Pare-feu : IPCOP

Mise en place d'un pare-feu

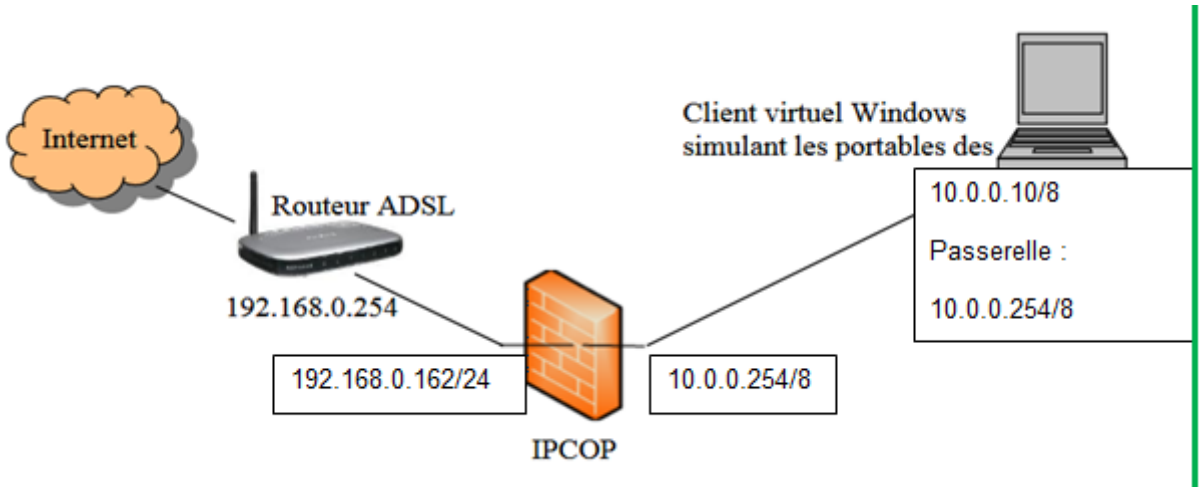
- IPCOP

IPCOP



Introduction

IPCop est une distribution Linux basée sur Linux, qui vise à fournir un pare-feu simple à gérer basé sur du matériel PC. IPCop est un pare-feu à états construit sur le framework netfilter de Linux.



Nous allons installer IPCop sur une machine virtuelle.

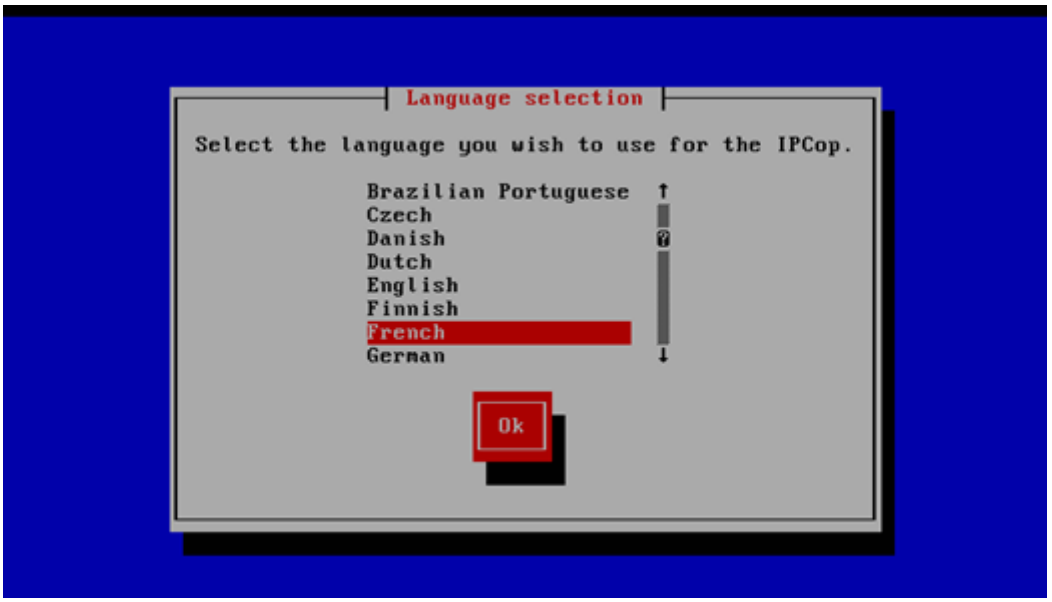
Développement

Configuration de la machine virtuelle

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SATA)	20 GB
CD/DVD (SATA)	Using file C:\Users\BONNET\...
Network Adapter	Bridged (Automatic)
Network Adapter 2	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

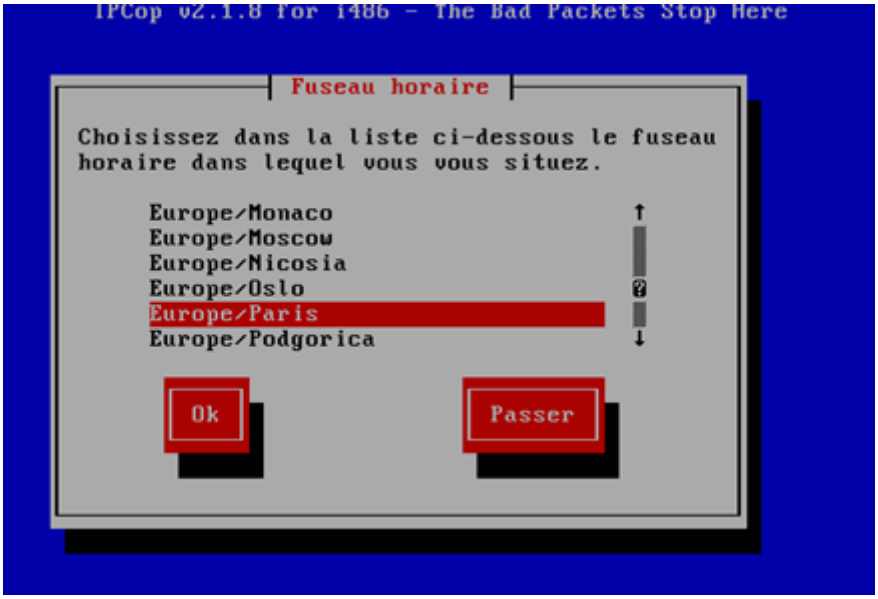
Installation





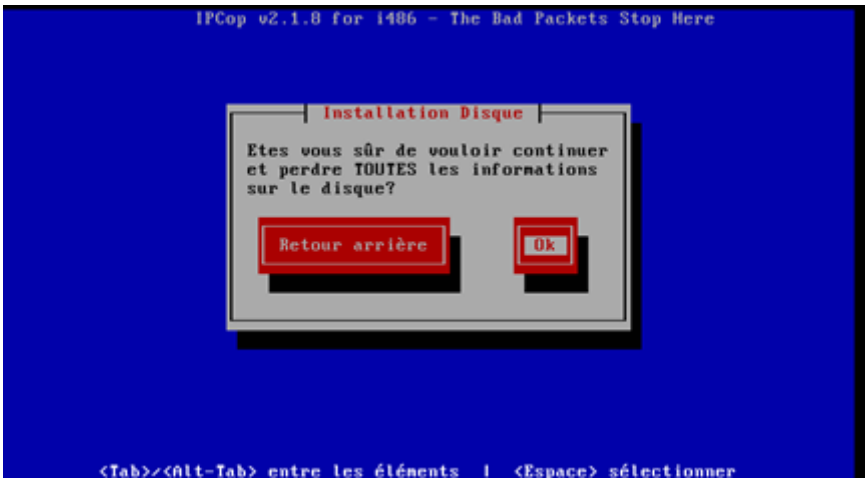

IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Bienvenue dans le programme
d'installation d'IPCop. Sélectionner
Annuler sur l'un des écrans suivants
redémarrera votre ordinateur.
Ok
Annuler


Configuration du clavier
Choisissez dans la liste ci-dessous le type de
clavier que vous utilisez.
fr
fr-latin1
fr-latin9
fr-pc
fr_CH
fr_CH-latin1
Ok
Passer

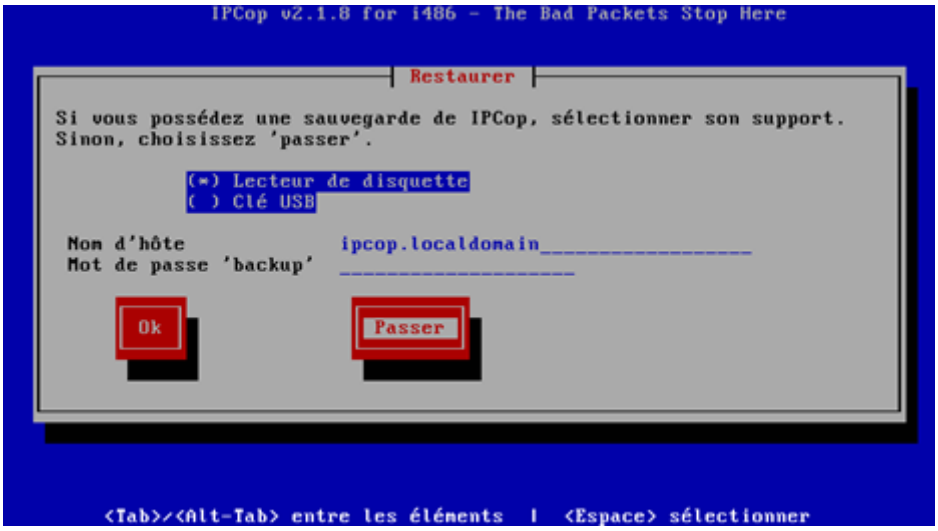

IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Fuseau horaire
Choisissez dans la liste ci-dessous le fuseau
horaire dans lequel vous vous situez.
Europe/Monaco
Europe/Moscow
Europe/Nicosia
Europe/Oslo
Europe/Paris
Europe/Podgorica
Ok
Passer


IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Date - Heure
Saisir la date et l'heure, sélectionner "passer" si vous le désirez pas effectuer de changement.
Date 2020-09-08
Heure 15:48:22
Ok
Passer
<Tab>/<Alt-Tab> entre les éléments | <Espace> sélectionner

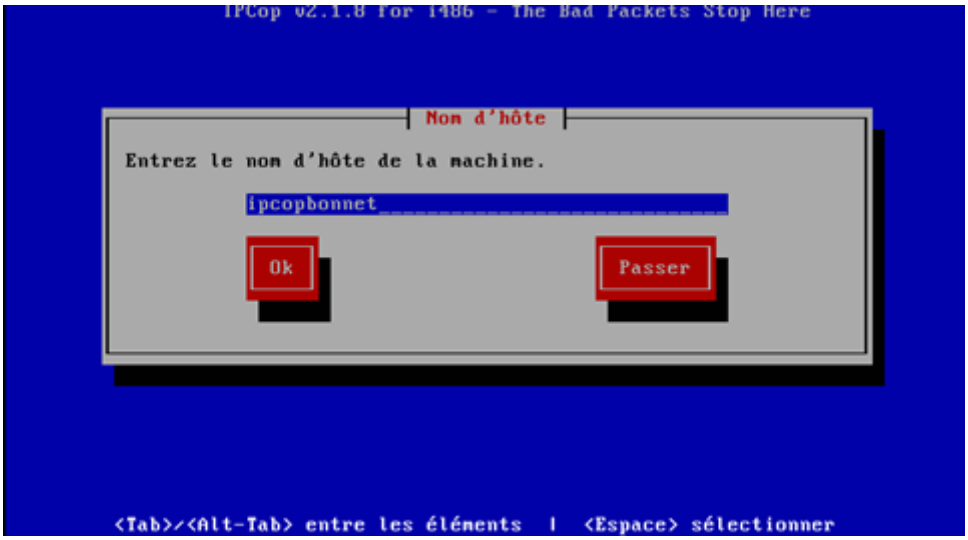

IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Installation Disque
Sélectionner le disque sur lequel installer IPCop. Le programme d'installation procèdera au partitionnement du disque, créera les systèmes de fichiers et copiera les fichiers. Cela signifie la perte de TOUTES les données existant sur le disque!
sda: VMware Virtual S (20 GiB)
Ok
Annuler
<Tab>/<Alt-Tab> entre les éléments | <Espace> sélectionner


IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Installation Disque
Etes vous sûr de vouloir continuer et perdre TOUTES les informations sur le disque?
Retour arrière
Ok
<Tab>/<Alt-Tab> entre les éléments | <Espace> sélectionner


IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Installation Disque
Voulez vous une installation 'Disque Dur' ou 'Flash'? Choisir Flash entraine plusieurs modifications qui minimisent le nombre d'écritures sur le disque, ce qui permet une plus grande durée de vie de la carte.
Disque Dur
Flash
Retour arrière
<Tab>/<Alt-Tab> entre les éléments | <Espace> sélectionner


IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Restaurer
Si vous possédez une sauvegarde de IPCop, sélectionner son support.
Sinon, choisissez 'passer'.
(*) Lecteur de disquette
( ) Clé USB
Nom d'hôte ipcop.localdomain
Mot de passe 'backup'
Ok
Passer
<Tab>/<Alt-Tab> entre les éléments | <Espace> sélectionner

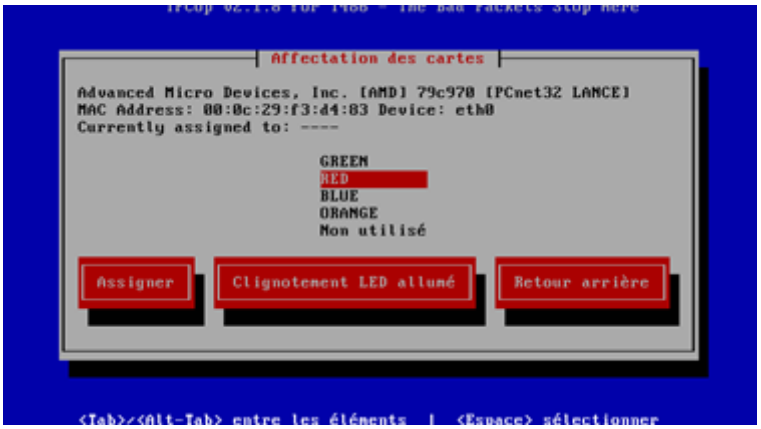

IPCop v2.1.8 for i486 - The Bad Packets Stop Here
IPCop v2.1.8 for i486 - The Bad Packets Stop Here
IPCop a été installé avec succès. Veuillez retirer toute disquette ou CD-ROM de l'ordinateur. L'utilitaire de configuration va maintenant s'exécuter et vous permettre de configurer les cartes réseaux, le RNIS et les mots de passe système. Une fois la configuration terminée, vous pourrez utiliser votre navigateur sur https://192.168.1.1:8443 ou https://ipcop:8443 (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 donner un mot de passe à l'utilisateur 'dial' ipcop, si vous voulez que des utilisateurs non 'admin' de IPCop puissent contrôler la connexion.
Félicitations!
<Tab>/<Alt-Tab> entre les éléments | <Espace> sélectionner

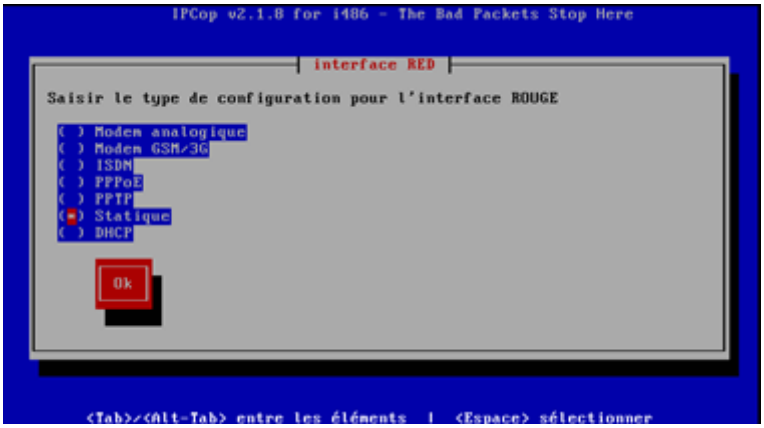


localdomain car pas de domaine.

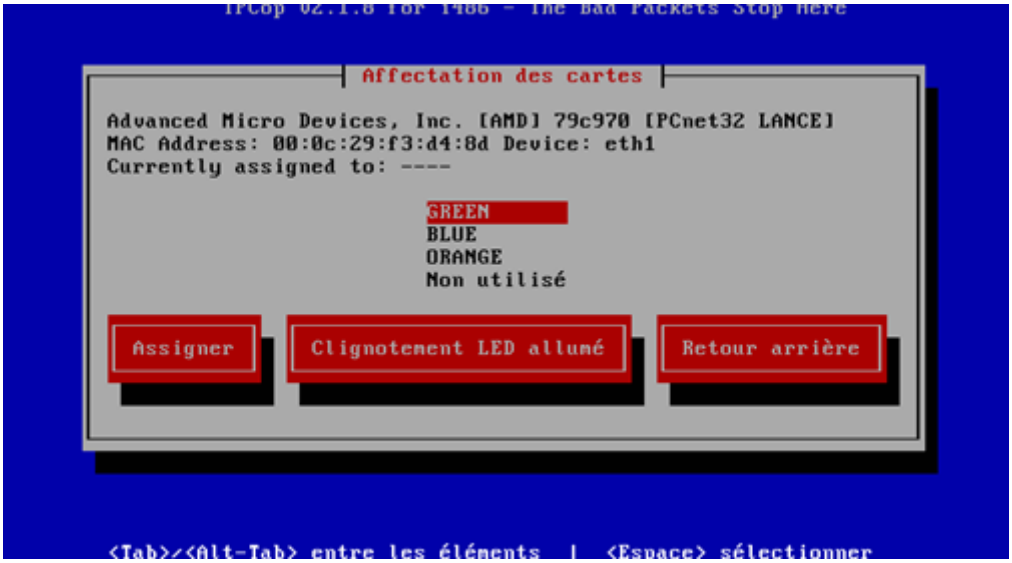


RED pour WAN





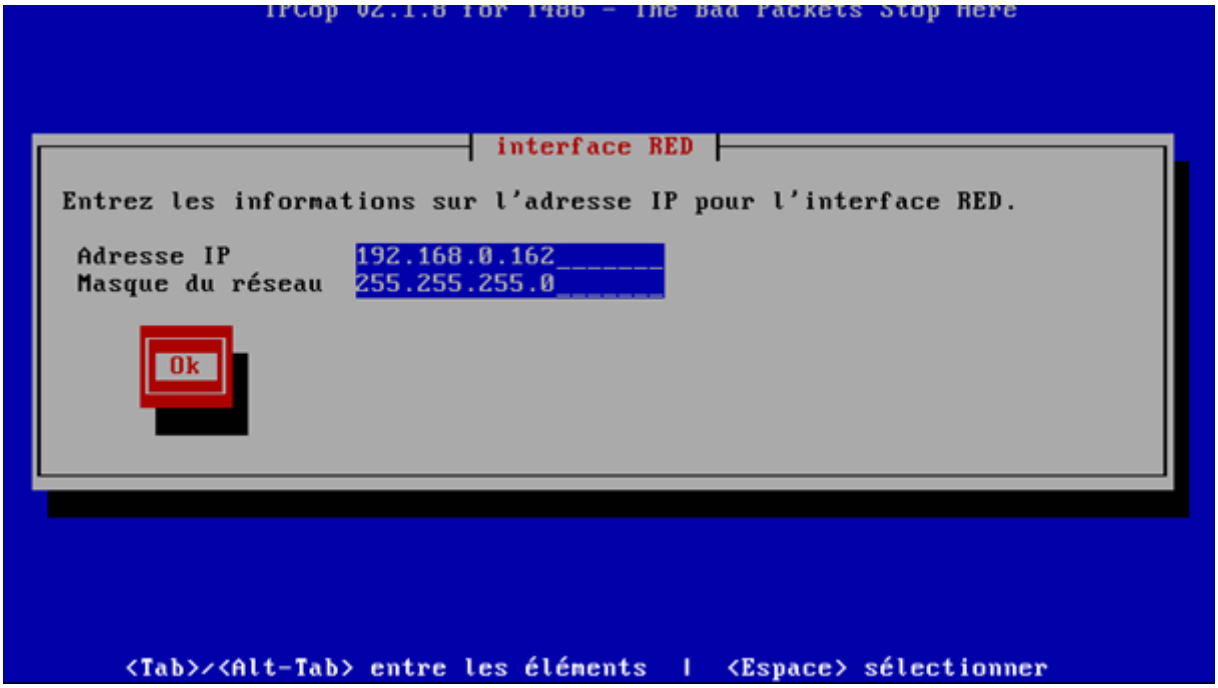
GREEN pour LAN

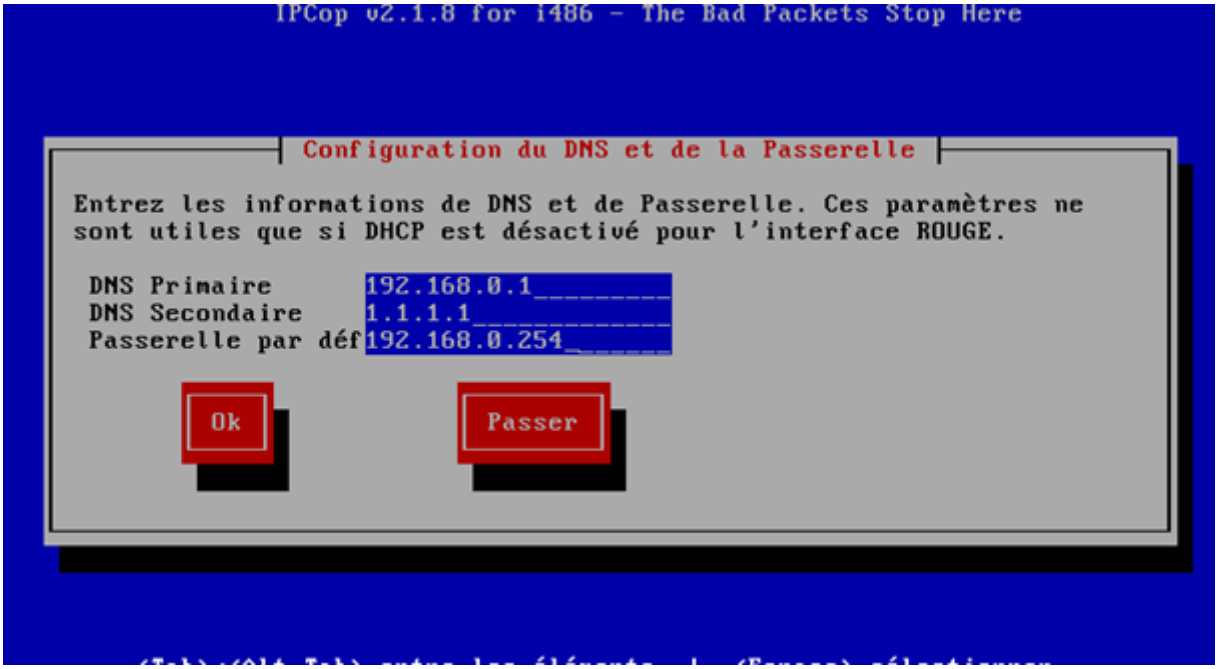


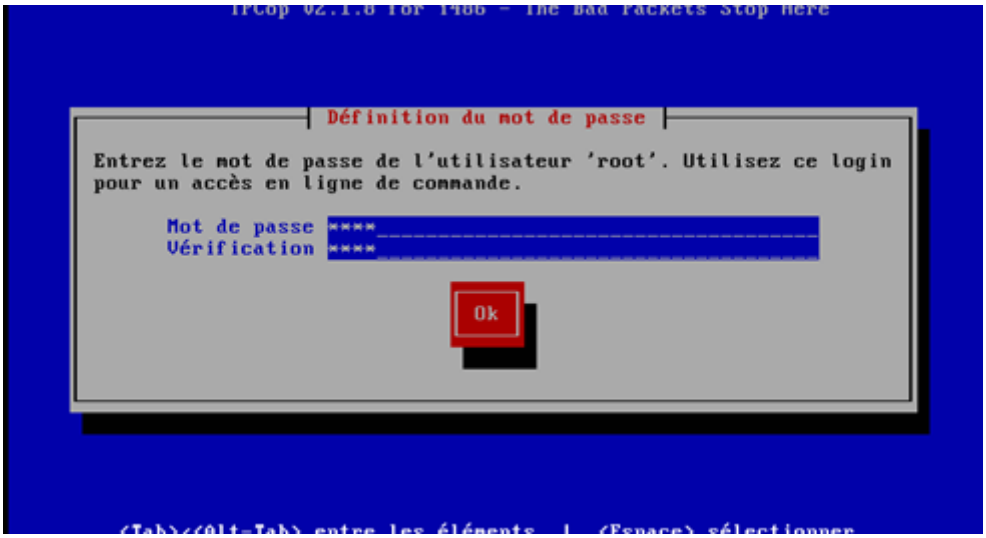


10.0.0.254 en 255.0.0.0 pour l'interface GREEN (LAN)

192.168.0.162 / 24 pour le Wan (RED)





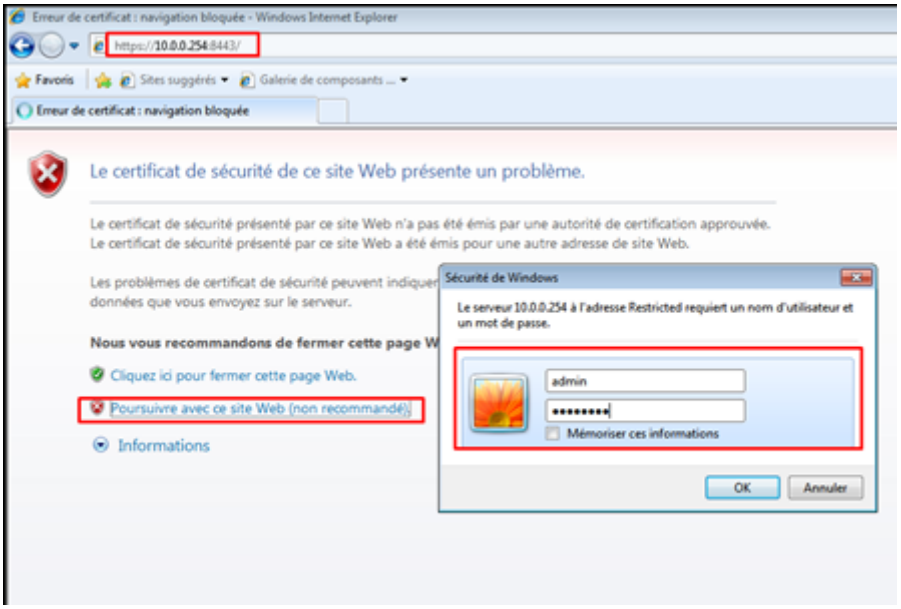


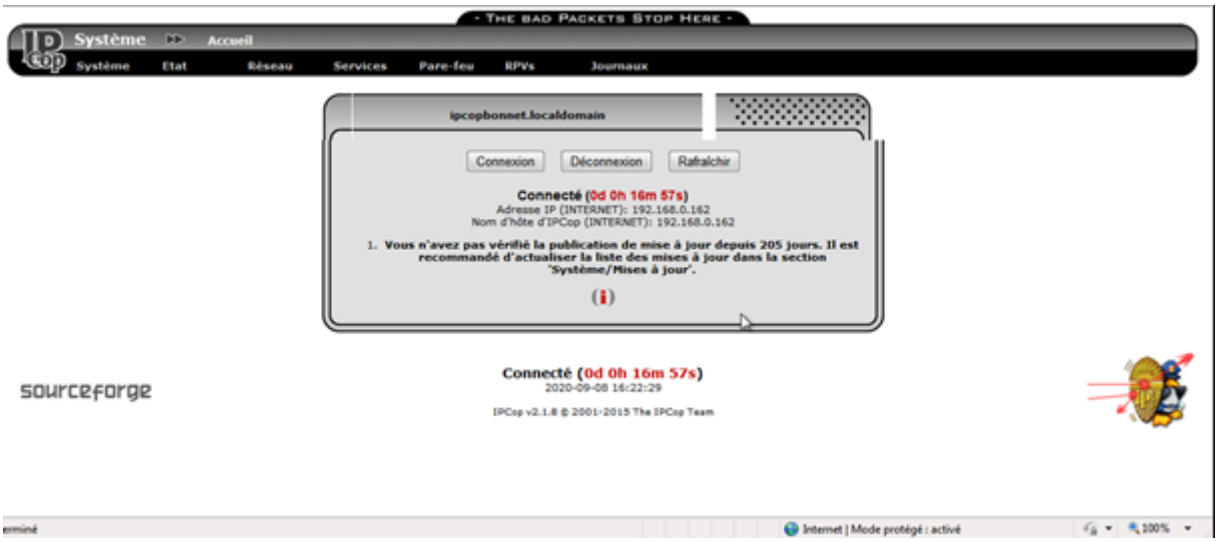
Il faut un nom d'utilisateur et mot de passe différent pour l'admin, idem pour le chiffrage des sauvegardes.

IPCOP est installé et configuré !

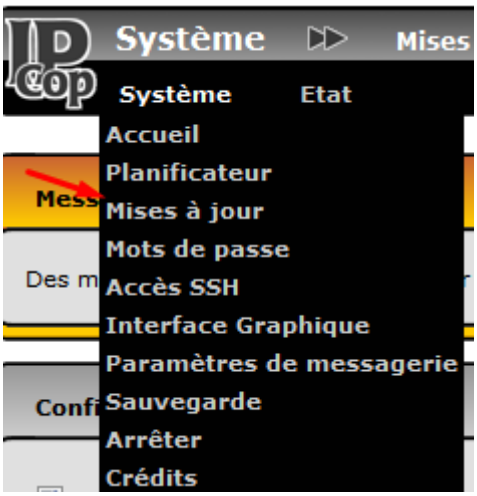
Configuration d'IPCOP

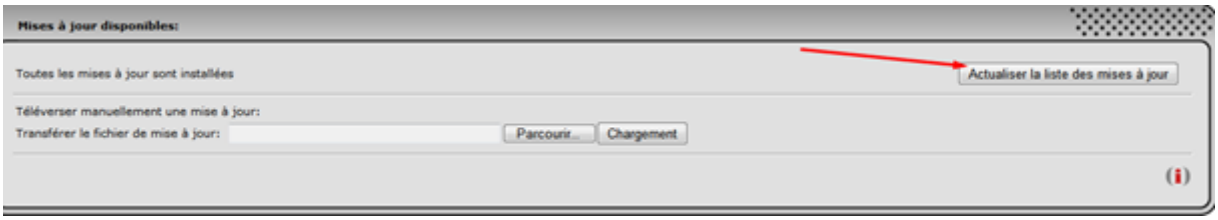
On peut se connecter en ligne de commande ou par navigateur web.



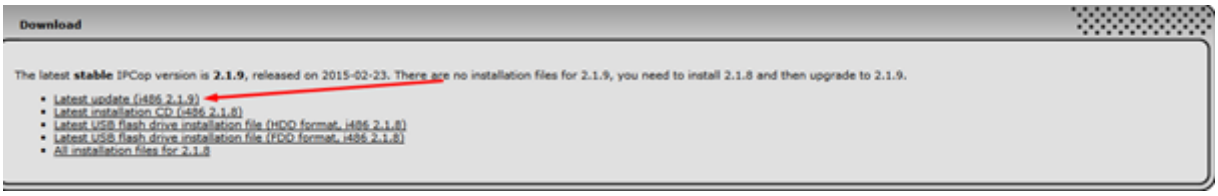

- The bad packets stop here -
Système
Accueil
Système
Etat
Réseau
Services
Pare-feu
RPVs
Journaux
ipcopbonnet.localdomain
Connexion
Déconnexion
Rafraîchir
Connecté (0d 0h 16m 57s)
Adresse IP (INTERNET): 192.168.0.162
Nom d'hôte d'IPCop (INTERNET): 192.168.0.162
1. Vous n'avez pas vérifié la publication de mise à jour depuis 205 jours. Il est recommandé d'actualiser la liste des mises à jour dans la section 'Système/Mises à jour'.
sourceforge
Connecté (0d 0h 16m 57s)
2020-09-08 16:22:29
IPCop v2.1.8 © 2001-2015 The IPCop Team
Internet | Mode protégé : activé
100%

Mise à jour


Système
Mises
Système
Etat
Accueil
Planificateur
Mises à jour
Mots de passe
Accès SSH
Interface Graphique
Paramètres de messagerie
Sauvegarde
Arrêter
Crédits



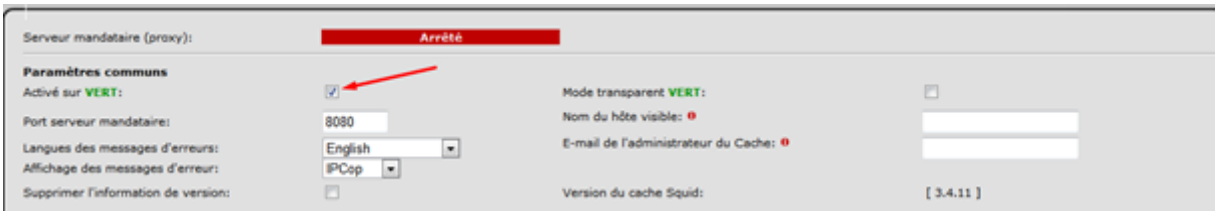
L'actualisation ne marchant pas, nous allons l'importer ici. Pour cela, on se rend sur le site d'ipcop et on télécharge la dernière mise à jour.



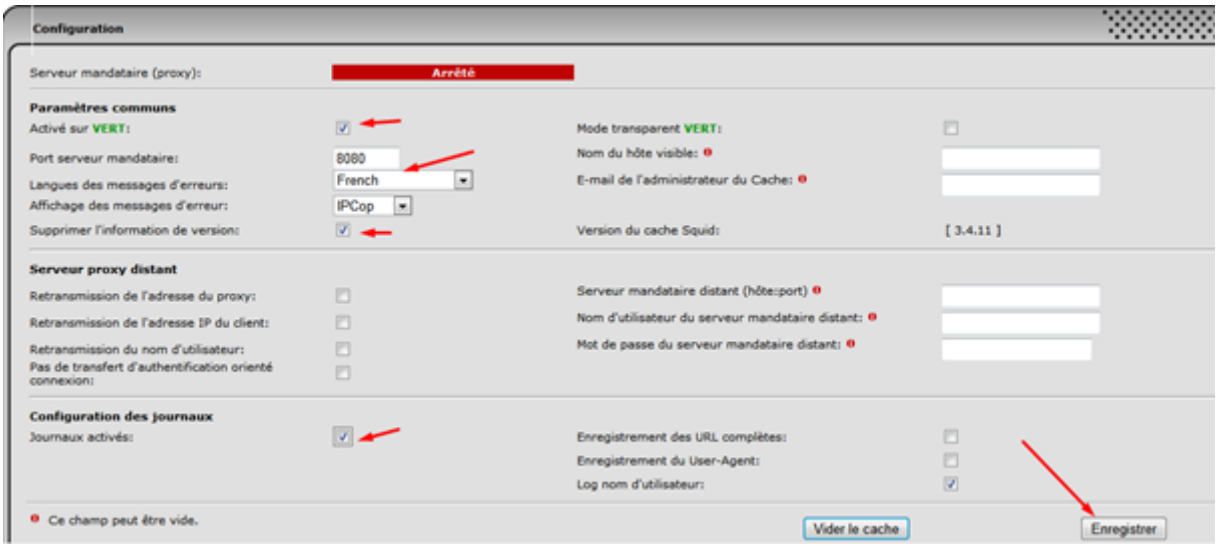
On la téléverse puis on l'applique.

Proxy



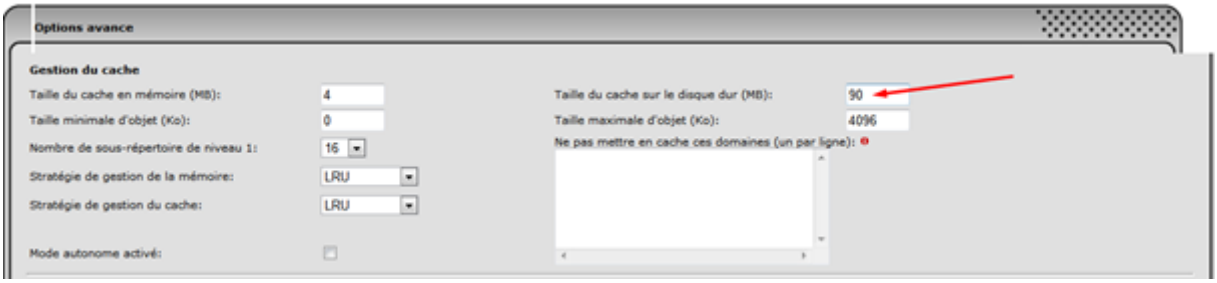


On peut modifier le port du proxy, la langue des messages d'erreurs etc.

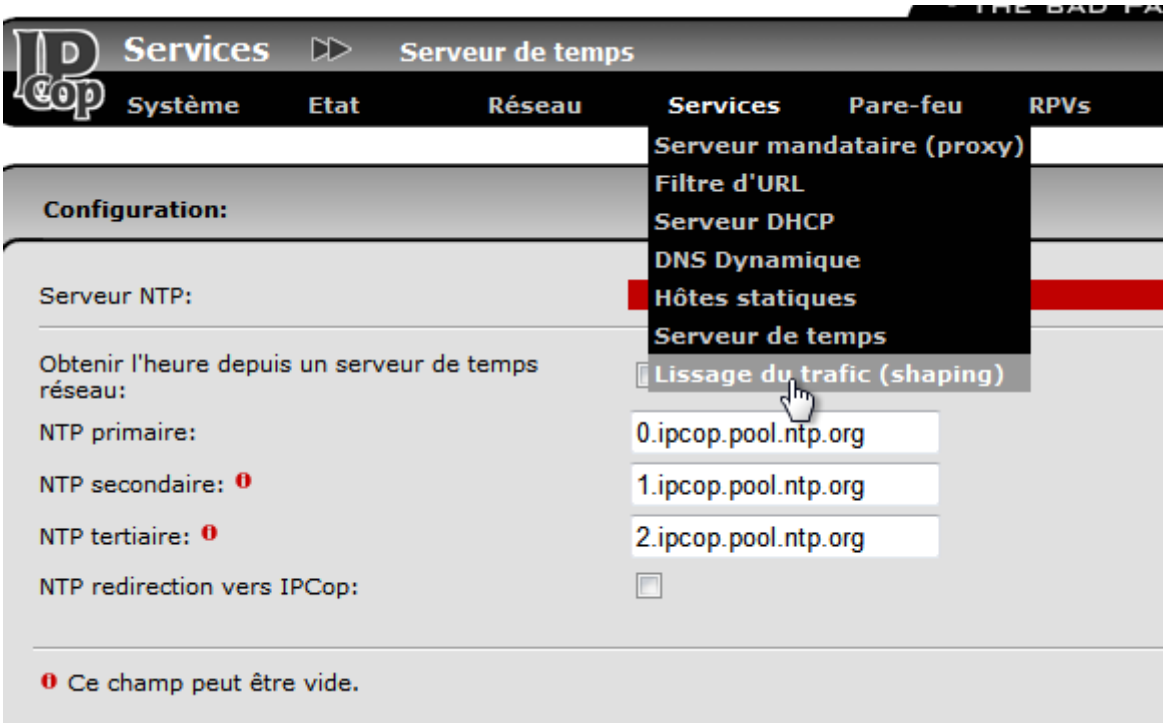


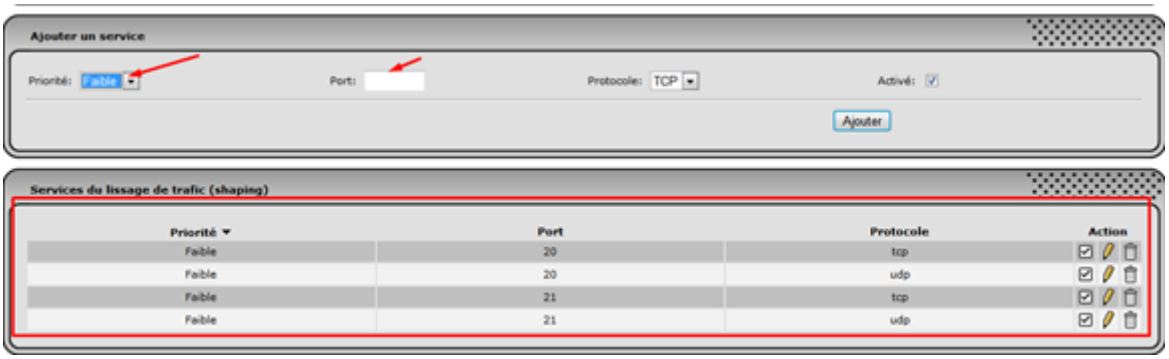
On active les journaux.

Plus bas :

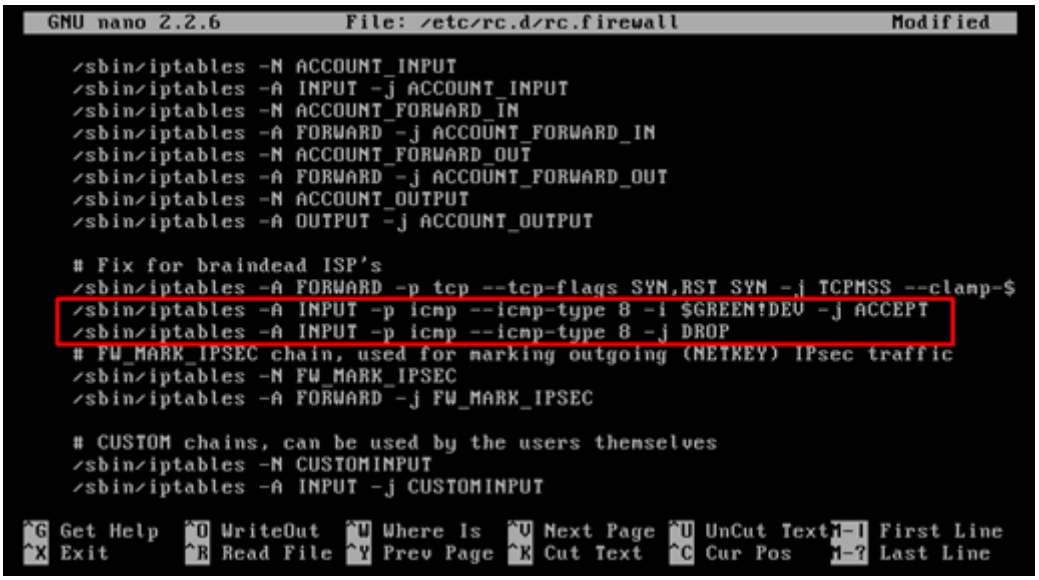


Limitation du trafic FTP





Blocage du ping coté internet



Il faut modifier le fichier rc.firewall dans le but de bloquer le ping, comme la capture d'au dessus.

```
nano 146 /etc/rc.d/rc.firewall
```

```
C:\Users\BONNET>ping 192.168.0.162

Envoi d'une requête 'Ping'  192.168.0.162 avec 32 octets de données :
Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64

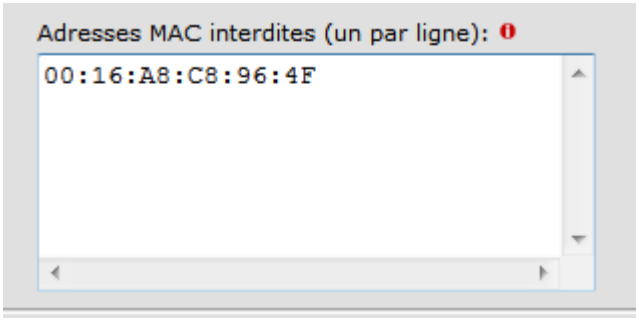
Statistiques Ping pour 192.168.0.162:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\BONNET>ping 192.168.0.162

Envoi d'une requête 'Ping'  192.168.0.162 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.0.162:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

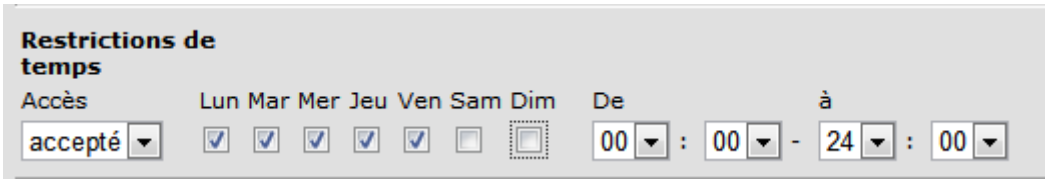
Blocage du portable

Dans services, serveur mandataire.



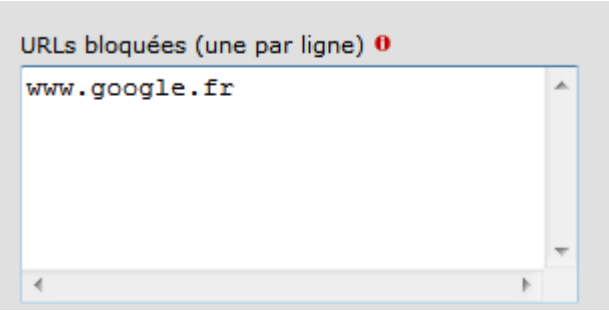
Impossible d'aller sur internet le week-end

Services, serveur mandataire

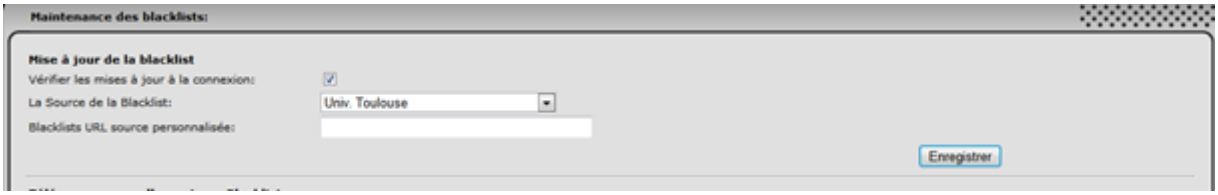


Blocage d'un site

Service, filtreur d'url

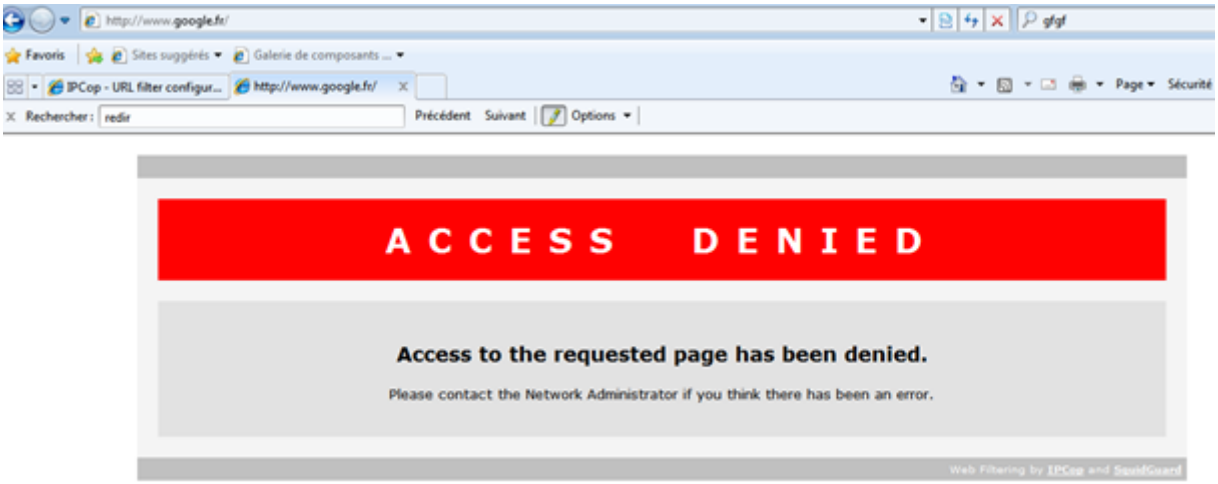


Mise en place d’une blacklist



On clique sur mise à jour immédiate

Test :



Conclusion

IPCop permet d’avoir un pare-feu logiciel à moindre coût. Cependant, IPCop est dépassé. La dernière version date de février 2015. Il faut donc passer à des solutions de pare-feu plus récentes, comme pfSense ou IPFire (spin-off de IPCop).