

CLIによるスイッチのSSHサーバ認証設定の設定

概要

セキュアシェル(SSH)は、特定のネットワークデバイスにセキュアなリモート接続を提供するプロトコルです。この接続は、暗号化されている点を除き、Telnet接続に似た機能を提供します。SSHを使用すると、管理者はコマンドラインインターフェイス(CLI)を使用して、サードパーティプログラムを使用してスイッチを設定できます。

スイッチは、ネットワーク内のユーザにSSH機能を提供するSSHクライアントとして機能します。スイッチはSSHサーバを使用してSSHサービスを提供します。SSHサーバ認証が無効になっている場合、スイッチは任意のSSHサーバを信頼できるサーバとして使用するため、ネットワークのセキュリティが低下します。スイッチでSSHサービスが有効になっている場合、セキュリティが強化されます。

この記事では、CLIを使用して管理対象スイッチでサーバ認証を設定する方法について説明します。

該当するデバイス

- Sx300シリーズ
- Sx350シリーズ
- SG350Xシリーズ
- Sx500シリーズ
- Sx550Xシリーズ

[Software Version]

- 1.4.7.06 - Sx300、Sx500
- 2.2.8.04 - Sx350、SG350X、Sx550X

SSHサーバの設定

SSHサーバ認証設定の設定

ステップ1：スイッチコンソールにログインします。デフォルトのユーザ名とパスワードはcisco/ciscoです。新しいユーザ名またはパスワードを設定している場合は、クレデンシャルを入力します。

注：SSHまたはTelnetを使用してSMBスイッチCLIにアクセスする方法については、[ここをクリックしてください](#)。

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

注：コマンドは、スイッチの正確なモデルによって異なる場合があります。この例では、SG350XスイッチにTelnetでアクセスします。

ステップ2: スイッチの特権EXECモードから、次のように入力してグローバルコンフィギュレーションモードに入ります。

```
SG350X#configure
```

ステップ3: SSHクライアントでリモートSSHサーバ認証を有効にするには、次のように入力します。

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

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

ステップ4: IPv4 SSHサーバとの通信に送信元IPv4アドレスとして使用する送信元インターフェイスを指定するには、次のように入力します。

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

- interface-id : 送信元インターフェイスを指定します。

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

注: この例では、送信元インターフェイスはVLAN 20です。

ステップ5: (オプション) IPv6アドレスをIPv6 SSHサーバとの通信の送信元IPv6アドレスとして使用する送信元インターフェイスを指定するには、次のように入力します。

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

- interface-id : 送信元インターフェイスを指定します。

注: この例では、送信元IPv6アドレスが設定されていません。

ステップ6: 信頼できるサーバを信頼できるリモートSSHサーバテーブルに追加するには、次のように入力します。

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

パラメータは、次のとおりです。

- host - SSHサーバのドメインネームサーバ(DNS)名。
- ip-address: SSHサーバのアドレスを指定します。IPアドレスには、IPv4、IPv6、またはIPv6zアドレスを指定できます。
- fingerprint - SSHサーバの公開キーのフィンガープリント (32文字の16進数) 。

```
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)#
```

注：この例では、サーバのIPアドレスは192.168.100.1で、使用されているフィンガープリントは76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8です。

ステップ7：特権EXECモードに戻るには、exitコマンドを入力します。

```
SG350X(config)#exit
```

```
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#
```

ステップ8：スイッチのSSHサーバ認証設定を表示するには、次のように入力します。

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

パラメータは、次のとおりです。

- host - SSHサーバのドメインネームサーバ(DNS)名。
- ip-address:SSHサーバのアドレスを指定します。IPアドレスには、IPv4、IPv6、またはIPv6zアドレスを指定できます。

```
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#
```

注：この例では、サーバのIPアドレス192.168.100.1が入力されています。

ステップ9: (オプション) スイッチの特権EXECモードで、次のように入力して、設定をスタートアップコンフィギュレーションファイルに保存します。

```
SG350X#copy running-config startup-config
```

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

ステップ10: (オプション) ファイルの上書き[startup-config]を実行した後に、キーボードでYを押して、Yesを押すかNを押します。プロンプトが表示されます。

```
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#
```

これで、CLIを使用して管理対象スイッチでサーバ認証を設定する手順が学習されました。