Telnet/SSH fonctionne seulement si la destination host en est spécifiée en tant que « » dans les Listes d'accès étendues

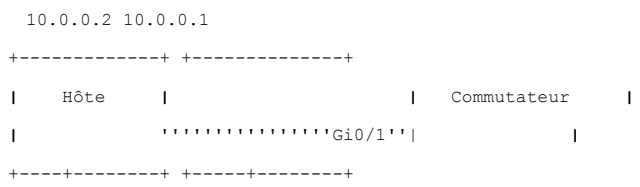
Contenu

Introduction

Ce document décrit la structure prise en charge de liste de contrôle d'accès (ACL) qui contrôle l'accès de telnet à un commutateur. Cette restriction s'applique au SSH aussi bien, bien que l'exemple spécifique ci-dessous soit seulement pour le telnet.

Problème

L'utilisateur veut permettre le telnet au commutateur de juste un hôte dans le réseau. Par exemple, seulement l'hôte 10.0.0.2 devrait pouvoir au telnet à l'IP 10.0.0.1 de commutateur.



Voici un exemple d'une configuration qui ne travaille pas sur une version d'Â® de Cisco IOS qui n'a pas la difficulté pour l'ID de bogue Cisco CSCuw89081.

```
ip access-list extended 100
permit tcp host 10.0.0.2 host 10.0.0.1 eq telnet

line vty 0 4
access-class 100 in
transport input telnet
login
password cisco
```

Pour une version de Cisco IOS qui a la difficulté pour l'ID de bogue Cisco CSCuw89081, la capacité à apparier sur une adresse IP spécifique de destination a été ajoutée et ce problème n'est pas vu.

Solution

Par conception, l'access-class apparie seulement l'adresse IP source de la liste d'accès. L'access-class permet l'accès au routeur dans son ensemble, pas accès au routeur seulement sur une adresse du routeur particulière. Ce comportement a changé par l'ID de bogue

Cisco CSCuw89081.

Voici un exemple d'une configuration qui travaille au Cisco IOS qui n'a pas la difficulté pour l'ID de bogue Cisco CSCuw89081.

```
ip access-list extended 100
permit tcp host 10.0.0.2 any eq telnet

line vty 0 4
access-class 100 in
transport input telnet
login
password cisco
```