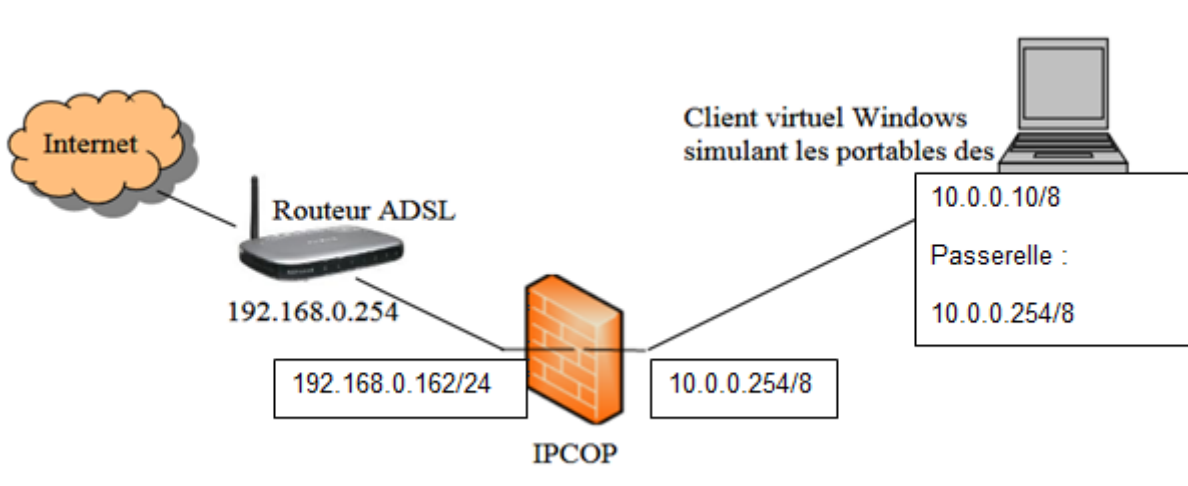


IPCop



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

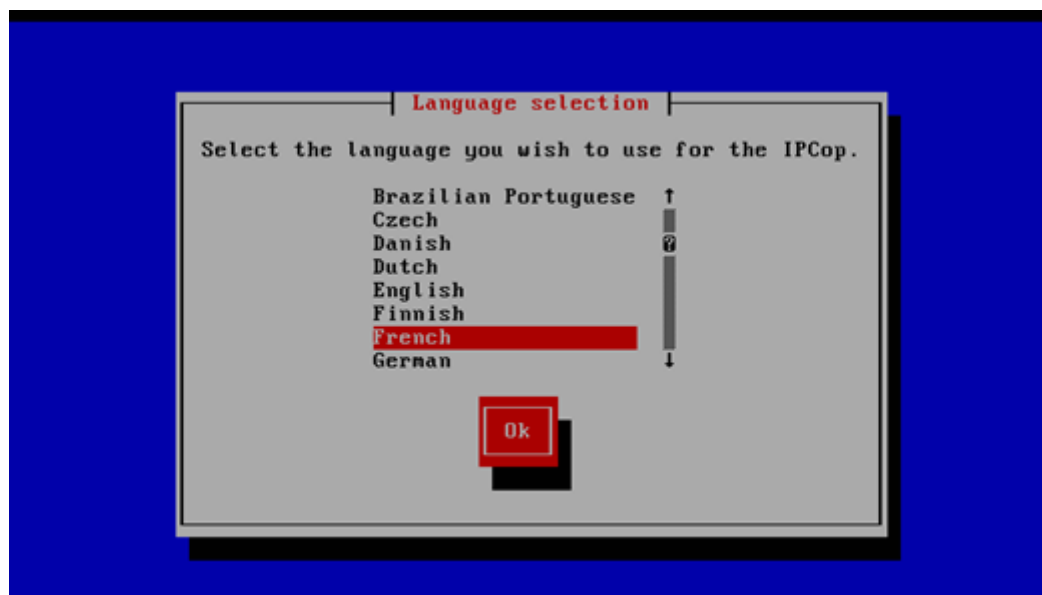
Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SATA)	20 GB
CD/DVD (SATA)	Using file C:\Users\BONNET\...
Network Adapter	Bridged (Automatic)
Network Adapter 2	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Installation

```
ISOLINUX 6.03 2014-10-06 ETCD Copyright (C) 1994-2014 H. Peter Anvin et al

Press RETURN to boot IPCop 2.1.8 default installation.
Press F1 for help and further information, TAB for boot targets list.
boot:
Loading vmlinuz... ok
Loading instroot.img...ok

Decompressing Linux... Parsing ELF... done.
Booting the kernel.
```



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

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

Installation Disque

Sélectionner le disque sur lequel installer IPCop. Le programme d'installation procédera 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

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

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

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

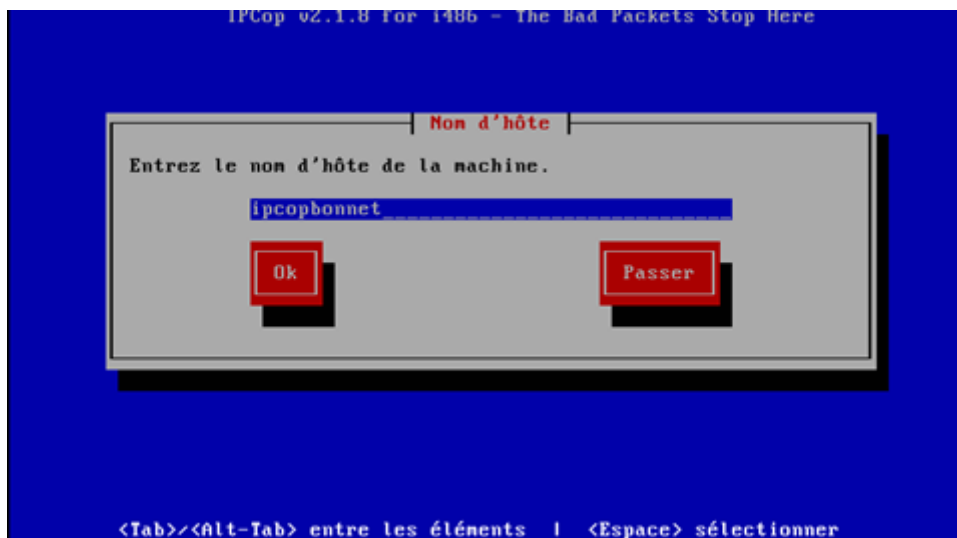
Passer

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

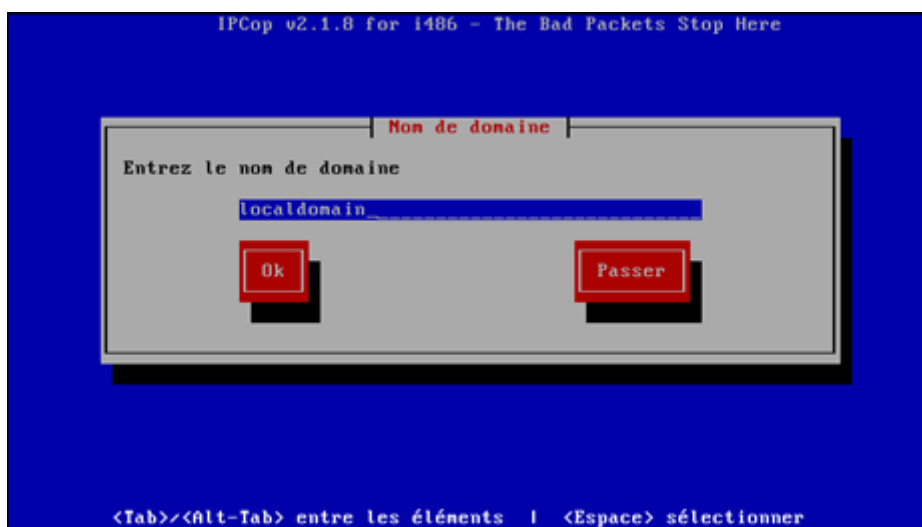
IPCop a été installé avec succès. Veuillez retirer toute disquette ou CD-ROM de l'ordinateur. L'utilitaire de configuration va maintenant s'exécuter et vous permettre de configurer les cartes réseaux, le RNIS et les mots de passe système. Une fois la configuration terminée, vous pourrez utiliser votre 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!

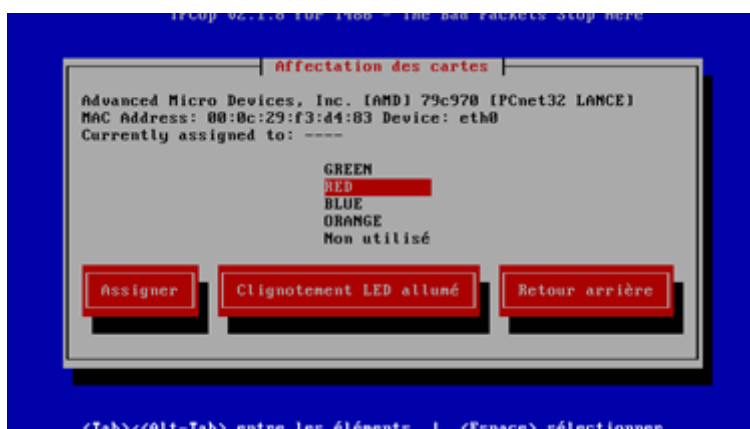
<Tab>/<Alt-Tab> entre les éléments | <Espace> sélectionner

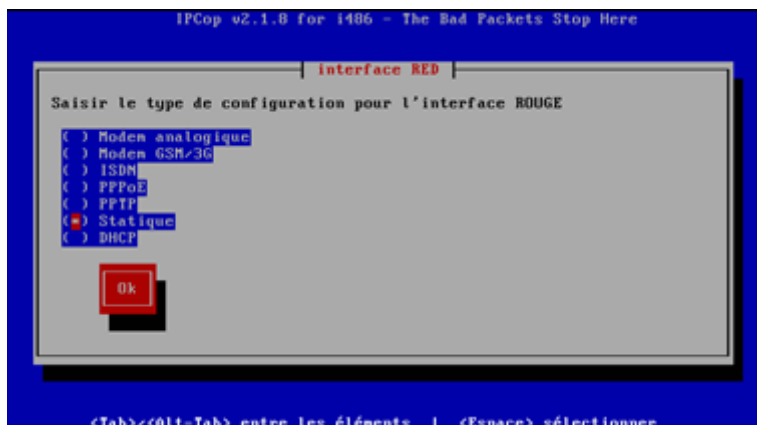


localdomain car pas de domaine.

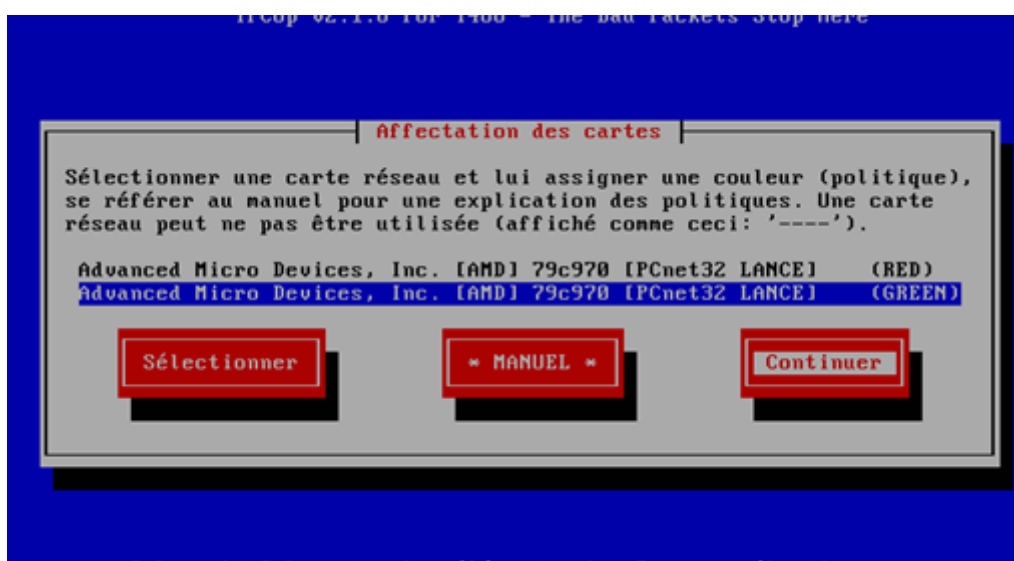
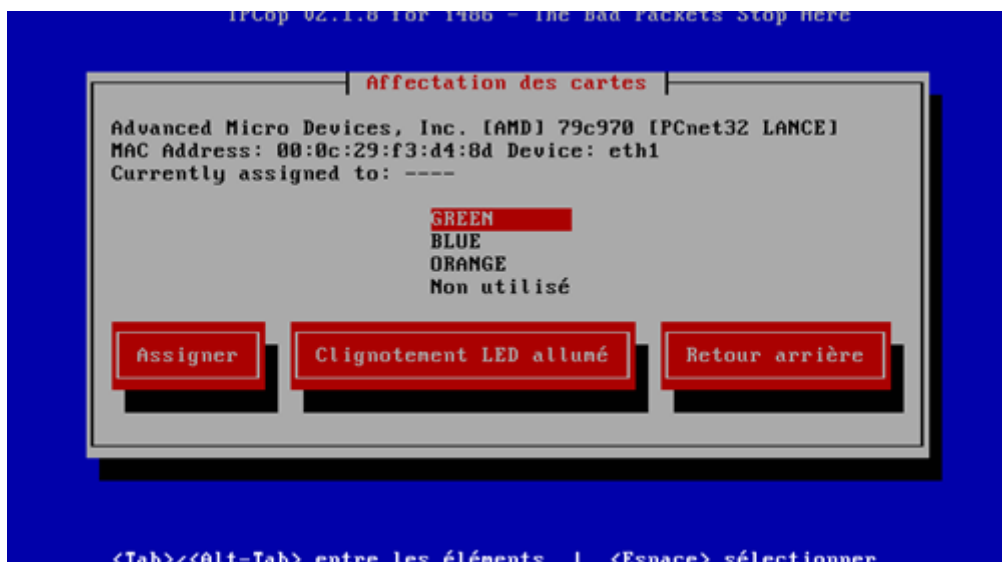


RED pour WAN



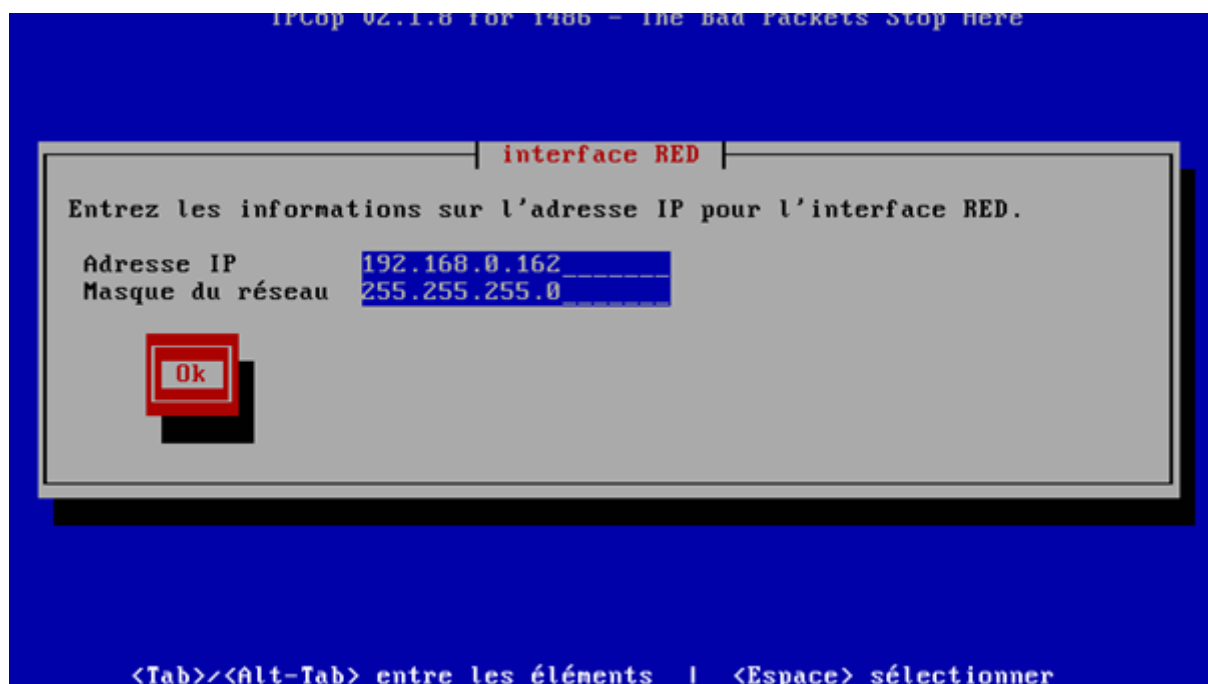


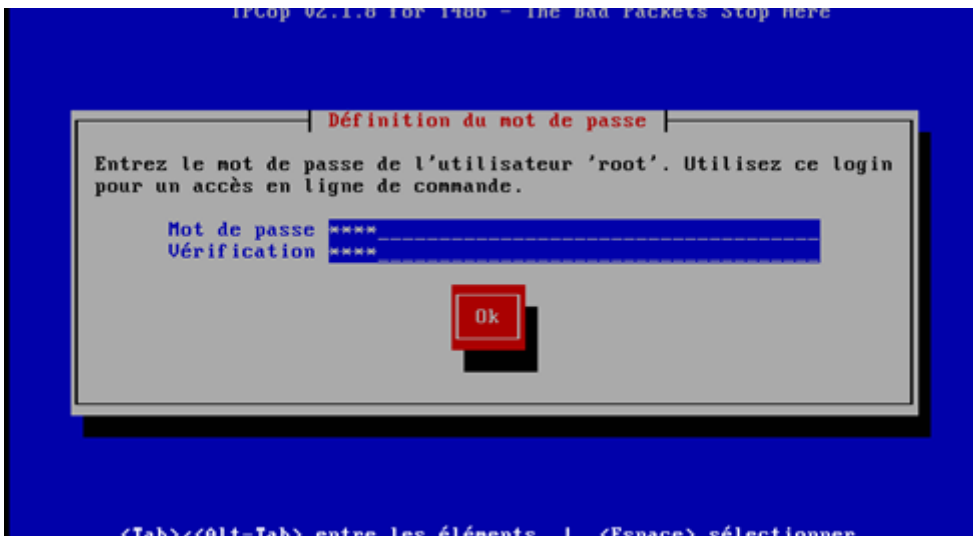
GREEN pour LAN



10.0.0.254 en 255.0.0.0 pour l'interface GREEN (LAN)

192.168.0.162 / 24 pour le Wan (RED)



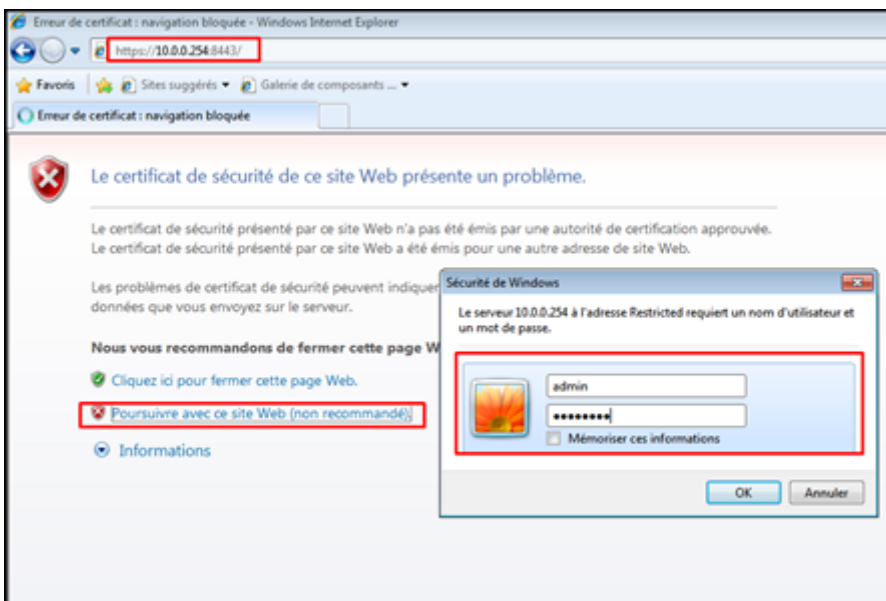


Il faut un nom d'utilisateur et mot de passe différent pour l'admin, idem pour le chiffage des sauvegardes.

IPCOP est installé et configuré !

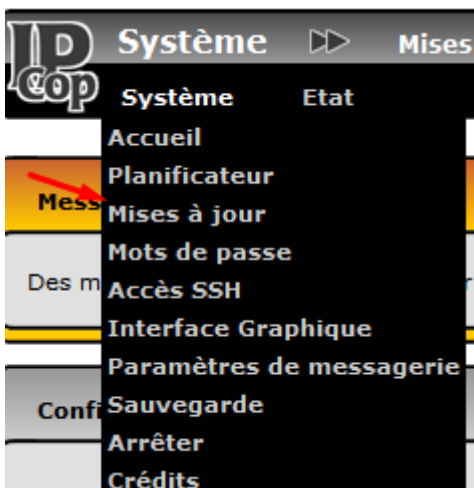
Configuration d'IPCOP

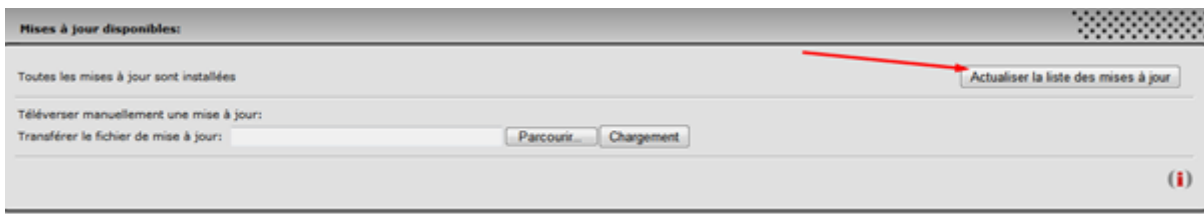
On peut se connecter en ligne de commande ou par navigateur web.



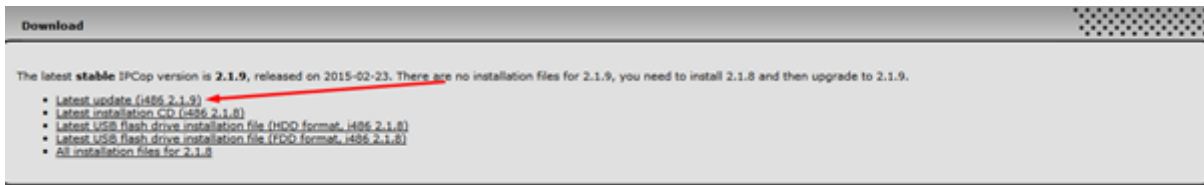


Mise à jour



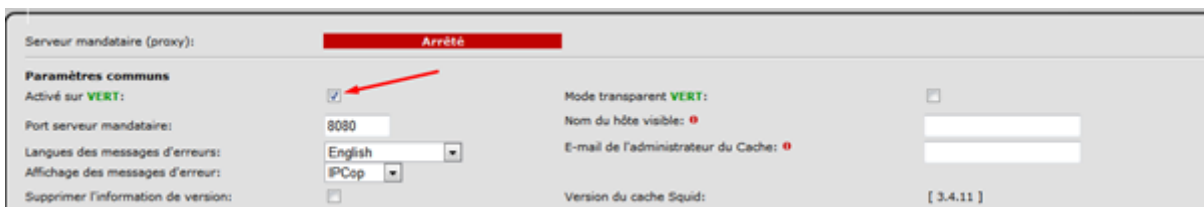


L'actualisation ne marchant pas, nous allons l'importer ici. Pour cela, on se rend sur le site d'ipcop et on télécharge la dernière mise à jour.



On la téléverse puis on l'applique.

Proxy



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

Configuration

Serveur mandataire (proxy): **Arrêté**

Paramètres communs

Activé sur **VERT**: ☒ **Mode transparent VERT**: ☐

Port serveur mandataire: **8080** **Nom du hôte visible**:

Langues des messages d'erreurs: **French** **E-mail de l'administrateur du Cache**:

Affichage des messages d'erreur: **IPCop** **Version du cache Squid**: **[3.4.11]**

Supprimer l'information de version: ☒

Serveur proxy distant

Retransmission de l'adresse du proxy: ☐ **Serveur mandataire distant (hôte:port)**:

Retransmission de l'adresse IP du client: ☐ **Nom d'utilisateur du serveur mandataire distant**:

Retransmission du nom d'utilisateur: ☐ **Mot de passe du serveur mandataire distant**:

Pas de transfert d'authentification orienté connexion: ☐

Configuration des journaux

Journaux activés: ☒ **Enregistrement des URL complètes**: ☐

Enregistrement du User-Agent: ☐

Log nom d'utilisateur: ☒

⚠ Ce champ peut être vide.

Vider le cache **Enregistrer**

On active les journaux.

Plus bas :

Options avance

Gestion du cache

Taille du cache en mémoire (MB): **4** **Taille du cache sur le disque dur (MB)**: **90**

Taille minimale d'objet (Ko): **0** **Taille maximale d'objet (Ko)**: **4096**

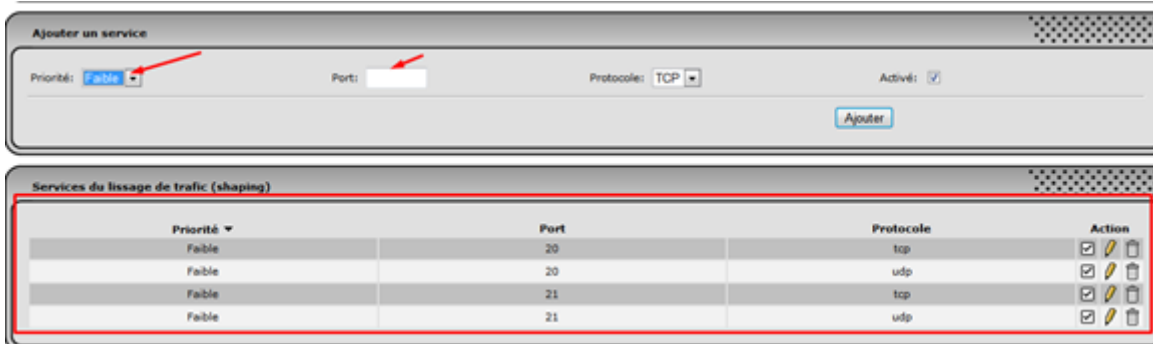
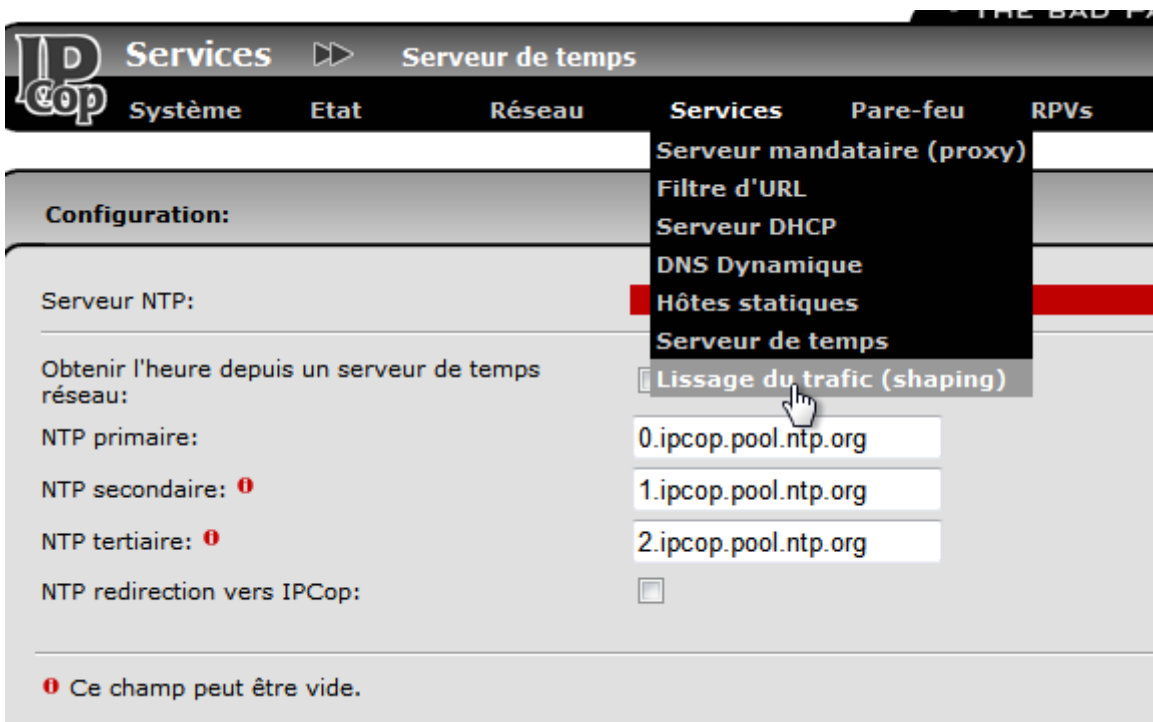
Nombre de sous-répertoire de niveau 1: **16** **Ne pas mettre en cache ces domaines (un par ligne)**:

Stratégie de gestion de la mémoire: **LRU**

Stratégie de gestion du cache: **LRU**

Mode autonome activé: ☐

Limitation du trafic FTP



Blocage du ping coté internet

```
GNU nano 2.2.6      File: /etc/rc.d/rc.firewall      Modified

/sbin/iptables -N ACCOUNT_INPUT
/sbin/iptables -A INPUT -j ACCOUNT_INPUT
/sbin/iptables -N ACCOUNT_FORWARD_IN
/sbin/iptables -A FORWARD -j ACCOUNT_FORWARD_IN
/sbin/iptables -N ACCOUNT_FORWARD_OUT
/sbin/iptables -A FORWARD -j ACCOUNT_FORWARD_OUT
/sbin/iptables -N ACCOUNT_OUTPUT
/sbin/iptables -A OUTPUT -j ACCOUNT_OUTPUT

# Fix for braindead ISP's
/sbin/iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-
/sbin/iptables -A INPUT -p icmp --icmp-type 8 -i $GREEN!DEV -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 8 -j DROP
# FW_MARK_IPSEC chain, used for marking outgoing (NETKEY) IPsec traffic
/sbin/iptables -N FW_MARK_IPSEC
/sbin/iptables -A FORWARD -j FW_MARK_IPSEC

# CUSTOM chains, can be used by the users themselves
/sbin/iptables -N CUSTOMINPUT
/sbin/iptables -A INPUT -j CUSTOMINPUT

^G Get Help  ^O WriteOut  ^W Where Is  ^U Next Page ^U UnCut Text ^I First Line
^X Exit      ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos   ^_ Last Line
```

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

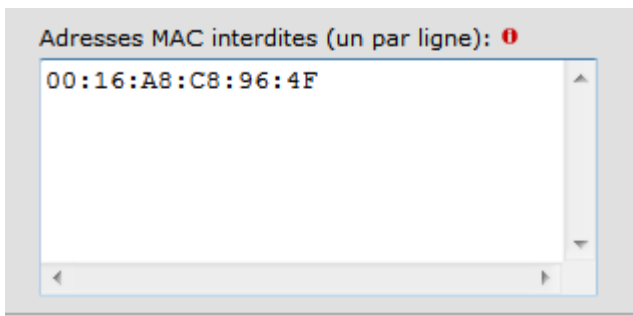
Statistiques Ping pour 192.168.0.162:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\BONNET>ping 192.168.0.162

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%),
```

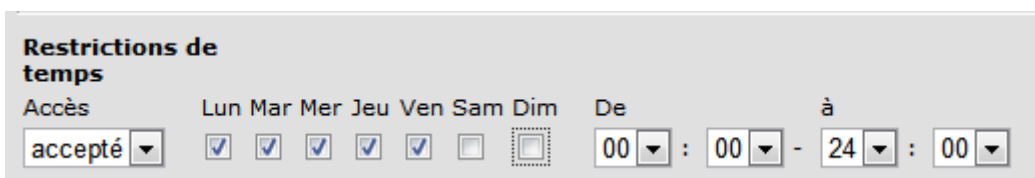
Blocage du portable

Dans services, serveur mandataire.



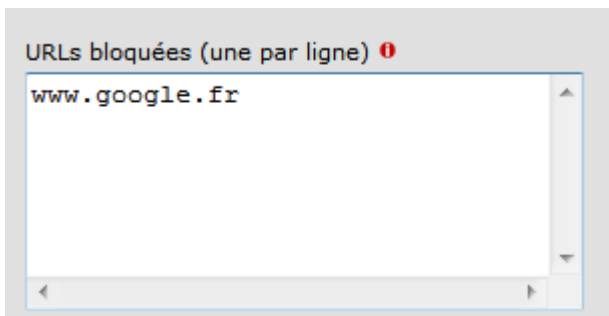
Impossible d'aller sur internet le week-end

Services, serveur mandataire

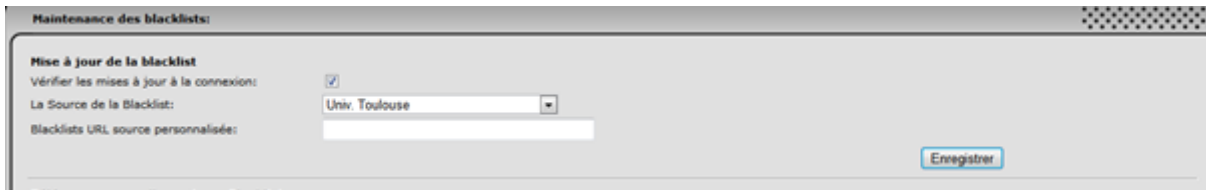


Blocage d'un site

Service, filtreur d'url

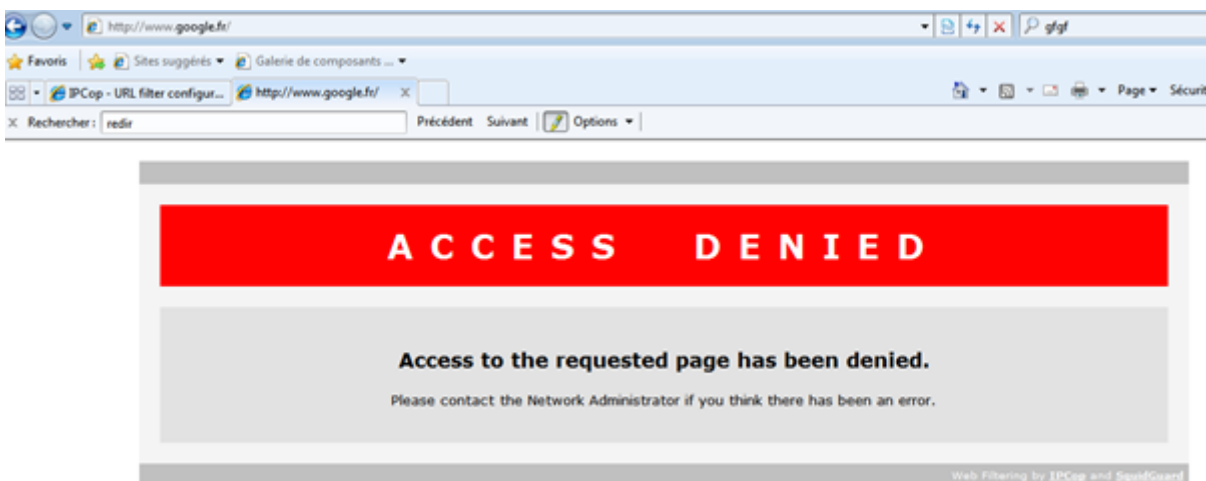


Mise en place d'une blacklist



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).