

Secure Malware Analytics 필수 IP 및 방화벽 규칙 구성

목차

[소개](#)

[문제](#)

[환경](#)

[해결](#)

[Secure Malware Analytics Appliance](#)

[관리 인터페이스](#)

[깨끗한 인터페이스](#)

[더티 인터페이스](#)

[더티 인터페이스 아웃바운드](#)

[더티 인터페이스 인바운드](#)

[보안 악성코드 분석 클라우드](#)

[미국\(US\) 클라우드](#)

[유럽\(EU\) 클라우드](#)

[캐나다\(CA\) 클라우드](#)

[호주\(AU\) 클라우드](#)

[인도\(IN\) 클라우드](#)

[관련 콘텐츠](#)

소개

이 문서에서는 Cisco Secure Malware Analytics(클라우드 및 어플라이언스)에 필요한 호스트 이름, IP 주소 및 포트에 대해 설명합니다.

문제

Cisco Secure Malware Analytics를 사용하려면 특정 호스트 이름, IP 주소 및 포트에 대한 아웃바운드 및 인바운드 연결이 필요합니다. 이러한 흐름이 차단되면 포털 액세스, 업데이트, 라이선싱, 원격 지원 및 통합과 같은 기능이 실패할 수 있습니다.

환경



참고: 다른 서비스에 대한 추가 IP 및 포트가 포함된 이 문서를 먼저 참조하십시오.



Threat Grid에 필요한 IP 및 포트

이 문서에는 어플라이언스 버전을 기반으로 하는 다른 서비스에 대한 추가 IP 및 포트가 포함되어 있습니다.

설치 및 업그레이드 가이드 설명서를 참조하십시오. [Threat Grid Appliance 설치 설명서](#)

해결

디바이스에 대한 방화벽 업스트림에 대한 방화벽 규칙:

*게시 당시 IP는 정확했습니다. nslookup을 통해 로컬에서 이것이 여전히 정확한지 확인하십시오.

Secure Malware Analytics Appliance

관리 인터페이스

소스	대상	프로토콜	포트	방향	작업	참고
모두	관리 인터페이스	TCP	22	수신	허용	SSH
모두	관리 인터페이스	TCP	80/443	수신	허용	관리 GUI 인터페이스에 대한 액세스를 허용합니다.
관리 인터페이스	NFS 서버 IP	TCP	2049	발신	허용	*NFS 백업 또는 클러스터링 기능을 사용하려면 열려 있어야 합니다.

깨끗한 인터페이스

소스	대상	프로토콜	포트	방향	작업	참고
모두	깨끗한 인터페이스	TCP	80/443	수	허	Clean GUI 인터페이스에 대한 액세스를 허용

	이스			신	용	합니다.
모두	깨끗한 인터페이스	TCP	8443	수신	허용	*Admin over Clean 기능을 사용하려면 열어야 합니다.
모두	깨끗한 인터페이스	TCP	9443	수신	허용	*샘플 글로벌박스 기능을 사용하려면 열어야 합니다.
깨끗한 인터페이스	구성된 이메일 릴레이 서버	TCP	25	발신	허용	어플라이언스는 de clean 인터페이스를 사용하여 구성된 메일 서버에 대한 SMTP 연결을 시작합니다.
깨끗한 인터페이스	구성된 정상 DNS 서버	TCP/UDP	53	발신	허용	*선택 사항이며, Clean DNS가 구성된 경우에만 필요합니다.
깨끗한 인터페이스	구성된 Syslog 서버	TCP/UDP	514	발신	허용	Syslog 메시지 및 Threat Grid 알림을 수신하도록 지정된 서버와의 연결을 허용합니다.
깨끗한 인터페이스	LDAP 서버	TCP/UDP	389/636	발신	허용	*선택 사항, LDAP가 구성된 경우에만 필요합니다.

더티 인터페이스

더티 인터페이스 아웃바운드

소스	대상	프로토콜	포트	작업	메모
더티 인터페이스	인터넷	모두	모두	허용	선택적으로 Cisco 데이터 센터를 통해 프록시되는 샘플의 아웃바운드 트래픽을 허용합니다. (정확한 결과를 얻으려면 악성코드가 사용하도록 설계된 포트와 프로토콜을 사용하여 C&C(command and control) 서버에 연결할 수 있어야 합니다.)

더티 인터페이스 인바운드

소스	대상	프로토콜	포트	작업	메모
모두	더티 인터넷	모두	모두	거부	모든 수신 연결을 거부합니다.

소스	대상	프로토콜	포트	작업	메모
더티 인터페이스	인터넷	TCP	22	허용	업데이트, 지원 스냅샷 및 라이선스 서비스
더티 인터페이스	인터넷	TCP/UDP	53	허용	아웃바운드 DNS 허용
더티 인터페이스	인터넷	UDP	123	허용	아웃바운드 NTP 허용
더티 인터페이스	인터넷	TCP	19791	허용	Secure Malware Analytics 지원에 대한 연결을 허용합니다.
더티 인터페이스	Cisco Umbrella	TCP	443	허용	서드파티 탐지 및 강화 서비스에 연결합니다.
더티 인터페이스	바이러스총계	TCP	443	허용	서드파티 탐지 및 강화 서비스에 연결합니다.
더티 인터페이스	티타늄클라우드	TCP	443	허용	서드파티 탐지 및 강화 서비스에 연결합니다.



경고: 나열된 IP 주소는 2023년 5월 29일 이후에도 활성 상태로 유지됩니다.

소스	대상	프로토콜	포트	방향	호스트 이름	세부사항
----	----	------	----	----	--------	------

더티 인터페이스	63.97.201.96 63.162.55.96	TCP	19791	발신	rash.threatgrid.com	원격 지원/어플라이언스 지원 모드
더티 인터페이스	63.97.201.97 63.162.55.97	TCP	22	발신	appliance-updates.threatgrid.com	자동 지원 진단 업로드에 사용됩니다.  참고: 소프트웨어 버전 1.2 이상 필요
더티 인터페이스	63.97.201.98 63.162.55.98	TCP	22	발신	support-snapshots.threatgrid.com	자동 지원 진단 업로드에 사용됩니다.  참고: 소프트웨어 버전 1.2 이상 필요
더티 인터페이스	63.97.201.99 63.162.55.99	TCP	22	발신	appliance-licensing.threatgrid.com	라이선스 관리

보안 악성코드 분석 클라우드

미국(US) 클라우드

액세스 URL: <https://panacea.threatgrid.com>

호스트 이름	IP	포트	세부사항
panacea.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)

	IPv6: 2602:811:9007:6::61 2602:811:900b:6::6e		
glovebox.chi.threatgrid.com	IPv4: 200.194.241.35 IPv6: 2602:811:900f:6::6e	443	샘플 상호작용 창
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6: 2602:811:9007:6::61	443	샘플 상호작용 창
glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6: 2602:811:900b:6::6e	443	샘플 상호작용 창
fmc.api.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6::6e	443	FMC/FTD 파일 분석 서비스

유럽(EU) 클라우드

액세스 URL: <https://panacea.threatgrid.eu>

호스트 이름	IP	포 트	세부사항
panacea.threatgrid.eu	IPv4: 62.67.214.195 200.194.242.35 200.194.245.35 IPv6: 2602:811:9006:6::6e 2602:811:900c:6::6e	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	IPv4: 62.67.214.195 200.194.245.35 IPv6: 2602:811:900c:6::6e	3	샘플 상호작용 창
glovebox.fam.threatgrid.eu	IPv4: 200.194.242.35 IPv6: 2602:811:9006:6::6e	443	샘플 상호작용 창
fmc.api.threatgrid.eu	IPv4: 62.67.214.195 200.194.242.35 200.194.245.35 IPv6: 2602:811:9006:6::6e 2602:811:900c:6::6e	443	FMC/FTDFile 분석 서비스

기존 IP 89.167.128.132가 폐기되었습니다. 이러한 IP로 방화벽 규칙을 업데이트하십시오.

캐나다(CA) 클라우드

액세스 URL: <https://panacea.threatgrid.ca>

호스트 이름	IP	포트	세부사항
panacea.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	샘플 상호작용 창
fmc.api.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	FMC/FTD 파일 분석 서비스

호주(AU) 클라우드

액세스 URL: <https://panacea.threatgrid.com.au>

호스트 이름	IP	포트	세부사항
panacea.threatgrid.com.au	IPv4:	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)

	200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6::6e		
glovebox.syd.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6::6e	443	샘플 상호작용 창
fmc.api.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6::6e	443	FMC/FTD 파일 분석 서비스

인도(IN) 클라우드

엑세스 URL: <https://panacea.threatgrid.in>

호스트 이름	IP	포 트	세부사항
panacea.threatgrid.in	IPv4: 200.194.244.35 IPv6:	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)

	2602:811:9001:6::6e		
glovebox.bom.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	샘플 상호작용 창
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	FMC/FTD 파일 분석 서비스

어플라이언스와 같은 Cisco Secure Malware Analytics 요구 사항에 대한 자세한 내용은 다음 문서를 참조하십시오.

관련 콘텐츠

최신 요구 사항은 을/를 참조하십시오.

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.