Cisco ESA/WSA/SMA의 원격 액세스 FAQ에 대한 Technote

목차

소개

이 문서에서는 Cisco Content Security Appliance에서 Cisco Technical Support가 원격 액세스를 사용하는 것과 관련하여 자주 묻는 질문에 대한 답변을 제공합니다. 여기에는 Cisco ESA(Email Security Appliance), Cisco WSA(Web Security Appliance) 및 Cisco SMA(Security Management Appliance)가 포함됩니다.

사전 요구 사항

사용되는 구성 요소

이 문서의 정보는 모든 버전의 AsyncOS를 실행하는 Cisco Content Security Appliance를 기반으로 합니다.

원격 액세스란?

원격 액세스는 Cisco Content Security Appliance에서 Cisco의 보안 호스트로 활성화된 SSH(Secure Shell) 연결입니다. 원격 세션이 활성화되면 Cisco 고객 지원에서만 어플라이언스에 액세스할 수 있습니다. 원격 액세스를 통해 Cisco 고객 지원에서 어플라이언스를 분석할 수 있습니다. 지원은 어플라이언스와 upgrades.ironport.com 서버 간에 이 절차가 생성하는 SSH 터널을 통

해 어플라이언스에 액세스합니다.

원격 액세스 작동 방식

원격 액세스 연결이 시작되면 어플라이언스는 다음 Cisco Content Security 서버 중 하나의 구성/선택한 포트에 어플라이언스의 SSH 연결을 통해 안전한 임의 고소스 포트를 엽니다.

IP 주소	호스트 이름	사용
63.251.108.107	upgrades.ironport.com	모든 Content Security Appliance
63.251.108.107	c.tunnels.ironport.com	C-Series 어플라이언스(ESA)
63.251.108.107	x.tunnels.ironport.com	X-Series 어플라이언스(ESA)
63.251.108.107	m.tunnels.ironport.com	M 시리즈 어플라이언스(SMA)
63.251.108.107	s.tunnels.ironport.com	S 시리즈 어플라이언스(WSA)

위에 나열된 서버 중 하나에 대한 아웃바운드 연결을 허용하도록 고객 방화벽을 구성해야 할 수도 있습니다.방화벽에 SMTP 프로토콜 검사가 활성화된 경우 터널이 설정되지 않습니다.Cisco에서 원격 액세스를 위해 어플라이언스로부터의 연결을 수락하는 포트는 다음과 같습니다.

- 22
- 25(기본값)
- 53
- 80
- 443
- 4766

원격 액세스 연결은 하드 코딩된 IP 주소가 아니라 호스트 이름에 대해 수행됩니다. 아웃바운드 연결을 설정하려면 어플라이언스에 DNS(Domain Name Server)를 구성해야 합니다.

고객 네트워크에서 일부 프로토콜 인식 네트워크 디바이스는 프로토콜/포트 불일치로 인해 이 연결을 차단할 수 있습니다. 일부 SMTP(Simple Mail Transport Protocol) 인식 디바이스는 연결을 중단할 수도 있습니다.차단된 프로토콜 인식 디바이스 또는 아웃바운드 연결이 있는 경우 기본값(25) 이외의 포트를 사용해야 할 수 있습니다.터널의 원격 끝에 대한 액세스는 Cisco 고객 지원부로만 제한됩니다. 어플라이언스에 대한 원격 액세스 연결을 설정하거나 문제를 해결하려는 경우 방화벽/네트워크에서 아웃바운드 연결을 검토했는지 확인하십시오.

> **참고:**Cisco 고객 지원 엔지니어가 원격 액세스를 통해 어플라이언스에 연결되면 어플라이언스의 시스템 프롬프트가 *(SERVICE)를 표시합니다*.

원격 액세스를 활성화하는 방법

> **참고:**"Enabling Remote Access for Cisco Technical Support Personnel"에 대한 지침은 어플라이언스의 사용 설명서 및 AsyncOS 버전을 참조하십시오.

> **참고:**attach@cisco.com으로 이메일을 통해 전송된 첨부 파일은 전송 중에 안전하지 않을 수 있습니다.Support Case Manager는 케이스에 정보를 업로드하는 Cisco의 기본 보안 옵션입니다.다른 파일 업로드 옵션의 보안 및 크기 제한 사항에 대해 자세히 알아보려면Cisco 기술 지원 센터에 고객 파일 업로드

인터넷에서 연결할 수 있는 포트를 식별합니다.기본값은 포트 25이며, 이는 대부분의 환경에서 작동합니다. 시스템은 이메일 메시지를 전송하기 위해 해당 포트를 통한 일반적인 액세스를 필요로 하기 때문입니다.이 포트를 통한 연결은 대부분의 방화벽 구성에서 허용됩니다.

CLI

CLI를 통해 원격 액세스 연결을 설정하려면 관리자 사용자로 다음 단계를 완료합니다.

1. techsupport 명령을 **입력합니다.**
2. TUNNEL **선택**
3. Generate(생성) 또는 *Enter(*임의 시드 문자열 입력)를 선택합니다.
4. 연결의 포트 번호 지정
5. 서비스 액세스를 활성화하려면 "**Y**"로 응답합니다.

현재 원격 액세스가 활성화됩니다. 이제 어플라이언스는 Cisco의 Secure Bastion 호스트에 대한 보안 연결을 설정합니다. 케이스를 지원하는 TAC 엔지니어에게 생성된 어플라이언스 일련 번호와 시드 문자열을 모두 제공합니다.

GUI

GUI를 통해 관리자 사용자로 원격 액세스 연결을 설정하려면 다음 단계를 완료합니다.

1. Help **and Support(도움말 및 지원) > Remote Access**(ESA, SMA용), **Support and Help(지원 및 도움말) > Remote Access**(WSA용)로 이동합니다.
2. Enable(활성화)을 **클릭합니다.**
3. 시드 문자열의 메서드를 선택합니다.
4. Initiate connection via secure tunnel(*보안 터널을 통해 연결 시작*) 확인란을 선택하고 연결에 대한 포트 번호를 지정해야 합니다.
5. Submit(제출)을 **클릭합니다.**

현재 원격 액세스가 활성화됩니다. 이제 어플라이언스는 Cisco의 Secure Bastion 호스트에 대한 보안 연결을 설정합니다. 케이스를 지원하는 TAC 엔지니어에게 생성된 어플라이언스 일련 번호와 시드 문자열을 모두 제공합니다.

원격 액세스를 비활성화하는 방법

CLI

1. techsupport 명령을 **입력합니다.**
2. 사용 안 함 **선택**
3. "서비스 액세스를 사용하지 않도록 설정하시겠습니까?"라는 메시지가 표시되면 "**Y**"로 응답합니다.

GUI

1. Help **and Support(도움말 및 지원) > Remote Access(원격 액세스**(ESA, SMA), Support and **Help(지원 및 도움말) > Remote Access(WSA**용)(WSA)로 이동합니다.
2. Disable(비활성화)을 **클릭합니다.**
3. GUI 출력에 "Success — Remote Access has been disabled(성공 — 원격 액세스가 비활성화

됨)"가 표시됩니다.

원격 액세스 연결을 테스트하는 방법

어플라이언스에서 Cisco로의 연결에 대한 초기 테스트를 수행하려면 다음 예를 사용하십시오.

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

위에 나열된 포트에 대해 연결을 테스트할 수 있습니다.22, 25, 53, 80, 443 또는 4766 연결이 실패하면 패킷 캡처를 실행하여 어플라이언스/네트워크에서 연결이 실패하는 위치를 확인해야 할 수 있습니다.

원격 액세스가 SMA에서 작동하지 않는 이유는 무엇입니까?

SMA가 인터넷에 직접 액세스하지 않고 로컬 네트워크에 있는 경우 SMA에서 원격 액세스를 활성화할 수 없습니다. 이 경우 ESA 또는 WSA에서 원격 액세스를 활성화할 수 있으며 SMA에서 SSH 액세스를 활성화할 수 있습니다.이를 통해 Cisco Support는 먼저 ESA/WSA에 대한 원격 액세스를 통해 연결한 다음 SSH를 통해 ESA/WSA에서 SMA에 연결할 수 있습니다. 이를 위해서는 포트 22에서 ESA/WSA와 SMA 간의 연결이 필요합니다.

> **참고:**"Enable Remote Access to Appliances Without a Direct Internet Connection(직접 인터넷 연결 없이 어플라이언스에 대한 원격 액세스 활성화)"에 대한 지침은 어플라이언스의 사용 설명서 및 AsyncOS 버전을 참조하십시오.

CLI

CLI를 통해 원격 액세스 연결을 설정하려면 관리자 사용자로 다음 단계를 완료합니다.

1. techsupport 명령을 **입력합니다.**
2. SSHACCESS **선택**
3. Generate(생성) 또는 *Enter(*임의 시드 문자열 입력)를 선택합니다.
4. 서비스 액세스를 활성화하려면 **"Y"**로 응답합니다.

현재 원격 액세스가 활성화됩니다. CLI 출력에 시드 문자열이 표시됩니다. Cisco 고객 지원 엔지니어에게 이 정보를 제공하십시오. CLI 출력에는 기기 일련 번호를 포함한 연결 상태 및 원격 액세스 세부 정보도 표시됩니다. 고객 고객 지원 엔지니어에게 이 일련 번호를 제공하십시오.

GUI

GUI를 통해 관리자 사용자로 원격 액세스 연결을 설정하려면 다음 단계를 완료합니다.

1. Help **and Support(도움말 및 지원) > Remote Access**(ESA, SMA용), **Support and Help(지원 및 도움말) > Remote Access**(WSA용)로 이동합니다.
2. Enable(활성화)을 **클릭합니다.**

3. 시드 문자열의 메서드를 선택합니다.
4. Initiate connection via secure tunnel(*보안 터널을 통해 연결 시작*) 확인란을 선택하지 마십시오.
5. Submit(제출)을 **클릭합니다.**

현재 원격 액세스가 활성화됩니다. GUI 출력은 성공 메시지와 어플라이언스의 시드 문자열을 표시합니다. Cisco 고객 지원 엔지니어에게 이 정보를 제공하십시오. GUI 출력에는 연결 상태 및 어플라이언스 일련 번호를 포함한 원격 액세스 세부사항도 표시됩니다. 고객 고객 지원 엔지니어에게 이 일련 번호를 제공하십시오.

SSHACCESS에 대해 활성화된 경우 원격 액세스를 비활성화하는 방법

SSHACCESS에 대한 원격 액세스를 비활성화하는 절차는 위에서 설명한 단계와 동일합니다.

문제 해결

어플라이언스가 원격 액세스를 활성화하지 못하고 나열된 포트 중 하나를 통해 upgrades.ironport.com에 연결할 수 없는 경우 어플라이언스에서 직접 패킷 캡처를 실행하여 아웃바운드 연결이 실패하는 원인을 검토해야 합니다.

> **참고:**"패킷 캡처 실행"에 대한 지침은 어플라이언스의 사용 설명서 및 AsyncOS 버전을 참조하십시오.

Cisco 고객 지원 엔지니어가 문제 해결을 검토하고 지원하기 위해 .pcap 파일을 제공하도록 요청할 수 있습니다.

관련 정보

- ESA FAQ:ESA에서 사용 가능한 관리 액세스 레벨은 무엇입니까?
- Cisco Email Security Appliance 제품 지원
- Cisco Web Security 제품 지원
- Cisco Content Security Management Appliance 제품 지원
- 기술 지원 및 문서 – Cisco Systems