Zugriff auf die Kommandozeile (CLI) Ihrer Cloud Email Security (CES)-Lösung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie mithilfe von Secure Shell (SSH) auf der Windows- oder Linux/MacOS-Plattform auf die CLI Ihrer CES-Geräte zugreifen.

Mitarbeiter: Dennis McCabe Jr, Cisco TAC Engineer.

Hintergrundinformationen

Es gibt zwei Stufen, die abgeschlossen werden müssen, um auf die CLI Ihrer CES Email Security Appliance (ESA) oder Security Management Appliance (SMA) zuzugreifen. Diese werden beide nachfolgend ausführlich beschrieben.

1. Generieren eines SSH-Schlüsselpaars
2. Konfigurieren des SSH-Clients

Hinweis: Die nachstehenden Anweisungen sollten den Großteil der im Umlauf befindlichen Betriebssysteme abdecken. Wenn Ihre Angaben jedoch nicht in der Liste enthalten sind oder Sie weiterhin Hilfe benötigen, wenden Sie sich an das Cisco TAC. Wir werden uns bemühen, Ihnen spezifische Anweisungen zu geben. Dies ist nur ein kleiner Ausschnitt der verfügbaren Tools und Clients, die für diese Aufgabe verwendet werden können.

Definitionen

Bitte machen Sie sich mit einigen der in diesem Artikel verwendeten Begriffe vertraut.

Proxyserver

Dies sind die CES SSH-Proxyserver, die Sie verwenden werden, um die SSH-Verbindung mit Ihrer CES-Instanz zu initiieren. Sie müssen einen Proxy-Server speziell für die Region verwenden, in der sich Ihr Gerät befindet. Wenn Ihr Anmelde-Hostname z. B. **esa1.test.iphmx.com** lautet, würden Sie einen der **iphmx.com-**Proxyserver in der **US-**Region verwenden.

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

Anmelde-Hostname

Dies ist der nicht-Proxy-Hostname Ihrer CES ESA oder SMA und beginnt mit etwas wie esa1 oder sma1. Sie finden sich oben rechts auf der Webseite, wenn Sie sich bei der Webbenutzeroberfläche (WUI) anmelden. Das Format sollte wie folgt sein: esa[1-20].<Allokation>.<datacenter>.com oder sma[1-20].<Allokation>.<datacenter>.com.

Generieren eines SSH-Schlüsselpaars

Um mit dem Zugriff auf Ihre CES-Geräte zu beginnen, müssen Sie zunächst ein privates/öffentliches SSH-Schlüsselpaar generieren und anschließend den öffentlichen Schlüssel für das Cisco TAC bereitstellen. Sobald der öffentliche Schlüssel vom Cisco TAC importiert wurde, können Sie mit den nächsten Schritten fortfahren. **Geben Sie Ihren privaten Schlüssel nicht frei**.

In beiden Schritten unten sollte der **Schlüsseltyp RSA** mit einer standardmäßigen **Bitlänge** von **2048** sein.

Für Windows:

PuTTYgen oder ein ähnliches Tool kann zum Generieren von Schlüsselpaaren verwendet werden. Wenn Sie das Windows Subsystem für Linux (WSL) verwenden, können Sie auch die folgenden Anweisungen befolgen.

Für Linux/MacOS:

In einem neuen Terminalfenster können Sie ssh-keygen ausführen, um ein Schlüsselpaar zu erstellen.

Beispiel:

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

Wo:

```
ssh-keygen -t
```

Wenn ein SSH-Schlüsselpaar erstellt wurde, geben Sie den öffentlichen Schlüssel zum Import an

das Cisco TAC an und fahren Sie mit der Client-Konfiguration fort. **Geben Sie Ihren privaten Schlüssel nicht frei**.

Konfigurieren des SSH-Clients

> **Hinweis: Die SSH-Verbindung für den CLI-Zugriff wird nicht direkt mit Ihrem CES-Gerät hergestellt, sondern über einen SSH-Tunnel weitergeleitet, der direkt mit einem unserer SSH-Proxys verbunden ist. Der erste Teil der Verbindung ist mit einem unserer Proxyserver und der zweite mit dem Weiterleitungsport des SSH-Tunnels auf Ihrem lokalen Host.**

Für Windows:

Wir verwenden PuTTY für unser Beispiel. Bitte beachten Sie, dass die Schritte möglicherweise leicht geändert werden müssen, wenn Sie einen anderen Client verwenden. Bitte stellen Sie auch sicher, dass der von Ihnen verwendete Client auf die neueste verfügbare Version aktualisiert wurde.

Windows - Schritt 1 - Herstellen einer Verbindung mit dem SSH-Proxy und dem offenen Weiterleitungs-Port

1. Geben Sie als **Hostnamen** den **Proxyserver** ein, der für Ihre CES-Zuweisung gilt.
2. Erweitern Sie **Verbindung**, klicken Sie auf **Daten**, und geben Sie **dh-user** als Benutzernamen für die automatische Anmeldung ein.
3. Wenn **Connection** noch erweitert ist, klicken Sie auf **SSH** und aktivieren Sie **keine Shell oder keinen Befehl**.
4. Erweitern Sie **SSH**, klicken Sie auf **Auth**, und **navigieren Sie** zum neu erstellten privaten Schlüssel.
5. Wenn **SSH** noch erweitert ist, klicken Sie auf **Tunnel**, geben Sie einen **Quellport** für die **lokale** Weiterleitung (alle verfügbaren Ports auf Ihrem Gerät) ein, geben Sie den **Anmeldenamen (nicht den Hostnamen, der mit dh beginnt) Ihres CES-Geräts ein, und klicken Sie dann auf Hinzufügen.** Wenn Sie mehrere Geräte hinzufügen möchten (d. h.: esa1, esa2 und sma1) können Sie zusätzliche Quellports und Hostnamen hinzufügen. Anschließend werden alle hinzugefügten Ports weitergeleitet, wenn diese Sitzung gestartet wird.
6. Sobald die oben genannten Schritte abgeschlossen sind, kehren Sie zur Kategorie **Sitzung** zurück, und nennen Sie dann die **Sitzung**, und **speichern Sie** sie.

Windows - Schritt 2 - Herstellen einer Verbindung zur CLI Ihres CES-Geräts

1. Öffnen Sie die Sitzung, und stellen Sie eine Verbindung zu der gerade erstellten Sitzung her.
2. **Öffnen Sie eine neue PuTTY-Sitzung, indem Sie mit der rechten Maustaste auf das Fenster klicken und Neue Sitzung auswählen. Geben Sie 127.0.0.1 als IP-Adresse ein, geben Sie den zuvor in Schritt 5 verwendeten Quellport ein, und klicken Sie dann auf Öffnen.**
3. Wenn Sie auf **Öffnen** klicken, werden Sie aufgefordert, Ihre CES-Anmeldeinformationen einzugeben, und sollten dann Zugriff auf die CLI haben. (Dies sind dieselben Anmeldeinformationen, die für den Zugriff auf die WUI verwendet werden.)

Für Linux/MacOS:

Linux/MacOS - Schritt 1: Herstellen einer Verbindung mit dem SSH-Proxy und dem offenen Weiterleitungs-Port

1. Geben Sie in einem neuen Terminalfenster den folgenden Befehl ein:

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

Wo:

```
ssh -i
```

Dadurch wird ein Port auf Ihrem lokalen Client geöffnet, der an den angegebenen Host und Port auf der Remote-Seite weitergeleitet wird.

Linux/macOS - Schritt 2 - Herstellen einer Verbindung zur CLI Ihres CES-Geräts

1. Geben Sie im gleichen oder im neuen Terminalfenster den folgenden Befehl ein. Nach der Eingabe werden Sie aufgefordert, Ihr CES-Kennwort einzugeben und sollten dann Zugriff auf die CLI haben. (Dies sind dieselben Anmeldeinformationen, die für den Zugriff auf die WUI verwendet werden.)

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

Wo:

```
ssh
```