Tunnel SSH

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les informations sont chiffrées. Il devient donc impossible de voir ce que fait l'utilisateur. La connexion est sécurisée entre le poste de l'utilisateur et le serveur. Sur tout serveur AbulÉdu (Pro ou PLM) un serveur SSH est installé. Les utilisateurs autorisés à l'utiliser sont différents et paramétrables.

Mise en place

Pour vous connecter sur l'interface d'administration de votre serveur AbulÉdu:

- **Version PRO 1.6 et AbulEdu 8.08**

Pensez avant tout à ajouter votre utilisateur dans le groupe “remotessh”, tant que l'utilisateur XXX n'est pas dans le groupe remotessh il ne pourra pas se connecter en SSH sur le serveur !

```
1) ssh identifiant@ip_du_serveur -f -N -L 8082:servecole:8082

ou

2) ssh identifiant@ip_du_serveur -f -N -L 8083:servecole:8082

ex: ssh paul.billou@serveur.dyn.abuledu.net -f -N -L 8083:servecole:8082
```

L'utilisateur “identifiant” doit être membre du groupe remotessh.

Une fois cette commande lancée vous pourrez accéder à l'administration web AbulÉdu par http://localhost:8082/ (ligne 1) ou http://localhost:8083/ (ligne 2).

- **Version PRO 1.4 et PLM 5.11**

```
ssh ip_du_serveur -f -N -L 8082:webadmin:80
```

Ensuite il faut ajouter webadmin sur la liste localhost 127.0.0.1 de votre fichier /etc/hosts. Relancez votre navigateur Web et pointez-le sur http://localhost:8082/

ATTENTION, si vous modifiez votre fichier /etc/hosts pensez à le remettre en situation “normale” après avoir administré le serveur AbulÉdu !

Libérer les ports ouverts

Pour clôturer le port 8082 ouvert à l'aide de la commande ssh ci-dessus vous pouvez tout simplement “tuer” le processus en question. Pour cela il faut travailler en deux étapes:

1. Trouver le numéro de processus qui a ouvert le port en question à l'aide de la commande “ps x”

```
ericS@plume:~$ps x
 6960 ?        Ss     0:00 ssh serveur -f -N -L 8082:localhost:8082
 6962 ?        Ss     0:00 ssh serveur_autre_ecole -f -N -L
8083:servecole:8082
```

2. lancer la commande “kill” sur les processus

```
kill 6960
kill 6962
```

Lancer des applications à distance

Pour lancer depuis chez soi des applications installées sur le serveur AbulÉdu, il est nécessaire de vérifier trois conditions :

- utiliser une distribution Linux (un Live CD Linux comme Kaella ou Ubuntu peut faire aussi l'affaire).
- être autorisé à utiliser l'accès ssh sur le serveur.
- avoir une connexion internet opérationnelle sur votre poste et sur votre serveur AbulÉdu.

Les utilisateurs d'AbulÉdu PLM sont par défaut tous autorisés à utiliser l'accès par ssh (voir la section suivante pour modifier cette option).

Les utilisateurs d'AbulÉdu PRO ne sont autorisés à utiliser cet accès que s'ils appartiennent au groupe “`remotessh`”.

Une fois face à votre distribution Linux lancée, vérifiez que votre connexion internet est bien opérationnelle. Ensuite ouvrez une console et lancez la commande :

```
ssh -XC nom_de_connexion_de_l_utilisateur@ip_du_serveur
```

Remarques

- `nom_de_connexion_de_l_utilisateur` est celui que vous utilisez sur le serveur pour vous authentifier.
- L'option X permet de lancer des applications graphiques et l'option C permet de compresser ces données pendant le transfert. Sans ces options, vous ne pourrez qu'utiliser des commandes depuis le terminal, mais ceci peut aussi être utile pour effacer, déplacer, copier des fichiers....
- Votre adresse `ip_du_serveur` peut être fixe selon votre fournisseur d'accès, modifiée toutes les 24 heures ou bien ressembler à xxx.dyn.abuledu.net si vous êtes sur un serveur PRO.

Ensuite il ne vous reste plus qu'à lancer les commandes propres à chaque application (comme `oowriter`, `abiword`...) pour les voir apparaître sur votre écran après une bonne dizaine de secondes, selon la taille de l'application. Toutefois, évitez les applications trop lourdes (vidéo...) qui

tourneraient trop lentement sur votre poste.

Si vous souhaitez lancer plusieurs applications simultanément, faites suivre votre commande du signe " &" (avec une espace entre les deux) pour retrouver la main dans la console. Par exemple :

```
associations &
```

Attention, si vous lancez une impression, elle aura lieu sur l'imprimante de votre serveur et non sur votre poste.

Une fois vos applications utilisées et fermées, tapez "exit" (ou faire Ctrl + D) dans la console pour quitter votre session SSH.

Sécuriser son serveur PLM

Par défaut, sur un serveur PLM, tous les utilisateurs sont autorisés à utiliser ce protocole, y compris root. Ceci peut être une faille de sécurité importante surtout si les mots de passe sont simples. Certains programmes (scraper) cherchent par tous les moyens à entrer sur des serveurs et tentent de forcer l'entrée en recherchant des mots de passe simples. Il est donc important de s'assurer que les mots de passe soient suffisamment complexes pour éviter ce type d'intrusions qui pourraient utiliser votre serveur.

Pour cela, il faut restreindre l'accès à votre serveur aux personnes qui en ont effectivement besoin. Leur nombre est en général limité et il convient surtout de pas autoriser root à utiliser ce protocole.

Comment faire ?

Il existe un fichier de configuration propre au serveur SSH sur votre serveur PLM qui contient certains paramètres, dont la liste des utilisateurs autorisés à se connecter au serveur.

En tant que root, éditez le fichier /etc/ssh/sshd_config (avec `gedit /etc/ssh/sshd_config` par exemple).

Modifiez la ligne contenant :

```
PermitRootLogin yes
```

en

```
PermitRootLogin no
```

Puis ajoutez à la fin, à la fin du fichier la ligne suivante :

```
AllowUsers nom_du_user1 nom_du_user2
```

où `nom_du_user1`, `nom_du_user2` sont les utilisateurs autorisés à utiliser les connexions par protocole ssh.

Ensuite toujours sous le compte root, il faut relancer le service SSH en lui faisant relire le fichier de configuration :

```
/etc/init.d/ssh reload
```

À l'avenir, y compris au prochain redémarrage, seuls les utilisateurs mentionnés pourront se connecter en ssh à ce serveur.