CES(Cloud Email Security) 솔루션의 CLI(Command Line Interface) 액세스

목차

소개

이 문서에서는 Windows 또는 Linux/macOS 플랫폼에서 SSH(Secure Shell)를 사용하여 CES 디바이스의 CLI에 액세스하는 방법에 대해 설명합니다.

기고자: Dennis McCable Jr, Cisco TAC 엔지니어

배경 정보

CES ESA(Email Security Appliance) 또는 SMA(Security Management Appliance)의 CLI에 액세스하기 위해 2단계를 완료해야 하는 단계가 있습니다. 이 두 단계 모두 아래에서 자세히 설명합니다.

1. SSH 키 쌍 생성
2. SSH 클라이언트 구성

참고: 아래 지침은 야생에서 사용되는 많은 운영 체제에 대해 설명합니다.그러나 사용 중인 항목이 목록에 없거나 지원이 계속 필요한 경우 Cisco TAC에 연락하여 특정 지침을 제공하기 위해 최선을 다하겠습니다.이 작업은 이 작업을 수행하는 데 사용할 수 있는 툴과 클라이언트의 작은 조각에 불과합니다.

정의

이 문서에서 사용할 용어 중 일부를 숙지하십시오.

프록시 서버

CES 인스턴스에 대한 SSH 연결을 시작하는 데 사용할 CES SSH 프록시 서버입니다.디바이스가

있는 지역에 해당하는 프록시 서버를 사용해야 합니다.예를 들어 로그인 호스트 이름이 esa1.test.iphmx.com인 경우 **미국** 지역에서 **iphmx.com** 프록시 서버 중 하나를 사용합니다.

- **AP(ap.iphmx.com)** f15-ssh.ap.iphmx.comf16-ssh.ap.iphmx.com
- **AWS(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
- **EU(eu.iphmx.com)** f17-ssh.eu.iphmx.comf18-ssh.eu.iphmx.com
- **미국(iphmx.com)** f4-ssh.iphmx.comf5-ssh.iphmx.com

로그인 호스트 이름

CES ESA 또는 SMA의 비 프록시 호스트 이름이며 esa1 또는 sma1 같은 것으로 시작되며, WUI(Web User Interface)에 로그인하면 웹 페이지의 오른쪽 위에 있습니다. 형식은 다음과 같아야 합니다.esa[1-20].<allocation>.<datacenter>.com 또는 sma[1-20].<allocation>.<datacenter>.com.

SSH 키 쌍 생성

CES 디바이스 액세스를 시작하려면 먼저 프라이빗/퍼블릭 SSH 키 쌍을 생성한 다음 Cisco TAC에 공개 키를 제공해야 합니다.Cisco TAC에서 공개 키를 가져오면 다음 단계로 진행할 수 있습니다.**개인 키를 공유하지 마십시오**.

아래 단계 중 하나에서 **키 유형**은 표준 **비트 길이**가 **2048**인 **RSA**여야 합니다.

Windows의 경우:

PuTTYgen 또는 유사한 툴을 사용하여 키 쌍을 생성할 수 있습니다.WSL(Windows Subsystem for Linux)을 사용하는 경우에도 아래 지침을 따를 수 있습니다.

Linux/macOS의 경우:

새 터미널 창에서 ssh-keygen을 실행하여 키 쌍을 생성할 수 있습니다.

예:

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

위치:

```
ssh-keygen -t
```

SSH 키 쌍이 생성되면 가져오기를 위해 Cisco TAC에 공개 키를 제공한 다음 클라이언트 구성으로 진행하십시오. **개인 키를 공유하지 마십시오**.

SSH 클라이언트 구성

> **참고: CLI 액세스를 위한 SSH 연결은 CES 디바이스에 직접 연결되지 않고 로컬 호스트를 통**

해 SSH 터널을 통해 전달되며, 이 터널은 SSH 프록시 중 하나에 직접 연결됩니다.연결의 첫 번째 부분은 프록시 서버 중 하나에 연결되며, 두 번째 부분은 로컬 호스트의 SSH 터널 전달 포트에 연결됩니다.

Windows의 경우:

여기서는 PuTTY를 사용하겠습니다. 다른 클라이언트를 사용하는 경우 단계를 약간 수정해야 할 수도 있습니다.또한 사용 중인 클라이언트가 가장 최근에 사용 가능한 버전으로 업데이트되었는지 확인하십시오.

Windows - 1단계 - SSH 프록시에 연결 및 포워딩 포트 열기

1. 호스트 **이름**에 CES 할당에 적용 가능한 **프록시 서버**를 입력합니다.
2. Connection(**연결**)을 확장하고 **Data(데이터)**를 클릭한 다음 자동 로그인 사용자 이름에 dh-user를 입력합니다.
3. Connection(**연결)이** 계속 확장되면 **SSH**를 클릭하고 Don**'t start a shell or command at all을 활성화하려면 선택합니다**.
4. SSH**를** 확장하고 **Auth**(인증)를 **클릭하고** 새로 생성한 개인 키를 찾습니다.
5. SSH**가** 계속 확장되면 **Tunnels**를 클릭하고 **로컬** 포워딩을 위한 **소스 포트**(디바이스의 사용 가능한 포트)를 제공하고 **CES 디바이스의 로그인 호스트 이름(dh로 시작하는 호스트 이름 아님)을 입력한 다음 Add를 클릭합니다.** 여러 디바이스(예:esa1, esa2 및 sma1) 소스 포트 및 호스트 이름을 추가할 수 있습니다.그러면 이 세션이 시작되면 추가된 모든 포트가 전달됩니다.
6. 위의 단계가 완료되면 **세션** 카테고리로 돌아가 이름을 지정하고 세션**을** 저장합니다.

Windows - 2단계 - CES 디바이스의 CLI에 연결

1. 방금 생성한 세션을 열고 연결합니다.
2. **SSH 프록시 서버 세션을 계속 연 상태로 유지하면서 창을 마우스 오른쪽 버튼으로 클릭하고 New Session(새 세션)을 선택하여 새 PuTTY 세션을 열고 IP 주소에 127.0.0.1을 입력하고 5단계에서 이전에 사용한 소스 포트를 입력한 다음 Open(열기)을 클릭합니다.**
3. **열기를 클릭하면 CES 자격 증명을 입력하라는 메시지가 표시되고 CLI에 액세스할 수 있어야 합니다. 이 자격 증명은 WUI에 액세스하는 데 사용되는 자격 증명과 같습니다.**

Linux/macOS의 경우:

Linux/macOS - 1단계 - SSH 프록시에 연결 및 포워딩 포트 열기

1. 새 터미널 창에서 다음 명령을 입력합니다.

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

위치:

```
ssh -i
```

이렇게 하면 로컬 클라이언트의 포트가 열려 원격 측의 지정된 호스트 및 포트로 전달됩니다.

Linux/macOS - 2단계 - CES 디바이스의 CLI에 연결

1. 동일한 터미널 또는 새 터미널 창에서 아래 명령을 입력합니다. CES 비밀번호를 입력하면

CLI에 대한 액세스 권한이 부여됩니다. WUI에 액세스하는 데 사용되는 자격 증명과 동일합니다.

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

위치:

```
ssh
```