Configuration SSH sur routeur

Routeur Cisco C921-4P

Tout se passe dans le mode configuration terminal, avec cette suite de commandes :

- **ip domain-name <nom de domaine>** : définit un nom de domaine dans lequel est le routeur, nécessaire pour configurer SSH
- **crypto key generate rsa :** génère une clé RSA
  - **How many bits in the modulus [512]: <taille de la clé>** : taille de la clé RSA à spécifier (512 est un exemple) (2048 au minimum de préférence)
- **ip ssh version 2** : active SSH
- **ip ssh logging events** : journalise les connexions SSH
- **ip ssh time-out <secondes>** : définit le temps d'inactivité avant la déconnexion d'un utilisateur qui a établi une connexion SSH sans encore s'être authentifié
- **ip ssh authentication-retries <nombre>** : définit le nombre de tentative ratées de connexion à l'utilisateur en SSH avant de le déconnecter
- **service password-encryption** : pour chiffrer le mot de passe des utilisateurs
- **username <nom d'utilisateur> password 0 <mot de passe>** : définit un utilisateur et un mot de passé associé pour la connexion SSH
- **line vty 0 3** : on entre dans la configuration de "line" en définissant le nombre de connexion distantes possibles en simultané (ici, 4)
  - "vty" : signifie les connexions à distance
  - "0 3" : pour faire très simple, le second nombre est le nombre de connexions simultanées possibles - 1 car on part de 0 (donc ici il y a 4 connexion simultanées possibles)
- (config-line) **transport input ssh** : autoriser la connexion SSH à distance
- (config-line) **login local** : définit la connexion à un compte local du routeur

Connexion SSH depuis une machine Linux (Fedora 43)

Certains éléments de connexion SSH qui sont demandés par le routeur peuvent être bloqués sur Linux. De ce fait, il faut modifier quelques éléments de configuration (ici, sur Fedora 43).
Dans le fichier /etc/ssh/ssh_config, on ajoute le contenu suivant à la fin du fichier (pour l'indentation, ne pas utiliser la tabulation, mais 4 espaces) :

```
Host 192.168.90.138
    KexAlgorithms +diffie-hellman-group1-sha1,diffie-hellman-group14-sha1
    PubkeyAcceptedAlgorithms +ssh-rsa
    PubkeyAcceptedKeyTypes +ssh-rsa
    HostKeyAlgorithms +ssh-rsa
    Ciphers aes256-ctr,3des-cbc
```

On entre la commande suivante :

```
update-crypto-policies --set DEFAULT:SHA1
```

Revision #4
Created 2026-05-02 13:23:27 UTC by SISR
Updated 2026-05-12 10:37:03 UTC by SISR