Utilisation d'un bastion SSH

Le passage des connexions SSH (ou SFTP) via un serveur de rebond (proxy ssh / bastion ssh / *jumphost* / *ProxyJump*) est parfois nécessaire (par exemple quand le site distant réclame les IP sources: on donne juste l'IP du bastion).

Vous trouverez ici quelques notes pour mettre en place ces connexions via un bastion SSH.

En ligne de commande

La commande est (exemple avec bastion-out.univ-nantes.fr) :

```
ssh -J nom-p@bastion-out.univ-nantes.fr login-distant@machine-distante
```

On peut aussi mettre en place une configuration dans son fichier $HOME/.ssh/config. On aura par exemple :

```
Host machine-distante
      AddressFamily inet
      User login-distant
      ProxyJump nom-p@bastion-out.univ-nantes.fr
```

La commande devient alors :

```
ssh machine-distante
```

> Les dernières version de Windows intègrent maintenant la commande native ssh dans son invite de commande.

Avec Putty

Il faut une version de Putty 0.81 (ou plus récente) pour bénéficier des fonctionnalités de machine de rebond (*jumphost*).

Dans l'exemple suivnant, on réalise une connexion vers la machine *remote.mondomaine.net* sur le port TCP/22 (SSH) avec le compte *login-distant* en utilisant le serveur de rebond *bastion-out.univ-nantes.fr* avec son compte université *nom-p*.

Créer une session pour la machine distante:

Renseigner votre login pour la machine distante:

Renseigner les paramètres du serveur de rebond (*proxy*) et le login utilisé sur ce serveur:

Ne pas oublier de retrouner dans la section *Session* et de sauvegarder la session.

Avec WinSCP

WinSCP permet le passage direct par un bastion SSH.

Exemple : on met en place une connexion SFTP vers une machine distante (adresse floutée) sur le port 50000 avec le compte distant *labxxxx* en passant par le serveur *bastion-out.univ-nantes.fr* avec son compte *nom-p*.

Création du profile de conenxion:

Renseigner les paramètres du bastion dans la section tunnel:

Valider (bouton OK) et **ne pas oublier de sauvegarder le profile**.

Lancer la connexion (bouton Connexion). Une première fenêtre apparait pour valider la clé SSH du serveur bastion-out.univ-nantes.fr. Puis WinSCP demande le mot de passe du compte nom-p sur bastion-out. Ensuite WinSCP demande à valider la clé SSH du serveur distant.

Puis enfin demande le mot de passe du compte sur le serveur distant.

Avec Filezilla au travers d'un tunnel SSH

L'outil Filezilla ne permet d'utiliser directement un serveur de rebond, il faut monter des tunnels SSH pour réaliser la connexion SFTP.

On monte d'abord un tunnel SSH via le serveur bastion qui va créer un port d'écoute de type SOCKS (ici le port 8080) :

```
ssh -N -D 8080 nom-p@bastion-out.univ-nantes.fr
```

On configure Filezilla pour utiliser un serveur mandataire générique de type SOCKS5 :

On peut alors créer la configuration pour le site distant, de type ***SFTP - SSH File Transfert Protocol***. Il faudra bien vérifier que la configuration n'ignore pas le Proxy (onglet Avancé).

Une fois l'utilisation de Filezilla terminée, on peut fermer la connexion SSH au bastion.

Usage de clés SSH

L'usage de clé SSH permet de s'affranchir de la demande de mot de passe sur les serveurs bastions de l'université (et éventuellement sur les serveurs distants si la clé publique SSH y est installée sur le compte distant).

> Les usagers de l'université peuvent télécharger leur(s) clé(s) publique(s) personnelle(s) dans leur compte en allant sur https://moncompte.univ-nantes.fr dans le rubrique *Sécurité > Clé SSH publique*.

Notes de sécurité

> Pour des questions de sécurité, il est fortement recommander de ne pas enregistrer ses mot de passe dans les profiles WinSCP ou Putty. Privilégiez l'usage de clés SSH.

> Lire aussi : Renfoncer sa configuration SSH

From:
https://wiki.univ-nantes.fr/ - **Wiki**

Permanent link:
https://wiki.univ-nantes.fr/doku.php?id=personnels:bastion-ssh

Last update: **2025/05/14 10:37**