Descargar el archivo de lista de permitidos/bloqueados desde CES SMA mediante SCP

Contenido

Introducción

Este documento describe cómo descargar el archivo de lista de permitidos/lista de bloqueo del dispositivo de administración segura de la nube mediante SCP para Cloud Email Security.

Prerequisites

El procedimiento requiere acceso a la interfaz de línea de comandos (CLI). Utiliza el protocolo de copia segura (SCP) para Cloud Email Security (CES).

Nota: Los valores de ejemplo de este documento son marcadores de posición. Sustitúyalos por los valores de la implementación.

Requirements

- Asegúrese de acceder a la interfaz de línea de comandos (CLI) en el SMA.
- Windows: PuTTY y PSCP instalados.
- Linux/macOS: Herramientas de cliente OpenSSH instaladas (`ssh` y `scp`).
- Asegúrese de acceder al host de proxy SSH, si es necesario.
- Registre el puerto reenviado localmente configurado para el acceso CLI de SMA.
- Registre el nombre de usuario de CES.

- Registre la ruta del archivo de clave privada si se requiere autenticación basada en claves.

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

Solución

El archivo CSV de lista de permitidos/lista de bloqueo (SLBL) se almacena en `/configuration/` en el SMA. Si no se conoce el nombre de archivo exacto, enumere los archivos disponibles e identifique el CSV de SLBL requerido por nombre de archivo y marca de tiempo.

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

Por ejemplo, utilice el resultado para identificar un nombre de archivo en el formato `slbl-<ID>-<TIMESTAMP>.csv`.

Para Windows

1. Abra una sesión PuTTY, u otro cliente SSH, y cargue la configuración de proxy utilizada para conectarse al SMA. Deje abierta la sesión de proxy.
2. Ejecute este comando:

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

- `<port>`: puerto reenviado localmente configurado para el acceso CLI de SMA.
- `<username>` — Nombre de usuario CES.

Por ejemplo:

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

3. Compruebe que el archivo CSV se descarga en la ruta de acceso de destino local.

Para Linux/macOS

1. Abra una ventana de terminal.
2. Ejecute este comando para crear el reenvío del puerto local a través del servidor proxy:

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

- `<private_key_path>`: ruta de clave privada.
- `<proxy_server>`: nombre de host del servidor proxy.
- `<port>`: puerto reenviado localmente configurado para el acceso CLI de SMA.
- `<hostname>`: nombre de host SMA.

Por ejemplo:

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

3. Ejecute este comando:

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

- `<port>`: puerto reenviado localmente configurado para el acceso CLI de SMA.
- `<username>` — Nombre de usuario CES.

Por ejemplo:

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

4. Compruebe que el archivo CSV se descarga en la ruta de acceso de destino local.

Contenido relacionado

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).