Configuration des mots de passe Telnet, Console et AUX sur les routeurs

Table des matières

Introduction

Ce document décrit des exemples de configuration pour configurer la protection par mot de passe pour les connexions d'exécution entrantes au routeur.

Conditions préalables

Exigences

Pour effectuer les tâches décrites dans ce document, vous devez disposer d'un accès privilégié à l'interface de ligne de commande (CLI) du routeur. Pour plus d'informations sur la ligne de commande et pour comprendre les modes de commande, consultez Utiliser l'interface de ligne de commande de Cisco IOS.

Pour obtenir des instructions sur la connexion d'une console à votre routeur, reportez-vous à la documentation fournie avec votre routeur ou à la documentation en ligne de votre équipement.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco 2509
- Logiciel Cisco IOS® version 12

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

L'utilisation de la protection par mot de passe pour contrôler ou restreindre l'accès à l'interface de ligne de commande (CLI) de votre routeur est l'un des éléments fondamentaux d'un plan global de sécurité.

Pour protéger le routeur contre les accès distants non autorisés, généralement Telnet, est la sécurité la plus courante qui doit être configurée, mais la protection du routeur contre les accès locaux non autorisés ne peut pas être négligée.

Remarque : la protection par mot de passe n'est qu'une des nombreuses étapes à suivre dans un régime de sécurité réseau approfondi et efficace. Les pare-feu, les listes d'accès et le contrôle de l'accès physique à l'équipement sont d'autres éléments à prendre en compte lors de la mise en oeuvre de votre plan de sécurité.

L'accès à la ligne de commande, ou EXEC, à un routeur peut être fait de façons diverses, mais dans tous les cas la connexion en entrée au routeur est établie sur une ligne TTY. Il existe quatre principaux types de lignes TTY, comme le montre cet exemple `show line` résultat :

```
<#root>

2509#

show line

   Tty

Typ
```

```
     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0
CTY
                -    -      -    -    -      0       0     0/0       -
     1
TTY
   9600/9600 -    -      -    -    -      0       0     0/0       -
     2
TTY
   9600/9600 -    -      -    -    -      0       0     0/0       -
     3
TTY
   9600/9600 -    -      -    -    -      0       0     0/0       -
     4
TTY
   9600/9600 -    -      -    -    -      0       0     0/0       -
     5
TTY
   9600/9600 -    -      -    -    -      0       0     0/0       -
     6
TTY
   9600/9600 -    -      -    -    -      0       0     0/0       -
     7
TTY
   9600/9600 -    -      -    -    -      0       0     0/0       -
     8
TTY
   9600/9600 -    -      -    -    -      0       0     0/0       -
     9
AUX
   9600/9600 -    -      -    -    -      0       0     0/0       -
    10
VTY
                -    -      -    -    -      0       0     0/0       -
    11
VTY
                -    -      -    -    -      0       0     0/0       -
    12
VTY
                -    -      -    -    -      0       0     0/0       -
    13
VTY
```

```
                -    -      -    -    -      0       0     0/0       -
    14
VTY
                -    -      -    -    -      0       0     0/0       -

2509#
```

Le type de ligne CTY est le port de console. Sur n'importe quel routeur, il apparaît dans la configuration du routeur sous la forme line con 0 et dans le résultat de la commande `show line` en tant que cty . Le port de console est principalement utilisé pour l'accès au système local avec un terminal de console.

Les lignes TTY sont des lignes asynchrones utilisées pour les connexions de modem et de terminal entrantes ou sortantes et peuvent être vues dans une configuration de routeur ou de serveur d'accès sous la forme line x . Les numéros de ligne spécifiques sont une fonction du matériel intégré ou installé sur le routeur ou le serveur d'accès.

La ligne AUX est le port auxiliaire, vu dans configuration en tant que line aux 0.

Les lignes VTY sont les lignes du terminal virtuel du routeur, utilisées seulement pour contrôler les connexions d'arrivée de Telnet. Elles sont virtuelles dans le sens où qu'elles sont une fonction du logiciel - aucun matériel ne leur est associé. Elles apparaissent dans la configuration en tant que line vty 0 4.

Chacun de ces types de ligne peut être configuré avec la protection par mot de passe. Des lignes peuvent être configurées pour utiliser un mot de passe pour tous les utilisateurs ou pour des mots de passe spécifiques au utilisateur. Des mots de passe spécifiques à des utilisateurs peuvent être configurés localement sur le routeur, ou vous pouvez utiliser un serveur d'authentification pour fournir l'authentification.

Il n'y a aucune interdiction de configuration de différentes lignes avec différents types de protection par mot de passe. Il est, en fait, courant de voir des routeurs avec un mot de passe unique pour la console et des mots de passe spécifiques aux utilisateurs pour d'autres connexions entrantes.

Ceci est un exemple de sortie de routeur de la `show running-config` commande :

<#root>

```
2509#
show running-config
Building configuration...

Current configuration : 655 bytes
!
version 12.2
.
.
```

```
.

!--- Configuration edited for brevity


line con 0
line 1 8
line aux 0
line vty 0 4
!
end
```

Configurer les mots de passe sur la ligne

Pour spécifier un mot de passe sur une ligne, utilisez la `password` en mode de configuration de ligne. Pour activer la vérification du mot de passe lors de la connexion, utilisez la `login` en mode de configuration de ligne.

Procédure de configuration

Dans cet exemple, un mot de passe est configuré pour tous les utilisateurs qui tentent d'utiliser la console.

1. À partir de l'invite du mode d'exécution privilégié (ou de l'invite enable), passez en mode de configuration, puis passez en mode de configuration de ligne avec ces commandes. Notez que l'invite change pour refléter le mode en cours.

   <#root>

   ```
   router#

   configure terminal

   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#

   line con 0

   router(config-line)#
   ```

2. Configurez le mot de passe et activez la vérification du mot de passe à la connexion.

   <#root>

   ```
   router(config-line)#

   password letmein

   router(config-line)#

   login
   ```

3. Quittez le mode de configuration.

```
<#root>

router(config-line)#

end

router#
%SYS-5-CONFIG_I: Configured from console by console
```

Remarque : n'enregistrez pas les modifications de configuration apportées à l'icône de ligne 0 tant que votre capacité à vous connecter n'a pas été vérifiée.

Remarque : sous la configuration de la console de ligne, `login` est une commande de configuration requise pour activer la vérification du mot de passe lors de la connexion. L'authentification de la console nécessite `password` et la `login` commandes pour travailler

Vérifier la configuration

Examinez configuration du routeur pour vérifier que les commandes ont été correctement saisies :

- **show running-config** - affiche la configuration actuelle du routeur.

```
<#root>

router#

show running-config

Building configuration...
...

!--- Lines omitted for brevity


!
line con 0

password letmein
login

line 1 8
line aux 0
line vty 0 4
!
end
```

Pour tester la configuration, déconnectez-vous de la console et reconnectez-vous, puis utilisez le mot de passe configuré pour accéder au routeur :

```
<#root>

router#

exit


router con0 is now available

Press RETURN to get started.

User Access Verification
Password:

!--- Password entered here is not displayed by the router


router>
```


Remarque : avant d'effectuer ce test, assurez-vous que vous disposez d'une autre connexion au routeur, telle que Telnet ou un accès commuté, en cas de problème lors de la reconnexion au routeur.

Dépannage de l'échec de connexion

Si vous ne parvenez pas à vous reconnecter au routeur et que vous n'avez pas enregistré la configuration, rechargez le routeur pour éliminer les modifications de configuration effectuées.

Si les modifications de configuration ont été enregistrées et que vous ne pouvez pas vous connecter au routeur, effectuez une récupération de mot de passe. Référez-vous à Procédures de récupération des mots de passe pour obtenir les instructions pour votre plate-forme particulière.

Configurer les mots de passe spécifiques aux utilisateurs locaux

Pour établir un système d'authentification basé sur le nom d'utilisateur, utilisez la username < /code> en mode de configuration globale. Pour activer la vérification du mot de passe à la connexion, utilisez la login local en mode de configuration de ligne.

Procédure de configuration

Dans cet exemple, les mots de passe sont configurés pour les utilisateurs qui tentent de se connecter au routeur sur les lignes VTY avec Telnet.

1. À partir de l'invite du mode d'exécution privilégié (ou de l'invite enable), passez en mode de configuration et entrez des combinaisons nom d'utilisateur/mot de passe, une pour chaque

utilisateur pour lequel vous voulez autoriser l'accès au routeur :

```
<#root>

router#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#

username russ password montecito

router(config)#

username cindy password belgium

router(config)#

username mike password rottweiler
```

2. Passez en mode de configuration de ligne et utilisez ces commandes. Notez que l'invite change pour refléter le mode en cours.

```
<#root>

router(config)#

line vty 0 4

router(config-line)#
```

3. Configurez une vérification du mot de passe à la connexion.

```
<#root>

router(config-line)#

login local
```

4. Quittez le mode de configuration.

```
<#root>

router(config-line)#

end

router#
%SYS-5-CONFIG_I: Configured from console by console
```

Remarque : pour désactiver la fonction Telnet automatique lorsque vous tapez un nom dans l'interface de ligne de commande, configurez aucune journalisation n'est préférée /strong>sur la ligne utilisée. Tandis que transport preferred none fournit la même sortie, il désactive également le Telnet automatique pour le hôte défini qui est configuré avec la commande ip host. Ce n'est pas comme no log preferred , qui l'arrête pour les hôtes non définis et le laisse fonctionner pour les hôtes définis.

Vérifier la configuration

Examinez configuration du routeur pour vérifier que les commandes ont été correctement saisies :

- **show running-config** - affiche la configuration actuelle du routeur.

<#root>

```
router#

show running-config

Building configuration...
!

!--- Lines omitted for brevity


!

username russ password 0 montecito
username cindy password 0 belgium
username mike password 0 rottweiler

!

!--- Lines omitted for brevity


!
line con 0
line 1 8
line aux 0
line vty 0 4


login local

!
end
```

Pour tester cette configuration, une connexion Telnet doit être faite au routeur. Cela peut être fait si vous vous connectez à partir d'un hôte différent sur le réseau, mais vous pouvez également tester à partir du routeur lui-même via Telnet l'adresse IP de n'importe quelle

interface sur le routeur qui est dans un état up/up comme le montre le résultat de la commande `show interfaces` erasecat4000_flash:.

Voici un exemple de résultat si l'adresse de l'interface ethernet 0 était 10.1.1.1 :

```
<#root>

router#

telnet 10.1.1.1

Trying 10.1.1.1 ... Open


User Access Verification


Username: mike
Password:

!--- Password entered here is not displayed by the router


router
```

Dépanner l'échec du mot de passe spécifique à l'utilisateur

Les noms d'utilisateur et mots de passe distinguent les majuscules et minuscules. Les utilisateurs qui tentent de se connecter avec un nom d'utilisateur ou un mot de passe incorrectement mis en cause sont rejetés.

Si les utilisateurs ne peuvent pas se connecter au routeur avec leur mot de passe spécifique, reconfigurez le nom d'utilisateur et le mot de passe sur le routeur.

Configuration du mot de passe de ligne AUX

Afin de spécifier un mot de passe sur la ligne AUX, émettez la commande `password` en mode de configuration de ligne. Afin d'activer une vérification de mot de passe à la connexion, émettez la commande `login` en mode de configuration de ligne.

Procédure de configuration

Dans cet exemple, un mot de passe est configuré pour tous les utilisateurs qui tentent d'utiliser le port AUX.

1. Émettez le e `show line` afin de vérifier la ligne utilisée par le port AUX.

```
<#root>
```

```
R1#
show line

   Tty Typ     Tx/Rx    A Modem Roty AccO AccI  Uses  Noise  Overruns  Int
*    0 CTY                  -    -     -    -    -     0      0     0/0       -
    65 AUX  9600/9600  -    -     -    -    -    0     1     0/0             -
    66 VTY                 -    -     -    -    -     0      0     0/0       -
    67 VTY                 -    -     -    -    -     0      0     0/0       -
```

2. Dans cet exemple, le port AUX se trouve sur la ligne 65. Émettez ces commandes afin de configurer la ligne AUX du routeur :

```
<#root>
R1#
configure terminal
R1(config)#
line 65
R1(config-line)#
modem inout
R1(config-line)#
speed 115200
R1(config-line)#
transport input all
R1(config-line)#
flowcontrol hardware
R1(config-line)#
login
R1(config-line)#
password cisco
R1(config-line)#
end
R1#
```

Vérification de la configuration

Examinez la configuration du routeur afin de vérifier que les commandes ont été entrées correctement :

- Les `show running-config` affiche la configuration actuelle du routeur :

```
<#root>

R1#

show running-config

Building configuration...
!

!--- Lines omitted for brevity.


line aux 0
 password cisco
 login
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware

!--- Lines omitted for brevity.

!
end
```

Configurer l'authentification AAA pour la connexion

Pour activer l'authentification AAA (Authentication, Authorization, and Accounting) pour les connexions, utilisez la **login authentication** en mode de configuration de ligne. Les services AAA doivent également être configurés.

Procédure de configuration

Dans cet exemple, le routeur est configuré pour récupérer les mots de passe d'utilisateurs depuis un serveur TACACS+ quand les utilisateurs essayent de se connecter au routeur.

Remarque : la configuration du routeur pour utiliser d'autres types de serveurs AAA (RADIUS, par exemple) est similaire. Voir Configurer l'authentification pour plus d'informations.

Remarque : ce document ne traite pas de la configuration du serveur AAA lui-même.

---

1. À partir de l'invite du mode d'exécution privilégié (ou de l'invite enable), passez en mode de configuration et entrez les commandes pour configurer le routeur afin qu'il utilise les services AAA pour l'authentification :

<#root>

```
router#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#

aaa new-model

router(config)#

aaa authentication login my-auth-list tacacs+

router(config)#

tacacs-server host 192.168.1.101

router(config)#

tacacs-server key letmein
```

2. Passez en mode de configuration de ligne et utilisez ces commandes. Notez que l'invite change pour refléter le mode en cours.

<#root>

```
router(config)#

line 1 8

router(config-line)#
```

3. Configurez une vérification du mot de passe à la connexion.

<#root>

```
router(config-line)#

login authentication my-auth-list
```

4. Quittez le mode de configuration.

<#root>

```
router(config-line)#

end

router#
%SYS-5-CONFIG_I: Configured from console by console
```

Vérifier la configuration

Examinez configuration du routeur pour vérifier que les commandes ont été correctement saisies :

- show running-config - affiche la configuration actuelle du routeur.

```
<#root>

router#

write terminal

Build configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!

aaa new-model
aaa authentication login my-auth-list tacacs+

!

!--- Lines omitted for brevity


...
!

tacacs-server host 192.168.1.101
tacacs-server key letmein

!
line con 0
line 1 8


login authentication my-auth-list

line aux 0
line vty 0 4
!
end
```

Pour tester cette configuration particulière, une connexion entrante ou sortante doit être établie sur la ligne. Reportez-vous au Modem - Router Connection Guide pour obtenir des informations spécifiques sur la configuration des lignes asynchrones pour les connexions par modem.

Vous pouvez également configurer une ou plusieurs lignes VTY pour effectuer l'authentification

AAA et effectuer votre test sur celles-ci.

Dépannage de l'échec de connexion AAA

Avant d'émettre `debug` , consultez Informations importantes sur les commandes de débogage.

Pour résoudre un échec de connexion, utilisez la commande `debug` approprié à votre configuration :

- debug aaa authentication
- debug radius
- debug kerberos

Informations connexes

- Référence des commandes de débogage Cisco IOS
- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.