El telnet/SSH trabaja solamente si la computadora principal de destino se especifica como “ningunos” en las listas de acceso ampliadas

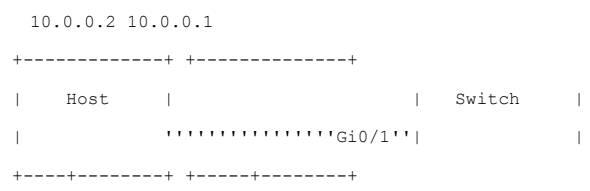
Contenido

Introducción

Este documento describe la estructura soportada de la lista de control de acceso (ACL) que controla el acceso telnet a un Switch. Esta restricción se aplica a SSH también, aunque el ejemplo específico abajo está solamente para el telnet.

Problema

El usuario quiere permitir el telnet al Switch de apenas un host en la red. Por ejemplo, solamente el host 10.0.0.2 debe poder al telnet al IP 10.0.0.1 del Switch.



Aquí está un ejemplo de una configuración que no trabaje en una versión de Â® del Cisco IOS que no tenga el arreglo para el Id. de bug 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
```

Para una versión deL Cisco IOS que tiene el arreglo para el Id. de bug Cisco CSCuw89081, la capacidad a hacer juego en un IP Address de destino específico se ha agregado y este problema no se considera.

Solución

Por el diseño, la acceso-clase hace juego solamente la dirección IP de origen de la lista de

acceso. la Acceso-clase permite el acceso al router en su conjunto, no acceso al router solamente en un direccionamiento del router determinado. Este comportamiento ha cambiado con el Id. de bug Cisco CSCuw89081.

Aquí está un ejemplo de una configuración que trabaje en el Cisco IOS que no tiene el arreglo para el Id. de bug 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
```