적절한 Cisco Secure Endpoint & 악성코드 분석 작업에 필요한 서버 주소

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[적절한 AMP 작업을 위해 필요한 서버 주소](#)
[서버 위치](#)
[북미](#)
[유럽](#)
[아시아 태평양, 일본, 중국](#)
[적절한 Cisco Secure Malware Analytics 클라우드 액세스를 위해 필요한 서버 주소](#)
[북미 클라우드(NAM) 클라우드](#)
[유럽(EU) 클라우드](#)
[적절한 궤도 사용을 위해 필요한 서버 주소](#)
[북미 클라우드(NAM) 클라우드](#)
[유럽(EU) 클라우드](#)
[APJC(아시아 태평양, 일본, 중국) 클라우드](#)
[고정 IP 주소](#)

소개

이 문서에서는 Cisco AMP(Secure Endpoint) 제품 및 Threat Grid(Malware Analytics) 제품이 통신하고 업데이트, 조회 및 보고서를 완료하는 데 필요한 서버에 대해 설명합니다. 작업을 성공적으로 완료하려면 방화벽이 커넥터/어플라이언스에서 필요한 서버로의 연결을 허용해야 합니다.

> **주의**: 모든 서버는 로드 밸런싱, 내결함성 및 업타임을 위해 라운드 로빈 IP 주소 스키마를 사용합니다. 따라서 IP 주소가 변경될 수 있으므로 방화벽은 IP 주소 대신 *CNAME*로 구성하는 것이 좋습니다.

> **주의**: Cisco 서버로 들어오는 모든 트래픽은 TLS 암호 해독의 대상이 될 수 없습니다.

사전 요구 사항

요구 사항

이 기술 영역 문서는 Cisco AMP(Secure Endpoint) 제품 및 Malware Analytics(Threat Grid)와 통합된 다음 Cisco 제품에 적용됩니다.

- Cisco AMP for Networks(Firepower Management Center 및 센서)
- Cisco 보안 엔드포인트 프라이빗 클라우드

- Cisco 보안 엔드포인트 퍼블릭 클라우드
- Cisco Secure Email Appliance 및 Cisco Email Security(ESA 및 CES)
- Cisco WSA(Secure Web Appliance)
- Cisco Secure Malware Analytics 클라우드 및/또는 어플라이언스(Threat Grid)
- SDWAN/IOS-XE

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

적절한 AMP 작업을 위해 필요한 서버 주소

서버 위치

AMP 및 Threat Grid 서버는 세 가지 위치에 있습니다.

- 북미(AMP 및 Threat Grid)
- 유럽(AMP 및 Threat Grid)
- 일본(AMP만 해당)

북미

이 표에는 북미의 서버 위치가 나열되어 있습니다. 계정 생성 날짜를 기준으로 서버 주소가 다를 수 있습니다.

		cloud-ec-asn.amp.cisco.com cloud-ec-est.amp.cisco.com enrolment.amp.cisco.com	TCP 443
	Console	console.amp.cisco.com	TCP 443
		mgmt.amp.cisco.com	TCP 443
		intake.amp.cisco.com	TCP 443
		policy.amp.cisco.com	TCP 443
		upgrades.amp.cisco.com	TCP 80 443
Cisco Secure Endpoint:		crash.amp.cisco.com	TCP 443
	IOC	ioc.amp.cisco.com	TCP 443
	TETRA	tetra-defs.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 443
	macOS Linux Clam	clam-defs.amp.cisco.com	TCP 80 443
		custom-signatures.amp.cisco.com	TCP 443
		rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net .	TCP 443
		apde.amp.cisco.com	TCP 443
		endpoints.amp.cisco.com	TCP 443
Android		cloud-android-asn.amp.cisco.com	TCP 443
CSC/iOS		cloud-ios-asn.amp.cisco.com cloud-ios-est.amp.cisco.com	TCP 443

Cisco Secure Endpoint:	<v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Upstream Disposition Server >v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
		support-sessions.amp.cisco.com	TCP 22
AMP for Networks: Firepower	(FMC)	6.0 - 6.2.x: cloud-sa.amp.sourcefire.com 6.3.x + : cloud-sa.amp.cisco.com	TCP 443
	(FMC)	5.x - 6.2.x: export.amp.sourcefire.com 6.3.x +: export.amp.cisco.com	TCP 443
	API(FMC)	5.x - 6.2.x: api.amp.sourcefire.com 6.3.x + : api.amp.cisco.com api.amp.sourcefire.com	TCP 443
	()	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com fmc.api.threatgrid.com *6.x URL .	TCP 443
ESA/WSA/SMA	(ESA/WSA)	>= 15.x: cloud-esa-asn.amp.cisco.com cloud-esa-est.amp.cisco.com < 15.x: cloud-sa.amp.cisco.com	TCP 443
	(ESA/WSA/SMA)	panacea.threatgrid.com	TCP 443
	API(ESA)	>= 15.x: api.amp.cisco.com < 15.x:	TCP 443
	(ESA)	>= 15.x: intake.amp.cisco.com < 15.x:	TCP 443
	(ESA)	>= 15.x: mgmt.amp.cisco.com < 15.x:	TCP 443
SDWAN		cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
		cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

유럽

이 표에는 유럽의 서버 위치가 나열되어 있습니다. 계정 생성 날짜를 기준으로 서버 주소가 다를 수 있습니다.

Cisco Secure Endpoint:		cloud-ec-asn.eu.amp.cisco.com . cloud-ec-est.eu.amp.cisco.com . enrolment.eu.amp.cisco.com .	TCP 443
	Console	console.eu.amp.cisco.com .	TCP 443
		mgmt.eu.amp.cisco.com .	TCP 443
		intake.eu.amp.cisco.com .	TCP 443
		policy.eu.amp.cisco.com .	TCP 443
		upgrades.eu.amp.cisco.com .	TCP 80 443
		crash.eu.amp.cisco.com .	TCP 443
	IOC	ioc.eu.amp.cisco.com .	TCP 443
	TETRA	tetra-defs.eu.amp.cisco.com . commercial.ocsp.identrust.com validation.identrust.com	TCP 80 443
	macOS Linux Clam	clam-defs.eu.amp.cisco.com .	TCP 80 443
		custom-signatures.eu.amp.cisco.com .	TCP 443
		rff.eu.amp.cisco.com . submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net .	TCP 443
		apde.eu.amp.cisco.com .	TCP 443
		endpoints.eu.amp.cisco.com .	TCP 443
Android		cloud-android-asn.eu.amp.cisco.com .	TCP 443
CSC/iOS		cloud-ios-asn.eu.amp.cisco.com .	TCP 443

		cloud-ios-est.eu.amp.cisco.com .	
	<v2.4	cloud-pc-est.eu.amp.cisco.com . cloud-pc-asn.eu.amp.cisco.com .	TCP 443
Cisco Secure Endpoint:	Disposition Server >v2.4	cloud-pc-est.eu.amp.cisco.com . cloud-pc-asn.eu.amp.cisco.com .	TCP 443
	Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
		support-sessions.amp.cisco.com	TCP 22
	(FMC)	6.0 - 6.2.x: cloud-sa.eu.amp.sourcefire.com 6.3.x+: cloud-sa.eu.amp.cisco.com	TCP 443
AMP for Networks: Firepower	(FMC)	5.x - 6.2.x: export.eu.amp.sourcefire.com 6.3.x+: export.eu.amp.cisco.com	TCP 443
	API(FMC)	5.x - 6.2.x: api.amp.sourcefire.com api.eu.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com api.eu.amp.cisco.com	TCP 443
	()	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.eu fmc.api.threatgrid.eu 6.x URL	TCP 443
	(ESA/WSA)	>= 15.x: cloud-esa-asn.eu.amp.cisco.com cloud-esa-est.eu.amp.cisco.com . < 15.x: cloud-sa.eu.amp.cisco.com	TCP 443
	(ESA/WSA/SMA)	panacea.threatgrid.eu	TCP 443
ESA/WSA/SMA	API(ESA)	>= 15.x: api.eu.amp.cisco.com < 15.x:	TCP 443
	(ESA)	>= 15.x: intake.eu.amp.cisco.com < 15.x:	TCP 443
	(ESA)	>= 15.x: mgmt.eu.amp.cisco.com < 15.x:	TCP 443
SDWAN		cloud-isr-asn.eu.amp.cisco.com . cloud-isr-est.eu.amp.cisco.com .	TCP 443

아시아 태평양, 일본, 중국

이 표에는 아시아 태평양, 일본 및 중국의 서버 위치가 나열되어 있습니다.

		cloud-ec-asn.apjc.amp.cisco.com cloud-ec-est.apjc.amp.cisco.com enrolment.apjc.amp.cisco.com	TCP 443
	Console	console.apjc.amp.cisco.com	TCP 443
		mgmt.apjc.amp.cisco.com	TCP 443
		intake.apjc.amp.cisco.com	TCP 443
		policy.apjc.amp.cisco.com	TCP 443
		upgrades.apjc.amp.cisco.com	TCP 80 443
Cisco Secure Endpoint:		crash.apjc.amp.cisco.com	TCP 443
	IOC	ioc.apjc.amp.cisco.com	TCP 443
	TETRA	tetra-defs.apjc.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 443
	macOS Linux Clam	clam-defs.apjc.amp.cisco.com	TCP 80 443
		custom-signatures.apjc.amp.cisco.com	TCP 443
		rff.apjc.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net .	TCP 443
		apde.apjc.amp.cisco.com	TCP 443
		endpoints.apjc.amp.cisco.com	TCP 443
Android		cloud-android-asn.apjc.amp.cisco.com	TCP 443
CSC/iOS		cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
	< v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
Cisco Secure Endpoint:	Disposition Server( ) > v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Yum	packages-v2.amp.sourcefire.com	TCP 443

		pc-packages.amp.cisco.com	TCP 443 TCP 443
		support-sessions.amp.cisco.com	TCP 22
AMP for Networks: Firepower		6.0 - 6.2.x: cloud-sa.apjc.amp.sourcefire.com(IP) 6.3.x+: cloud-sa.apjc.amp.cisco.com	TCP 443
		5.x - 6.2.x:export.apjc.amp.sourcefire.com 6.3.x+: export.apjc.amp.cisco.com	TCP 443
	API	5.2 - 6.2.x api.apjc.amp.sourcefire.com api.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com api.apjc.amp.cisco.com	TCP 443
		APJC Threat Grid .	TCP 443
	(ESA/WSA)	>= 15.x: cloud-esa-asn.apjc.amp.cisco.com cloud-esa-est.apjc.amp.cisco.com < 15.x: cloud-sa.apjc.amp.cisco.com	TCP 443
	(ESA/WSA/SMA)	APJC Threat Grid .	TCP 443
ESA/WSA/SMA	API(ESA)	>= 15.x: api.apjc.amp.cisco.com < 15.x:	TCP 443
	(ESA)	>= 15.x: intake.apjc.amp.cisco.com < 15.x:	TCP 443
	(ESA)	>= 15.x: mgmt.apjc.amp.cisco.com < 15.x:	TCP 443
SDWAN		cloud-isr-asn.apjc.amp.cisco.com cloud-isr-est.apjc.amp.cisco.com	TCP 443

적절한 Cisco Secure Malware Analytics 클라우드 액세스를 위해 필요한 서버 주소

북미 클라우드(NAM) 클라우드

호스트 이름	IP	포트	세부사항
panacea.threatgrid.com	63.97.201.67 , 63.162.55.67	443	Threat Grid (ESA/WSA/FTD/ODNS/Meraki)
glovebox.scl.threatgrid.com	63.162.55.67	443	
glovebox.rcn.threatgrid.com	63.97.201.67	443	
fmc.api.threatgrid.com	63.97.201.67 , 63.162.55.67	443	FMC/FTD

유럽(EU) 클라우드

호스트 이름	IP	포트	세부사항
panacea.threatgrid.eu	89.167.128.132	443	Threat Grid (ESA/WSA/FTD/ODNS/Meraki)
glovebox.threatgrid.eu	89.167.128.132	443	
fmc.api.threatgrid.eu	89.167.128.132	443	FMC/FTD

어플라이언스와 같은 Threat Grid 요구 사항에 대한 자세한 내용은 다음 문서를 참조하십시오.
Threat Grid의 필수 IP 및 포트

적절한 궤도 사용을 위해 필요한 서버 주소

Orbital 1.7+용 고정 IP

북미 클라우드(NAM) 클라우드

호스트 이름	IP	포트
orbital.amp.cisco.com	54.71.115.87 54.68.234.245 54.200.174.54	443
ncp.orbital.amp.cisco.com	52.88.16.211 52.43.91.219 54.200.152.114	443
update.orbital.amp.cisco.com	54.71.197.112 54.188.114.190 54.188.131.5	443

NAT IP

34.223.219.240
35.160.108.105
52.11.13.222

자세한 내용은 궤도 도움말 가이드(https://orbital.amp.cisco.com/help/)를 참조하십시오.

유럽(EU) 클라우드

-	IP	
orbital.eu.amp.cisco.com .	3.120.91.16 18.196.194.92 3.121.5.209	443
ncp.orbital.eu.amp.cisco.com .	18.194.154.159 18.185.217.177 18.184.249.36	443
update.orbital.eu.amp.cisco.com .	3.123.83.189 18.184.240.159 35.158.29.104	443

NAT IP

52.29.47.197
52.57.222.67
52.58.172.218

자세한 내용은 궤도 도움말 가이드(https://orbital.eu.amp.cisco.com/help/)를 참조하십시오.

APJC(아시아 태평양, 일본, 중국) 클라우드

-	IP	
orbital.apjc.amp.cisco.com	3.114.186.175 52.198.6.9 18.177.242.101	443
ncp.orbital.apjc.amp.cisco.com	18.177.250.245 13.230.62.75 18.176.196.172	443
update.orbital.apjc.amp.cisco.c	54.248.22.154	443

om	18.178.184.79 54.95.125.218
	NAT IP
	52.194.143.206 52.69.138.67 54.95.9.136

자세한 내용은 궤도 도움말 가이드(https://orbital.apjc.amp.cisco.com/help/)를 참조하십시오.

고정 IP 주소

방화벽이 포트 443에서 아웃바운드 TCP 연결을 차단하는 경우(일반적으로 그렇지 않음) 정책을 업데이트하기 전에 방화벽 설정을 변경해야 합니다. 계정이 2016년 2월 이후에 설정된 경우 표준 정책에 고정 IP 주소가 이미 기록되어 있습니다. 2016년 2월 이전에 어카운트가 설정된 경우 Cisco TAC(Technical Assistance Center)에 문의하여 고정 IP 주소로 정책 마이그레이션을 요청할 수 있습니다.

> **참고**: 운영의 연속성을 보장하고 탐지된 파일 악성코드 속성이 두 Firepower Management Center 모두에서 동일하도록 하려면 기본 및 보조 Management Center에서 이 문서에 나열된 서버에 액세스할 수 있어야 합니다.

> **참고**: AMP Console은 고정 IP를 사용하지 않으며 DNS를 통해 액세스해야 합니다.

북미의 고정 IP 주소	유럽의 고정 IP 주소	APJC의 고정 IP 주소
23.23.197.169	46.51.181.139	54.250.127.0
23.23.198.191	46.51.182.195	52.197.2.58
23.23.224.83	46.51.182.202	52.197.22.41
50.16.242.171	46.137.99.242	52.69.16.172
50.16.244.193	52.16.63.115	13.112.137.80
50.16.250.236	52.16.95.58	52.198.208.254
52.0.55.209	52.16.105.95	13.112.162.167
52.2.63.194	52.16.166.193	54.249.244.218
52.2.128.246	52.16.177.94	54.249.246.210
52.3.149.24	52.16.193.225	54.249.243.85
52.3.178.163	52.16.220.180	54.249.240.219
52.3.190.47	52.17.93.43	54.248.98.94
52.4.98.101	52.17.102.100	176.34.47.0
52.4.151.41	52.17.106.35	52.192.82.189
52.4.245.162	52.17.179.163	52.68.180.106
52.4.246.178	52.17.211.190	52.196.247.47
52.5.92.125	52.17.233.49	52.196.185.158
52.6.103.57	52.18.9.153	52.197.74.4
52.6.197.200	52.18.28.229	52.69.39.127
52.20.14.163	52.18.79.226	54.248.113.224
52.20.123.238	52.18.109.209	54.238.55.12
52.20.141.147	52.18.187.129	54.249.248.16
52.21.52.149	52.18.187.166	52.197.50.93
52.21.117.50	52.18.223.41	52.193.124.132
52.21.134.210	52.19.84.244	52.69.108.228
52.22.64.192	52.19.167.56	52.197.72.147

52.22.156.183
52.23.13.34
52.23.16.199
52.23.73.146
52.23.87.4
52.23.107.89
52.23.134.105
52.23.140.222
52.70.11.137
52.70.13.27
52.70.35.37
52.70.47.45
52.70.56.136
52.70.58.10
52.70.59.59
52.70.59.121
52.70.60.74
52.70.61.174
52.70.61.181
52.70.61.193
52.70.63.25
54.83.45.221
54.88.208.235
54.204.8.61
54.221.210.7
54.221.255.190
54.225.226.117
54.225.227.9
54.225.227.30
54.225.227.45
54.225.227.105
54.225.228.145
54.225.228.166
54.225.228.244
54.227.247.102
107.20.158.55
107.20.203.8
107.20.229.191
107.20.234.220
107.21.212.157
107.21.217.202
107.21.218.60
128.177.8.0/24
174.129.203.65
54.161.128.60
54.234.131.176
52.206.206.244
34.225.208.192
52.22.120.193
34.199.250.32
34.199.238.4
34.194.224.132
34.198.112.150

52.30.25.70
52.30.74.163
52.30.124.82
52.30.160.113
52.30.175.205
52.30.179.236
52.30.196.206
52.30.208.114
52.30.217.4
52.30.217.226
52.30.255.133
52.31.30.249
52.31.66.59
52.31.83.94
52.31.119.97
52.31.122.77
52.31.127.190
52.31.137.201
54.195.248.52
54.195.249.18
54.217.232.226
54.217.232.234
54.217.232.241
54.217.232.244
54.217.232.249
54.228.250.255
54.246.88.192
54.247.189.117
54.74.229.75
107.21.250.31
107.21.236.143
52.2.128.246
52.18.202.103
52.18.119.87
192.111.5.0/24
34.249.48.182
34.248.52.55
99.81.233.22
3.123.83.189
18.184.240.159
35.158.29.104
192.35.177.23
104.18.39.201
172.64.148.55

52.197.22.165
52.68.82.200
52.197.35.73
52.197.39.251
52.68.251.104
54.249.253.42
54.249.253.65
176.34.60.211
52.192.198.119
52.196.96.41
54.248.116.199
52.196.117.29
52.196.134.7
176.34.60.30
52.192.145.214
52.192.221.107
52.193.182.191
52.193.201.169
52.193.223.43
52.193.233.17
52.196.115.166
52.196.31.86
52.197.121.237
52.198.147.230
52.198.195.125
52.198.202.24
52.198.221.53
52.198.223.169
52.198.225.221
52.198.226.104
52.198.26.36
52.198.94.104
52.199.124.11
52.199.127.80
52.199.92.142
52.68.1.146
54.248.107.84
54.248.109.124
54.248.126.98
54.248.236.127
54.248.236.141
54.248.236.144
54.248.236.151
54.248.237.93
54.249.246.7
54.250.127.131
192.111.6.0/24
54.248.22.154
18.178.184.79
54.95.125.218
192.35.177.23
104.18.39.201
172.64.148.55

34.224.236.198
52.20.233.31
192.111.4.0/24
192.111.7.0/24
54.71.197.112
54.188.114.190
54.188.131.5
192.35.177.23
104.18.39.201
172.64.148.55

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.