

인터넷 서버에 대한 firepower 연결

목차

[소개](#)

[인터넷 서버에 대한 firepower 연결](#)

소개

이 문서에서는 네트워크 보안 요구 사항을 충족하기 위해 firepower 디바이스를 통한 아웃바운드 인터넷 연결에 대해 설명합니다.

인터넷 서버에 대한 firepower 연결

Firepower 장치는 네트워크 보안 요구 사항을 위해 인터넷 서버에 대한 아웃바운드 연결을 필요로 합니다.

FMC, firepower 또는 FTD 디바이스는 디바이스에서 활성 상태인 네트워크 보안 서비스를 위해 인터넷 서버에 대한 온디맨드 아웃바운드 연결 및 예약된 아웃바운드 연결을 모두 수행합니다. 이러한 서비스는 악성코드 차단, URL 필터링 등의 고급 기능에 적합한 라이선스를 통해 활성화됩니다.

 참고: 라이선싱 및 사용에 대한 자세한 내용은 제품 및 버전과 관련된 해당 컨피그레이션 가이드를 참조하십시오.

다음은 인터넷 서버 웹 사이트입니다.

- cloud-sa.amp.sourcefire.com
 - AMP(Advanced Malware Protection) 클라우드 기반 인텔리전스(Malware Lic만 사용)
- cloud-sa-589592150.us-east-1.elb.amazonaws.com을 참조하십시오.
 - AMP 클라우드 기반 인텔리전스(Malware Lic만 사용)
- database.brightcloud.com
 - 클라우드 기반 URL 분류 및 평판 서비스(URL 필터링 기능이 활성화된 경우에만 연결)
- service.brightcloud.com
 - 클라우드 기반 URL 분류 및 평판 서비스(URL 필터링 기능이 활성화된 경우에만 연결)
- amp.updates.vrt.sourcefire.com
 - Cisco Talos
- intelligence.sourcefire.com
 - Cisco Talos(보안 인텔리전스 기능을 사용하는 경우에만 연결)
- sourcefire.com
 - 업데이트 자동 다운로드
- panacea.threatgrid.com
 - 악성코드용 Threatgrid 서비스

- blogs.cisco.com/talos 또는 cloud.google.com
 - Cisco 제품에 대한 위협 인텔리전스 - google 클라우드에 문의 (기본적으로 활성화되어 있음)
- tools.cisco.com
 - 스마트 라이선싱
- updates.vrt.sourcefire.com
 - Clam 업데이트
- api.sse.cisco.com:8989을 참조하십시오.
 - 원격 측정을 위한 SSE

AMP가 활성화된 firepower의 경우 외부 서버에 대한 다음 문서 링크를 참조하십시오.

<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-amp-appliances/118121-technote-sourcefire-00.html>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.