Agence Nationale
de la Sécurité des
Systèmes d'Information

Mémo : Mise en place de l'administration à distance des passerelles Clip

Configuration de l'accès distant via SSH sur une passerelle Clip

Mots-clés : configuration, passerelle, SSH

Table des matières

1 Pré-requis **1**

2 Mise en place des clés publiques **1**

3 Utilisation de la connexion SSH à distance **1**

~~DIFFUSION LIMITÉE~~

1 Pré-requis

Liste des pré-requis :
- Passerelle CLIP installée ;
- Clef USB contenant les clés publiques SSH des administrateurs.

2 Mise en place des clés publiques

Il est possible de se connecter en SSH à la passerelle IPSec pour réaliser des tâches d'administration à distance. Deux comptes sont disponibles, *_audit* et *_admin*, destinés respectivement à la consultation des logs et à la modification de la configuration (réseau, principalement). La connexion n'est possible que via une identification par clefs asymétriques ; il va donc être nécessaire d'installer les clefs publiques des utilisateurs qui auront accès à la machine.

L'utilisateur "admin", créé à l'installation de la machine, recouvre par défaut les deux comptes unix *_audit* et *_admin*. Commencez donc par vous logger en tant que "admin".

Des clefs SSH sont déjà présentes dans les fichiers « ~/.ssh/authorized_keys » de chacun des comptes *_audit* et *_admin*. Elles permettent l'accès graphique de l'utilisateur "admin" aux fonctions de *_audit* et *_admin*. Il est donc important de ne pas y toucher (ce n'est de toute façon pas possible en fonctionnement normal, pour des questions de permissions). Les clefs SSH pour un accès distant sont en fait à placer dans des répertoires « ~/.ssh-remote », à créer s'ils n'existent pas. L'import de clefs se fait via le montage d'une clé USB.

Ouvrez un terminal ADMIN (sous un menu "fonctions avancées" dans les menus de la barre de gauche). Vous êtes directement placé dans le répertoire home du compte *_admin*.

Entrez dans le répertoire « .ssh-remote » (créez-le s'il n'existe pas).

```
$ mkdir .ssh-remote
$ cd .ssh-remote
```

Copiez ou créez ici votre clef publique ssh avec pour nom de fichier « authorized_keys ». Vous pouvez concaténer plusieurs clefs à la suite, à raison de une par ligne.

Pour le compte *_audit*, effectuez la même manipulation depuis un terminal AUDIT accessible de la même manière via les menus de la barre de confiance.

3 Utilisation de la connexion SSH à distance

Votre machine est désormais accessible par un utilisateur connecté sur l'interface de supervision (`eth2`) de la machine disposant de la clef privée correspondante. Le compte *_admin* est accessible sur le port 22, le compte *_audit* sur le port 23.

Par exemple :

```
$ ssh -p 23 \
      -I ~/clefs_privees_ssh/id_rsa.passerelleIPSec_audit.pem \
      _audit@gwipsec
```

Où « ~/clefs_privees_ssh/id_rsa.passerelleIPSec_audit.pem » correspond à la clef SSH privée installée sur le compte *_audit*, et où « gwipsec » renvoit vers l'adresse de supervision de la passerelle IPSec.