正确的思科安全终端和amp；恶意软件分析操作所需的服务器地址

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[正确的思科安全终端操作所需的服务器地址](#)

- [服务器位置](#)
  - [北美](#)
  - [欧洲](#)
  - [亚太地区、日本、中国](#)

[正确的思科安全恶意软件分析云访问所需的服务器地址](#)

[正常轨道使用所需的服务器地址](#)

- [北美云(NAM)云](#)
- [欧洲(EU)云](#)
- [亚太、日本、中国(APJC)云](#)

[静态IP地址](#)

简介

本文档介绍使思科安全终端（以前称为Cisco AMP）产品和思科安全恶意软件分析（以前称为Threat Grid）产品能够通信并完成更新、查找和报告所需的服务器。为了成功完成操作，您的防火墙必须允许从连接器/设备到所需服务器的连接。

⚠ 注意：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地址可能会更改，Cisco建议防火墙配置为CNAME而不是IP地址。

⚠ 注意：任何传入思科服务器的流量都不能使用TLS解密。

先决条件

要求

本技术区文章适用于以下与思科安全终端(AMP)产品和恶意软件分析(Threat Grid)集成的思科产品：

- 面向网络的思科安全终端（Firepower管理中心和传感器）
- 思科安全终端私有云
- 思科安全终端公共云

- 思科安全邮件设备和思科邮件安全（ESA和CES）
- 思科安全Web设备(WSA)
- 思科安全恶意软件分析云和/或设备(Threat Grid)
- 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。

正确的思科安全终端操作所需的服务器地址

服务器位置

思科安全终端和思科安全恶意软件分析服务器位于三个不同的位置：

- 北美（思科安全终端和思科安全恶意软件分析）
- 欧洲（思科安全终端和思科安全恶意软件分析）
- 日本（仅限思科安全终端）

北美

此表列出了北美的服务器位置。根据帐户创建日期，服务器地址可能不同：

分类	目的	服务器	端口
思科安全终端：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	TCP 80和443

		commercial.ocsp.identrust.com validation.identrust.com	
	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
思科安全终端：私有云	Upstream Disposition Server <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
面向网络的AMP：Firepower	处置服务器（来自FMC）	6.0 – 6.2.x：cloud-sa.amp.sourcefire.com 6.3.x +：cloud-sa.amp.cisco.com	TCP 443
	事件（来自FMC）	5.x - 6.2.x：export.amp.sourcefire.com	TCP 443

		6.3.x +：export.amp.cisco.com	
	API（来自FMC）	5.x - 6.2.x：api.amp.sourcefire.com 6.3.x +：api.amp.cisco.com和 api.amp.sourcefire.com	TCP 443
	动态分析（来自传感器）	5.x：intel.api.sourcefire.com 6.x：panacea.threatgrid.com和 fmc.api.threatgrid.com * 根据6.x补丁版本，可以使用任一URL	TCP 443
ESA/WSA/SMA	文件信誉(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
	文件分析(ESA/WSA/SMA)	panacea.threatgrid.com	TCP 443
	API (ESA)	>= 15.x：api.amp.cisco.com < 15.x：不适用	TCP 443
	事件服务器(ESA)	>= 15.x：intake.amp.cisco.com < 15.x：不适用	TCP 443
	管理服务器(ESA)	>= 15.x：mgmt.amp.cisco.com < 15.x：不适用	TCP 443
Meraki	处置服务器	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
SDWAN	处置服务器	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

欧洲

此表列出了欧洲的服务器位置。根据帐户创建日期，服务器地址可能不同：

分类	目的	服务器	端口
思科安全终端：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
思科安全终端：私有云	Upstream Disposition Server <v2.4	cloud-pc-est.eu.am p.cisco.com cloud-pc-asn.eu.am p.cisco.com	TCP 443
	上行处置服务器>v2.4	cloud-pc-est.eu.am p.cisco.com cloud-pc-asn.eu.am p.cisco.com	TCP 443
	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
面向网络的AMP：Firepower	处置服务器（来自FMC）	6.0 – 6.2.x：cloud-sa.eu.amp.sourcefire.com 6.3.x+：cloud-sa.eu.amp.cisco.com	TCP 443
	事件（来自FMC）	5.x - 6.2.x：export.eu.amp.sourcefire.com 6.3.x+：export.eu.amp.cisco.com	TCP 443
	API（来自FMC）	5.x - 6.2.x：api.amp.sourcefire.com和api.eu.amp.sourcefire.com 6.3.x+：api.amp.sourcefire.com和api.eu.amp.cisco.com	TCP 443
	动态分析（来自传感器）	5.x：intel.api.sourcefire.com 6.x：panacea.threatgrid.eu和fmc.api.threatgrid.eu 根据6.x补丁版本，可以使用任一URL	TCP 443
ESA/WSA/SMA	文件信誉(ESA/WSA)	>= 15.x：cloud-esa-asn.eu.amp.cisco.com cloud-esa-est.eu.am p.cisco.com < 15.x： cloud-sa.eu.amp.cisco.com	TCP 443
	文件分析(ESA/WSA/SMA)	panacea.threatgrid.eu	TCP 443
	API (ESA)	>= 15.x：api.eu.amp.cisco.com	TCP 443

		< 15.x：不适用	
	事件服务器(ESA)	>= 15.x：intake.eu.amp.cisco.com < 15.x：不适用	TCP 443
	管理服务器(ESA)	>= 15.x：mgmt.eu.amp.cisco.com < 15.x：不适用	TCP 443
SDWAN	处置服务器	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

下表列出了亚太地区、日本和中国的服务器位置：

分类	目的	服务器	端口
思科安全终端：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	上游处置服务器< v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	上游处置服务器> 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 TCP 443
	技术支持会话	support-sessions.amp.cisco.com	TCP 22
面向网络的AMP：Firepower	处置服务器	6.0 – 6.2.x：cloud-sa.apjc.amp.sourcefire.com（静态IP） 6.3.x+：cloud-sa.apjc.amp.cisco.com	TCP 443
	事件	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和 api.amp.sourcefire.com 6.3.x+：api.amp.sourcefire.com和 api.apjc.amp.cisco.com	TCP 443
	动态分析	APJC中当前没有Threat Grid数据中心，因此 必须使用欧洲或北美主机名。	TCP 443
ESA/WSA/SMA	文件信誉(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
	文件分析 (ESA/WSA/SMA)	APJC中当前没有Threat Grid数据中心，因此 必须使用欧洲或北美主机名。	TCP 443
	API (ESA)	>= 15.x：api.apjc.amp.cisco.com < 15.x：不适用	TCP 443
	事件服务器(ESA)	>= 15.x：intake.apjc.amp.cisco.com < 15.x：不适用	TCP 443
	管理服务器(ESA)	>= 15.x：mgmt.apjc.amp.cisco.com < 15.x：不适用	TCP 443
SDWAN	处置服务器	cloud-isr-asn.apjc.amp.cisco.com cloud-isr-est.apjc.amp.cisco.com	TCP 443

正确的思科安全恶意软件分析云访问所需的服务器地址

有关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]

正常轨道使用所需的服务器地址

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(EU)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.amp.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、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），则必须在更新任何策略之前更改防火墙设置。如果您的帐户是在2016年2月之后建立的，则您已经将静态IP地址写入标准策略中。如果您的帐户在2016年2月之前建立，您可以联系思科技术支持中心(TAC)，请求将策略迁移到静态IP地址。

注意：为确保操作的连续性，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。

注意：思科安全终端控制台不使用静态IP，必须通过DNS进行访问。

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	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	52.30.25.70	52.197.22.165
	52.30.74.163	52.68.82.200
	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	52.18.202.103	52.199.124.11
54.225.228.145	52.18.119.87	52.199.127.80
54.225.228.166	192.111.5.0/24	52.199.92.142
54.225.228.244	34.249.48.182	52.68.1.146
54.227.247.102	34.248.52.55	54.248.107.84
107.20.158.55	99.81.233.22	54.248.109.124
107.20.203.8	3.123.83.189	54.248.126.98
107.20.229.191	18.184.240.159	54.248.236.127
107.20.234.220		54.248.236.141
107.21.212.157		54.248.236.144
107.21.217.202		54.248.236.151
107.21.218.60		54.248.237.93
128.177.8.0/24		54.249.246.7
174.129.203.65		54.250.127.131
54.161.128.60		192.111.6.0/24

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	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	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

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）。