Compte utilisateur local & accès SSH sur un équipement Cisco

Philippe Latu
philippe.latu(at)inetdoc.net

http://www.inetdoc.net

Résumé

Comment accéder à un équipement réseau Cisco™ directement au niveau super utilisateur avec le protocole SSH.

Table des matières

1. Copyright et Licence

1.1. Méta-information

Cet article est écrit avec DocBook[1] XML sur un système Debian GNU/Linux[2]. Il est disponible en version imprimable au format PDF : `ssh-ios.pdf`[3].

Toutes les commandes utilisées sont issues des paquets de la distribution Debian GNU/Linux. Elles ne sont cependant pas spécifiques à une version particulière des systèmes UNIX ou GNU/Linux.

[1] http://www.docbook.org
[2] http://www.debian.org
[3] http://www.inetdoc.net/pdf/ssh-ios.pdf

2. Compte utilisateur local et authentification SSH

Les équipements réseau Cisco disposent d'un mode d'authentification minimal avec plusieurs niveaux de «privilèges». Historiquement, les deux niveaux couramment utilisés sont le premier et le dernier. Le niveau 1, baptisé User EXEC mode, est comparable à l'utilisateur normal d'un système GNU/Linux. Il ne donne accès qu'à la consultation d'informations telles que l'état des interfaces ou la table de routage. Le niveau 15, baptisé Privileged EXEC mode, est comparable au super utilisateur d'un même système GNU/Linux.

Comme les capacités d'un équipement réseau en matière d'usages multimédias sur l'Internet sont pour le moins limitées, l'utilisation du compte utilisateur normal ne présente pratiquement aucun intérêt. Si on se connecte à un équipement, c'est fatalement pour effectuer une opération de configuration qui nécessite des droits étendus sur le système. Voici donc la liste des commandes à implanter pour accéder directement au niveau Privileged EXEC mode tout en chiffrant les communications à l'aide du protocole SSH.

```
! Activation du modèle d'authentification AAA
aaa new-model

! Création de la liste d'authentification par défaut.
! Elle est appliquée automatiquement à toutes les interfaces.
! Elle utilise les comptes utilisateurs définis localement.
aaa authentication login default local

! Définition de la base locale comme source d'information
! sur les autorisations.
aaa authorization exec default local

! Création du compte utilisateur local avec les droits étendus.
username myusername privilege 15 secret mysecretpassword

! Définition du nom de domaine nécessaire pour la génération
! des clés SSH
ip domain name my-own.lab

! Génération des clés SSH
crypto key generate rsa label SSH-KEY modulus 4096

! Paramétrage du protocole SSH
! . version 2
ip ssh version 2
! . temps d'attente maximum pendant l'établissement de la connexion
ip ssh time-out 60
! . nombre maximum de tentatives de connexion avant réinitialisation
!   de l'interface
ip ssh authentication-retries 4

! Paramétrage interface d'accès console
! . déconnexion automatique après 5 minutes d'inactivité
! . entrée directe au niveau super utilisateur
! . synchronisation des messages système et de la journalisation
line con 0
 exec-timeout 5
 privilege level 15
 logging synchronous

! Paramétrage interface d'accès distant
! . déconnexion automatique après 5 minutes d'inactivité
! . accès via le protocole SSH uniquement
line vty 0 4
 exec-timeout 5 0
 transport input ssh
```