Sécurisation

- AJOUT D'UN MOT DE PASSE
- MISE EN PLACE DE LA CONNEXION VIA SSH SUR UN ROUTEUR

AJOUT D'UN MOT DE PASSE

1. Se mettre en mode configuration

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
```

2. Mettre en place une sécurité renforcée:

```
enable secret 4 MONPASSWORD
```

3. Mettre en place le mot de passe en clair dans le conf

```
R1(config)#enable password MONMOTDEPASSE
```

4. Test du mot de passe

```
R1#disable
R1>enable
Password:
R1#
```

5. Rendre le mot de passe illisible dans le configuration

```
R1(config)#service password-encryption
```

MISE EN PLACE DE LA CONNEXION VIA SSH SUR UN ROUTEUR

Dans un premier temps il faut mettre en place un domaine sur le routeur et il faut aussi que le routeur ai un hostname.

1. Mise en place du domaine

```
R2#ena
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip domain-name megaproduction.local
```

2. Activation du SSH version 2 sur le routeur
   - Génération de la clé SSH

```
R2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R2.megaproduction.local


% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
```

   - Activation de SSH

```
R2(config)#ip ssh version 2
```

Mise en place de certaine options (Pas obligatoire)

- Log des connexion sur la console
  `ip ssh logging events`
- Trois essaie max pour la connexion
  `ip ssh authentication-retries 3`

On va maintenant mettre en place l'authentification pour le SSH

1. Mise en place de l'authentification

```
R2(config)#aaa new-model
R2(config)#aaa authentication login default local
R2(config)#aaa authorization exec default local
```

2. Ajout d'un nouvel utilisateur

```
username admin secret MONPASSWORD
```

3. Vérification de la version de SSH

```
R2(config)#do show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQChcducKh2B5ggTiLfh5MssfYNvX7v/NZpTWImO7pw0
rBpZ9efkb1aUNZ0pv6lTQHE5Fp4wqh3cjgIiPrK5VmgihmerKDonLJF7cPWdEWXLJHFnS0Lk1Q0UI11x
DmAcI0iMs3nb1B18e//hasJYyS8XfgnE0bnbp5FHvM+DF3bnNQ==
```

PROBLÈMES RENCONTRES:

Des problèmes d’algorithme de chiffrement à la connexion:

```
root@debian:~# ssh admin@192.168.1.1
Unable to negotiate with 192.168.1.1 port 22: no matching key exchange method found. Their
offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-
sha1
```

Solution:

```
ssh admin@192.168.1.1 -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa -o
KexAlgorithms=diffie-hellman-group1-sha1  -o Ciphers=aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
```