



06/10/2017

lpcop

Antoine BRULIN – Even MARIE



Labo 1

ANTOINE BRULIN – EVEN MARIE

Table des matières

○ Prérequis :	2
○ Paramétrage des cartes réseaux	3
○ Connexion à l'interface et installation du service Proxy	4
○ Mise en place d'un filtrage horaire	6
○ Mise en place d'une limitation de débit pour le téléchargement.....	7
○ Mise en place d'un filtre URL	8
○ Mise en place d'une liste noire	10
○ Mise en place d'un cache	12
○ Personnalisation de la page de refus	13
○ Paramétrage d'un poste administrateur sans restriction	14
○ Mise en place de quota de navigation	15

o Prérequis :

Nous commençons par l'installation de l'OS IPCOP :

```
ISOLINUX 2.08 2003-12-12 Copyright (C) 1994-2003 H. Peter Anvin

Welcome to IPCop, Licensed under GNU GPL version 2.

PLEASE BEWARE! This installation process will kill all
existing partitions on your PC or server. Please be aware
of this before continuing this installation.

-----
----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
----
-----

Press RETURN to boot IPCop default installation.

Or, if you are having trouble you can try these options...

Type:  nopcmcia to disable PCMCIA detection
       nousb to disable USB detection
       nousborpcmcia to disable both PCMCIA & USB detection

boot: _
```

IPCop v1.4.0 - The Bad Packets Stop Here

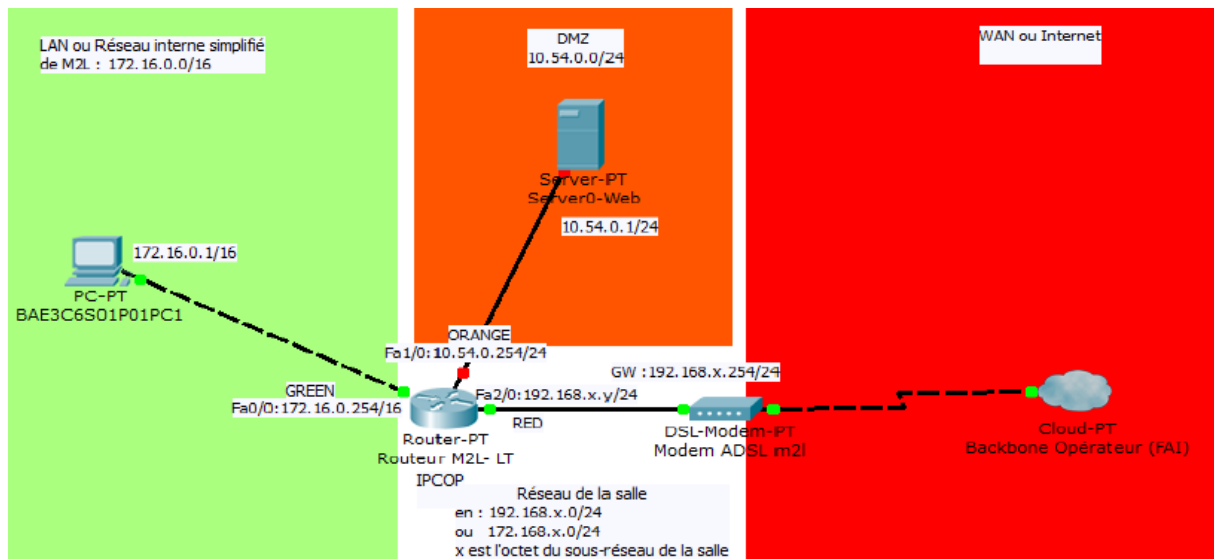
Félicitations!

IPCop a été installé avec succès. Veuillez retirer toute disquette ou CD-ROM de l'ordinateur. L'utilitaire de configuration va maintenant s'exécuter et vous permettre de configurer les cartes réseaux, le RNIS et les mots de passe système. Une fois la configuration terminée, vous pourrez utiliser votre navigateur sur <http://ipcop:81> ou <https://ipcop:445> (ou tout autre nom que vous aurez donné à votre IPCop), et configurer la connexion via modem (si requise) et l'accès externe. Pensez à fixer un mot de passe pour l'utilisateur 'dial' IPCop, si vous voulez que des utilisateurs non 'admin' de IPCop puissent contrôler la connexion.

Ok

<Tab>/<Alt-Tab> entre les éléments | <Espace> sélectionner

o Paramétrage des cartes réseaux



Lors du paramétrage des deux cartes réseaux, il faut faire attention aux cartes que l'on va assigner au réseau interne et externe. Dans ce TP nous ne nous occupons pas de l'interface orange.

Nous assignerons une carte réseau à l'interface rouge (red) pour le réseau externe qui nous donnera l'accès à internet. La seconde carte réseau sera assigné à l'interface vert (green), elle servira pour connecter le serveur Ipcop au réseau interne d'où nous allons administrer le serveur Proxy.

o Connexion à l'interface et installation du service Proxy

Pour pouvoir se connecter à l'interface, il faut entrer l'adresse du serveur que nous avons choisis lors de son installation dans un navigateur suivis du port « 8443 ».

<https://192.168.2.1:8443/cgi-bin/index.cgi>

Ensuite, pour avoir un accès à internet dans la zone verte (celle protégée par le serveur proxy) il faut activer un service, cliquer sur services puis serveur mandataire (proxy).

Services >> **Serveur mandataire (proxy)**

Il faut activer l'interface « vert » et autoriser l'affichage des messages d'erreur.

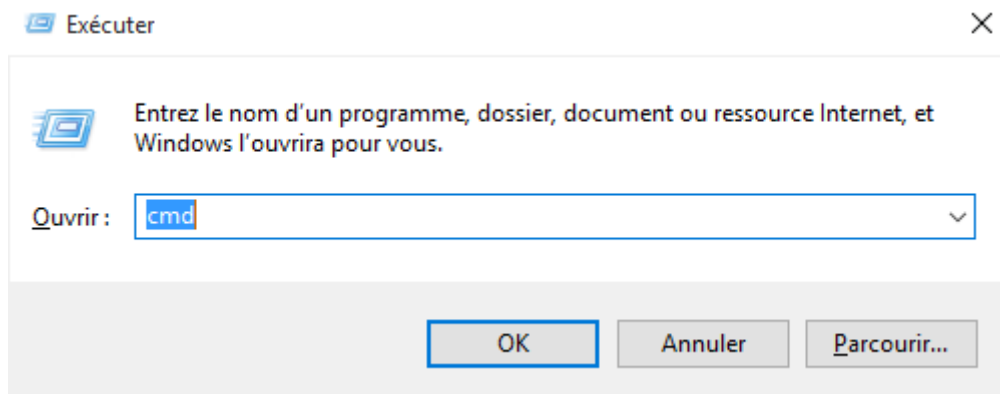
The screenshot shows the Mikrotik WinBox interface. At the top, there is a navigation bar with the following items: "Services" (selected), "Etat", "Réseau", "Services", "Pare-feu", "RVPs", and "Journaux". Below this is a "Configuration" section for the "Serveur mandataire (proxy)" service. The status of the service is shown as "Arrêté" (Stopped) in a red box. Under the "Paramètres communs" (Common Parameters) section, the following settings are visible:

- Activé sur VERT:
- Port serveur mandataire: 8080
- Langues des messages d'erreurs: English
- Affichage des messages d'erreur: Standard
- Supprimer l'information de version:

Et pour finir, désactiver le mode transparent car il servira plus tard pour que le filtrage soit effectif.

The screenshot shows a single configuration option: "Mode transparent VERT:" followed by an unchecked checkbox.

Ouvrir à l'aide de la combinaison de touches Windows + R, l'application invite de commande en tapant « cmd »



Ensuite, nous allons effectuer un ping vers les serveur DNS de google 8.8.8.8 à l'aide de la commande suivante : ping 8.8.8.8.

```
C:\Users\Labo 1 PC 1>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=72 ms TTL=57
Réponse de 8.8.8.8 : octets=32 temps=122 ms TTL=57
Réponse de 8.8.8.8 : octets=32 temps=114 ms TTL=57
Réponse de 8.8.8.8 : octets=32 temps=140 ms TTL=57

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 72ms, Maximum = 140ms, Moyenne = 112ms

C:\Users\Labo 1 PC 1>
```

Ici, tout fonctionne.

○ Mise en place d'un filtrage horaire

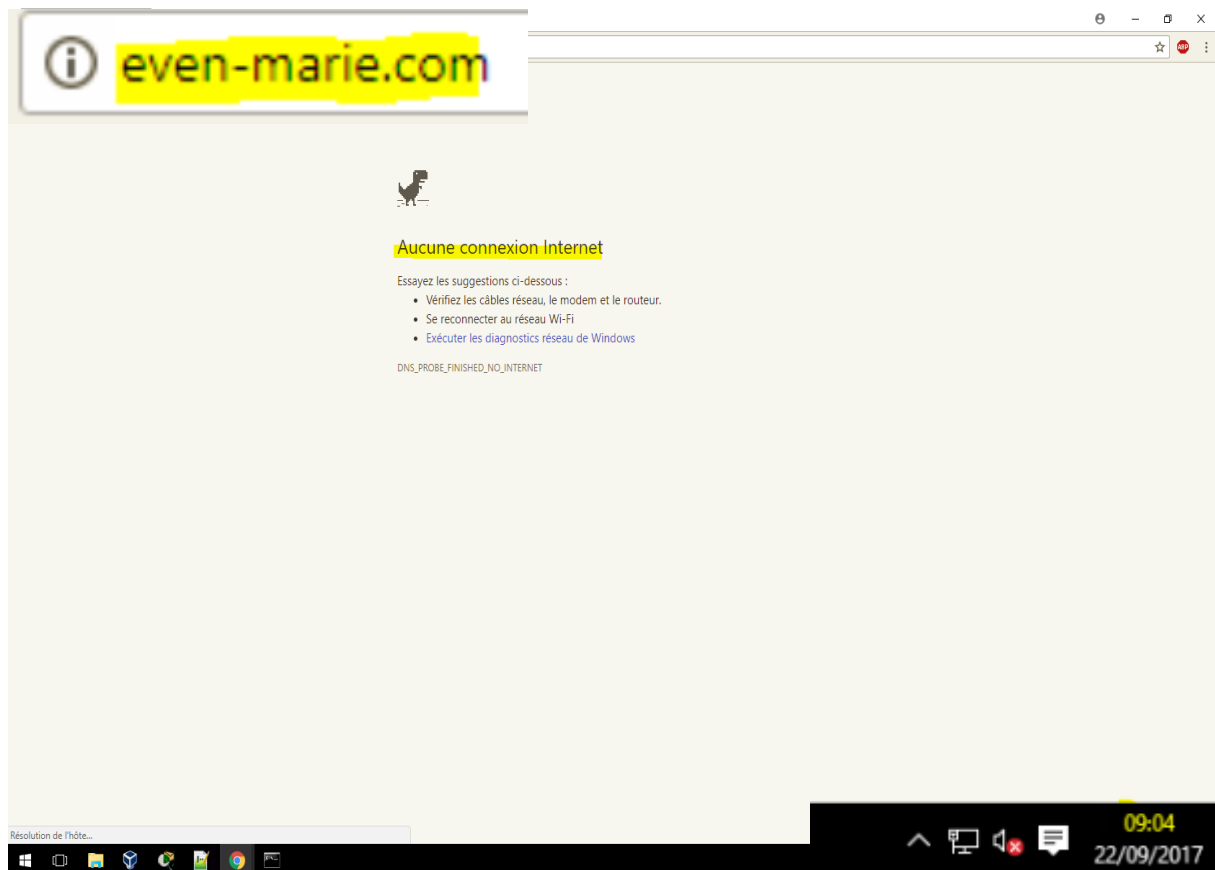
La prochaine manipulation sera d'initialiser un filtrage selon un horaire défini.

Pour ce faire nous allons nous rendre sur cette interface, nous allons initialiser un filtrage entre 9 : 00 et 9 : 15

Restrictions de temps

Accès	Lun	Mar	Mer	Jeu	Ven	Sam	Dim	De		à				
refusé ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	09 ▼	:	00 ▼	-	09 ▼	:	15 ▼

Ici, nous pouvons constater que l'accès à internet est bloqué alors que l'ordinateur est toujours connecté au proxy (ici à 9h04).




- Mise en place d'une limitation de débit pour le téléchargement

Toujours dans la même interface, nous pouvons aussi mettre en place une réduction du débit de téléchargement.


Il suffit d'indiquer les limites souhaité comme ci-dessous :

Réduction du téléchargement			
Limitation totale sur VERT:	64 kBit/s	Limitation par hôte sur VERT:	64 kBit/s
Activer la réduction basée sur le contenu:			
Fichiers binaires:	<input checked="" type="checkbox"/>	Images de CD:	<input checked="" type="checkbox"/>
		Multimédia:	<input checked="" type="checkbox"/>

Après avoir enregistré, le résultat devrait être visible dès le prochain téléchargement

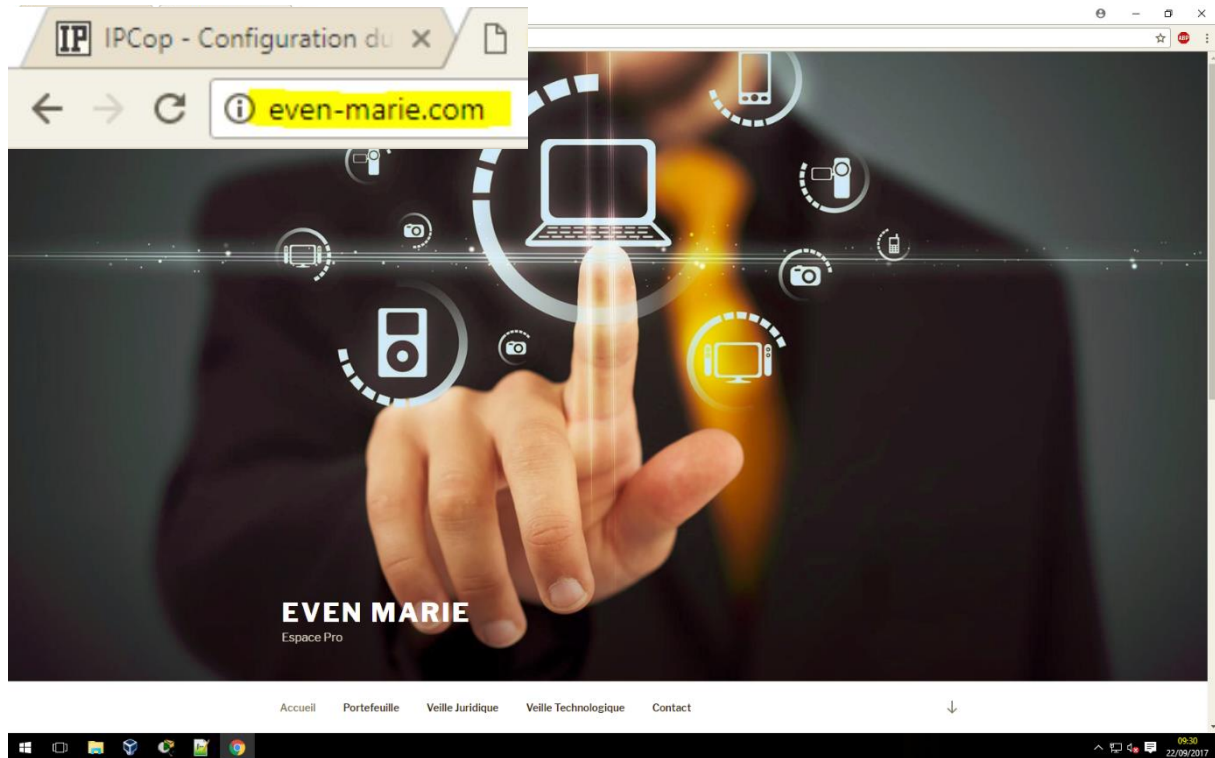
	<p>vlc-2.2.6-win32.exe http://ec.ccm2.net/www.commentcamarche.net/download/files/vlc-2.2.6-win32.exe</p> <p>7,8 Ko/s - 113 Ko sur 29,5 Mo, 1 heure restante</p> <hr/> <p>SUSPENDRE ANNULER</p>
---	--

Lorsqu'on désactive la restriction, le résultat est visible immédiatement :

	<p>vlc-2.2.6-win32.exe http://ftp.rezopole.net/vlc/vlc/2.2.6/win32/vlc-2.2.6-win32.exe</p> <p>230 Ko/s - 8,2 Mo sur 29,5 Mo, 2 min restantes</p> <hr/> <p>SUSPENDRE ANNULER</p>
---	---

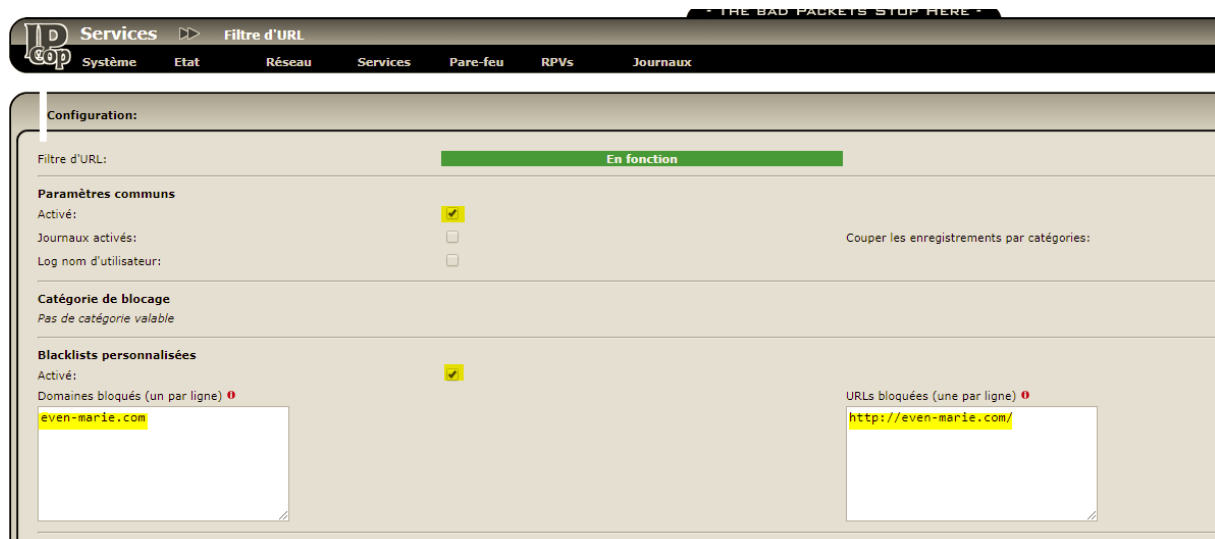
- Mise en place d'un filtre URL

Nous allons tenter maintenant de bloquer un site par le biais de son URL , nous voyons ici que le site choisis (even-marie.com) fonctionne bien.

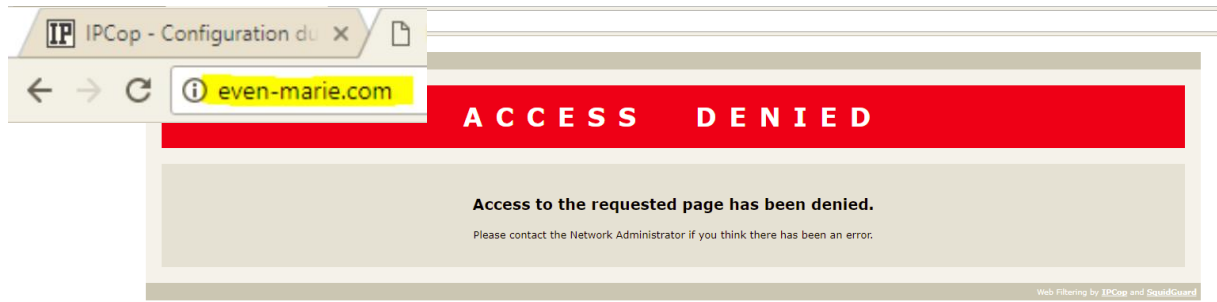


Pour initialiser ce service, il faut se rendre dans l'onglet filtre d'URL et renseigner l'URL que l'on souhaite bloquer.

Services >> Filtre d'URL



Si tout fonctionne, le message de refus s'affichera.



- o Mise en place d'une liste noire

Dans un premier temps nous avons téléchargé la liste noire que propose l'Université de Toulouse.

Catégorie	Nombre de sites	Description
dating	3572	Sites de rencontres
ddos	232	Sites de déni de services
dialer	0	Sites de dialer
download	66	Sites qui permettent de télécharger d
drogue	1055	Drogue.
educational_games	10	Sites de jeux éducatifs
filehosting	833	Sites qui hébergent des contenus (vi
financial	80	Informations financières, bourses.
forums	209	Forums.
gambling	1118	Sites de jeux en ligne, casino, etc.
games	11131	Sites de jeux, en ligne, ou de distribu
hacking	301	Sites de piratage et d'agressions info
jobsearch	385	Site pour trouver un emploi
lingerie	71	Sites de lingerie
liste_bu	2825	Une liste très "univ-tlse1.fr" de sites é
malware	16034	Tout site qui injecte des malwares
manga	729	Tout ce qui est lié à l'univers des mar
marketingware	820	Sites de marketing très spéciaux
mixed_adult	152	Sites qui contiennent des portions ad
mobile-phone	46	Sites pour les mobiles (sonneries, etc
phishing	63508	Sites de phishing, de pièges bancaire
press	4451	Tout site de presse d'information
publicite	1429	Publicité.
radio	491	Sites de radio sur Internet
reaaffected	8	Sites qui ont changé de propriétaire e
redirector	125966	Quelques sites qui permettent de cor
remote-control	42	Site permettant la prise de contrôle à
sect	144	Secte
sexual_education	18	Sites qui parlent d'éducation sexuelle
shopping	36396	Sites de vente et achat en ligne
shortener	262	Raccourcisseur d'URL
social_networks	636	Tous les sites de réseaux sociaux
sports	2275	Sports
strict_redirector	125684	Comme redirector, mais avec les mot

Ensuite, dans le menu « Maintenance des blacklists » nous allons importer la liste noire et la sélectionner.

Maintenance des blacklists:

Mise à jour de la blacklist
Vérifier les mises à jour à la connexion:

La Source de la Blacklist: **Univ. Toulouse** ▼

Blacklists URL source personnalisée:

Mise à jour immédiate

Une fois que la Black list enregistré, un petit message de maintenance apparaîtra :

Services >> Filtre d'URL

Systeme Etat Réseau Services Pare-feu RPVs Journaux

Messages d'information:

La nouvelle blacklist va être automatiquement compilée dans la base de donnée déjà établie. En fonction de la taille de la blacklist, cela peut prendre quelques minutes. Veuillez attendre que cette tâche soit terminée avant de redémarrer le Filtre d'URL.

Pour plus de précision sur ce que l'on souhaite bloquer, nous pouvons sélectionner le thème des sites à bloquer. Ici nous avons sélectionné sport :

Catégorie de blocage		
ads:	<input type="checkbox"/>	dangerous_material: <input type="checkbox"/>
adult:	<input type="checkbox"/>	dating: <input type="checkbox"/>
aggressive:	<input type="checkbox"/>	ddos: <input type="checkbox"/>
agressif:	<input type="checkbox"/>	dialer: <input type="checkbox"/>
arjel:	<input type="checkbox"/>	download: <input type="checkbox"/>
associations_religieuses:	<input type="checkbox"/>	drogue: <input type="checkbox"/>
astrology:	<input type="checkbox"/>	drugs: <input type="checkbox"/>
audio-video:	<input type="checkbox"/>	educational_games: <input type="checkbox"/>
bank:	<input type="checkbox"/>	filehosting: <input type="checkbox"/>
bitcoin:	<input type="checkbox"/>	financial: <input type="checkbox"/>
blog:	<input type="checkbox"/>	forums: <input type="checkbox"/>
celebrity:	<input type="checkbox"/>	gambling: <input type="checkbox"/>
chat:	<input type="checkbox"/>	games: <input type="checkbox"/>
child:	<input type="checkbox"/>	hacking: <input type="checkbox"/>
cleaning:	<input type="checkbox"/>	jobsearch: <input type="checkbox"/>
cooking:	<input type="checkbox"/>	lingerie: <input type="checkbox"/>
		liste_blanche: <input type="checkbox"/>
		liste_bu: <input type="checkbox"/>
		mail: <input type="checkbox"/>
		malware: <input type="checkbox"/>
		manga: <input type="checkbox"/>
		marketingware: <input type="checkbox"/>
		mixed_adult: <input type="checkbox"/>
		mobile-phone: <input type="checkbox"/>
		phishing: <input type="checkbox"/>
		porn: <input type="checkbox"/>
		press: <input type="checkbox"/>
		proxy: <input type="checkbox"/>
		publicite: <input type="checkbox"/>
		radio: <input type="checkbox"/>
		reaffected: <input type="checkbox"/>
		redirector: <input type="checkbox"/>
		remote-control: <input type="checkbox"/>
		sect: <input type="checkbox"/>
		sexual_education: <input type="checkbox"/>
		shopping: <input type="checkbox"/>
		shortener: <input type="checkbox"/>
		social_networks: <input type="checkbox"/>
		special: <input type="checkbox"/>
		sports: <input checked="" type="checkbox"/>
		strict_redirector: <input type="checkbox"/>
		strong_redirector: <input type="checkbox"/>
		translation: <input type="checkbox"/>
		tricheur: <input type="checkbox"/>
		update: <input type="checkbox"/>
		violence: <input type="checkbox"/>
		warez: <input type="checkbox"/>
		webmail: <input type="checkbox"/>

Le site matchendirect.fr étant dans la liste, nous ne pouvons pas y accéder.

← → ⓘ www.matchendirect.fr

ACCESS DENIED

Access to the requested page has been denied.

Please contact the Network Administrator if you think there has been an error.

Web Filtering by IPCop and SquidGuard

○ Mise en place d'un cache

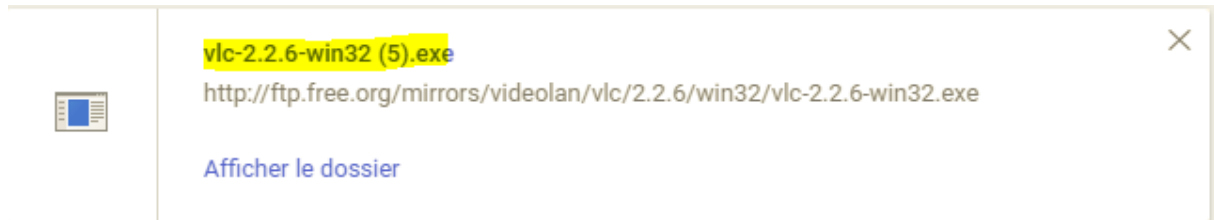
Dans les options avancées d'Ipcop, il y a possibilité de mettre en place un cache, dans un premier temps nous allons initialiser la taille maximale du cache.



The screenshot shows the 'Options avancées' (Advanced Options) configuration page for Ipcop. The 'Gestion du cache' (Cache Management) section is active. The following settings are visible:

- Taille du cache en mémoire (MB): 100
- Taille minimale d'objet (Ko): 0
- Nombre de sous-répertoire de niveau 1: 16
- Stratégie de gestion de la mémoire: LRU
- Stratégie de gestion du cache: LRU
- Taille du cache sur le disque dur (MB): 100
- Taille maximale d'objet (Ko): 100000
- Ne pas mettre en cache ces domaines (un par ligne): 0
- Mode autonome activé:

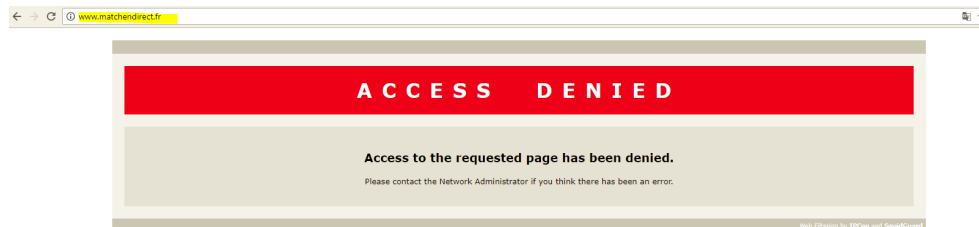
Une fois le cache initialisé, nous avons téléchargé VLC sur un des ordinateurs connectés à Ipcop. Une fois le téléchargement terminé, il est entré en cache sur notre serveur et lorsque nous l'avons lancé sur un autre pc connecté à Ipcop, le téléchargement a été instantané grâce au cache.



o Personnalisation de la page de refus

Comme fait précédemment, nous avons laissé bloquer les sites de sports, ici nous allons initialiser une page personnalisé lorsqu'un site est bloqué.

Le message de base affiché est celui-ci :



Dans la rubrique filtre URL, nous pouvons accéder à la modification de la page de refus, il suffit de remplir les champs comme voulu et si on veut ajouter une photo il faut insérer du HTML. Voici ci-dessous le rendu :

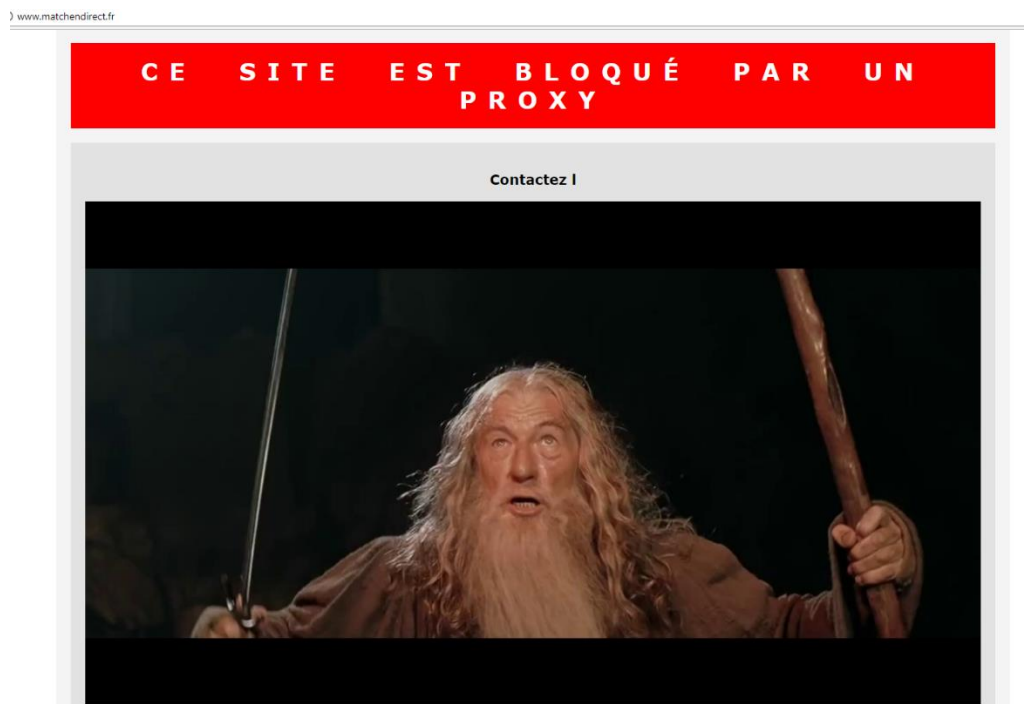
Paramètres des pages bloquées	
Afficher les catégories dans la page bloquée:	<input type="checkbox"/>
Afficher l'URL dans la page bloquée:	<input type="checkbox"/>
Afficher l'adresse IP dans la page bloquée:	<input type="checkbox"/>
Utiliser 'DNS Error' pour bloquer les URLs:	<input type="checkbox"/>
Activer l'image de fond:	<input type="checkbox"/>

Rediriger vers cette URL:

Message ligne 1:

Message ligne 2:

Message ligne 3:



- Paramétrage d'un poste administrateur sans restriction

Toujours dans le filtre d'URL, nous devons juste ajouter l'IP du poste que nous voulons définir comme administrateur dans la rubrique des accès par le réseau, si le poste est configuré de manière à avoir une adresse IP dynamique il suffit d'entrer son adresse MAC.

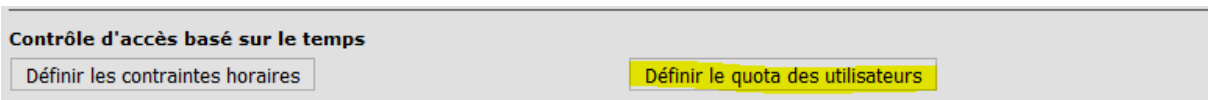


Une fois cela fait, le poste ne sera pas affecté par les paramètres de blocage du serveur Proxy et aura les pleins pouvoirs sur ce dernier.

- Mise en place de quota de navigation


Services  Filtre d'URL

C'est dans la rubrique Filtre d'URL, que l'on peut définir un quota. Dans la rubrique contrôle d'accès basé sur le temps, cliquer sur « définir le quota des utilisateurs »







Il suffit ensuite de paramétrer le temps, ici nous avons choisi 5 minutes et affecter tous les utilisateurs.

Ajouter une nouvelle règle de quota:

Quota de temps:	<input type="text"/>	Utilisateurs affectés par le quota (un par ligne):	<div style="border: 1px solid gray; height: 60px;"></div>
Détection d'activité:	désactivé		
Rafraîchir:	heure		
Activé:	<input checked="" type="checkbox"/>	Ajouter	RAZ config 

Règles actuelles

Quota de temps	Détection d'activité	Rafraîchir	Utilisateurs affectés	
5 Minutes	désactivé	jour	all	<input checked="" type="checkbox"/>  

Légende: Activé (cliquer pour désactiver) Désactivé (cliquer pour activer)  Modifier  Supprimer

Les utilisateurs sont donc limité à 5min de navigation par jours.