

Licence Professionnel ASRALL
Projet tuteuré.

Ufwi

Sommaire

1	Introduction	3
2	Liste des solutions de pare-feu par identification	4
3	Externalisation des logs dans une BD MySQL	5
4	Daemon ufwi-authd	7

1

Introduction

Début du doc de Ufwi

2

Liste des solutions de pare-feu par identification

Les pare-feu par identification les plus connus :

- AuthPF : Fonctionne sous OpenBSD et qui se repose sur SSH pour l'identification des utilisateurs : <http://www.openbsd.org/faq/pf/authpf.html>
- NuFW : projet ayant donné naissance à UFWI suite à la liquidation de l'éditeur "EdenWall Technologies"
- Cyberoam : pare-feu entièrement basé sur l'identification, en utilisant une corrélation entre adresse MAC et utilisateur : <http://www.cyberoam.com/fr/firewall.html>
- CheckPoint (NAC Blade) : utilisation des règles de filtrage en fonction d'une authentification basée sur Kerberos, l'identité de son poste et du niveau de sécurité du poste (mise à jour de sécurité / antivirus) : <http://www.cyberoam.com/fr/firewall.html>

3

Externalisation des logs dans une BD MySQL

Configuration du serveur BD

Installation des paquets :

```
apt-get install apache2 php5 mysql-server nolog
```

Configuration de la passerelle :

Configuration IP :

```
ifconfig eth0 192.168.1.137/24 ifconfig eth1 172.20.8.1/24
```

Installation des paquets :

```
apt-get install ulogd ulogd-mysql
```

Correction d'un bug : ajout d'une ligne dans le script de démarrage qui va charger un module

```
nano /etc/init.d/ulogd export LD_PRELOAD = /usr/lib/libmysqlclient.so.16
```

Configuration de ulogd : modification de son fichier de configuration

```
nano /etc/ulogd.conf
```

Décommenter la ligne 46 (pour charger un module supplémentaire)

Renseigner les informations de connexion à la base de données :

```
paragraphe «[MYSQL]» ligne 59 : table="ulog" pass="passulog" user="ulog" db="ulog" host="172.20.8.2"
```

Configuration du serveur de BD :

Configuration IP :

```
ifconfig eth0 172.20.8.2/24
```

Lister tous les fichiers installés à l'installation de nolog :

```
dpkg -L nolog | more
```

Ouvrir le fichier suivant (démarche à suivre pour créer les tables de la base de données)

```
nano /usr/share/doc/nolog/README.Debian
```

Connexion à la base de données et création de l'utilisateur (les deux programmes vont se connecter avec ce compte) :

```
mysql -u root -p create database ulog; create user 'ulog'@'%' identified by 'passulog'; grant all privileges on ulog.* to ulog; exit
```

Commandes de création de la base :

```
cd /usr/share/doc/nolog/scripts gunzip ipv4.sql.gz cat ipv4.sql | mysql -uulog -p ulog
```

Modification du fichier de configuration de mysql

```
nano /etc/mysql/my.cnf ligne 47
```

Il faut qu'il écoute sur l'interface 172.20.8.2

```
bind address= "172.20.8.2"
```

Renommer les fichiers de configuration :

```
cd /etc/nulog cp default.core.conf core.conf cp default.nulog.conf nulog.conf cp default.wrapper.conf wrapper.conf
```

Renseigner les informations de connexion à la base de données :

```
nano core.conf host=localhost db=ulog user=ulog password=passulog table=ulog
```

Prise en compte des changements : redémarrage de services Sur la passerelle :

```
/etc/init.d/ulogd restart
```

Sur le serveur :

```
/etc/init.d/ulogd restart
```

On choisit ce que l'on veut loguer avec iptables

4

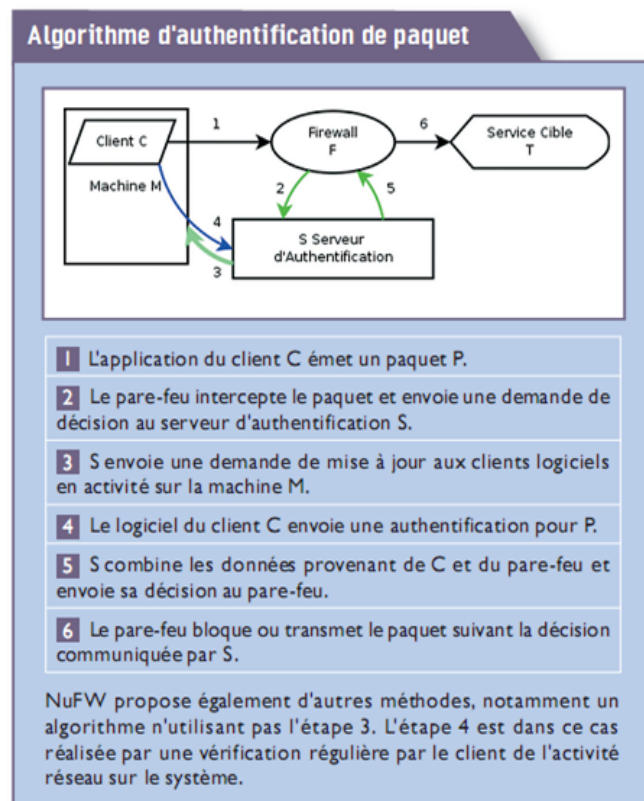
Daemon ufw-authd

Introduction

Nuauth command est une interface qui permet de contrôler des fonctions importantes du daemon authd, comme l'obtention de la liste des utilisateurs connectés par exemple. Chaque fois qu'un client envoie un paquet(1) pour commencer une connexion à travers la passerelle, la station cliente envoie un paquet(2) d'identification au daemon authd. Le pare-feu de la passerelle met en file d'attente le paquet et envoie directement des informations au daemon authd.

Le travail du daemon va être d'analyser les deux paquets (1) et (2) et de vérifier si le client a le droit d'initialiser la connexion qu'il demande. Si ufw-authd indique que le paquet(1) est autorisé alors la connexion est initialisée, sinon la connexion est annulée. Ufw-authd peut aussi utiliser un serveur LDAP pour la définition des utilisateurs et groupes.

Ci-dessous le un schéma montrant le processus d'authentification utilisé par NuFW, resté inchangé avec UFWI :



Intallation

Pré-requis :

Script autogen.sh :

- version automake1.7

Compilation Nufw :

- GNU libtool
- GNU make
- libpam-dev
- glib 2.4+
- libipq (iptables-dev pour debian) ou libnetfilter queue
- libldap
- libsasl2
- libgnutls
- libgcrypt

Noyau :

Il est recommandé d'utiliser un noyau récent afin de bénéficier de toutes les dernières nouveautés implémenter dans ce dernier. Une version de noyau supérieur à 2.6.18 est un bon choix. Le patch dump-connection-mark.diff (disponible dans patches/) peut être appliqué au noyau afin d'améliorer les performances de ce dernier lorsque nous utiliserons le log de session.

Compilation :

La compilation du daemon est relativement simple, elle se déroule en quatre étapes :

- Lancement du script ./autogen.sh
- Exécution de ./configure
- make
- Et pour finir make install

Lors de la première installation, il faut penser à copier le fichier de configuration avec la commande suivante :

```
cp ./conf/nuauth.conf /usr/local/etc/nuauth.conf
```

Quelques commandes liées au daemon

Commandes principales :

- quit : déconnexion
- refresh cache : rafraichit tous les caches
- reload : recharge la configuration du daemon d'authentification

Information :

- help : affiche la liste des commandes utilisables
- version : affiche la version du daemon
- uptime : affiche depuis combien de temps tourne le daemon

Gestion des utilisateurs :

- users : affiche els utilisateurs connectés
- disconnect all : déconnecte tous les utilisateurs
- disconnect ID : déconnecte un utilisateur grâce à son identifiant (ID)