适当安全终端和恶意软件分析所需的服务器地址

目录

简介

先决条件

- 要求
- 使用的组件

安全终端所需的服务器地址

- 服务器位置
  - 北美
  - 欧洲
  - 亚太地区、日本、中国

AMP生态系统所需的服务器地址

- 北美
- 欧洲
- 亚太地区、日本、中国

安全恶意软件分析云所需的服务器地址

Orbital所需的服务器地址

- 轨道1.7+的静态IP
  - 北美云(NAM)云
  - 欧洲（欧盟）云
  - 亚太地区、日本、中国(APJC)云

静态IP地址

简介

本文档介绍启用思科安全终端连接器产品通信所需的服务器。

先决条件

要使思科安全终端（以前称为Cisco AMP）和思科安全恶意软件分析（以前称为Threat Grid）产品能够通信和完成更新、查找和报告，您的防火墙必须允许从连接器/设备到所需服务器的连接。

要求

本技术区文章适用于这些与思科安全终端(AMP)集成的思科产品。

- 网络安全终端（Firepower管理中心和传感器）

- 安全终端私有云
- 安全终端公共云
- 安全邮件设备和思科邮件安全（ESA和CES）
- 安全Web设备(WSA)
- Catalyst SDWAN/IOS-XE

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

⚠ 警告：所有服务器都使用轮询IP地址方案来实现负载均衡、容错和正常运行时间。因此，IP地址可以更改，Cisco建议使用主机名而不是IP地址配置防火墙。如果无法根据主机名进行防火墙，请确保本文档底部列出的所有IP地址都是允许的目标。

⚠ 警告：任何流向Cisco服务器的流量都不能进行TLS解密。

安全终端所需的服务器地址

服务器位置

思科安全终端服务器位于三个不同的位置：

- 北美
- 欧洲
- 日本

北美

分类	目的	服务器	端口
Cisco Secure Endpoint:公共云	处置服务器	cloud-ec-asn.amp.cisco.com cloud-ec-est.amp.cisco.com enrolment.amp.cisco.com	TCP 443

	控制台	console.amp.cisco.com	TCP 443
	管理服务器	mgmt.amp.cisco.com	TCP 443
	事件服务器	intake.amp.cisco.com	TCP 443
	策略	policy.amp.cisco.com	TCP 443
	连接器下载和更新	upgrades.amp.cisco.com	TCP 80和443
	错误报告	crash.amp.cisco.com	TCP 443
	终端IOC	ioc.amp.cisco.com	TCP 443
	TETRA更新服务器	tetra-defs.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80和443
	macOS和Linux Clam定义	clam-defs.amp.cisco.com	TCP 80和443
	高级自定义检测	custom-signatures.amp.cisco.com	TCP 443
	远程文件获取	rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	行为保护	apde.amp.cisco.com	TCP 443
	设备控制	endpoints.amp.cisco.com	TCP 443
Android连接器	处置服务器	cloud-android-asn.amp.cisco.com	TCP 443
CSC/iOS连接器	处置服务器	cloud-ios-asn.amp.cisco.com cloud-ios-est.amp.cisco.com	TCP 443
Cisco Secure Endpoint:私有云	上游处置服务器<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服务器	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	技术支持会话	support-sessions.amp.cisco.com	TCP 22

欧洲

分类	目的	服务器	端口
Cisco Secure Endpoint:公共云	处置服务器	cloud-ec-asn.eu.am p.cisco.com cloud-ec-est.eu.am p.cisco.com enrolment.eu.am p.cisco.com	TCP 443
	控制台	console.eu.am p.cisco.com	TCP 443
	管理服务器	mgmt.eu.am p.cisco.com	TCP 443
	事件服务器	intake.eu.am p.cisco.com	TCP 443
	策略	policy.eu.am p.cisco.com	TCP 443
	连接器下载和更新	upgrades.eu.am p.cisco.com	TCP 80和443
	错误报告	crash.eu.am p.cisco.com	TCP 443
	终端IOC	ioc.eu.am p.cisco.com	TCP 443
	TETRA更新服务器	tetra-defs.eu.am p.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80和443
	macOS和Linux Clam定义	clam-defs.eu.am p.cisco.com	TCP 80和443
	高级自定义检测	custom-signatures.eu.am p.cisco.com	TCP 443
	远程文件获取	rff.eu.am p.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443

	行为保护	apde.eu.am p.cisco.com	TCP 443
	设备控制	endpoints.eu.am p.cisco.com	TCP 443
Android连接器	处置服务器	cloud-android-asn.eu.am p.cisco.com	TCP 443
CSC/iOS连接器	处置服务器	cloud-ios-asn.eu.am p.cisco.com cloud-ios-est.eu.am p.cisco.com	TCP 443
Cisco Secure Endpoint:私有云	上游处置服务器<v2.4	cloud-pc-est.eu.am p.cisco.com cloud-pc-asn.eu.am p.cisco.com	TCP 443
	上游性质服务器>v2.4	cloud-pc-est.eu.am p.cisco.com cloud-pc-asn.eu.am p.cisco.com	TCP 443
	Yum服务器	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	技术支持会话	support-sessions.amp.cisco.com	TCP 22

亚太地区、日本、中国

分类	目的	服务器	端口
Cisco Secure Endpoint:公共云	处置服务器	cloud-ec-asn.apjc.amp.cisco.com cloud-ec-est.apjc.amp.cisco.com enrolment.apjc.amp.cisco.com	TCP 443
	控制台	console.apjc.amp.cisco.com	TCP 443
	管理服务器	mgmt.apjc.amp.cisco.com	TCP 443
	事件服务器	intake.apjc.amp.cisco.com	TCP 443
	策略	policy.apjc.amp.cisco.com	TCP 443
	连接器下载和更新	upgrades.apjc.amp.cisco.com	TCP 80和443
	错误报告	crash.apjc.amp.cisco.com	TCP 443

	终端IOC	ioc.apjc.amp.cisco.com	TCP 443
	TETRA更新服务器	tetra-defs.apjc.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80和443
	macOS和Linux Clam定义	clam-defs.apjc.amp.cisco.com	TCP 80和443
	高级自定义检测	custom-signatures.apjc.amp.cisco.com	TCP 443
	远程文件获取	rff.apjc.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	行为保护	apde.apjc.amp.cisco.com	TCP 443
	设备控制	endpoints.apjc.amp.cisco.com	TCP 443
Android连接器	处置服务器	cloud-android-asn.apjc.amp.cisco.com	TCP 443
CSC/iOS连接器	处置服务器	cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
Cisco Secure Endpoint: 私有云	上游处理服务器< v2.4	cloud-pc-est.apjc.amp.cisco.com cloud-pc-asn.apjc.amp.cisco.com	TCP 443
	上游处理服务器> v2.4	cloud-pc-est.apjc.amp.cisco.com cloud-pc-asn.apjc.amp.cisco.com	TCP 443
	Yum服务器	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	技术支持会话	support-sessions.amp.cisco.com	TCP 22

AMP生态系统所需的服务器地址

本节介绍AMP集成设备（例如思科安全防火墙、安全邮件网关等）所需的主机名。

北美

安全防火墙（适用于网络的AMP）	文件信誉（来自FMC，如果由FDM管理，则来自NGFW）	cloud-sa.amp.cisco.com cloud-ngfw-asn.amp.cisco.com cloud-ngfw-est.amp.cisco.com	TCP 443
	事件接收（来自FMC）	intake.amp.cisco.com	TCP 443
	控制台注册（来自FMC）	mgmt.amp.cisco.com	TCP 443
	事件交付（来自FMC）	export.amp.cisco.com	TCP 443
	API（来自FMC）	api.amp.cisco.com	TCP 443
安全邮件网关(ESA)	文件信誉	cloud-esa-asn.amp.cisco.com cloud-esa-est.amp.cisco.com cloud-sa.amp.cisco.com	TCP 443
	API	api.amp.cisco.com	TCP 443
	事件服务器	intake.amp.cisco.com	TCP 443
	管理服务器	mgmt.amp.cisco.com	TCP 443
安全Web设备(WSA)	文件信誉	cloud-sa.amp.cisco.com	TCP 443
	API	api.amp.cisco.com	TCP 443
Meraki MX	文件信誉	cloud-meraki-asn.amp.cisco.com	TCP 443

		cloud-meraki-est.amp.cisco.com	
Catalyst SDWAN	文件信誉	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

欧洲

安全防火墙（适用于网络的AMP）	文件信誉（来自FMC，如果由FDM管理，则来自NGFW）	cloud-sa.eu.am p.cisco.com cloud-ngfw-asn.eu.am p.cisco.com cloud-ngfw-est.eu.am p.cisco.com	TCP 443
	事件接收（来自FMC）	intake.eu.am p.cisco.com	TCP 443
	控制台注册（来自FMC）	mgmt.eu.am p.cisco.com	TCP 443
	事件交付（来自FMC）	export.eu.am p.cisco.com	TCP 443
	API（来自FMC）	api.eu.am p.cisco.com	TCP 443
安全邮件网关(ESA)	文件信誉	cloud-esa-asn.eu.am p.cisco.com cloud-esa-est.eu.am p.cisco.com cloud-sa.eu.am p.cisco.com	TCP 443
	API	api.eu.am p.cisco.com	TCP 443
	事件服务器	intake.eu.am p.cisco.com	TCP 443
	管理服务器	mgmt.eu.am p.cisco.com	TCP 443
安全Web设备(WSA)	文件信誉	cloud-sa.eu.am p.cisco.com	TCP 443
	API	api.eu.am p.cisco.com	TCP 443
Catalyst SDWAN	文件信誉	cloud-isr-asn.eu.am p.cisco.com cloud-isr-est.eu.am p.cisco.com	TCP 443

亚太地区、日本、中国

安全防火墙（适用于网络的AMP）	文件信誉（来自FMC，如果由FDM管理，则来自NGFW）	cloud-sa.apjc.amp.cisco.com cloud-ngfw-asn.apjc.amp.cisco.com cloud-ngfw-est.apjc.amp.cisco.com	TCP 443
	事件接收（来自FMC）	intake.apjc.amp.cisco.com	TCP 443
	控制台注册（来自FMC）	mgmt.apjc.amp.cisco.com	TCP 443
	事件交付（来自FMC）	export.apjc.amp.cisco.com	TCP 443
	API（来自FMC）	api.apjc.amp.cisco.com	TCP 443
安全邮件网关(ESA)	文件信誉	cloud-esa-asn.apjc.amp.cisco.com cloud-esa-est.apjc.amp.cisco.com cloud-sa.apjc.amp.cisco.com	TCP 443
	API	api.apjc.amp.cisco.com	TCP 443
	事件服务器	intake.apjc.amp.cisco.com	TCP 443
	管理服务器	mgmt.apjc.amp.cisco.com	TCP 443
安全Web设备(WSA)	文件信誉	cloud-sa.apjc.amp.cisco.com	TCP 443
	API	api.apjc.amp.cisco.com	TCP 443
Catalyst SDWAN	文件信誉	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

安全恶意软件分析云所需的服务器地址

有关思科安全恶意软件分析云和设备的详细信息，请参阅以下文章：安全恶意软件分析所需的IP和端口

Orbital所需的服务器地址

轨道1.7+的静态IP

北美云(NAM)云

主机名	IP	端口
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
用于远程数据存储的NAT IP		
	34.223.219.240 35.160.108.105 52.11.13.222	高随机端口号

有关更多信息，请查看轨道帮助指南：https://orbital.amp.cisco.com/help/

欧洲（欧盟）云

主机名	IP	端口

orbital.eu.am p.cisco.com	3.120.91.16 18.196.194.92 3.121.5.209	443
ncp.orbital.eu.am p.cisco.com	18.194.154.159 18.185.217.177 18.184.249.36	443
update.orbital.eu.am p.cisco.com	3.123.83.189 18.184.240.159 35.158.29.104	443
用于远程数据存储的NAT IP		
	52.29.47.197 52.57.222.67 52.58.172.218	高随机端口号

有关更多信息，请查看轨道帮助指南：https://orbital.eu.amp.cisco.com/help/

亚太地区、日本、中国(APJC)云

主机名	IP	端口
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.com	54.248.22.154 18.178.184.79 54.95.125.218	443
用于远程数据存储的NAT IP		
	52.194.143.206 52.69.138.67 54.95.9.136	高随机端口号

有关更多信息，请查看轨道帮助指南：https://orbital.apjc.amp.cisco.com/help/

静态IP地址

如果防火墙阻止端口443上的出站TCP连接（通常情况并非如此），您必须确保此处列出的所有IP地址都是允许的目标。

注意：为了确保操作的连续性，并确保两个Firepower管理中心上检测到的文件恶意软件性质相同，主要和次要管理中心都必须能够访问本文档中列出的服务器。

北美的静态IP地址	欧洲的静态IP地址	APJC中的静态IP地址
23.23.197.169 23.23.198.191 23.23.224.83 50.16.242.171 50.16.244.193 50.16.250.236 52.0.55.209 52.2.63.194 52.2.128.246 52.3.149.24 52.3.178.163 52.3.190.47 52.4.98.101	46.51.181.139 46.51.182.195 46.51.182.202 46.137.99.242 52.16.63.115 52.16.95.58 52.16.105.95 52.16.166.193 52.16.177.94 52.16.193.225 52.16.220.180 52.17.93.43 52.17.102.100 52.17.106.35 52.17.179.163	54.250.127.0 52.197.2.58 52.197.22.41 52.69.16.172 13.112.137.80 52.198.208.254 13.112.162.167 54.249.244.218 54.249.246.210 54.249.243.85 54.249.240.219 54.248.98.94 176.34.47.0 52.192.82.189 52.68.180.106

52.4.151.41	52.17.211.190	52.196.247.47
52.4.245.162	52.17.233.49	52.196.185.158
52.4.246.178	52.18.9.153	52.197.74.4
52.5.92.125	52.18.28.229	52.69.39.127
52.6.103.57	52.18.79.226	54.248.113.224
52.6.197.200	52.18.109.209	54.238.55.12
52.20.14.163	52.18.187.129	54.249.248.16
52.20.123.238	52.18.187.166	52.197.50.93
52.20.141.147	52.18.223.41	52.193.124.132
52.21.52.149	52.19.84.244	52.69.108.228
52.21.117.50	52.19.167.56	52.197.72.147
52.21.134.210	52.30.25.70	52.197.22.165
52.22.64.192	52.30.74.163	52.68.82.200
52.22.156.183	52.30.124.82	52.197.35.73
52.23.13.34	52.30.160.113	52.197.39.251
52.23.16.199	52.30.175.205	52.68.251.104
52.23.73.146	52.30.179.236	54.249.253.42
52.23.87.4	52.30.196.206	54.249.253.65
52.23.107.89	52.30.208.114	176.34.60.211
52.23.134.105	52.30.217.4	52.192.198.119
52.23.140.222	52.30.217.226	52.196.96.41
52.70.11.137	52.30.255.133	54.248.116.199
52.70.13.27	52.31.30.249	52.196.117.29
52.70.35.37	52.31.66.59	52.196.134.7
52.70.47.45	52.31.83.94	176.34.60.30
52.70.56.136	52.31.119.97	52.192.145.214
52.70.58.10	52.31.122.77	52.192.221.107
52.70.59.59	52.31.127.190	52.193.182.191
52.70.59.121	52.31.137.201	52.193.201.169
52.70.60.74	54.195.248.52	52.193.223.43
52.70.61.174	54.195.249.18	52.193.233.17
52.70.61.181	54.217.232.226	52.196.115.166
52.70.61.193	54.217.232.234	52.196.31.86
52.70.63.25	54.217.232.241	52.197.121.237
54.83.45.221	54.217.232.244	52.198.147.230
54.88.208.235	54.217.232.249	52.198.195.125
54.204.8.61	54.228.250.255	52.198.202.24
54.221.210.7	54.246.88.192	52.198.221.53
54.221.255.190	54.247.189.117	52.198.223.169
54.225.226.117	54.74.229.75	52.198.225.221
54.225.227.9	107.21.250.31	52.198.226.104
54.225.227.30	107.21.236.143	52.198.26.36
54.225.227.45	52.2.128.246	52.198.94.104
54.225.227.105		52.199.124.11
54.225.228.145		52.199.127.80
		52.199.92.142

54.225.228.166 54.225.228.244 54.227.247.102 107.20.158.55 107.20.203.8 107.20.229.191 107.20.234.220 107.21.212.157 107.21.217.202 107.21.218.60 174.129.203.65 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 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 54.188.131.5 192.35.177.23 104.18.39.201 172.64.148.55 104.18.4.5 104.18.5.5 52.3.48.165 52.6.245.67 34.120.67.236 34.98.122.109 2600:1f18:4016:be00::/64 2600:1f18:4016:be01::/64	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 35.158.29.104 192.35.177.23 104.18.39.201 172.64.148.55 104.18.4.5 104.18.5.5 52.3.48.165 52.6.245.67 34.120.67.236 34.98.122.109	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 18.180.25.43 54.95.253.127 54.249.195.77 104.18.4.5 104.18.5.5 52.3.48.165 52.6.245.67 34.120.67.236 34.98.122.109

2600:1f18:4016:be02::/64		

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。