

대상 호스트가 확장 액세스 목록에서 "Any"로 지정된 경우에만 텔넷/SSH가 작동합니다.

목차

[소개](#)

[문제](#)

[솔루션](#)

소개

이 문서에서는 스위치에 대한 텔넷 액세스를 제어하는 지원되는 ACL(Access Control List) 구조에 대해 설명합니다.이 제한은 SSH에도 적용되지만, 아래 예제는 텔넷에만 적용됩니다.

문제

사용자는 네트워크에 있는 하나의 호스트에서만 스위치에 대한 텔넷을 허용하려고 합니다.예를 들어 호스트 10.0.0.2만 스위치 IP 10.0.0.1에 텔넷할 수 있어야 합니다.

```
10.0.0.2 10.0.0.1
++ +-+
| | | | |
| "Gi0/1"| | | | |
+-+ +----+
```

다음은 Cisco 버그 ID CSCuw89081에 대한 수정 사항이 없는 Cisco IOS® 버전에서 작동하지 않는 컨피그레이션의 예입니다.

```
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
```

Cisco 버그 ID CSCuw89081에 대한 수정 사항이 있는 Cisco IOS 버전의 경우 특정 대상 IP 주소에 일치시키는 기능이 추가되었으며 이 문제는 표시되지 않습니다.

솔루션

설계상 access-class는 access-list의 소스 IP 주소만 매칭합니다.Access-class는 라우터 전체에 대한 액세스를 허용하며, 특정 라우터 주소에서만 라우터에 액세스할 수 있는 것은 아닙니다.이 동작은 Cisco 버그 ID CSCuw89081을 통해 변경되었습니다.

다음은 Cisco 버그 ID CSCuw89081에 대한 수정 사항이 없는 Cisco IOS에서 작동하는 컨피그레이션의 예입니다.

```
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
```