Alcançando o comando line interface(cli) de sua solução da Segurança do email da nuvem (CES)

Índice

Introdução

Este documento descreve como alcançar o CLI de seus dispositivos CES utilizando o Shell Seguro (ssh) na plataforma de Windows ou de Linux/macOS.

Contribuído pelo júnior de Dennis McCabe, engenheiro de TAC da Cisco.

Informações de Apoio

Há duas fases que precisam de ser terminadas a fim alcançar o CLI de sua ferramenta de segurança do email CES (ESA) ou de dispositivo do Gerenciamento de segurança (S A), ambo será discutido em detalhe abaixo.

1. Gerando um par de chaves SSH
2. Configurando o cliente SSH

   Nota: Os sentidos abaixo devem cobrir o volume dos sistemas operacionais usados no selvagem; contudo, se o que você está usando não é listado ou você ainda precisa o auxílio, contacte por favor o tac Cisco e nós faremos nosso melhor para fornecer a instrução específica. Estes são apenas um snippet pequeno das ferramentas e os clientes disponíveis que possam ser usados para realizar esta tarefa.

Definições

Familiarize-se por favor com as algumas das terminologias que serão usadas neste artigo.

Servidores proxy

Estes são os servidores proxy que CES SSH você se usará para iniciar a conexão de SSH a seu exemplo CES. Você precisará de utilizar um específico do servidor proxy à região que seu dispositivo é encontrado dentro. Por exemplo, se seu hostname do início de uma sessão é **esa1.test.iphmx.com**, você usaria um dos servidores proxy de **iphmx.com na** região **E.U**.

- **AP (ap.iphmx.com)** f15-ssh.ap.iphmx.comf16-ssh.ap.iphmx.com
- **AW (r1.ces.cisco.com)** p3-ssh.r1.ces.cisco.comp4-ssh.r1.ces.cisco.com
- **CA (ca.iphmx.com)** f13-ssh.ca.iphmx.comf14-ssh.ca.iphmx.com
- **EU (c3s2.iphmx.com)** f10-ssh.c3s2.iphmx.comf11-ssh.c3s2.iphmx.com
- **E.U. (iphmx.com)** f4-ssh.iphmx.comf5-ssh.iphmx.com

Hostname do início de uma sessão

Este é o hostname do NON-proxy de seu CES ESA ou S A e começará com algo como esa1 ou sma1, e pode ser encontrado no direita superior do página da web quando você vai entrar à relação de usuário de web (WUI). O formato deve ser como segue: esa[1-20].<allocation>.<datacenter>.com ou sma[1-20].<allocation>.<datacenter>.com.

Gerando um par de chaves SSH

A fim obter começada em alcançar seus dispositivos CES, a primeira coisa que você precisará de fazer é gerar par de chaves privado/público SSH e fornecer então a chave pública ao tac Cisco. Uma vez que o tac Cisco importou sua chave pública, você pode então continuar às próximas etapas. **Não compartilhe de sua chave privada**.

Para uma ou outra etapas abaixo, o **tipo chave** deve ser **RSA** com um **comprimento de bit** padrão de **2048**.

Para Windows:

PuTTYgen ou uma ferramenta similar podem ser usados gerando pares de chaves. Você pode igualmente seguir as instruções abaixo se você utiliza o subsistema de Windows para Linux (WSL).

Para Linux/macOS:

De uma janela terminal nova, você pode executar o SSH-keygen para criar um par de chaves.

Exemplo:

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

Where:

```
ssh-keygen -t <key type> -b <bit length> -f <filename>
```

Uma vez que um par de chaves SSH foi criado, forneça por favor sua chave pública ao tac Cisco para a importação e continue então à configuração de cliente. **Não compartilhe de sua chave privada**.

Configurando o cliente SSH

> Nota: A conexão de SSH para o acesso CLI não é feita diretamente a seu dispositivo CES, mas pelo contrário através de um túnel SSH dianteiro através de seu host local que é conectado diretamente a um de nossos proxys SSH. O primeiro parte da conexão será a um de nossos servidores proxy e o segundo será à porta da transmissão do túnel SSH em seu host local.

Para Windows:

Nós estaremos usando a massa de vidraceiro para nosso exemplo, satisfazemos assim notamos que as etapas podem precisar de ser alterado levemente se usando um cliente diferente. Também, certifique-se por favor de que qualquer cliente que você se está usando foi atualizado à versão recentemente disponível.

Windows - Etapa um - Conecte ao proxy SSH e abra a porta da transmissão

1. Para o **hostname**, entre no **servidor proxy** aplicável a sua atribuição CES.
2. Expanda a **conexão**, clique **dados** e incorpore o DH-**USER** para o username do auto-início de uma sessão.
3. Com a **conexão** ainda expandida, clique o **SSH** e a verificação para permitir **não começam um shell ou um comando de todo**.
4. Expanda o **SSH**, clique o **AUTH** e **consulte a** sua chave privada recém-criado.
5. Com o **SSH** ainda expandido, os **túneis do** clique, fornecem uma **porta de origem** para a transmissão **local** (algum porto disponível em seu dispositivo), entram no **hostname do início de uma sessão** (não o hostname que começa com AO) de seu dispositivo CES e clicam então **adicionam**. Caso que você deseja adicionar os dispositivos múltiplos (IE: esa1, esa2, e sma1), você pode adicionar portas de origem e nomes de host adicionais. Então, todas as portas adicionadas serão enviadas quando esta sessão é começada.
6. Uma vez as etapas acima foram terminadas, continuam de volta à categoria da **sessão** e então nomeiam e **salvar** sua sessão.

Windows - Etapa dois - Conexão ao CLI de seu dispositivo CES

1. Abra e conecte à sessão que você apenas criou.
2. **Ao manter a sessão do servidor proxy SSH aberta, abra uma sessão nova da massa de vidraceiro clicando com o botão direito no indicador e selecionando a sessão nova, entre em 127.0.0.1 para o endereço IP de Um ou Mais Servidores Cisco ICM NT, entre na porta de origem usada previamente na etapa 5 e clique então aberto.**
3. Uma vez que você clica **aberto**, você estará alertado incorporar suas credenciais CES e deve então ter o acesso ao CLI. (Estas seriam as mesmas credenciais usadas para alcançar o WUI)

Para Linux/macOS:

Linux/macOS - Etapa um - Conecte ao proxy SSH e abra a porta da transmissão

1. De uma janela terminal nova, inscreva o comando seguinte:

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

Where:

```
ssh -i <your private key> -l dh-user -N -f <proxy server for your allocation> -L <source port>:<login hostname>:22
```

Isto abrirá uma porta em seu cliente local a ser enviado ao host dado e a porta no lado remoto.

Linux/macOS - Etapa dois - Conexão ao CLI de seu dispositivo CES

1. Do mesmo ou da janela terminal nova, incorpore o comando abaixo. Uma vez que inscrito, você será alertado incorporar sua senha CES e deve então ter o acesso ao CLI. (Estas seriam as mesmas credenciais usadas para alcançar o WUI)

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

Where:

```
ssh <your CES username>@127.0.0.1 -p <source port for forwarding assigned in previous step>
```