Télécharger le fichier Allowlist/Blocklist à partir de CES SMA en utilisant SCP

Table des matières

Introduction

Ce document décrit comment télécharger le fichier allowlist/blocklist à partir de l'appliance de gestion sécurisée du cloud en utilisant SCP pour la sécurité de messagerie du cloud.

Conditions préalables

La procédure nécessite un accès à l'interface de ligne de commande (CLI). Il utilise le protocole Secure Copy Protocol (SCP) pour la sécurité de la messagerie électronique dans le cloud (CES).

Remarque : Les exemples de valeurs de ce document sont des espaces réservés. Remplacez-les par les valeurs du déploiement.

Exigences

- Vérifiez l'accès à l'interface de ligne de commande (CLI) sur le SMA.
- Fenêtres: PuTTY et PSCP installés.
- Linux/macOS : Outils clients OpenSSH installés (`ssh` et `scp`).
- Vérifiez l'accès à l'hôte proxy SSH, si nécessaire.
- Notez le port transféré localement configuré pour l'accès CLI SMA.
- Enregistrez le nom d'utilisateur CES.
- Enregistrez le chemin d'accès au fichier de clé privée si l'authentification basée sur la clé est requise.

Reportez-vous à la section Accès à l'interface de ligne de commande (CLI) de la solution de sécurité de la messagerie électronique dans le cloud (CES).

Solution

Le fichier CSV de liste d'autorisation/liste de blocage (SLBL) est stocké sous `/configuration/` sur le SMA. Si le nom de fichier exact est inconnu, répertoriez les fichiers disponibles et identifiez le CSV SLBL requis par nom de fichier et horodatage.

```
ls -l /configuration/slbl-*.csv
```

Par exemple, utilisez le résultat pour identifier un nom de fichier au format `slbl-<ID>-<TIMESTAMP>.csv`.

Pour Windows

1. Ouvrez une session PuTTY, ou un autre client SSH, et chargez la configuration de proxy utilisée pour se connecter au SMA. Laissez la session proxy ouverte.
2. Exécutez cette commande :

```
pscp -P <port> <username>@127.0.0.1:/configuration/slbl-<ID>-<TIMESTAMP>.csv C:/path/localsystem
```

- `<port>` : port transféré localement configuré pour l'accès SMA CLI.
- `<username>` : nom d'utilisateur CES.

Exemple :

```
pscp -P 2201 cesuser@127.0.0.1:/configuration/slbl-420DE9AD994-CBF5261-20190925T3228.csv C:/Users/examp
```

3. Vérifiez que le fichier CSV est téléchargé vers le chemin de destination local.

Pour Linux/macOS

1. Ouvrez une fenêtre de terminal.

2. Exécutez cette commande pour créer le transfert du port local via le serveur proxy :

```
ssh -i <private_key_path> -l dh-user -N -f <proxy_server> -L <port>:<hostname>:22
```

- `<chemin_clé_privée>` — chemin de clé privée.
- `<proxy_server>` : nom d'hôte du serveur proxy.
- `<port>` : port transféré localement configuré pour l'accès SMA CLI.
- `<hostname>` : nom d'hôte SMA.

Exemple :

```
ssh -i ~/.ssh/id_rsa -l dh-user -N -f proxy.example.com -L 2201:sma.example.com:22
```

3. Exécutez cette commande :

```
scp -P <port> <username>@127.0.0.1:/configuration/slbl-<ID>-<TIMESTAMP>.csv /path/localsystem
```

- `<port>` : port transféré localement configuré pour l'accès SMA CLI.
- `<username>` : nom d'utilisateur CES.

Exemple :

```
scp -P 2201 cesuser@127.0.0.1:/configuration/slbl-42ODE9AD994-CBF5261-20190925T3228.csv /Users/exampleu
```

4. Vérifiez que le fichier CSV est téléchargé vers le chemin de destination local.

Autres informations utiles

Accès à l'interface de ligne de commande (CLI) de la solution cloud de sécurisation de la messagerie électronique (CES)

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.