Accesso all'interfaccia della riga di comando (CLI) della soluzione Cloud Email Security (CES)

Sommario

Introduzione

Questo documento descrive come accedere alla CLI dei dispositivi CES utilizzando Secure Shell (SSH) sulla piattaforma Windows o Linux/macOS.

Contributo di Dennis McCabe Jr, Cisco TAC Engineer.

Premesse

Per accedere alla CLI di CES Email Security Appliance (ESA) o Security Management Appliance (SMA), è necessario completare due fasi, entrambe descritte in dettaglio di seguito.

1. Generazione di una coppia di chiavi SSH
2. Configurazione del client SSH

Nota: le istruzioni che seguono devono coprire la maggior parte dei sistemi operativi utilizzati in natura; tuttavia, se quello che stai utilizzando non è presente nell'elenco o hai ancora bisogno di assistenza, contatta Cisco TAC e faremo del nostro meglio per fornire istruzioni specifiche. Si tratta solo di un piccolo frammento degli strumenti e dei client disponibili che possono essere utilizzati per eseguire questa attività.

Definizioni

Si prega di familiarizzare con alcune delle terminologie che saranno utilizzate in questo articolo.

Server proxy

Questi sono i server proxy SSH CES che verranno utilizzati per avviare la connessione SSH all'istanza CES. È necessario utilizzare un server proxy specifico per la regione in cui si trova il dispositivo. Ad esempio, se il nome host per l'accesso è **esa1.test.iphmx.com**, è necessario utilizzare uno dei server proxy **iphmx.com** dell'area **Stati Uniti**.

- **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
- **UE (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
- **USA (iphmx.com)** f4-ssh.iphmx.comf5-ssh.iphmx.com

Nome host di accesso

Questo è il nome host non proxy del CES ESA o SMA e inizierà con esa1 o sma1, e si trova in alto a destra della pagina Web quando si accede al Web User Interface (WUI). Il formato dovrebbe essere il seguente: esa[1-20].<allocazione>.<datacenter>.com o sma[1-20].<allocazione>.<datacenter>.com.

Generazione di una coppia di chiavi SSH

Per iniziare ad accedere ai dispositivi CES, occorre prima generare una coppia di chiavi SSH pubblica/privata e quindi fornire la chiave pubblica a Cisco TAC. Dopo che Cisco TAC ha importato la chiave pubblica, è possibile procedere con i passaggi successivi. **Non condividere la chiave privata**.

Per entrambi i passaggi riportati di seguito, il **tipo di chiave** deve essere **RSA** con una **lunghezza in bit** standard di **2048**.

Per Windows:

PuTTYgen o uno strumento simile può essere utilizzato per generare coppie di chiavi. Se si utilizza il sottosistema Windows per Linux (WSL), è inoltre possibile seguire le istruzioni riportate di seguito.

Per Linux/macOS:

Da una nuova finestra del terminale, è possibile eseguire ssh-keygen per creare una coppia di chiavi.

Esempio:

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

Dove:

```
ssh-keygen -t
```

Dopo aver creato una coppia di chiavi SSH, fornire la chiave pubblica a Cisco TAC per

l'importazione e procedere alla configurazione del client. **Non condividere la chiave privata**.

Configurazione del client SSH

> **Nota: la connessione SSH per l'accesso CLI non viene effettuata direttamente al dispositivo CES, bensì tramite un tunnel SSH in avanti attraverso l'host locale direttamente connesso a uno dei nostri proxy SSH. La prima parte della connessione sarà a uno dei nostri server proxy e la seconda alla porta di inoltro del tunnel SSH sull'host locale.**

Per Windows:

Per l'esempio verrà utilizzato PuTTY, quindi potrebbe essere necessario modificare leggermente i passaggi se si utilizza un client diverso. Verificare inoltre che il client in uso sia stato aggiornato alla versione più recente disponibile.

Windows - Primo passo - Connessione al proxy SSH e apertura della porta di inoltro

1. Per il **nome host**, immettere nel **server proxy** applicabile all'allocazione CES.
2. Espandere **Connessione**, fare clic su **Dati** e immettere **dh-user** come nome utente per l'accesso automatico.
3. Con **Connection** ancora espanso, fare clic su **SSH** e selezionare per abilitare **Don't start a shell or command** (Non avviare affatto una shell o un comando).
4. Espandere **SSH**, fare clic su **Auth** e **individuare** la chiave privata appena creata.
5. Con il protocollo SSH ancora espanso, fare clic su Tunnel, fornire una porta di origine per l'inoltro **locale** (qualsiasi porta disponibile sul dispositivo), immettere il **nome host di accesso** (non il nome host che inizia con dh) del dispositivo CES e fare clic su **Aggiungi**. Se si desidera aggiungere più dispositivi (ad esempio: esa1, esa2 e sma1), è possibile aggiungere ulteriori porte di origine e nomi host. Eventuali porte aggiunte verranno quindi inoltrate all'avvio della sessione.
6. Una volta completati i passaggi precedenti, tornare alla categoria **sessione**, quindi assegnare un nome alla sessione e **salvarla**.

Windows - Fase due - Connessione alla CLI del dispositivo CES

1. Aprire e connettersi alla sessione appena creata.
2. **Mantenendo aperta la sessione del server proxy SSH, aprire una nuova sessione PuTTy facendo clic con il pulsante destro del mouse sulla finestra e selezionando New Session, immettere 127.0.0.1 per l'indirizzo IP, immettere la porta di origine utilizzata in precedenza nel passaggio 5 e fare clic su Open.**
3. Dopo aver fatto clic su **Apri**, verrà richiesto di immettere le credenziali CES e di disporre dell'accesso alla CLI. Si tratta delle stesse credenziali utilizzate per accedere alla WUI

Per Linux/macOS:

Linux/macOS - Fase 1 - Connessione al proxy SSH e apertura della porta di inoltro

1. Da una nuova finestra del terminale, immettere il seguente comando:

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

```
ssh -i
```
Verrà aperta una porta sul client locale da inoltrare all'host specificato e alla porta sul lato remoto.

Linux/macOS - Fase due - Connessione alla CLI del dispositivo CES

1. Dalla stessa finestra o da una nuova finestra del terminale, immettere il comando seguente. Una volta immesso, verrà richiesto di immettere la password CES e di avere accesso alla CLI. (Si tratta delle stesse credenziali utilizzate per accedere alla WUI)

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

```
ssh
```