Fiche n° :4

diafor organisation

Epreuve de Pratique des Techniques Informatiques

Nom et prénom : **ALO David**

Nature de l'activité

Mise en place d'un firewall, d'un serveur mandataire et d'un filtre URL

Contexte : Plusieurs personnes de l'entreprise se permettent de naviguer sur des sites au contenu douteux. De plus, le réseau à un accès direct à Internet et des attaques quotidiennes sont repérées

Objectifs :

- Sécuriser le réseau
- Limiter l'accès à certains sites

Compétences mises en œuvre pour la réalisation de cette activité

C21	Installer et configurer un ordinateur
C22	Installer et configurer un réseau
C23	Installer et configurer un dispositif de sécurité
C31	Assurer les fonctions de base de l'administration d'un réseau

Conditions de réalisations

Matériels :	Logiciels :
- 1 serveur avec 2 cartes réseaux - 1 poste client - Un switch 5 ports 10/100 Mbps	- IPCOP 1.4.18 - Windows XP - Putty - WinSCP - Urlfilter 1.9.1
Durée : 45 mn	
Autres contraintes et difficultés : Déployer une solution tout en un qui soit facile à administrer	

Description de l'activité réalisée

Situation initiale : Il n'y a aucun dispositif dédié à la sécurisation du réseau et au contrôle de l'accès internet.

Situation finale : Le réseau de l'entreprise a désormais un réseau protégé par un pare-feu et son accès Internet est optimisé et filtré par un serveur mandataire.

I. Installation d'IPCOP

IPCOP est une distribution Linux qui permet de s'adapter à tout type d'architecture réseau. Dans un premier temps, il est donc nécessaire d'analyser le réseau existant pour qu'IPCOP soit configuré de façon cohérente.
IPCOP définit les niveaux et zones de sécurité par des codes de couleur :

GREEN : Zone correspondant au réseau local.
BLUE : Zone correspondant au réseau WIFI.
ORANGE : Zone correspondant à la DMZ.
RED : Zone correspondant à Internet.

Mettre le CD IPCOP version 1.4.18 dans le lecteur.
Au cours de cette installation, IPCOP nous propose de configurer certains paramètres plus ou moins importants que je vais détailler :

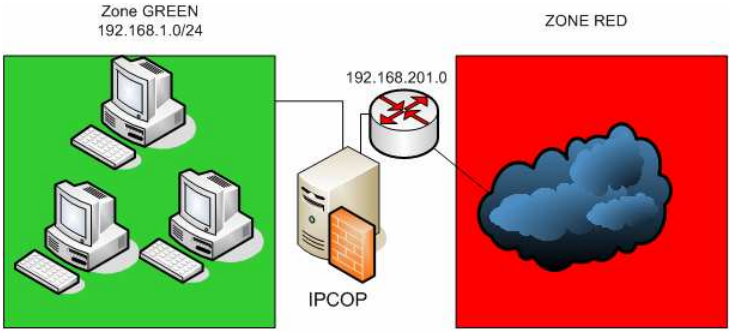
1. le langage utilisé
2. choix du support d'installation
3. choix de restauration d'une sauvegarde existante
4. configuration de l'interface GREEN (réseau local et etho en 192.168.1.1/24)
5. configuration du clavier et du fuseau horaire
6. nom netbios de la machine
7. nom du domaine
8. configuration RNIS
9. configuration du réseau avec :
   - type de configuration réseau
   - configuration de l'interface RED (Internet sur eth1 et d'adresse 192.168.201.181/24)
   - configuration du DNS et de la passerelle
   - configuration du serveur DHCP
10. les mots de passe
    - > root
    - > admin
    - > backup

Une fois tous ces paramètres enregistrés, l'ordinateur redémarre. Il sera toujours possible de changer des informations en utilisant la commande : « setup ».

Le pare-feu est opérationnel

II. Configuration du pare-feu

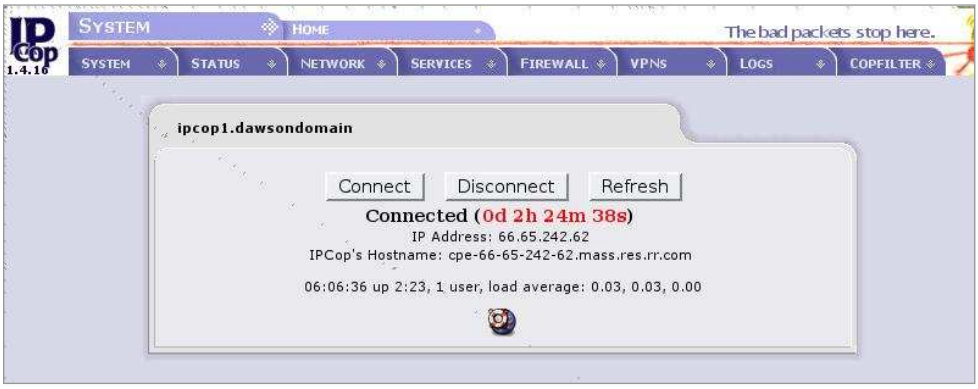
Par défaut, IPCOP autorise le passage des trames du réseau local vers Internet mais bloque les trames de l'Internet vers le réseau local.



L'interface GREEN correspond au réseau local (etho)

L'interface RED correspond à Internet (eth1)

Maintenant que IPCOP est installé, on peut faire le reste sur le PC client en travaillant à distance avec une connexion sécurisée.
Utiliser l'adresse « https://192.168.1.1:445 » dans le navigateur pour utiliser l'interface web de IPCOP.



Nous pouvons alors autoriser l'administration par SSH. Par défaut, la connexion en SSH est refusée et celle-ci s'utilise à travers un port de convention différent pour sécuriser son entrée.
Sur le PC client on tape l'adresse de l'interface GREEN dans putty :

La chaîne FORWARD nous intéresse particulièrement pour notre configuration puisque c'est elle qui autorise le transit des paquets ou non.

On bloque toutes les sorties vers Internet avec :

```
>> iptables -I FORWARD -s 192.168.1.0/24 -j DROP
```

Aucune connexion ne peut s'effectuer.

On peut ajouter quelques autorisations comme le port 80 (http).

```
>> iptables -I FORWARD -p TCP -s 192.168.1.0/24 --dport 80 -j ACCEPT
```

On peut alors accéder à un site web par le biais d'un navigateur.

Il est à noter que ces informations sont inscrites dans la mémoire cache et qu'au prochain redémarrage elles seront perdues. Pour plus de sécurité, il est préférable de les inscrire dans le fichier « /etc/rc.d/rc.firewall.local »
De plus, dans un environnement professionnel, il est souvent nécessaire d'avoir une boite mail dédiée. Il faut alors permettre le rapatriement de ces informations en ouvrant les ports adéquats. (Exemples : port 25 pour SMTP ;110 pour POP3 et 143 pour IMAP)

III. Installation et configuration d'un serveur mandataire

Afin de limiter une utilisation abusive d'Internet, on peut utiliser le proxy proposé par IPCOP.
La mise en place d'un proxy avec IPCOP est relativement simple. La configuration sur chaque poste quand à elle, est fastidieuse car il faut indiquer sur chaque navigateur comment accéder au serveur mandataire. Pour éviter cela, nous avons la possibilité d'utiliser le proxy d'IPCOP en mode transparent.
Pour obliger le passage par le proxy, on va bloquer l'autorisation de l'http dans la chaîne FORWARD.
>> iptables -L FORWARD (pour connaître le numéro de la ligne a supprimer)
>> iptables -D FORWARD $ligne
L'intérêt d'avoir un serveur mandataire est de pouvoir assurer les fonctions suivantes:

- mémoire cache ;
- la journalisation des requêtes (« logging ») ;
- la sécurité du réseau local ;
- le filtrage et l'anonymat.

Nous avons la possibilité de refuser l'accès à certains sites en utilisant un filtrage d'URL.
Téléchargeons l'addons "url-filter" à partir du PC client car nous n'en avons pas la possibilité directement avec IPCOP.
Le fichier d'installation se trouve facilement sur Internet. IPCOP ne disposant pas des outils nécessaires au téléchargement, nous le récupérons d'un poste client. Rapatrié, on l'envoie sur IPCOP par le biais de WinSCP.

Sur le pare-feu IPCOP il faut dézipper le fichier dans un répertoire et l'installer :

>> tar -xvzf url-filter.tar.gz	(détarrer le fichier)
>> cd url-filter/	(déplacement dans l'arborescence)
>> ./install	(installation d'url-filter)

Dans l'onglet
On peut maintenant refuser des domaines, des URL, des extensions, des mots clé.
Si un site n'est pas autorisé, l'utilisateur est prévenu que l'accès est restreint et qu'il peut contacter l'administrateur.

Analyse des résultats obtenus
Objectif atteint : Le réseau est totalement sécurisé dans les 2 sens. De plus, les utilisateurs passent par un proxy dont ils n'ont connaissance que lorsqu'ils veulent visiter des sites « sensibles ». .
Bilan de l'activité : Le réseau est sécurisé. Aucune entrée n'est possible, et les sorties sont limitées.