

콘텐츠 보안 FAQ:Content Security Appliance에서 CLI에 액세스하려면 어떻게 해야 합니까?

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[Content Security Appliance에서 CLI에 액세스하려면 어떻게 해야 합니까?](#)

소개

이 문서에서는 Cisco Content Security Appliance에서 텔넷 또는 SSH(Secure Shell) 클라이언트를 통해 CLI에 액세스하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA(Email Security Appliance)
- Cisco WSA(Web Security Appliance)
- Cisco SMA(Security Management Appliance)
- AsyncOS

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ESA AsyncOS, 모든 버전
- Cisco WSA AsyncOS, 모든 버전
- Cisco SMA 버전 AsyncOS, 모든 버전

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

참고:이 문서는 Cisco에서 유지 관리하거나 지원하지 않는 소프트웨어를 참조합니다.이 정보

는 귀하의 편의를 위해 제공됩니다. 자세한 내용은 소프트웨어 공급업체에 문의하십시오.

Content Security Appliance에서 CLI에 액세스하려면 어떻게 해야 하나요?

텔넷 클라이언트 또는 SSH 클라이언트를 사용하여 어플라이언스의 CLI에 액세스할 수 있습니다. 그러나 텔넷 프로토콜은 암호화되지 않으므로 텔넷을 통해 어플라이언스에 로그인할 때 자격 증명을 더 쉽게 도난당할 수 있습니다.

Cisco는 모든 프로덕션 시스템에서 SSH 클라이언트를 사용하는 것이 좋습니다. 또한 표준 Microsoft Windows Telnet 클라이언트를 사용하기 어렵습니다. 기본적으로 텔넷은 관리 포트에 구성됩니다.

텔넷을 비활성화하려면 다음 단계를 완료합니다.

1. 웹 GUI에 로그인합니다.
2. Network(네트워크) > IP Interfaces(IP 인터페이스)로 이동합니다.
3. 수정할 인터페이스의 이름을 클릭합니다.
4. 서비스 필드에서 **텔넷** 확인란 선택을 취소합니다.

SSH(포트 22)를 통해 어플라이언스에 액세스하려면 다음 단계를 완료합니다.

1. PuTTY와 같이 Microsoft Windows에 SSH 클라이언트를 [설치합니다](#).
2. SSH 클라이언트를 시작합니다.

어플라이언스에 대한 호스트 정보(예: `c650.example.com`)를 추가합니다.

Load를 클릭합니다.

사용자 이름을 입력합니다.

비밀번호를 입력합니다.

3. `*nix`로 명령 프롬프트를 엽니다.
4. `$ ssh exampleC650.com` 명령을 입력합니다.
5. 다른 사용자를 지정해야 하는 경우 `$ ssh <user>@exampleC650.com` 명령을 입력합니다. 사용자 이름이 admin인 경우 `$ ssh admin@C650.example.com` 명령을 입력합니다.

텔넷을 통해 어플라이언스에 액세스하려면 다음 단계를 완료하십시오.

참고:Cisco에서는 액세스를 위해 SSH 클라이언트를 사용하는 것이 좋습니다.텔넷을 사용하지 않는 것이 좋습니다.

1. 명령 프롬프트를 엽니다.
2. **telnet c650.example.com** 명령을 입력합니다.
3. 사용자 이름을 입력합니다.
4. 비밀번호를 입력합니다.