Direction des systèmes d'information	**Date : 1/12/09** **Version : V 1** **Etat : ~~travail / vérifié~~ / validé** **Rédacteur : CMF/JCF** **Réf. : CNRS/DSI/ parefeuFTP_Manuel_Installation_Et_Utilisateur_v1 0 .doc** **Annexes :**

Manuel d'installation et d'utilisation de l'outil parefeuFTP

Objet du document : Ce document décrit les étapes d'installation et configuration de l'outil parefeuFTP (filtrage des connexions ftp sur une machine de communication).

Table des évolutions

Date	Version	Détail des évolutions
1/12/09	1.0	Version initiale

Sommaire

1 Introduction

L'outil parefeuFTP permet de filtrer les accès FTP aux machines de COM « GRAAL » en :

- permettant aux sites XLAB utilisateurs de se connecter.
- se prémunissant d'une attaque de type force brute sur un compte FTP, même d'un site répertorié XLAB.
- se prémunissant d'un « spoofing » d'adresse IP et tentative d'accès par force brute.

Ce document est composé de 2 parties :

- Une partie qui détaille l'installation et la configuration de l'outil « parefeuFTP » sur une machine MCOM
- Une partie qui détaille les fonctions des différents processus pris en charge par l'outil.

2 Installation et configuration

2.1 Installation

L'installation est faite par sosipatch dans le répertoire /**opt/parefeuFTP**

Le script crée le répertoire d'installation pour y décompresser l'arborescence de l'outil parefeuFTP comprenant les répertoires, les **scripts Perl** et les modules spécifiques utilisés.

Il place également sous /**etc/init.d, le script parefeuFTP** qui prend les paramètres stop, start et status. Un lien symbolique est également créé sous /etc/rc5.d et /etc/rc0.d pour permettre le démarrage et l'arrêt automatique du processus de bannissement au boot de la machine, ainsi que la lecture automatique des règles Netfilter au boot du serveur.

Enfin, une entrée est ajoutée à la crontab de root pour permettre :

- une collecte régulière (par défaut tous les jours à 08:00 le matin)
- une supervision régulière (par défaut tous les vendredi à 12:00)

2.2 Configuration

Elle est effectuée par l'équipe SSI.

2.2.1 Variables à configurer

Les variables paramétrables se trouvent dans le fichier **`(/opt/parefeuFTP/conf/parefeuFTPconfig.pl`**

Editer ce fichier et modifier les variables suivantes :

- **`$serveurSMTP :`** mettre l'adresse IP du routeur SMTP pour l'envoi des méls aux destinataires (en général, le graal de la DR).

- **`$expediteur :`** cette variable permet de paramétrer le nom de l'expediteur (from) qui apparaît dans les méls envoyés par l'outil. Par défaut cette variable vaut

`"parefeuFTP\@dsi.cnrs.fr"` mais vous pouvez spécifier n'importe quelle chaine de votre choix (par exemple `"filtrage\@graal"`, etc …).

- `@listeDestinataires` : mettre la liste des adresses méls des destinataires de l'outil séparées par des virgules. Par exemple : `@listeDestinataires = [ "jean.dupont\@dsi.cnrs.fr", "francois.martin\@dsi.cnrs.fr" ]`

ATTENTION au "\" devant le "@" dans l'adresse mél pour éviter toute interprétation par le code Perl.

REMARQUE : il s'agit d'une variable de type tableau, donc vous pouvez préciser une (dans ce cas pas de virgule séparatrice) ou plusieurs adresses. Vous pouvez aussi donner une adresse correspondant à une liste de distribution pour en simplifier l'administration.

- `$modePassifPortMin, $modePassifPortMax` : ces variables correspondent à la plage de ports utilisée par le mode FTP passif. En principe vous utilisez la plage 19000 -> 19100. Si ce n'est pas le cas, positionnez les valeurs correspondant au serveur FTP de la machine.

- `$vsftpdLog` : en principe les logs du serveur vsftpd sont sous /var/log/vsftpd.log. Si ce n'est pas le cas, modifier la variable en conséquence.

- `$maxTentativeEchec, $delaiTentiveEchec` : ces variables correspondent au paramètres pour le « bannissement » d'une adresse IP qui effectuerait des erreurs de connexion FTP répétées.

Il n'est pas nécessaire de modifier les autres variables.

3 Utilisation de l'outil parefeuFTP

3.1 Stratégie de mise en place du filtrage

L'utilisation de l'outil parefeuFTP s'inscrit dans une stratégie de mise en place de filtres IP sur les flux FTP qui se décline en **deux phases** :

1- **la phase de collecte** : récupération des adresses IP provenant de connexions FTP réussies dans les journaux vsftpd.

Cette phase a une durée à définir par l'administrateur du site (1 à 2 semaines)

Elle se termine par la mise en place du filtre : initialisation des règles NetFilter avec les adresses IP "collectées".

2- **la phase de production** au cours de laquelle :

- des adresses (ou classes d'adresses) pourront être manuellement ajoutées, supprimées
- des adresses seront automatiquement refusées (adresses IP ayant initié plusieurs connexions FTP en échec dans un intervalle de temps donné).

3.1.1 La phase de « collecte »

Pendant cette phase, l'outil analyse les logs du serveur FTP et récupère les adresses IP ayant effectué des connexions correctes pour alimenter un fichier « collecte ». Cette phase est réalisée automatiquement chaque jour (par planification dans la crontab de root) et envoie un mél à l'issue de chaque exécution.

Chaque mél indique si :

- De nouvelles adresses méls ont été collectées. Dans ce cas, cela signifie que vous avez de nouveaux clients FTP qui se connectent à la machine de MCOM depuis de nouveaux postes PC.
- Aucune nouvelle adresse IP n'a été trouvée. Si ce message apparaît régulièrement c'est que vous avez probablement déjà collectés pratiquement toutes les adresses IP qui se connectent à la machine de MCOM. Vous pouvez dans ce cas passer à la phase suivante (mise en place du filtre initial).

3.1.2 La phase d'initialisation du filtre FTP

Cette phase permet la mise en place des règles de filtrage IP sur les flux FTP en partant des adresses IP récupérées pendant la phase de « collecte ».

Une sauvegarde des filtres déjà créés est effectuée avant la mise en place des nouvelles règles.

Pendant cette phase, l'outil effectue les tâches suivantes :

- Identification des règles déjà présentes sur FTP pour information
- Mise en place des nouvelles règles selon la stratégie suivante :
  - Toutes les adresses IP collectées sont autorisées sur les ports FTP
  - Toutes autres adresses IP sont refusées sur les ports FTP
  - Tous les autres ports (non FTP) sont autorisés ou continuent de fonctionner selon les règles déjà en place.

3.1.3 La phase de bannissement

Dès que le processus est démarré (après un reboot du serveur ou par lancement manuel), il scrute en permanence les logs du serveur FTP à la recherche d'une adresse IP qui ne parvient pas à se connecter correctement au serveur FTP. Si cette adresse IP rentre dans les critères dits de « bannissement » (plus de x echecs dans un intervalle de temps), elle est automatiquement refusée au niveau des filtres IP sur les ports FTP.

Cette phase permet d'éviter les « Deny Of Service » qui peuvent être préjudiciables aux utilisateurs légaux du service.

Un mél est envoyé pour informer du bannissement d'une adresse.

Vous avez toujours la possibilité de réintégrer une adresse après un bannissement (cas d'erreurs répétées d'un utilisateur distrait …) ou d'ajouter de nouvelle adresses IP qui n'ont pas été récupérées pendant la phase de collecte (voir les commandes au chapitre 3.3)

3.2 Le script /etc/init.d/parefeuFTP

Ce script a pour rôle d'arrêter ou démarrer le processus de bannissement. Il est appelé automatiquement après un boot de la machine graal, ou bien lors d'un arrêt (shutdown, reboot, etc …).

On peut aussi l'appeler manuellement (par exemple après la première installation) pour éviter de rebooter le serveur pour cette seule raison.

Dans ce cas, exécuter en tant qu'utilisateur root :

`service parefeuFTP start` (= démarre le processus de bannissement)

`service parefeuFTP stop` (= arrête le processus de bannissement)

`service parefeuFTP status` (= donne l'état d'exécution du processus de bannissement)

Ce script n'a pas pour rôle d'arrêter ou démarrer le filtrage IP. Cette fonction est assurée par l'outil Netfilter (iptables) qui est un firewall intégré au noyau Linux sur les distributions Red Hat.

Si vous avez besoin d'arrêter le filtrage, il faut aller au chapitre 3.4 qui décrit comment restaurer une ancienne configuration des iptables.

3.3 Le script parefeuFTP.pl

Le script s'exécute en tant que root.

Les différents commutateurs :

`/opt/parefeuFTP/parefeuFTP.pl -version`

Exemple : `/opt/parefeuFTP/parefeuFTP.pl -version`

affiche la version du script.

`/opt/parefeuFTP/parefeuFTP.pl -man`

Exemple : `/opt/parefeuFTP/parefeuFTP.pl -man`

affiche la syntaxe d'appel du script avec les différents commutateurs possibles.

`/opt/parefeuFTP/parefeuFTP.pl -collecte`

Exemple : `/opt/parefeuFTP/parefeuFTP.pl -collecte`

récupère les adresses IP provenant de connexions FTP réussies dans les journaux vsftpd et les place dans un fichier CSV avec un état « collecte ». Ce fichier sert ensuite au processus de mise en place des filtres iptables initiaux. Après chaque collecte, un mél est envoyé aux destinataires avec en attachement le fichier CSV. Il est possible d'y ajouter des entrées manuellement.

`/opt/parefeuFTP/parefeuFTP.pl -initFiltre [-preview]`

Exemple : `/opt/parefeuFTP/parefeuFTP.pl -initFiltre`

initialise les règles NetFilter avec les adresses IP "collectées" (mode prévisualisation optionnel). Le mode prévisualisation affiche à l'ecran les règles ajoutées, ainsi que les impacts potentiels avec des règles déjà en place pour les ports FTP.

En cas de mise en place d'un nouveau filtre, un mél est envoyé avec les nouvelles règles iptables.

/opt/parefeuFTP/parefeuFTP.pl -autorise <IP / classe IP>

Exemple : /opt/parefeuFTP/parefeuFTP.pl -autorise 192.168.1.27/24

modifie les règles NetFilter pour autoriser l'accès aux ports du serveur FTP à l'IP ou la classe IP

- l'adresse IP doit avoir le format IPv4 xx.xx.xx.xx
- la classe IP doit avoir le format IPv4 xx.xx.xx.xx/nn

où nn est le chiffre décimal des bits à 1 du masque de réseau

ce processus peut être appelé manuellement pour autoriser une nouvelle IP ou classe IP. Sinon il est appelé par le processus de mise en place des filtres iptables initiaux.

Un mél est envoyé pour informer de la nouvelle autorisation (sauf s'il s'agit d'une IP « collectée » afin de ne pas spammer les boites aux lettres).

/opt/parefeuFTP/parefeuFTP.pl -refuse <IP / classe IP>

Exemple : /opt/parefeuFTP/parefeuFTP.pl -refuse 192.168.1.27/24

modifie les règles NetFilter pour refuser l'accès aux ports du serveur FTP à l'IP ou la classe IP

- l'adresse IP doit avoir le format IPv4 xx.xx.xx.xx
- la classe IP doit avoir le format IPv4 xx.xx.xx.xx/nn

où nn est le chiffre décimal des bits à 1 du masque de réseau

ce processus peut être appelé manuellement pour refuser une nouvelle IP ou classe IP. Sinon il est appelé par le processus de bannissement décrit plus bas.

Un mél est envoyé pour informer du nouveau refus.

/opt/parefeuFTP/parefeuFTP.pl -bannissement

Exemple : /opt/parefeuFTP/parefeuFTP.pl -bannissement

démarre la fonction de bannissement qui scrute en permanence les connexions FTP en échec dans un intervalle de temps et modifie les règles NetFilter en refusant de nouveaux accès pour les adresses IP qui crént ce type de connexion (système anti "spoofing"). Cette fonction est normalement exécutée en tâche de fond et démarre automatiquement au boot du serveur.

/opt/parefeuFTP/parefeuFTP.pl -arretBannissement

Exemple : /opt/parefeuFTP/parefeuFTP.pl -arretBannissement

arrête la fonction de bannissement. Cette option peut-être appelée manuellement ou au shutdown de la machine.

/opt/parefeuFTP/parefeuFTP.pl -supervision

Exemple : /opt/parefeuFTP/parefeuFTP.pl –supervision

récupère les logs des différents processus, les historise et les réinitialise. En principe cette fonction est planifiée en crontab de root, mais peut aussi être appelée en ligne de commande.

Remarques sur le fonctionnement de l'outil :

- Les comptes utilisateurs absents de /etc/vsftpd.user_list n'apparaissent pas en échec de login dans les logs du serveur FTP. Ceci signifie que si des adresses IP autorisées utilisent de mauvais login de connexion, il ne pourra pas y avoir de bannissement automatique.
- Tous les processus (collecte, initFiltre, autorise, refuse, bannissement, supervision) utilisent des verrous pour garantir leur unicité d'exécution et d'accès aux ressources. Ces verrous sont des fichiers qui portent le nom du processus et se trouvent sous `/opt/parefeuFTP/verrous`. En cas d'arrêt brutal ou d'incident d'exécution, vous pouvez être amené à supprimer manuellement un fichier verrou pour pouvoir relancer un processus donné :

  `rm /opt/parefeuFTP/verrous/<nomDuFichier>`

3.4 Utilisation des commandes natives « iptables » (Netfilter)

3.4.1 Sauvegarder ou restaurer la configuration « iptables »

A chaque modification (autorise ou refuse) l'outil parefeuFTP va automatiquement sauvegarder l'ancienne version des iptables dans un fichier qui se trouve sous :

`/opt/parefeuFTP/sauvegardes`

Le fichier de sauvegarde porte un nom de la forme :

`iptables-save.<JourMoisAnHeureMinutesSecondes_De_la_Modification>`

Pour les trier rapidement, utiliser la commande :

```
# ls -ltr /opt/parefeuFTP/sauvegardes
```

Remarque : L'outil n'intègre pas de fonction de purge de ces fichiers. Vous êtes libre de les purger selon vos critères.
Par exemple sur un critère temporel (purge les fichiers de plus de 6 mois) :

```
# find /opt/parefeuFTP/sauvegardes -mtime +180 -exec rm -f {} \;
```

si vous voulez restaurer une ancienne configuration des iptables à partir d'un de ces fichiers , il faut exécuter en tant que root la commande :

```
# /sbin/iptables-restore < /opt/parefeuFTP/sauvegardes/iptables-save.<date>
```

Remarque : une sauvegarde d'origine des iptables est effectuée en plus par le processus « initFiltre » dans le fichier **`/etc/sysconfig/iptables.ori`**

3.4.2 Interventions manuelles sur les règles iptables

En principe l'outil parefeuFTP se charge de gérer les règles iptables pour les flux FTP. Cependant, en cas de besoin d'intervention manuelle, les commandes suivantes (à exécuter avec le compte root) peuvent être utiles.

Sauvegarder la table actuelle pour qu'elle soit remise en place après un reboot :

```
# iptables-save > /etc/sysconfig/iptables
```

Supprimer toutes les règles iptables (« flush ») :

```
# iptables -F
# iptables-save > /etc/sysconfig/iptables
```

Supprimer une règle :

- Afficher les numéros des règles : `# iptables -L --line-numbers`
- Supprimer la règle numéro *num* : `# iptables -D INPUT num`

Attention refaire un `iptables -L --line-numbers` à chaque fois car les numéros de règle sont modifiés.