Sécurité de base

Table des matières

1 Protection de base

(Aucun mot de passe par défaut)

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable password secret
R1(config)#exit
*Mar  1 00:19:22.183: %SYS-5-CONFIG_I: Configured from console by
console
R1#disable
R1>enable
Password:
```

(on ne voit rien. Pas de * ni curseur)

```
R1(config)#enable secret secret
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.

R1(config)#enable secret cisco
```

```
R1#show running-config | i enable
enable secret 5 $1$SKcC$HIx/24sUqg1G9bM/vJvXd1
enable password secret
```

(Si mot de passe pas bon)

```
R1#logout

R1>enable
Password:
Password:
Password:
% Bad secrets
```

(**enable secret** a la priorité sur **enable password**)

```
R1(config)#line console 0
R1(config-line)#password montreal
```

```
R1(config)#line aux 0
R1(config-line)#password quebec
```

```
R1(config)#line vty 0 4
R1(config-line)#password laval
```

```
R1#show running-config | section line
line con 0
 exec-timeout 0 0
 password montreal
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 password quebec
 logging synchronous
line vty 0 4
 password laval
 login
```

(**enable secret** est le seul mot de passe chiffré par défaut)

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

2 Telnet

Telnet permet l'authentification par mot de passe seulement. Il est aussi possible de s'authentifier en fournissant un nom d'utilisateur et un mot de passe.

Telnet n'est pas activé par défaut.

SSH ne permet pas l'authentification par mot passe. Il faut fournir un nom d'utilisateur et un mot passe.

A l'ouverture d'une session Telnet, on est placé par défaut dans le mode d'exécution utilisateur. On doit connaitre le mot de passe du mode privilégié pour accéder au mode privilégié.

On peut assigner le niveau de privilège 15 à un utilisateur pour éviter qu'on lui demande le mot de passe du mode privilégié.

Le niveau de privilège 15 peut aussi être assigné aux lignes VTY pour permettre l'accès à n'importe quel utilisateur qui connait le mot de passe du niveau 15.

```
#telnet 192.168.93.99
Trying 192.168.93.99 ... Open

Password required, but none set

[Connection to 192.168.93.99 closed by foreign host]
```

```
R1(config)#line vty 0 4
R1(config-line)#login
% Login disabled on line 162, until 'password' is set
% Login disabled on line 163, until 'password' is set
% Login disabled on line 164, until 'password' is set
% Login disabled on line 165, until 'password' is set
% Login disabled on line 166, until 'password' is set
R1(config-line)#password cisco
```

```
#telnet 192.168.93.99
Trying 192.168.93.99 ... Open
User Access Verification
Password:
R1>enable
% No password set
R1>
```

Option 1 (définir le mot de passe du mode privilégié)

```
R1(config)#enable secret cisco
```

```
telnet 192.168.93.99
Trying 192.168.93.99 ... Open
User Access Verification
Password:
R1>enable
Password:
R1#
```

Option 2

```
R1(config)#no enable secret

R1(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#password secret
R1(config-line)#login
```

```
telnet 192.168.93.99
Trying 192.168.93.99 ... Open
User Access Verification
Password:
R1#
```

Attribuer un privilège à un usager spécifique

```
R1(config)#username hakimb privilege 15 secret cisco

R1(config)#line vty 0 4
R1(config-line)#login local
```

```
telnet 192.168.93.99
Trying 192.168.93.99 ... Open
User Access Verification

Username: hakimb
Password:
R1#
```

```
R1(config)#username bob secret cisco
```

```
telnet 192.168.93.99
Trying 192.168.93.99 ... Open
User Access Verification

Username: bob
Password:
R1>
```

3 SSH

- Il faut définir un domaine avec la commande ***ip domaine-name***
- Vous devez attribuer un nom au routeur. Vous ne pouvez pas garder le nom par défaut ***router***
- Il faut générer une clé avec la commande ***crypto key generate***
- Vous devez créer un utilisateur

```
Router(config)#crypto key generate rsa
% Please define a hostname other than Router.

Router(config)#hostname R1

R1(config)#crypto key generate rsa
% Please define a domain-name first.

R1(config)#ip domain-name orabec.com

R1(config)#crypto key generate rsa
The name for the keys will be: R1.orabec.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than 512
may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar  1 00:45:56.595: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
R1(config)#ip ssh version 2
```

```
ssh 192.168.93.99
login as: hakimb
Using keyboard-interactive authentication.
Password:
```

```
R1#show ssh
Connection Version Mode Encryption  Hmac      State
Username
1          2.0     IN   aes256-cbc  hmac-sha1 Session started hakimb
1          2.0     OUT  aes256-cbc  hmac-sha1 Session started hakimb
%No SSHv1 server connections running.
R1#
```

```
R1#show ssh vty 1
```

4 Views

Les vues sont faciles à utiliser et très flexibles. Il est possible d'associer des commandes exactes ou des sous-ensembles de commandes à une vue. L'utilisateur assigner à la vue pourra exécuter ces commandes.

Deux prérequis pour pouvoir utiliser les vues :

- Assigner un mot de passe au mode privilégié

```
R1(config)#enable secret cisco
```

- Activer le modèle triple A (AAA)

```
R1(config)#aaa new-model
```

4.1 Activer les vues

Vous devez fournir le mot de passe du mode privilégié.

```
R1#enable view
Password:

*Mar  1 00:39:07.907: %PARSER-6-VIEW_SWITCH: successfully set to
view 'root'.
R1#
```

4.2 Créer une vue

Pour créer une vue nommée SUPPORT :

```
R1(config)#parser view SUPPORT
R1(config-view)#
*Mar  1 00:40:29.751: %PARSER-6-VIEW_CREATED: view 'SUPPORT'
successfully created.

R1(config-view)#secret support

R1(config-view)#commands exec include ping
R1(config-view)#commands exec include all show
```

4.3 Afficher la vue courante

```
R1#show parser view
Current view is 'root'
```

```
R1#enable view SUPPORT
Password:

*Mar  1 00:44:32.611: %PARSER-6-VIEW_SWITCH: successfully set to
view 'SUPPORT'.
```

```
R1#show parser view
Current view is 'SUPPORT'
```

```
R1#ping 192.168.93.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.93.99, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4
ms

R1#traceroute 192.168.93.99
   ^
% Invalid input detected at '^' marker.
```

4.4 Ajouter une commande a une vue

```
R1>enable
Password:
R1#show parser view
No view is active ! Currently in Privilege Level Context
```

```
R1#enable view
Password:

R1#
*Mar  1 00:48:06.439: %PARSER-6-VIEW_SWITCH: successfully set to
view 'root'.
```

```
R1(config)#parser view SUPPORT
R1(config-view)#commands exec include traceroute
```

```
R1#show parser view
Current view is 'root'
```

```
R1#enable view SUPPORT
Password:

R1#
*Mar  1 00:50:42.743: %PARSER-6-VIEW_SWITCH: successfully set to
view 'SUPPORT'.
```

```
R1#traceroute 192.168.93.99

Type escape sequence to abort.
Tracing the route to 192.168.93.99

  1 192.168.93.99 0 msec 4 msec 0 msec
```

```
R1(config)#username hakimb view SUPPORT
```

```
R1(config)#username hakimb view SUPPORT secret hakimb
```

5 Privilege access control

Trois niveaux de privilège par défaut :

- Niveau 0
- Niveau 1 (user exec)
- Niveau 15 (privilege exec)

Chaque niveau a accès aux commandes des niveaux précédents.

Il est possible de créer un niveau personnalisé (2 à 14).

5.1 Afficher le niveau courant

```
R1>show privilege
Current privilege level is 1
```

```
R1>enable
R1#show privilege
Current privilege level is 15
```

(Level 15 by default)

5.2 Assigner un mot de passe à un le niveau

```
R1(config)#enable secret level 5 cisco
```

```
telnet 192.168.93.99
Trying 192.168.93.99 ... Open


User Access Verification

Password:
R1>enable
% No password set
```

```
telnet 192.168.93.99
Trying 192.168.93.99 ... Open

User Access Verification

Password:
R1>enable 5
Password:

R1#show privilege
Current privilege level is 5
```

Pas besoin du mot de passe pour aller à un niveau inférieur :

```
R1#enable 4
R1#enable 5
Password:
```

5.3 Associer une commande à un niveau

```
R1(config)#privilege configure level 5 interface
R1#enable 5
R1#show privilege
Current privilege level is 5
R1#conf t
      ^
% Invalid input detected at '^' marker.

R1(config)#privilege exec level 5 configure terminal

R1(config)#privilege configure all level 5 line
R1(config)#privilege interface level 5 shutdown
```