Cisco IOS ?

Support pour SSH

Il est important de noter que pour supporter HTTPS, SSH, SCP, etc., les appareils Cisco doivent exécuter une version de Cisco IOS supportant l'encryption. Il est possible d'identifier si l'encryption est supportée par le firmware par son nom. La structure des noms de firmware de Cisco est généralement composée du modèle de l'appareil, le niveau de licence (ex adventerprise pour "Advantage Enterprise" ou "lanlite" pour les fonctionnalités de base seulement), le numéro de version majeure (portant généralement un nom géographique associé tel que "Gibraltar", "Fuji", "Amsterdam", "Denali", "Everest", "Cupertino" et "Bengaluru" pour les versions 16.x et plus récentes), la révision du logiciel, le "Throttle" entre parenthèses indique la révision mineure du logiciel incluant généralement des nouvelles fonctionnalités ou quelques correctifs et le nom se termine enfin par un identifiant déterminant le type de publication ou le "train" ainsi que sa révision.

La structure suivante identifie donc le numéro de version complète et le nom complet du fichier de logiciel considérant que les fonctionnalités avancées d'entreprise ainsi que l'encryption soient inclus dans le logiciel serait "cat4500e-entservicesk9-mz.151-2.SG2.bin"

15	.1	(2)	SG	2
Major release number	Minor release number	New feature release number	Branch/train/platform identifier	Maintenance rebuild number

> TL; DR : Pour pouvoir activer toute forme de service d'encryption sur un appareil Cisco IOS, le nom du "firmware" doit contenir "k9"

Configuration du service

Lors de l'installation de OpenSSH sur la majorité des systèmes, une clé publique identifiant le système de façon unique est généralement générée automatiquement. Sur les appareils Cisco IOS, il est nécessaire de générer cette identité pour activer le service.

Afin de générer cette clé, il est impératif de configurer un nom de domaine sur l'appareil. Il faut ensuite s'assurer que le service soit activé. Si le support pour SCP est nécessaire (ex. pour prendre des sauvegardes de la configuration), il devra être activé séparément. Il faudra ensuite configurer un utilisateur avec lequel il sera possible de s'identifier (peut aussi être délégué à un serveur RADIUS) et spécifier aux terminaux virtuels d'être à l'écoute de connexions SSH ainsi que la liste d'utilisateurs à consulter pour l'authentification.

Les commandes suivantes suffisent généralement à activer SSH sur un appareil Cisco IOS.

```
Switch> enable
Switch# configure terminal

# Il est généralement recommandé de définir le nom de l'appareil puisque son identité sera générée en conséquence
Switch(config)# ip domain-name tamere.local

# Le niveau de privilège de la ligne suivante peut être ajusté, 15 est un administrateur global
Switch(config)# username bob privilege 15 password bob

# La ligne suivante affichera un avertissement lors au cours de la génération de la clé
Switch(config)# crypto key generate rsa modulus 4096

Switch(config)# ip ssh version 2
Switch(config)# ip scp server enable

# La ligne suivante peut être ajustée en fonction du nombre de terminaux à configurer pour SSH ou Telnet
Switch(config)# line vty 0 4

# La ligne suivante réserve ces terminaux virtuels pour SSH mais il est aussi possible de laisser ceux-ci à "all"
Switch(config-line)# transport input ssh

# La ligne suivante indique à ces terminaux de consulter la liste d'utilisateurs locaux pour permettre l'authentification
Switch(config-line)# login local
```

> Dans cet exemple, les terminaux virtuels 0 à 4 sont réservés à utilisation pour SSH. Il est également bonne pratique de réserver les terminaux 5 à 15 pour éviter des tentatives d'authentification par des protocoles moins sécurisés comme Telnet si possible.

Revision #13
Created 2025-01-18 00:31:24 UTC by Alexandre Arsenault-Jetté
Updated 2025-01-18 06:27:41 UTC by Alexandre Arsenault-Jetté