Configuration du mail

Postfix

Sur postfix il faut modifier les ports d'entrées et de sorties ! Il ne faut pas utiliser le même port pour communiquer avec les MUA que pour communiquer avec MTA/MDA. On veut utiliser le port 25 pour communiquer entre server et le port 587 pour communiquer avec les clients.
Pour cela on fait :

On décommente la ligne : `submission inet n - n - - smtpd` dans **master.cf**. Cela permet d'activer le port 587 en soumission (submission). Mais le problème est que on peut toujours communiquer et envoyer des mails sur ce port.

On veut modifier les interfaces autorisées à envoyer des mails, en revanche avec notre configuration actuelle il ne faut rien changer car on ne peut pas isoler depuis **infra** nos machines de l'extérieur. On veut aussi empêcher les erreurs et se simplifier la vie en autorisant simplement **ipv4**. On veut que les serveurs nous disent bonjour donc on va obliger ces dernier à commencer par **HELO**

```
postconf -e inet_interfaces=all
postconf -e inet_protocols=ipv4
postconf -e smtpd_helo_required=yes
```

Tout le monde peut communiquer avec notre serveur de mail malheureusement.

On veut aussi paramétrer `mynetworks` on veut uniquement mettre les adresses nous appartenant, ces adresses auront plus de privilèges que celles qui n'y sont pas. En revanche sans modifications supplémentaires, rien n'interdit les clients extérieurs à communiquer avec notre serveur.

```
postconf -e mynetworks="127.0.0.0/8" + reseau_interne
```

Il ne faut pas oublier de rajouter aussi les réseaux interne. (100.120.0.0/24 pour isp-a par exemple)

On doit aussi modifie `mydestination` pour éviter d'être un openrelay.

Dans **main.cf** on rajouter ces configurations la :

```
mydestination = isp-a.milxc, $myhostname, hash:/etc/postfix/access
mua_sender_restrictions = reject_unlisted_sender
mua_client_restrictions = permit_mynetworks, reject
```

`reject_unlisted_sender` regarde dans `mydestination` ce qu'il doit autoriser. On va alors rajouter un fichier pour définir les noms de domaines autorisés. On autorise uniquement les noms de domaines listés dans `/etc/postfix/access`. Le fichier contient simplement la ligne ci-dessous :

```
isp-a.milxc OK
```

Il ne faut pas oublier de faire : `postmap /etc/postfix/access`

Dans master.cf :

```
submission inet n - n - - smtpd
  -o smtpd_client_restrictions=$mua_client_restrictions
  -o smtpd_sender_restrictions=$mua_sender_restrictions
```

On peut maintenant envoyer des mails directement au serveur sur le port 587 que depuis le réseau interne ! On peut toujours usurper le nom de domaine et nous n'avons pas sécurisé le port 25. On pourrait sécuriser le port 25 avec **postfix** mais on va le faire indirectement avec **SPF**.

SPF

Maintenant que notre serveur est presque bien configuré, nous allons configuré **SPF** pour augmenter encore la sécurité. **SPF** est utile pour vérifier qu'un mail utilise un nom de domaine qu'il a le droit d'utiliser. Pour cela, on implémente une politique SPF qui va associer un nom de domaine et des adresses IP. Ainsi, si un mail comportant le nom de domaine **target.milxc** est utilisé, on va vérifier en regardant la politique SPF que celui qui envoie est bien autorisé par cette dernière.

On va utiliser **policyd-spf** en python, il faut l'installer avant la suite.

On rajoute cette ligne dans **master.cf** :

```
policyd-spf  unix  -       n       n       -       0       spawn
    user=policyd-spf argv=/usr/bin/policyd-spf
```

Et on modifie **main.cf** comme ci dessous :

```
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
   reject_unauth_destination,
   check_policy_service unix:private/policyd-spf
```

On modifie le fichier de zone en rajoutant simplement cette ligne. Et il faut restart **nsd**.

```
IN TXT "v=spf1 mx -all"
```

À la fin de toutes ces manipulations, nous avons les fichiers suivants :

```
---
/etc/postfix/main.cf
---
...
mynetworks = 127.0.0.0/8, 100.80.0.0/16
mydestination = target.milxc, $myhostname, hash:/etc/postfix/access
inet_interfaces = all
inet_protocols = ipv4
smtpd_helo_required = yes
policyd-spf_time_limit = 3600
mua_sender_restrictions = reject_unlisted_sender
mua_client_restrictions = permit_mynetworks, reject
smtpd_recipient_restrictions =
    permit_mynetworks,
    reject_unauth_destination,
```

```
    check_policy_service unix:private/policyd-spf
```

```
---
/etc/postfix/master.cf
---
...
smtp      inet  n       -       y       -       -       smtpd
  -o smtpd_relay_restrictions=check_policy_service,unix:private/policyd-
spf,permit
submission inet n       -       y       -       -       smtpd
  -o smtpd_client_restrictions=$mua_client_restrictions
  -o smtpd_sender_restrictions=$mua_sender_restrictions
policyd-spf  unix  -       n       n       -       0       spawn
    user=policyd-spf argv=/usr/bin/policyd-spf
```

```
---
/etc/nsd/target.milxc.zone
---
       IN  NS     ns.target.milxc.
       IN  MX  10 smtp.target.milxc.
       IN  TXT    "v=spf1 mx -all"
```