftp, telnet...).
- Le mode tunnel complet qui donne accès, sous réserve d'autorisation par les règles de filtrage, à la totalité d'un réseau local.

3.2. Mise en place d'un serveur OpenVPN (tunnel VPN complet).

OpenVPN est une solution qui se base sur SSL. Elle permet d'assurer l'authentification du client et du serveur ainsi que la sécurisation du canal de transmission.
OpenVPN s'utilise dans deux cas de figure :

- Le type **routed** pour mettre en relation des machines distantes par Internet (exploité dans ce projet).
- Le type **bridged** pour mettre en relation deux sous-réseaux différents.

4. Sites à visiter.

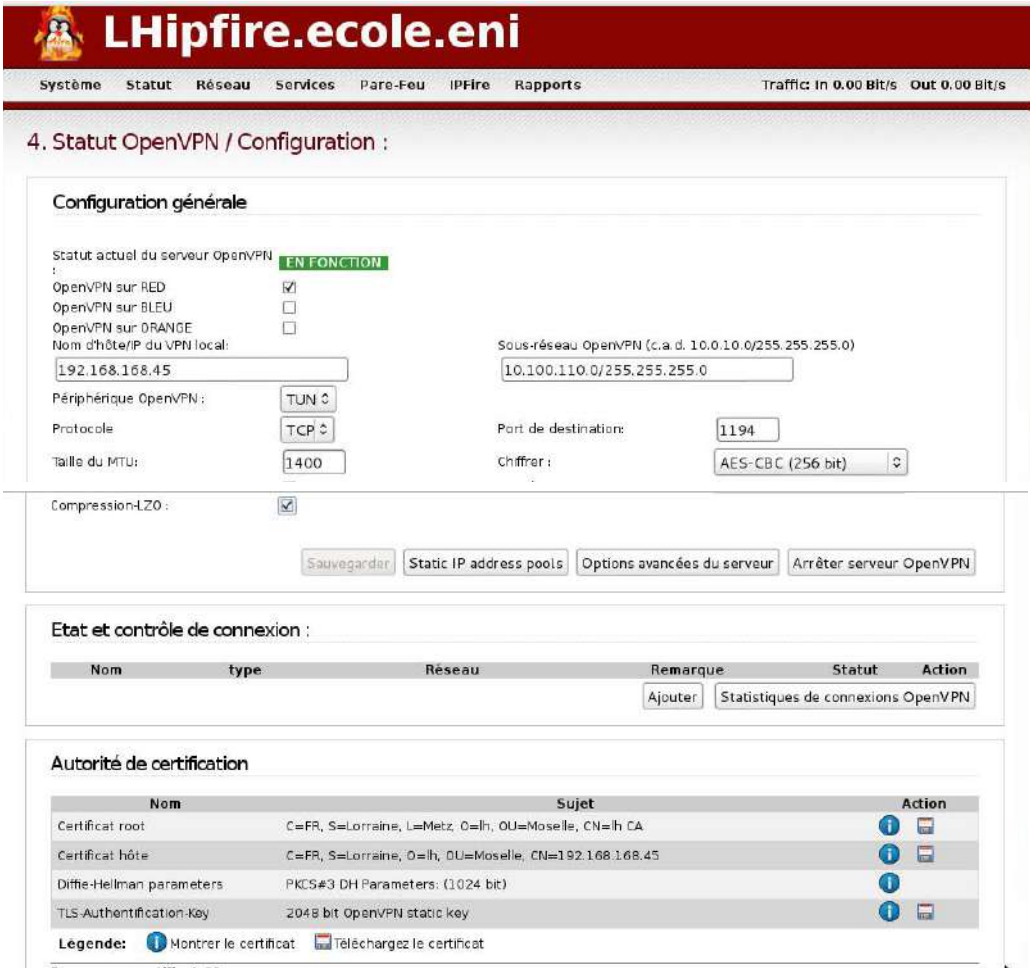
https://www.frameip.com/vpn/
http://www.openmaniak.com/openvpn.php

Étape 2 : Mise en place d'OPENVPN sur IPFIRE (serveur)

- Depuis l'interface Web : https://adresse IP:444
- Dans Services : OpenVPN,

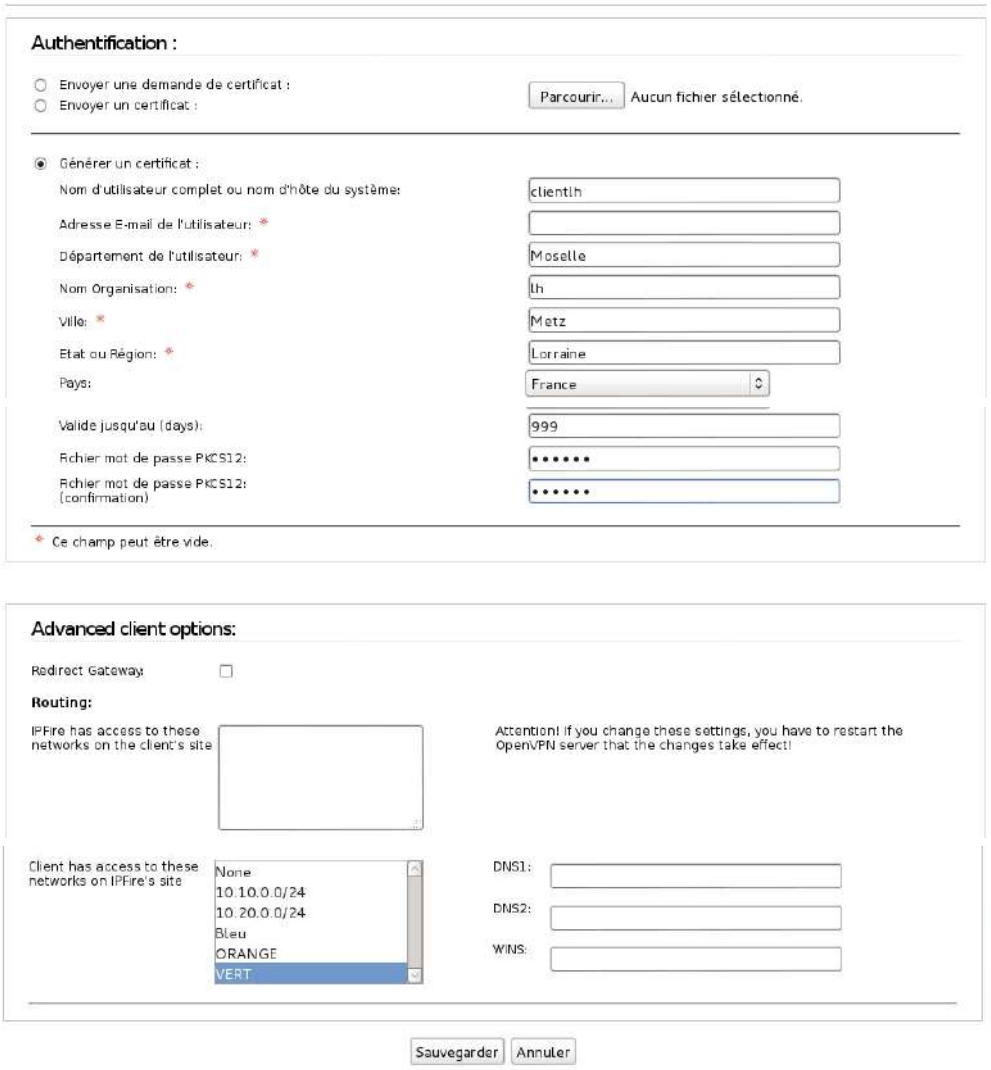
- Commencer par générer les certificats de Root/Hôte

Sauver et Complétez la fenêtre principale en cochant la case « OpenVPN sur RED », en cliquant « Compression LZO » puis terminez en cliquant le bouton « Démarrer le serveur OpenVPN » de manière à obtenir ceci :

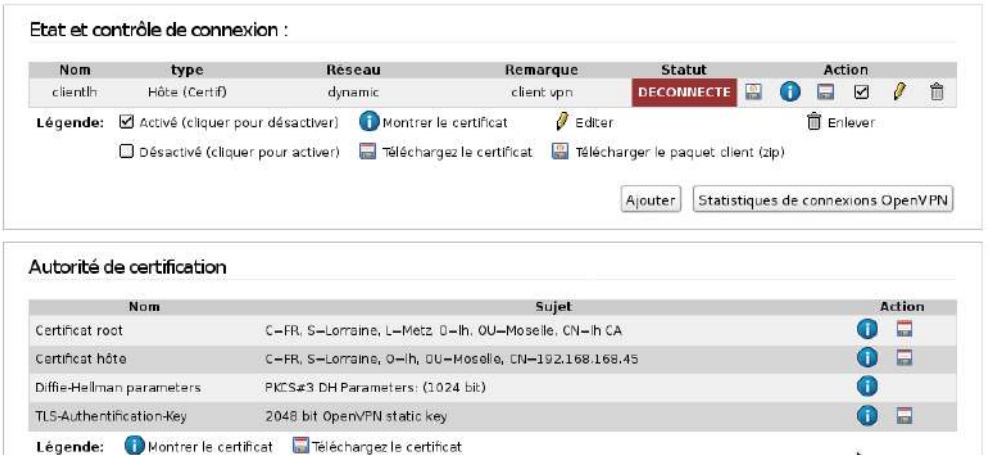


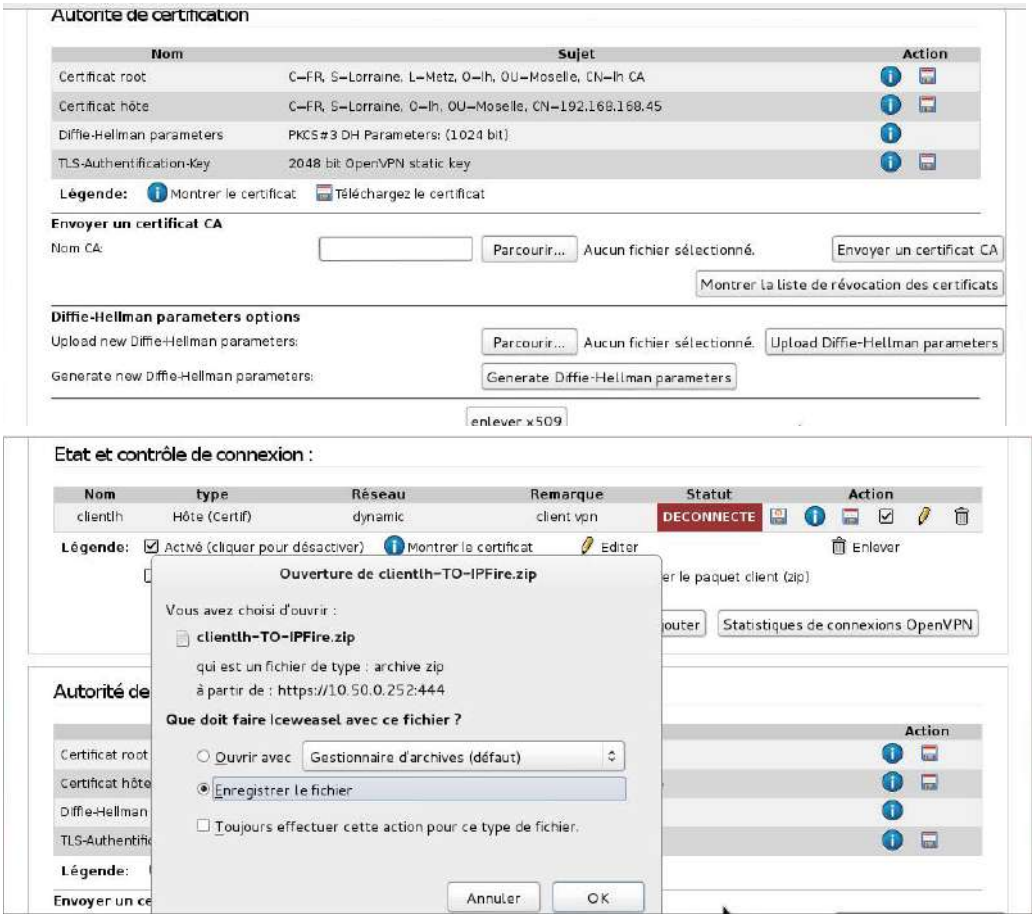
- Dans Etat et contrôle de connexion, créer des connexions clients en cliquant sur « Ajouter »

- Puis encore Ajouter
- Saisir le nom du client et générer le certificat

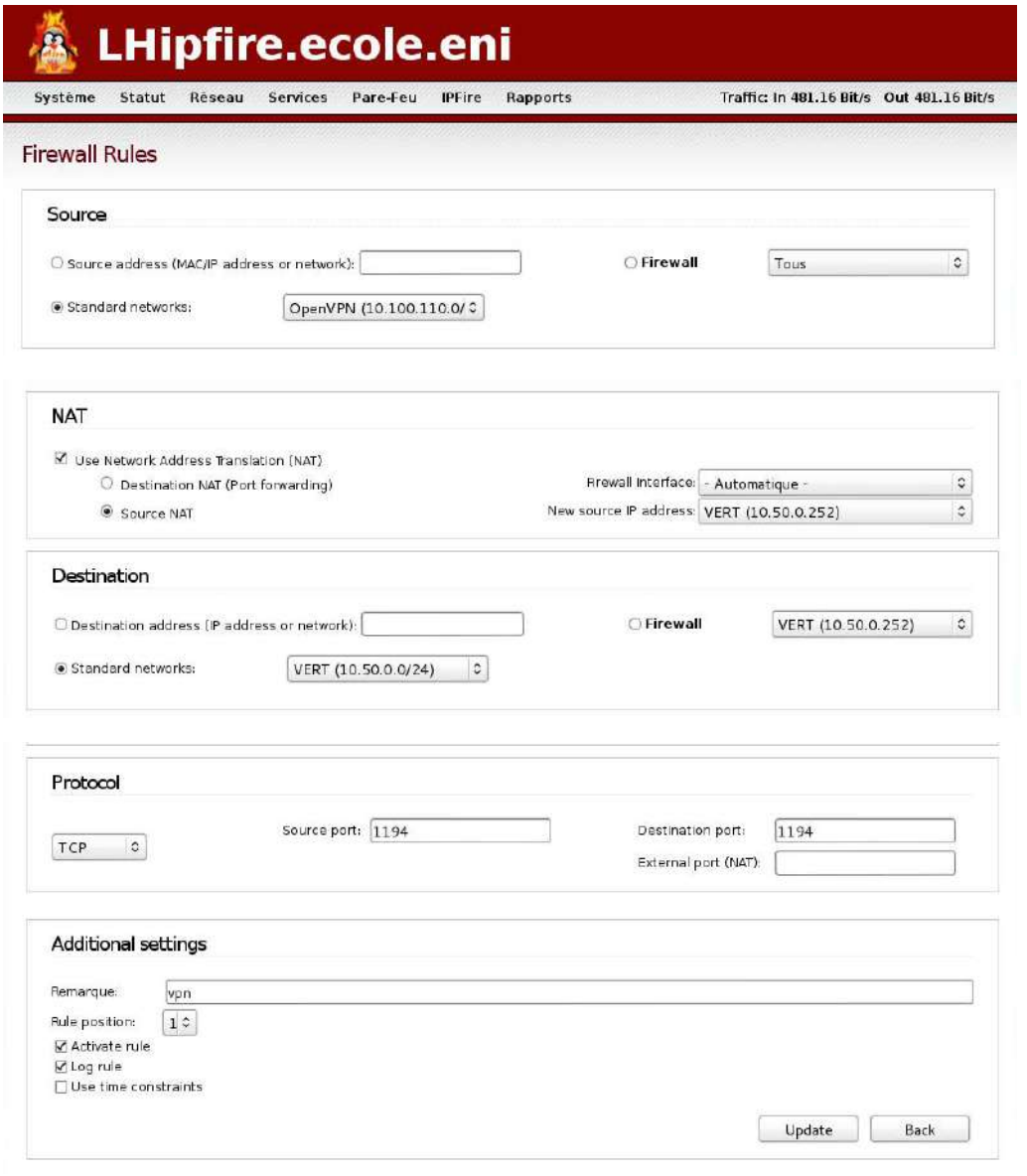


Sauvegarder et télécharger le certificat ET le **package pour le client** (un point zip a décompresser).





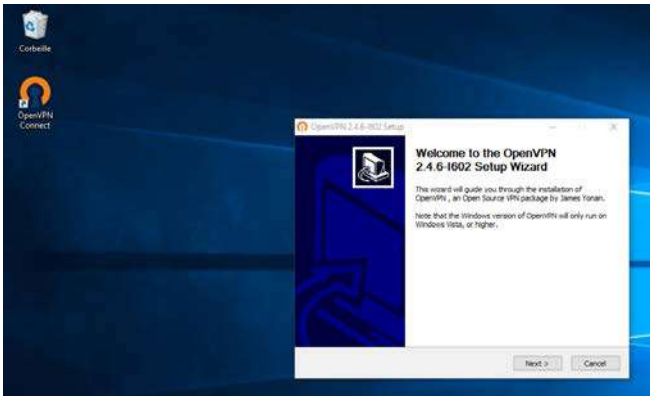
Ajout d'une règle dans le pare feu d'ipFire pour la connexion au VPN
Cliquez, dans le menu principal d'ipFire, sur « Pare feu » et « Firewall rules »
Cliquez sur « New rule »
Configurer la règle

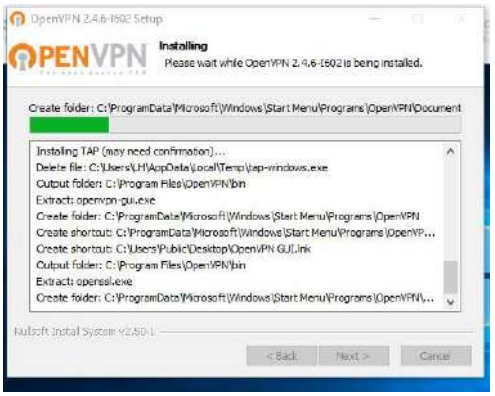


Étape 3 : Mise en place du client OpenVPN sous Windows.

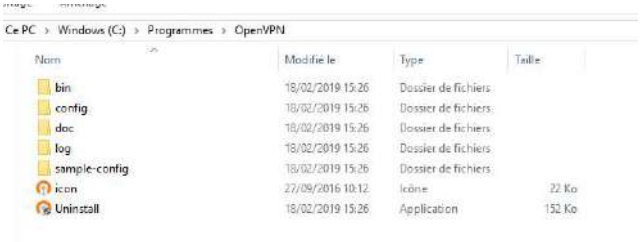
Télécharger OpenVPN

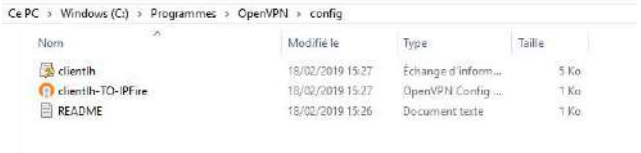
Installer openvpn



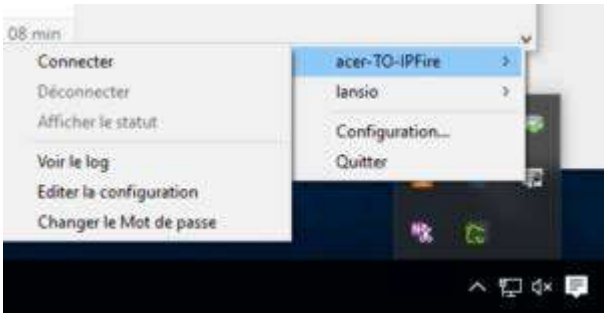


- Dans le répertoire Programmes, OpenVPN, config, mettez les fichiers du package





- Dans la zone des icônes en bas à droite de windows, vous aurez alors openVPn et via le bouton droit la possibilité de vous connecter



Puis via RDP, SSH ou HTTPS vous pouvez accéder aux hôtes sur réseau local interne.

Partie 6 :	**Haute disponibilité de pare-feu**

https://wiki.ipfire.org/addons/keepalived/start
https://docplayer.fr/5393879-Securisation-acces-reseau-internet.html

En utilisant VRRP à travers KeeAlived qui est paquet Adons d'IPFire on mettre en place une redondance et une haute disponibilité d'IPfire.

Expliquer le principe, l'installation et la configuration de KeepAlived sur les serveurs IPFire.

Partie 7 :	**IPSEC**

https://wiki.ipfire.org/configuration/services/ipsec

Expliquer le principe, l'installation et la configuration d'un VPN site à site avec IPSEC sur les serveurs IPFire.

Partie 8 :	**Sauvegarde, mise à jour et WIFI**

https://wiki.ipfire.org/configuration/system/backup
https://wiki.ipfire.org/addons/wireless/start