Secure Malware Analytics에 필요한 IP 및 포트

목차

소개

이 문서에서는 Secure Malware Analytics가 제대로 작동하기 위해 방화벽에 추가해야 하는 네트워크 정보에 대해 설명합니다.

기고자: Cisco TAC 엔지니어

보안 악성코드 분석 클라우드

미국 클라우드

액세스 URL: https://panacea.threatgrid.com)

호스트 이름	IP	포트	세부사항
panacea.threatgrid.com	63.97.201.67 4.14.36.148 63.162.55.67	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	샘플 상호작용 창
glovebox.rcn.threatgrid.com	63.97.201.67	443	샘플 상호작용 창

glovebox.scl.threatgrid.com	63.162.55.67	443	샘플 상호작용 창
fmc.api.threatgrid.com	63.97.201.67 4.14.36.148	443	FMC/FTD 파일 분석 서비스

EU(유럽) 클라우드

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

호스트 이름	IP	포트	세부사항
panacea.threatgrid.eu	89.167.128.132	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.threatgrid.eu	89.167.128.132	443	샘플 상호작용 창
fmc.api.threatgrid.eu	89.167.128.132	443	FMC/FTD 파일 분석 서비스

2024년 1월 13일부터 EU 클라우드에 대한 IP가 변경됩니다. 이전 IP는 사용 중지됩니다. 이는 변경될 수 있으며, 만약 지연될 경우 문서는 그에 따라 업데이트됩니다.

이러한 IP는 Malware Analytics Cloud 기능이 제대로 작동하기 위해 아웃바운드로 허용되어야 하는 새 IP입니다.

호스트 이름	IP	포트	세부사항
panacea.threatgrid.eu	62.67.214.195 200.194.242.35	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	62.67.214.195	443	샘플 상호작용 창
glovebox.fam.threatgrid.eu	200.194.242.35	443	샘플 상호작용 창
fmc.api.threatgrid.eu	62.67.214.195 200.194.242.35	443	FMC/FTD 파일 분석 서비스

CA(캐나다) 클라우드

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

호스트 이름	IP	포	세부사항

		트	
panacea.threatgrid.ca	200.194.240.35	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatgrid.ca	200.194.240.35	443	샘플 상호작용 창
fmc.api.threatgrid.ca	200.194.240.35	443	FMC/FTD 파일 분석 서비스

AU(호주) 클라우드

액세스 URL: https://panacea.threatgrid.au

호스트 이름	IP	포트	세부사항
panacea.threatgrid.com.au	124.19.22.171	443	보안 악성코드 분석 포털 및 통합 디바이스 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	124.19.22.171	443	샘플 상호작용 창
fmc.api.threatgrid.com.au	124.19.22.171	443	FMC/FTD 파일 분석 서비스

Secure Malware Analytics Appliance

Secure Malware Analytics Appliance의 인터페이스당 권장 방화벽 규칙입니다.

더티 인터페이스

샘플이 DNS를 확인하고 C&C(Command and Control) 서버와 통신할 수 있도록 VM에서 인터넷과 통신하는 데 사용됩니다.
허용:

방향	프로토콜	포트	대상	호스트 이름	세부사항
아웃바운드	IP	모두	모두		여기서 Deny 섹션에 지정된 위치를 제외하고는 권장됩니다. Used 분석을 위해 연결을 허용합니다.
아웃바운드	TCP	22	54.173.231.161 1 63.97.201.98 2 63.162.55.98 2	support-snapshots.threatgrid.com	자동 지원 진단 업로드에 사용됩니다. 참고: 소프트웨어 버전 1.2 이상이 필요합니다.
아웃바운드	TCP	22	54.173.181.217 1 54.173.182.46 1	appliance-updates.threatgrid.com	어플라이언스 업데이트

			63.162.55.97 2 63.97.201.97 2		
아웃바운드	TCP	19791	54.164.165.137 1 34.199.44.202 1 63.97.201.96 2 63.162.55.96 2	rash.threatgrid.com	원격 지원/어플라이언스 지원 모드
아웃바운드	TCP	22	63.97.201.99 63.162.55.99	appliance-licensing.threatgrid.com	라이센스 관리

1 조만간 이러한 IP를 사용할 수 없게 됩니다.

2. 1의 IP를 대체할 IP입니다. 가까운 시일 내에 IP 변경에 대한 통신이 이루어질 때까지 두 IP를 모두 추가하는 것이 좋습니다.

원격 네트워크 종료

어플라이언스에서 이전에 tg-tunnel로 알려진 원격 출구에 VM 트래픽을 터널링하는 데 사용됩니다
.

방향	프로토콜	포트	대상
아웃바운드	TCP	21413	163.182.175.193
아웃바운드	TCP	21417	69.55.5.250
아웃바운드	TCP	21415	69.55.5.250
아웃바운드	TCP	21413	76.8.60.91

참고: 원격 출구 4.14.36.142가 제거되어 더 이상 운영 중이 아닙니다. 언급된 모든 IP를 방화벽 예외 목록에 추가해야 합니다.

거부:

방향	프로토콜	포트	대상	세부사항
아웃바운드	SMTP	모두	모두	악성코드가 스팸을 전송하지 않도록 합니다.
인바운드	IP	모두	Secure Malware Analytics Appliance 더티 인터페이스	위의 Allow 섹션에 지정된 경우를 제외하고는 권장됩니다. 분석을 위해 통신을 허용하는 데 사용됩니다.

깨끗한 인터페이스

분석가를 위한 UI 액세스와 샘플을 제출하기 위해 연결된 다양한 서비스에서 사용됩니다.
허용:

방향	프로토콜	포트	대상	세부사항
인바운드	TCP	443 8443	Secure Malware Analytics Appliance 안전한 인터페이스	WebUI 및 API 액세스
인바운드	TCP	9443	Secure Malware Analytics Appliance 안전한 인터페이스	글로브박스에 사용
아웃바운드	TCP	19791	호스트: rash.threatgrid.com IP: 54.164.165.137 [1] IP: 34.199.44.202 [1] IP: 63.97.201.96 [2] IP: 63.162.55.96 [2]	Secure Malware Analytics 지원을 위한 복구 모드

[1] 조만간 이러한 IP를 사용할 수 없게 됩니다.

[2]. [1]의 IP를 대체할 IP입니다. 가까운 시일 내에 IP 변경에 대한 통신이 이루어질 때까지 두 IP를 모두 추가하는 것이 좋습니다.

관리 인터페이스

관리 UI에 액세스합니다.
허용:

방향	프로토콜	포트	대상	세부사항
인바운드	TCP	443 8443	Secure Malware Analytics Appliance 관리 인터페이스	하드웨어 및 라이센스에 대한 설정을 구성하는 데 사용됩니다.

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.