クラウドEメールセキュリティ(CES)ソリューションのコマンドラインインターフェイス(CLI)へのアクセス

内容

概要

このドキュメントでは、WindowsまたはLinux/macOSプラットフォームでセキュアシェル(SSH)を使用して、CESデバイスのCLIにアクセスする方法について説明します。

著者：Cisco TACエンジニア、Dennis McCabe Jr

背景説明

CES Eメールセキュリティアプライアンス(ESA)またはセキュリティ管理アプライアンス(SMA)のCLIにアクセスするには、2つの段階を完了する必要があります。これらの段階の詳細については、次で説明します。

1. SSHキーペアの生成
2. SSHクライアントの設定

注：次の手順は、野生で使用されるオペレーティングシステムの大部分をカバーしている必要があります。ただし、ご使用の内容が記載されていない場合、またはサポートが必要な場合は、Cisco TACにお問い合わせください。また、具体的な指示を提供するために最善を尽くします。これらは、このタスクを実行するために使用できるツールとクライアントの一部にすぎません。

定義

この記事で使用する用語について理解してください。

プロキシサーバ

これらは、CESインスタンスへのSSH接続を開始するために使用するCES SSHプロキシサーバです。デバイスがある地域に固有のプロキシサーバを使用する必要があります。たとえば、ログインホスト名がesa1.test.iphmx.comの場合は、米国の地域でiphmx.comプロキシサーバのいずれかを使用します。

- AP (ap.iphmx.com) f15-ssh.ap.ip hmx.comf16-ssh.ap.ip hmx.com
- AWS (r1.ces.cisco.com) p3-ssh.r1.ces.cisco.comp4-ssh.r1.ces.cisco.com
- CA(ca.iphmx.com)
  f13-ssh.ca.ip hmx.comf14-ssh.ca.ip hmx.com
- EU(c3s2.iphmx.com) f10-ssh.c3s2.iphmx.comf11-ssh.c3s2.iphmx.com
- EU (eu.iphmx.com) f17-ssh.eu.ip hmx.comf18-ssh.eu.ip hmx.com
- US(iphmx.com) f4-ssh.iphmx.comf5-ssh.iphmx.com

ログインホスト名

これはCES ESAまたはSMAの非プロキシホスト名で、esa1またはsma1で始まります。Webユーザインターフェイス(WUI)にログインすると、Webページの右上に表示されます。 形式は次のとおりです。esa[1-20].<allocation>.<datacenter>.comまたはsma[1-20].<allocation>.<datacenter>.com

SSHキーペアの生成

CESデバイスへのアクセスを開始するには、まずプライベート/パブリックSSHキーペアを生成し、Cisco TACに公開キーを提供する必要があります。Cisco TACが公開キーをインポートしたら、次の手順に進むことができます。**秘密キーを共有しないでください。**

次のいずれかの手順で、キーの種類はRSAで、標準ビット長は2048です。

Windows の場合：

PuTTYgenまたは同様のツールを使用してキーペアを生成できます。Windows Subsystem for Linux(WSL)を使用している場合は、次の手順に従うこともできます。

Linux/macOSの場合：

新しいターミナルウィンドウから、ssh-keygenを実行してキーペアを作成できます。

例：

```
ssh-keygen -t rsa -b 2048 -f ~/.ssh/mykey
```

場所：

```
ssh-keygen -t
```

SSHキーペアが作成されたら、Cisco TACに公開キーを提供してインポートし、クライアントの設定に進みます。秘密キーを共有しないでください。

SSHクライアントの設定

注:CLIアクセス用のSSH接続は、CESデバイスに直接行われるのではなく、localhost経由でSSHトンネルを転送します。これは、SSHプロキシの1つに直接接続されています。接続の最初の部分は私たちのプロキシサーバの1つであり、2番目の部分はローカルホストのSSHトンネル転送ポートです。

Windows の場合：

この例ではPuTTYを使用するため、別のクライアントを使用する場合は、手順を少し変更する必要があります。また、使用しているクライアントが最新バージョンに更新されていることを確認してください。

Windows – ステップ1 - SSHプロキシおよびオープン転送ポートへの接続

1. ホスト名として、CES割り当てに適用するプロキシサーバを入力します。
2. [Connection]を展開し、[Data]をクリックし、自動ログインのユーザ名としてdh-userと入力します。
3. [Connection]を展開した状態で、[SSH]をクリックし、[Don't start a shell or command at all]をオンにします。
4. [SSH]を展開して、[Auth]をクリックし、新しく作成された秘密キーを参照します。
5. SSHを展開して、[Tunnels]をクリックして、ローカル転送の送信元ポート（デバイスで使用可能な任意のポート）を指定し、CESデバイスのlogin hostname（dhで始まるホスト名ではない）を入力し、 、 複数のデバイス(例：esa1、esa2、およびsma1)を使用して、送信元ポートとホスト名を追加できます。その後、追加されたポートは、このセッションの開始時に転送されます。
6. 上記の手順が完了したら、セッションのカテゴリに戻り、セッションに名前を付けて保存します。

Windows – ステップ2 - CESデバイスのCLIへの接続

1. 作成したセッションを開き、接続します。
2. **SSHプロキシサーバセッションを開いたまま、ウィンドウを右クリックして新しいPuTTYセッションを開き、New Sessionを選択し、IPアドレスに127.0.0.1を入力し、ステップ5で使用した送信元ポートを入力しOpen。**
3. [Open]をクリックすると、CESクレデンシャルを入力するように求められます。その後、CLIにアクセスできます（これらはWUIへのアクセスに使用されるクレデンシャルと同じです）。

Linux/macOSの場合：

Linux/macOS – ステップ1 - SSHプロキシとオープン転送ポートへの接続

1. 新しいターミナルウィンドウから、次のコマンドを入力します。

```
ssh -i ~/.ssh/id_rsa -l dh-user -N -f f4-ssh.iphmx.com -L 2200:esa1.test.iphmx.com:22
```

場所：

```
ssh -i
```
これにより、ローカルクライアントのポートが開き、リモート側の特定のホストとポートに転送されます。

Linux/macOS – ステップ2 - CESデバイスのCLIへの接続

1. 同じターミナルウィンドウまたは新しいターミナルウィンドウから、次のコマンドを入力します。 入力すると、CESパスワードを入力するように求められます。その後、CLIにアクセスできます（これらはWUIへのアクセスに使用されるクレデンシャルと同じです）。

```
ssh dmccabej@127.0.0.1 -p 2200
```
場所：

```
ssh
```