**SSH**

Avant toutes choses il faut savoir que pour se connecter en réseau sur un équipement actif *(Routeur ou Switch)* il faut utiliser les **ports virtuels (VTY)**, donnant accès à la console à travers TCP/IP.

Les services (Telnet, SSH, RLOGIN, etc.) sont activés à travers les lignes.

**La solution SSH :**

Secure Shell (**SSH**) est un **protocole** de communication sécurisé, il impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP (communications) sont authentifiés et chiffrés.

Son utilisation est recommandée contrairement à Telnet qui ne permet pas de sécuriser l’authentification et la gestion d’un équipement actif.

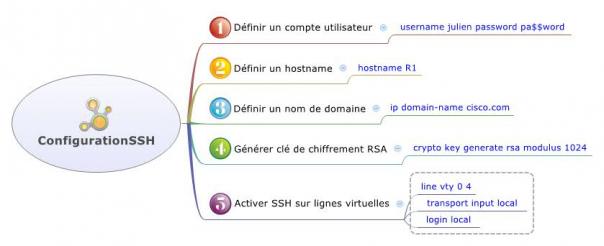
Cependant Telnet reste une solution viable en LAN (pas de passage par internet) ou via des VPN chiffrés qui ne laisse pas passer les données en clair (SSL/TLS).

**Précision : Pour pouvoir mettre en place SSH sur un équipement actif il faut vérifier que la version le permette ! Pour cela il faut effectuer la commande « show version ».**

**Si le nom de la version contient « K9 » cela veut dire que l’équipement actif supporte le protocole SSH.**

**Exemple de version :**

****

**Voici une façon schématique d’appréhender la configuration du protocole SSH :** 

**Commandes de configuration :**

|  |  |  |
| --- | --- | --- |
| Pour pouvoir utiliser SSH il faut obligatoirement configurer un nom et un domaine sur l’équipement actif  *(ces informations sont utilisées pour générer la clé de chiffrement)* | hostname <**NomElementActif**>  ip domaine-name <**nom.domaine**> | |
| Ensuite on génère une clé de chiffrement RSA pour que les échanges soient sécurisés.  *(la valeur est à choisir mais par défaut on utilise souvent une clé de 1024 ou 2048 bits)* | crypto key generate rsa general-key modulus <**xxxx**>  Exemple :  crypto key generate rsa general-key modulus 1024 | |
| Choix de la version du protocole SSH | ip ssh version <**1-2**> | |
| Pour que les connexions soient enregistrées dans un fichier de log  *(non obligatoire mais recommander pour surveiller les connexions)* | ip ssh logging events | |
| Définir un timeout qui éjecte un utilisateur inactif d’une session depuis un nombre de secondes définit | ip ssh time-out <**1-120**>  exemple : ip ssh time-out 120  *(120 = 2 \* 60 -> 2 minutes)* | |
| Définir un nombre de tentatives de connexions en ssh sur un équipement actif *(dans notre exemple l’utilisateur aura 3 tentatives)* | ip ssh authentication-retries <**0-5**>  exemple :  ip ssh authentication-retries 3 | |
| Ensuite il faut ajouter un compte administrateur pour se connecter  *(cependant nous activerons avant le chiffrement du MDP pour qu’il ne soit pas lisible en claire dans la configuration avec la commande service password-encryption)* | service password-encryption  username <**NomCompteSSH**> password 0 <**LeMotDePasse**>  exemple :  service password-encryption  username **toto** password 0 **AZERTY102030** | |
| * Ensuite avant de pouvoir utiliser SSH sur l’équipement actif il faut définir le nombre de ports virtuels (session max) pour ssh   *(dans notre exemple 3 sessions)*   * Puis on active ces ports virtuels de 0 à 2 *(3 sessions)* pour le ssh * Puis nous activons ensuite l’authentification avec le compte local prédéfini précédemment (dans notre exemple toto avec le mot de passe « AZERTY102030 » | | line vty 0 2  transport input ssh  login local |
| Pour vous connecter depuis un équipement actif vers un autre équipement en SSH | | ssh –l <**NOMUTILISATEUR**> <**IP**>  exemple de connexion :  ssh –l toto 192.168.1.100 |