Telnet/SSH funciona sólo si el host de destino se especifica como "Any" en las listas de acceso extendidas

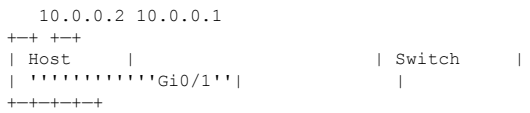
Contenido

Introducción

Este documento describe la estructura de lista de control de acceso (ACL) admitida que controla el acceso telnet a un switch. Esta restricción también se aplica a SSH, aunque el ejemplo específico a continuación es sólo para telnet.

Problema

El usuario desea permitir Telnet al switch desde un solo host en la red. Por ejemplo, solamente el host 10.0.0.2 debe ser capaz de telnet al switch IP 10.0.0.1.



Aquí hay un ejemplo de una configuración que no funciona en una versión de Cisco IOS® que no tiene la corrección 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 de Cisco IOS que tiene la corrección para el Id. de bug Cisco CSCuw89081, se ha agregado la capacidad de coincidencia en una dirección IP de destino específica y este problema no se ve.

Solución

Por diseño, la clase de acceso sólo coincide con la dirección IP de origen de la lista de acceso. La clase de acceso permite el acceso al router como un todo, no al router sólo en una dirección de router determinada. Este comportamiento ha cambiado a través del ID de bug de Cisco CSCuw89081.

Este es un ejemplo de una configuración que funciona en Cisco IOS que no tiene la corrección 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
```