Scarica il file Allowlist/Blocklist da CES SMA utilizzando SCP

Sommario

Introduzione

In questo documento viene descritto come scaricare il file allowlist/blocklist da cloud Secure Management Appliance utilizzando SCP per Cloud Email Security.

Prerequisiti

La procedura richiede l'accesso all'interfaccia della riga di comando (CLI). Utilizza Secure Copy Protocol (SCP) per Cloud Email Security (CES).

Nota: I valori di esempio in questo documento sono segnaposto. Sostituirli con i valori per la distribuzione.

Requisiti

- Garantire l'accesso all'interfaccia CLI (Command Line Interface) sullo SMA.
- Windows: PuTTY e PSCP installati.
- Linux/macOS: Strumenti client OpenSSH installati (`ssh` e `scp`).
- Verificare l'accesso all'host proxy SSH, se necessario.
- Registrare la porta inoltrata localmente configurata per l'accesso alla CLI di SMA.
- Registrare il nome utente CES.
- Registrare il percorso del file della chiave privata se è necessaria l'autenticazione basata su chiavi.

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

Soluzione

Il file CSV allowlist/blocklist (SLBL) viene archiviato in `/configuration/` sullo SMA. Se non si conosce il nome esatto del file, elencare i file disponibili e identificare il file SLBL CSV richiesto in base al nome e all'indicatore orario.

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

Ad esempio, utilizzare l'output per identificare un nome file nel formato `slbl-<ID>-<TIMESTAMP>.csv`.

Per Windows

1. Aprire una sessione PuTTy o un altro client SSH, quindi caricare la configurazione proxy utilizzata per connettersi all'SMA. Lasciare aperta la sessione proxy.
2. Eseguire questo comando:

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

- `<porta>`: porta inoltrata localmente configurata per l'accesso alla CLI di SMA.
- `<username>` — Nome utente CES.

Ad esempio:

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

3. Verificare che il file CSV venga scaricato nel percorso di destinazione locale.

Per Linux/macOS

1. Aprire una finestra di terminale.
2. Eseguire questo comando per creare la porta locale per l'inoltro tramite il server proxy:

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

- <private_key_path> — percorso della chiave privata.
- <proxy_server> — nome host del server proxy.
- <porta>: porta inoltrata localmente configurata per l'accesso alla CLI di SMA.
- <hostname> — Nome host SMA.

Ad esempio:

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

3. Eseguire questo comando:

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

- <porta>: porta inoltrata localmente configurata per l'accesso alla CLI di SMA.
- <username> — Nome utente CES.

Ad esempio:

```
scp -P 2201 cesuser@127.0.0.1:/configuration/slbl-420DE9AD994-CBF5261-20190925T3228.csv /Users/exampleu
```

4. Verificare che il file CSV venga scaricato nel percorso di destinazione locale.

Contenuto correlato

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).