Accédez à l'interface de ligne de commande de votre solution CES

Table des matières

Introduction

Informations générales

Définitions

- Serveurs proxy
- Log In Nom d'hôte

Générer une paire de clés SSH

- Pour Windows :
- Pour Linux/macOS :

Configuration du client SSH

- Pour Windows :
- Pour Linux/macOS :

Introduction

Ce document décrit comment accéder à l'interface de ligne de commande (CLI) de vos périphériques de sécurité de messagerie électronique cloud (CES) en utilisant SSH sur la plate-forme Windows ou Linux/macOS.

Informations générales

Deux étapes doivent être effectuées pour accéder à l'interface de ligne de commande (CLI) de votre appliance de sécurité de la messagerie CES (ESA) ou de votre appliance de gestion de la sécurité (SMA). Ces deux étapes sont décrites en détail.

1. Générez une paire de clés SSH.
2. Configurez le client SSH.

Remarque : ces instructions couvrent la majeure partie des systèmes d'exploitation utilisés dans la nature ; toutefois, si ce que vous utilisez n'est pas répertorié ou si vous avez toujours besoin d'aide, contactez le TAC Cisco pour obtenir de l'aide et des instructions spécifiques. Il ne s'agit que d'un petit extrait des outils et des clients disponibles qui peuvent être utilisés pour accomplir cette tâche.

Définitions

Veuillez vous familiariser avec certaines des terminologies utilisées dans cet article.

Serveurs proxy

Il s'agit des serveurs proxy CES SSH que vous utilisez pour initier la connexion SSH à votre instance CES. Vous devez utiliser un serveur proxy spécifique à la région dans laquelle se trouve votre périphérique. Par exemple, si votre nom d'hôte de connexion est esa1.test.iphmx.com, vous utiliserez l'un des serveurs proxy iphmx.com de la région des États-Unis.

- AP (ap.iphmx.com)
  - f15-ssh.ap.iphmx.com
  - f16-ssh.ap.iphmx.com

- AWS (r1.ces.cisco.com)
  - p3-ssh.r1.ces.cisco.com
  - p4-ssh.r1.ces.cisco.com

- CA (ca.iphmx.com)
  - f13-ssh.ca.iphmx.com
  - f14-ssh.ca.iphmx.com

- UE (c3s2.iphmx.com)
  - f10-ssh.c3s2.iphmx.com
  - f11-ssh.c3s2.iphmx.com

- UE (eu.iphmx.com)
  - f17-ssh.eu.iphmx.com
  - f18-ssh.eu.iphmx.com

- États-Unis (iphmx.com)
  - f4-ssh.iphmx.com
  - f5-ssh.iphmx.com

Log In Nom d'hôte

Il s'agit du nom d'hôte non proxy de votre ESA ou SMA CES. Il commence par esa1 ou sma1 et se trouve en haut à droite de la page Web lorsque vous vous connectez à l'interface utilisateur

Web (WUI). Le format peut être : esa[1-20].<allocation>.<datacenter>.com ou sma[1-20].<allocation>.<datacenter>.com.

Générer une paire de clés SSH

Afin de commencer à accéder à vos périphériques CES, la première chose que vous devez faire est de générer une paire de clés SSH privées/publiques, puis de fournir la clé publique au TAC Cisco. Une fois que le TAC Cisco a importé votre clé publique, vous pouvez passer aux étapes suivantes.



Remarque : Ne partagez pas votre clé privée.

Pour les deux étapes répertoriées, le type de clé peut être RSA avec une longueur de bit standard de 2048.

Pour Windows :

PuTTYgen ou un outil similaire peut être utilisé pour générer des paires de clés. Vous pouvez également suivre les instructions indiquées si vous utilisez le sous-système Windows pour Linux (WSL).

Pour Linux/macOS :

À partir d'une nouvelle fenêtre de terminal, vous pouvez exécuter ssh-keygen pour créer une paire de clés.

Exemple :

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

Where:

```
ssh-keygen -t
```

```
-b

 -f
```

Une fois qu'une paire de clés SSH a été créée, fournissez votre clé publique au TAC Cisco pour l'importation, puis passez à la configuration du client.

Configuration du client SSH

Remarque : la connexion SSH pour l'accès CLI n'est pas faite directement à votre périphérique CES, mais plutôt par un tunnel SSH vers l'avant via votre localhost qui est directement connecté à l'un de nos proxys SSH. La première partie de la connexion est à l'un de nos serveurs proxy et la seconde partie est au port de transfert du tunnel SSH sur votre hôte local.

Pour Windows :

Vous utilisez PuTTY dans cet exemple. Veuillez noter que les étapes peuvent être légèrement modifiées si vous utilisez un autre client. Assurez-vous également que le client que vous utilisez a été mis à jour vers la dernière version disponible.

Windows - Étape 1 - Connectez-vous au proxy SSH et ouvrez le port de transfert

1. Pour le nom d'hôte, entrez dans le serveur proxy applicable à votre allocation CES.
2. Développez Connection, cliquez sur Data et entrez dh-user pour le nom d'utilisateur de connexion automatique.
3. Connection étant toujours développé, cliquez sur SSH et cochez la case pour activer Don't start a shell or command at all.
4. Développez SSH, cliquez sur Auth et accédez à votre clé privée nouvellement créée.
5. Avec SSH toujours développé, cliquez sur Tunnels, fournissez un port source pour le transfert local (tout port disponible sur votre périphérique), entrez dans le nom d'hôte de connexion (pas le nom d'hôte qui commence par dh) de votre périphérique CES, puis cliquez sur Add.
    1. Si vous souhaitez ajouter plusieurs périphériques (par exemple : esa1, esa2 et sma1), vous pouvez ajouter des ports source et des noms d'hôte supplémentaires. Tous les

ports ajoutés sont ensuite transférés au démarrage de cette session.

6. Une fois les étapes précédentes terminées, revenez à la catégorie session, puis nommez et enregistrez votre session.

Windows - Étape 2 - Connexion à l'interface de ligne de commande de votre périphérique CES

1. Ouvrez la session que vous venez de créer et connectez-vous.
2. Tout en maintenant la session du serveur proxy SSH ouverte, ouvrez une nouvelle session PuTTY en cliquant avec le bouton droit sur la fenêtre et en sélectionnant Nouvelle session. Entrez 127.0.0.1 pour l'adresse IP, entrez le port source utilisé précédemment à l'étape 5, puis cliquez sur Ouvrir.
3. Une fois que vous avez cliqué sur Open, vous êtes invité à saisir vos informations d'identification CES, puis à accéder à l'interface de ligne de commande. (Ces informations d'identification sont les mêmes que celles utilisées pour accéder à l'interface WUI.)

Pour Linux/macOS :

Linux/macOS - Étape 1 - Connectez-vous au proxy SSH et ouvrez le port de transfert

1. Dans une nouvelle fenêtre de terminal, entrez la commande suivante :

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

Where:

```
ssh -i
```

```
      -l dh-user -N -f
```

```
       -L
```

```
      :
```

```
       :22
```

Cela ouvre un port sur votre client local pour être transféré à l'hôte et au port donnés sur le côté distant.

Linux/macOS - Étape 2 - Connexion à l'interface de ligne de commande de votre périphérique CES

1. À partir de la même fenêtre de terminal ou d’une nouvelle fenêtre, entrez cette commande.
    1. Une fois entré, vous êtes invité à saisir votre mot de passe CES, puis à accéder à l'interface de ligne de commande (CLI). (Il s'agit des mêmes informations d'identification que celles utilisées pour accéder à l'interface WUI.)

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

Where:

```
ssh

     @127.0.0.1 -p
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.