

Telnet/SSH fonctionne uniquement si l'hôte de destination est spécifié comme « Any » dans les listes d'accès étendues

Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

Introduction

Ce document décrit la structure ACL (Access Control List) prise en charge qui contrôle l'accès Telnet à un commutateur. Cette restriction s'applique également à SSH, bien que l'exemple spécifique ci-dessous ne concerne que Telnet.

Problème

L'utilisateur souhaite autoriser la connexion Telnet au commutateur à partir d'un seul hôte du réseau. Par exemple, seul l'hôte 10.0.0.2 doit pouvoir établir une connexion Telnet avec l'adresse IP 10.0.0.1 du commutateur.

```
      10.0.0.2 10.0.0.1
    +-+ +-+
    | Hôte   | | Commutateur |
    | .....'Gi0/1'| |         |
    +-+ +-+ +-+
```

Voici un exemple de configuration qui ne fonctionne pas sur une version de Cisco IOS® qui n'a pas le correctif 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 le correctif pour l'ID de bogue Cisco [CSCuw89081](#), la capacité de correspondance sur une adresse IP de destination spécifique a été ajoutée et ce problème n'est pas visible.

Solution

Par conception, access-class ne correspond qu'à l'adresse IP source de la liste d'accès. Access-class permet d'accéder au routeur dans son ensemble, et non à celui-ci uniquement sur une adresse de routeur spécifique. Ce comportement a changé grâce à l'ID de bogue Cisco

[CSCuw89081](#).

Voici un exemple de configuration qui fonctionne sur Cisco IOS et qui n'a pas le correctif 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
```