Acceso a la interfaz de línea de comandos (CLI) de la solución Cloud Email Security (CES)

Contenido

Introducción

Este documento describe cómo acceder a la CLI de sus dispositivos CES mediante Secure Shell (SSH) en la plataforma Windows o Linux/MacOS.

Contribuido por Dennis McCabe Jr, ingeniero del TAC de Cisco.

Antecedentes

Hay dos etapas que deben completarse para acceder a la CLI de su dispositivo de seguridad CES Email Security Appliance (ESA) o Security Management Appliance (SMA), que se tratarán en detalle a continuación.

1. Generación de un par de claves SSH
2. Configuración del cliente SSH

Nota: Las instrucciones que figuran a continuación deberían abarcar la mayor parte de los sistemas operativos utilizados en el medio silvestre; sin embargo, si lo que está utilizando no aparece en la lista o sigue necesitando ayuda, póngase en contacto con el TAC de Cisco y haremos todo lo posible para proporcionar instrucciones específicas. Estos son sólo un pequeño fragmento de las herramientas y clientes disponibles que se pueden utilizar para realizar esta tarea.

Definiciones

Familiarícese con algunas de las terminologías que se utilizarán en este artículo.

Servidores proxy

Estos son los servidores proxy SSH CES que utilizará para iniciar la conexión SSH a su instancia de CES. Deberá utilizar un servidor proxy específico de la región en la que se encuentra el dispositivo. Por ejemplo, si su nombre de host de inicio de sesión es **esa1.test.iphmx.com**, utilizaría uno de los **servidores proxy iphmx.com** en la región **US**.

- **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
- **UE (eu.iphmx.com)** f17-ssh.eu.iphmx.comf18-ssh.eu.iphmx.com
- **EE. UU. (iphmx.com)** f4-ssh.iphmx.comf5-ssh.iphmx.com

Nombre de host de inicio de sesión

Este es el nombre de host no proxy de su CES ESA o SMA y comenzará con algo como esa1 o sma1, y se puede encontrar en la parte superior derecha de la página web cuando vaya a iniciar sesión en la interfaz de usuario web (WUI). El formato debe ser el siguiente: esa[1-20].<location>.<datacenter>.com o sma[1-20].<location>.<datacenter>.com.

Generación de un Par de Llaves SSH

Para empezar a acceder a los dispositivos CES, lo primero que tendrá que hacer es generar un par de claves SSH público/privado y, a continuación, proporcionar la clave pública al TAC de Cisco. Una vez que el TAC de Cisco haya importado su clave pública, puede continuar con los siguientes pasos. **No comparta su clave privada**.

Para cualquiera de los pasos siguientes, el **tipo de clave** debe ser **RSA** con una **longitud de bit** estándar de **2048**.

Para Windows:

PuTTYgen o una herramienta similar se puede utilizar para generar pares de claves. También puede seguir las instrucciones siguientes si utiliza el subsistema de Windows para Linux (WSL).

Para Linux/MacOS:

Desde una nueva ventana de terminal, puede ejecutar ssh-keygen para crear un par de claves.

Ejemplo:

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

Where:

```
ssh-keygen -t
```

Una vez que se ha creado un par de claves SSH, proporcione su clave pública al TAC de Cisco para su importación y, a continuación, continúe con la configuración del cliente. **No comparta su clave privada**.

Configuración del Cliente SSH

> **Nota: La conexión SSH para el acceso CLI no se realiza directamente a su dispositivo CES, sino a través de un túnel SSH hacia adelante a través de su host local que está conectado directamente a uno de nuestros proxies SSH. La primera parte de la conexión será a uno de nuestros servidores proxy y la segunda será al puerto de reenvío de túnel SSH en su host local.**

Para Windows:

Utilizaremos PuTTY para nuestro ejemplo, así que tenga en cuenta que los pasos pueden tener que modificarse ligeramente si se utiliza un cliente diferente. Además, asegúrese de que el cliente que esté utilizando se ha actualizado a la versión más reciente disponible.

Windows - Paso uno - Conexión al proxy SSH y puerto de reenvío abierto

1. Para el **nombre de host**, ingrese en el **servidor proxy** aplicable a su asignación de CES.
2. Expanda **Connection**, haga clic en **Data** e ingrese **dh-user** para el nombre de usuario de inicio de sesión automático.
3. Con **Connection** aún expandida, haga clic en **SSH** y marque para habilitar **No inicie ningún shell o comando**.
4. Expanda **SSH**, haga clic en **Auth** y **busque** su clave privada recién creada.
5. Con SSH aún expandido, haga clic en Túneles, proporcione un puerto de origen para **reenvío local** (cualquier puerto disponible en su dispositivo), ingrese el nombre de host de inicio de sesión (no el nombre de host que comienza con dh) de su dispositivo CES y luego haga clic en **Agregar**. En caso de que desee agregar varios dispositivos (por ejemplo: esa1, esa2 y sma1), puede agregar puertos de origen y nombres de host adicionales. A continuación, cualquier puerto agregado se reenviará cuando se inicie esta sesión.
6. Una vez que se hayan completado los pasos anteriores, vuelva a la categoría **session** y, a continuación, asigne el nombre y **guarde** su sesión.

Windows - Paso dos - Conexión a la CLI de su dispositivo CES

1. Abra y conéctese a la sesión que acaba de crear.
2. **Mientras mantiene abierta la sesión del servidor proxy SSH, abra una nueva sesión PuTTY haciendo clic con el botón derecho del ratón en la ventana y seleccionando Nueva sesión, ingrese 127.0.0.1 para la dirección IP, ingrese el puerto de origen usado anteriormente en el paso 5 y luego haga clic en Abrir.**
3. Una vez que haga clic en **Abrir**, se le solicitará que introduzca sus credenciales de CES y, a continuación, tendrá acceso a la CLI. (Estas serían las mismas credenciales utilizadas para acceder a la WUI)

Para Linux/MacOS:

Linux/MacOS - Paso uno: Conexión al proxy SSH y al puerto de reenvío abierto

1. Desde una nueva ventana de terminal, ingrese el siguiente comando:

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

Where:

`ssh -i`

Esto abrirá un puerto en su cliente local para ser reenviado al host y puerto dados en el lado remoto.

Linux/macOS - Paso dos - Conexión a la CLI de su dispositivo CES

1. Desde la misma o nueva ventana de terminal, ingrese el siguiente comando. Una vez introducida, se le pedirá que introduzca la contraseña de CES y, a continuación, deberá tener acceso a la CLI. (Estas serían las mismas credenciales utilizadas para acceder a la WUI)

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

Where:

`ssh`