LPNHE
PARIS

Mise en place d'un proxy SSH

François Legrand

JI 2014

Introduction

LPNHE PARIS

Tentatives d'intrusion ssh très fréquentes

Environ 1000 tentatives d'intrusion/mois/serveur

Problème de « surface d'attaque »

Authentification centralisée

=> Surface d'attaque

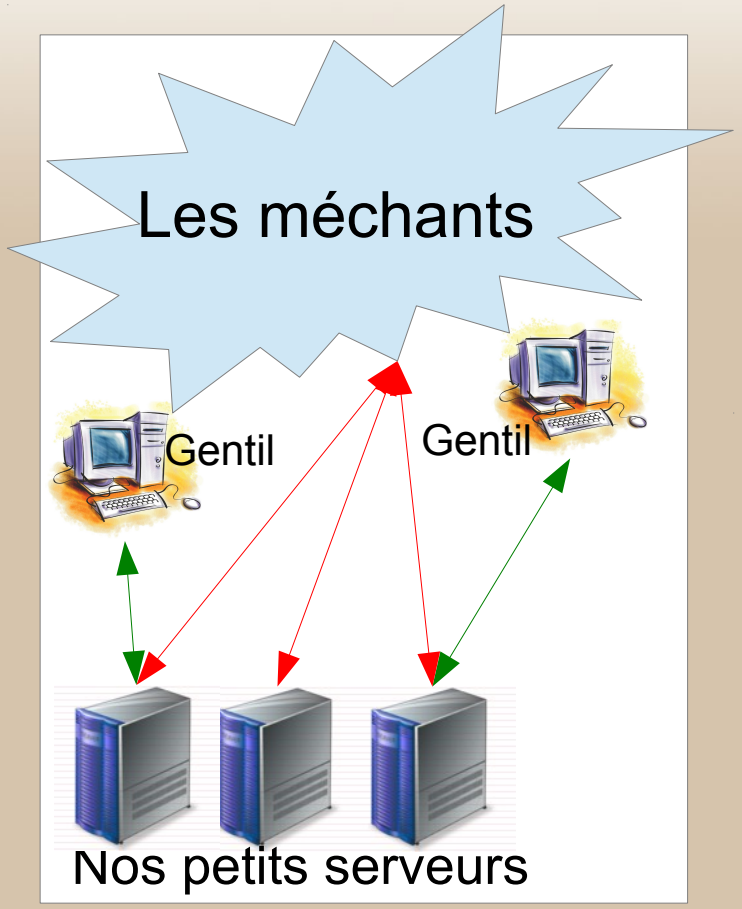
= nb de serveurs x 1000 x nb d'essais autorisé

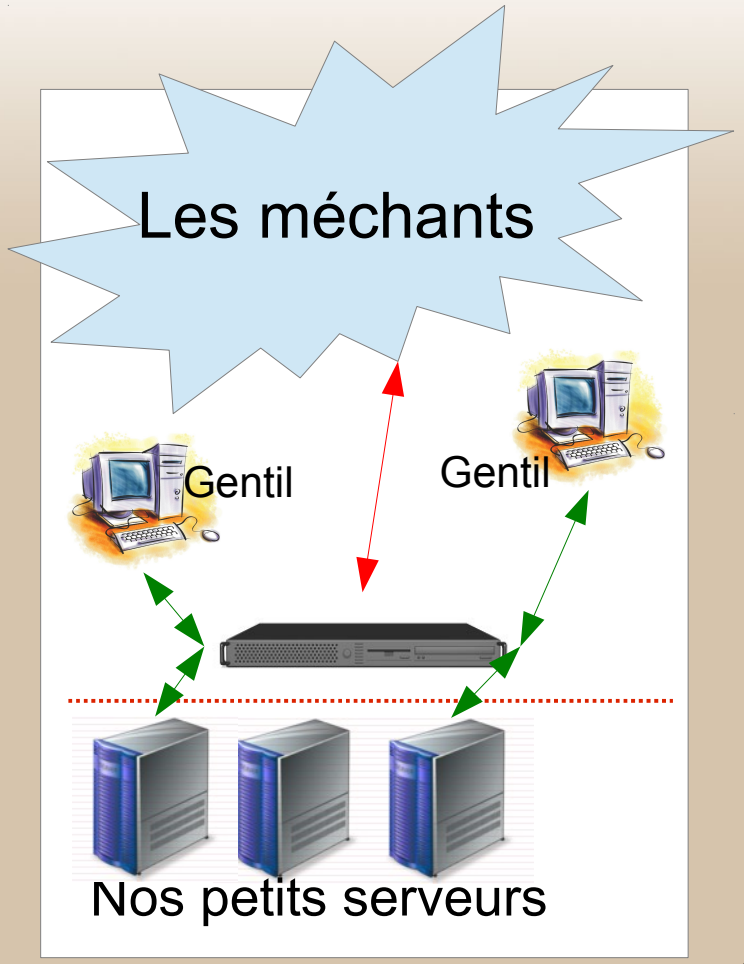
=> Un mot de passe faible peut tomber assez facilement

Objectif : Réduire la surface d'attaque

Objectifs

- **Limiter la surface d'attaque à 1 (ou 2) machines**
- **Proxy ssh**





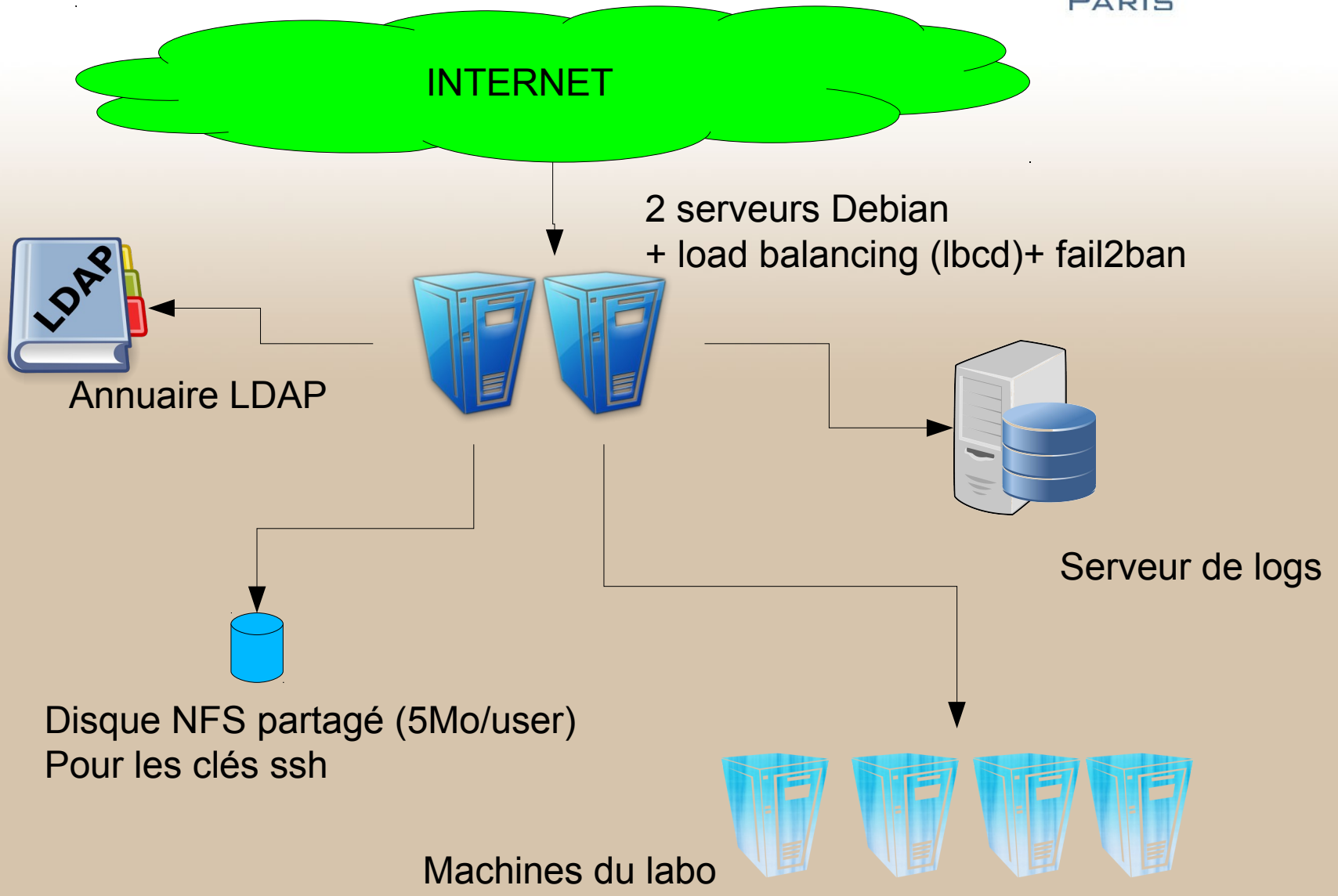
Objectif

LPNHE PARIS

Impératifs

- Pas de données sur le proxy i.e. les utilisateurs ne peuvent rien y stocker.
- Le proxy ne peut servir qu'à « rebondir »
- Pas de perte de fonctionnalités (possibilité de forward X, sftp, etc...)
- Sécurisation du serveur (fail2ban, log externes, etc...)

Architecture



Configuration

LPNHE PARIS

rbash est mon ami

- rbash pour « restricted bash » → on définit les commandes accessibles dans /usr/rbin en créant des liens logiques vers les commandes souhaitées

```
ln -s /usr/bin/ssh /usr/rbin/ssh
ln -s /usr/bin/scp /usr/rbin/scp
ln -s /bin/nc /usr/rbin/nc
```

- Protection « naturelle » contre les failles de bash (car les commandes env ou bash ne sont pas accessibles) !
- On force les « users normaux » à rbash et on autorise le bash standard aux admins (dans /etc/ldap.conf et /etc/profile)
- Fail2ban et jail recidive

→ Détails dans le poster dynamique

Utilisation

- Accès ssh (double ssh)

```
ssh -t login@proxy ssh login@serveur
```

- Simplifier les lignes de commande :

  Ajouter les lignes suivantes à ~/.ssh/config

```
Host serveur
    ProxyCommand ssh -W %h:%p login@proxy
```

  → On peut alors faire un simple ssh login@serveur

Utilisation

LPNHE PARIS

- Upload de clé ssh

```
scp authorized_keys login@proxy:/home/login/.ssh/authorized_keys
```

- Ce qui fonctionne :
  - Ssh
  - Scp
  - Rsync
  - Sshvnc
  - Double ssh avec forward des ports et socks pour accéder avec foxyproxy à un vlan interne via une machine autorisée (comprenne qui pourra)

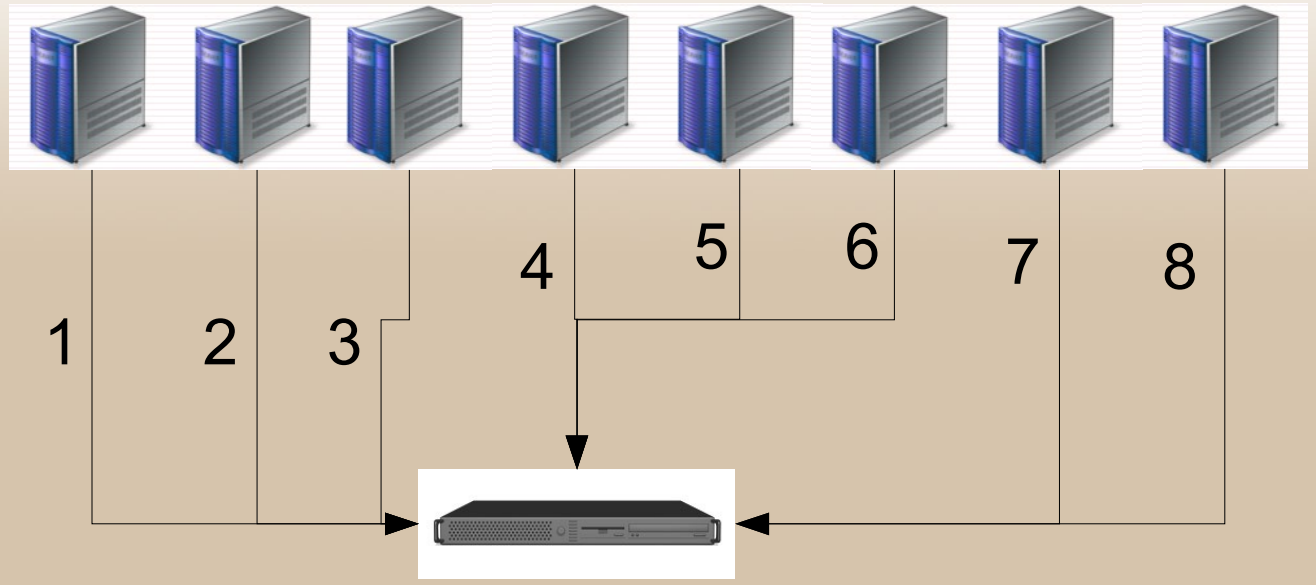
Conclusion

- Configuration mise en production depuis le mois d'avril
- Un peu de pédagogie à faire auprès des utilisateurs, mais au final, pas de soucis particulier
- Pas de perte de fonctionnalités

Allez voir le poster

Perspectives

- Ne suffit pas aux attaques « coordonnées »



Pour le fun

- Double ssh avec port forwarding
  - Objectif : On a un serveur « Vserveur » qui a accès à un vlan interne (par ex vlan d'administration). Le proxy n'a pas accès à ce vlan.

```
 ssh -f -N -D 8080 -oProxyCommand="ssh -W %h:%p proxyssh"
Vserveur
```

Ou bien

```
host Vserveur
        ProxyCommand ssh -X -t -i ~/.ssh/id_rsa -W %h:%p proxyssh
```

dans .ssh/config et on fait

```
ssh -D 8080 Vserveur
```

cf. http://superuser.com/questions/332850/ssh-as-socks-proxy-through-multiple-hosts