

CLI를 통해 스위치에서 SSH 서버 인증 설정 구성

소개

SSH(Secure Shell)는 특정 네트워크 디바이스에 대한 보안 원격 연결을 제공하는 프로토콜입니다. 이 연결은 암호화된다는 점을 제외하고 텔넷 연결과 유사한 기능을 제공합니다. 관리자는 SSH를 사용하여 서드파티 프로그램을 사용하여 CLI(Command Line Interface)를 통해 스위치를 구성할 수 있습니다.

이 스위치는 네트워크 내의 사용자에게 SSH 기능을 제공하는 SSH 클라이언트 역할을 합니다. 스위치는 SSH 서버를 사용하여 SSH 서비스를 제공합니다. SSH 서버 인증이 비활성화되면 스위치에서는 모든 SSH 서버를 신뢰할 수 있는 것으로 간주하여 네트워크의 보안을 낮춥니다. 스위치에서 SSH 서비스가 활성화된 경우 보안이 강화됩니다.

이 문서에서는 CLI를 통해 관리되는 스위치에서 서버 인증을 구성하는 방법에 대한 지침을 제공합니다.

적용 가능한 디바이스

- SX300 시리즈
- SX350 시리즈
- SG350X 시리즈
- SX500 시리즈
- SX550X 시리즈

소프트웨어 버전

- 1.4.7.06 - SX300, SX500
- 2.2.8.04 - SX350, SG350X, SX550X

SSH 서버 설정 구성

SSH 서버 인증 설정 구성

1단계. 스위치 콘솔에 로그인합니다. 기본 사용자 이름 및 비밀번호는 cisco/cisco입니다. 새 사용자 이름 또는 비밀번호를 구성한 경우 대신 자격 증명을 입력합니다.

참고: SSH 또는 텔넷을 통해 SMB 스위치 CLI에 액세스하는 방법을 알아보려면 [여기](#)를 클릭하십시오.

```
[User Name:cisco  
[Password:*****
```

참고: 명령은 스위치의 정확한 모델에 따라 달라질 수 있습니다. 이 예에서는 텔넷을 통해 SG350X 스위치에 액세스합니다.

2단계. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 Global Configuration 모드로 들어갑니다.

SG350X#

3단계. SSH 클라이언트에서 원격 SSH 서버 인증을 활성화하려면 다음을 입력합니다.

SG350X(config)#ip ssh-client

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#
```

4단계. IPv4 주소가 IPv4 SSH 서버와의 통신에 소스 IPv4 주소로 사용될 소스 인터페이스를 지정하려면 다음을 입력합니다.

SG350X(config)#ip ssh-client source-interface [interface-id]

- interface-id - 소스 인터페이스를 지정합니다.

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#
```

참고:이 예에서 소스 인터페이스는 VLAN 20입니다.

5단계. (선택 사항) IPv6 주소가 IPv6 SSH 서버와의 통신에 소스 IPv6 주소로 사용될 소스 인터페이스를 지정하려면 다음을 입력합니다.

SG350X(config)#ipv6 ssh-client source-interface [interface-id]

- interface-id — 소스 인터페이스를 지정합니다.

참고:이 예에서는 소스 IPv6 주소가 구성되지 않았습니다.

6단계. 신뢰할 수 있는 서버를 Trusted Remote SSH Server Table에 추가하려면 다음을 입력합니다

SG350X(config)#ip ssh-client server fingerprint [host | ip-address] [fingerprint]

매개변수는 다음과 같습니다.

- host - SSH 서버의 DNS(Domain Name Server) 이름입니다.
- ip-address - SSH 서버의 주소를 지정합니다.IP 주소는 IPv4, IPv6 또는 IPv6z 주소일 수 있습니다.
- fingerprint - SSH 서버 공개 키의 지문(16진수 32자).

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
SG350X(config)#
```

참고:이 예에서 서버 IP 주소는 192.168.100.1이고 사용되는 핑거프린트는 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8입니다.

7단계. 특별 권한 EXEC 모드로 돌아가려면 **exit** 명령을 입력합니다.

SG350X(config)#

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#$00 1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
SG350X(config)#exit
SG350X#
```

8단계. 스위치에 SSH 서버 인증 설정을 표시하려면 다음을 입력합니다.

SG350X#show ip ssh-client server [host | ip-address]

매개변수는 다음과 같습니다.

- host - SSH 서버의 DNS(Domain Name Server) 이름입니다.
- ip-address - SSH 서버의 주소를 지정합니다.IP 주소는 IPv4, IPv6 또는 IPv6z 주소일 수 있습니다.

```
SG350X(config)#exit
SG350X#show ip ssh-client server 192.168.100.1
SSH Server Authentication IS Enabled

Server address          : 192.168.100.1
Server Key Fingerprint : 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8

SG350X#
```

참고:이 예에서는 서버 IP 주소 192.168.100.1을 입력합니다.

9단계. (선택 사항) 스위치의 Privileged EXEC 모드에서 다음을 입력하여 구성된 설정을 시작 구성 파일에 저장합니다.

SG350X#copy running-config startup-config

```
[SG350X#copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[N] ?
```

10단계. (선택 사항) Overwrite file [startup-config]... 키보드에서 Y를 누르거나 N을 키보드에서 누릅니다.프롬프트가 나타납니다.

```
[SG350X#copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[N] ?Y
22-Sep-2017 04:09:18 %COPY-I-FILECOPY: Files Copy - source URL running-config destination URL flash://system/configuration/startup-config
22-Sep-2017 04:09:20 %COPY-N-TRAP: The copy operation was completed successfully

SG350X#
```

이제 CLI를 통해 관리되는 스위치에서 서버 인증을 구성하는 단계를 배웠습니다.