Download de arquivo de lista de permissão/bloqueio do CES SMA usando SCP

Contents

Introdução

Este documento descreve como baixar o arquivo de lista de permissão/bloqueio do dispositivo de gerenciamento seguro de nuvem usando o SCP para segurança de e-mail na nuvem.

Pré-requisitos

O procedimento requer acesso à Interface de Linha de Comando (CLI). Ele usa o protocolo SCP (Secure Copy Protocol, protocolo de cópia segura) para o Cloud Email Security (CES).

Note: Exemplos de valores neste documento são espaços reservados. Substitua-os pelos valores da implantação.

Requisitos

- Assegure o acesso à Interface de Linha de Comando (CLI) no SMA.
- Windows: PuTTY e PSCP instalados.
- Linux/MacOS: Ferramentas de cliente OpenSSH instaladas (`ssh` e `scp`).
- Assegure o acesso ao host proxy SSH, se necessário.
- Registre a porta encaminhada localmente configurada para acesso SMA CLI.
- Registre o nome de usuário CES.
- Registre o caminho do arquivo de chave privada se a autenticação baseada em chave for necessária.

Consulte Como acessar a interface de linha de comando (CLI) da solução Cloud Email Security (CES).

Solução

O arquivo CSV allowlist/blocklist (SLBL) é armazenado em `/configuration/` no SMA. Se o nome exato do arquivo não for conhecido, liste os arquivos disponíveis e identifique o CSV SLBL necessário por nome de arquivo e carimbo de data/hora.

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

Por exemplo, use a saída para identificar um nome de arquivo no formato `slbl-<ID>-<TIMESTAMP>.csv`.

Para Windows

1. Abra uma sessão PuTTY ou outro cliente SSHe carregue a configuração de proxy usada para se conectar ao SMA. Deixe a sessão proxy aberta.
2. Execute este comando:

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

- `<port>` — porta encaminhada localmente configurada para acesso SMA CLI.
- `<username>` — Nome de usuário CES.

Por exemplo:

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

3. Verifique se o arquivo CSV foi baixado para o caminho de destino local.

Para Linux/macOS

1. Abra uma janela do terminal.

2. Execute este comando para criar a porta local adiante através do servidor proxy:

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

- `<private_key_path>` — caminho da chave privada.
- `<proxy_server>` — nome do host do servidor proxy.
- `<port>` — porta encaminhada localmente configurada para acesso SMA CLI.
- `<hostname>` — Nome de host do SMA.

Por exemplo:

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

3. Execute este comando:

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

- `<port>` — porta encaminhada localmente configurada para acesso SMA CLI.
- `<username>` — Nome de usuário CES.

Por exemplo:

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

4. Verifique se o arquivo CSV foi baixado para o caminho de destino local.

Conteúdo relacionado

Acesso à interface de linha de comando (CLI) da solução Cloud Email Security (CES)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.