O Telnet/SSH funciona somente se o host de destino for especificado como "Any" nas listas de acesso estendidas

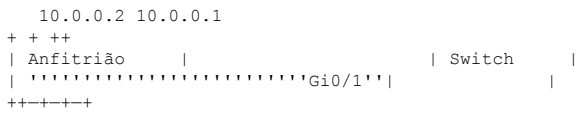
Contents

Introduction

Este documento descreve a estrutura da ACL (Access Control List, lista de controle de acesso) suportada que controla o acesso telnet a um switch. Essa restrição também se aplica ao SSH, embora o exemplo específico abaixo seja apenas para telnet.

Problema

O usuário deseja permitir o telnet para o switch de apenas um host na rede. Por exemplo, somente o host 10.0.0.2 deve ser capaz de executar telnet para o switch IP 10.0.0.1.



Aqui está um exemplo de uma configuração que não funciona em uma versão do Cisco IOS® que não tem a correção para o bug da Cisco ID 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 uma versão do Cisco IOS que tenha a correção para o bug da Cisco ID CSCuw89081, a capacidade de corresponder em um endereço IP de destino específico foi adicionada e esse problema não foi observado.

Solução

Por design, a classe de acesso só corresponde ao endereço IP de origem da lista de acesso. A classe de acesso permite o acesso ao roteador como um todo, não o acesso ao roteador somente em um endereço de roteador específico. Esse comportamento mudou com a ID de bug da Cisco CSCuw89081.

Aqui está um exemplo de uma configuração que funciona no Cisco IOS que não tem a correção para o bug da Cisco ID 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
```