正確的思科安全終端&；惡意軟體分析操作所需的伺服器地址

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[正確的思科安全終端操作所需的伺服器地址](#)

- [伺服器位置](#)
  - [北美洲](#)
  - [歐洲](#)
  - [亞太地區、日本、中國](#)

[正確的 Cisco Secure Malware Analytics Cloud 存取所需的伺服器位址](#)

[正確使用 Orbital 所需的伺服器位址](#)

- [北美 (NAM) 雲端](#)
- [歐盟 (EU) 雲端](#)
- [亞太地區、日本、中國 (APJC) 雲端](#)

[靜態 IP 位址](#)

簡介

本文檔介紹啟用思科安全終端（以前稱為Cisco AMP）產品和思科安全惡意軟體分析（以前稱為Threat Grid）產品進行通訊並完成更新、查詢和報告所需的伺服器。為了順利完成操作，您的防火牆必須允許從連接器/設備到所需伺服器的連線。

⚠ 注意：所有伺服器都使用循環配置的IP地址方案來實現負載平衡、容錯和正常運行時間。因此，IP 位址可能會變更，思科建議設定防火牆時使用 CNAME，而非 IP 位址。

⚠ 注意：任何流向Cisco伺服器的流量均不能進行TLS解密。

必要條件

需求

此「技術區」文章適用於與 Cisco Secure Endpoint (AMP) 產品和 Malware Analytics (Threat Grid) 整合的下列思科產品：

- 思科網路安全終端（Firepower管理中心和感測器）
- Cisco Secure Endpoint Private Cloud

- Cisco Secure Endpoint Public Cloud
- Cisco Secure Email Appliance (ESA) 和 Cisco Email Security (CES)
- Cisco Secure Web Appliance (WSA)
- Cisco Secure Malware Analytics Cloud 和/或 Appliance (Threat Grid)
- SDWAN/IOS-XE

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

正確的思科安全終端操作所需的伺服器地址

伺服器位置

思科安全終端和思科安全惡意軟體分析伺服器位於三個不同的位置：

- 北美（思科安全終端和思科安全惡意軟體分析）
- 歐洲（思科安全終端和思科安全惡意軟體分析）
- 日本（僅限思科安全終端）

北美洲

此表列出北美的伺服器位置。根據帳戶建立日期，伺服器位址可能有所不同：

類別	目的	伺服器	連接埠
思科安全終端：公共雲	處置伺服器	cloud-ec-asn.amp.cisco.com cloud-ec-est.amp.cisco.com enrolment.amp.cisco.com	TCP 443
	主控台	console.amp.cisco.com	TCP 443
	管理伺服器	mgmt.amp.cisco.com	TCP 443
	事件伺服器	intake.amp.cisco.com	TCP 443
	政策	policy.amp.cisco.com	TCP 443
	連接器下載和更新	upgrades.amp.cisco.com	TCP 80 和 443
	錯誤報告	crash.amp.cisco.com	TCP 443
	端點 IOC	ioc.amp.cisco.com	TCP 443

	TETRA 更新伺服器	tetra-defs.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 和 443
	macOS 和 Linux Clam 定義	clam-defs.amp.cisco.com	TCP 80 和 443
	進階自訂偵測	custom-signatures.amp.cisco.com	TCP 443
	遠端檔案擷取	rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	行為保護	apde.amp.cisco.com	TCP 443
	裝置控制	endpoints.amp.cisco.com	TCP 443
Android 連接器	處置伺服器	cloud-android-asn.amp.cisco.com	TCP 443
CSC/iOS 連接器	處置伺服器	cloud-ios-asn.amp.cisco.com cloud-ios-est.amp.cisco.com	TCP 443
思科安全終端：私有雲	上游部署伺服器<v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	上游部署伺服器>v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Yum 伺服器	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	支援會話	support-sessions.amp.cisco.com	TCP 22
面向網路的 AMP:Firepower	處置伺服器（來自FMC）	6.0 - 6.2.x:cloud-sa.amp.sourcefire.com 6.3.x +:cloud-sa.amp.cisco.com	TCP 443

	事件（來自FMC）	5.x - 6.2.x:export.amp.sourcefire.com 6.3.x +:export.amp.cisco.com	TCP 443
	API（來自FMC）	5.x - 6.2.x:api.amp.sourcefire.com 6.3.x +:api.amp.cisco.com和 api.amp.sourcefire.com	TCP 443
	動態分析（來自感應器）	5.x:intel.api.sourcefire.com 6.x:panacea.threatgrid.com和 fmc.api.threatgrid.com *視 6.x 修補程式版本而定，可使用其中一個 URL	TCP 443
ESA/WSA/SMA	檔案信譽 (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
	檔案分析 (ESA/WSA/SMA)	panacea.threatgrid.com	TCP 443
	API(ESA)	>= 15.x:api.amp.cisco.com < 15.x：不適用	TCP 443
	事件伺服器(ESA)	>= 15.x:intake.amp.cisco.com < 15.x：不適用	TCP 443
	管理伺服器(ESA)	>= 15.x:mgmt.amp.cisco.com < 15.x：不適用	TCP 443
Meraki	處置伺服器	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
SDWAN	處置伺服器	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

歐洲

此表列出歐洲的伺服器位置。根據帳戶建立日期，伺服器位址可能有所不同：

類別	目的	伺服器	連接埠
思科安全終端：公共雲	處置伺服器	cloud-ec-asn.eu.amp.cisco.com cloud-ec-est.eu.amp.cisco.com enrolment.eu.amp.cisco.com	TCP 443
	主控台	console.eu.amp.cisco.com	TCP 443
	管理伺服器	mgmt.eu.amp.cisco.com	TCP 443
	事件伺服器	intake.eu.amp.cisco.com	TCP 443
	政策	policy.eu.amp.cisco.com	TCP 443
	連接器下載和更新	upgrades.eu.amp.cisco.com	TCP 80 和 443
	錯誤報告	crash.eu.amp.cisco.com	TCP 443
	端點 IOC	ioc.eu.amp.cisco.com	TCP 443
	TETRA 更新伺服器	tetra-defs.eu.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 和 443
	macOS 和 Linux Clam 定義	clam-defs.eu.amp.cisco.com	TCP 80 和 443
	進階自訂偵測	custom-signatures.eu.amp.cisco.com	TCP 443
	遠端檔案擷取	rff.eu.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	行為保護	apde.eu.amp.cisco.com	TCP 443
	裝置控制	endpoints.eu.amp.cisco.com	TCP 443

Android 連接器	處置伺服器	cloud-android-asn.eu.amp.cisco.com	TCP 443
CSC/iOS 連接器	處置伺服器	cloud-ios-asn.eu.amp.cisco.com cloud-ios-est.eu.amp.cisco.com	TCP 443
思科安全終端：私有雲	上游部署伺服器<v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	上游 處置伺服器>v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Yum 伺服器	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	支援會話	support-sessions.amp.cisco.com	TCP 22
面向網路的 AMP:Firepower	Disposition Server（來自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（來自FMC）	5.x - 6.2.x:export.eu.amp.sourcefire.com 6.3.x+:export.eu.amp.cisco.com	TCP 443
	API（來自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
	動態分析（來自感應器）	5.x:intel.api.sourcefire.com 6.x:panacea.threatgrid.eu和fmc.api.threatgrid.eu 視 6.x 修補程式版本而定，可使用其中一個 URL	TCP 443
ESA/WSA/SMA	檔案信譽 (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
	檔案分析 (ESA/WSA/SMA)	panacea.threatgrid.eu	TCP 443

	API(ESA)	>= 15.x:api.eu.amp.cisco.com < 15.x：不適用	TCP 443
	事件伺服器(ESA)	>= 15.x:intake.eu.amp.cisco.com < 15.x：不適用	TCP 443
	管理伺服器(ESA)	>= 15.x:mgmt.eu.amp.cisco.com < 15.x：不適用	TCP 443
SDWAN	處置伺服器	cloud-isr-asn.eu.amp.cisco.com cloud-isr-est.eu.amp.cisco.com	TCP 443

亞太地區、日本、中國

此表列出亞太地區、日本和中國的伺服器位置：

類別	目的	伺服器	連接埠
思科安全終端：公共雲	處置服務器	cloud-ec-asn.apjc.amp.cisco.com cloud-ec-est.apjc.amp.cisco.com enrolment.apjc.amp.cisco.com	TCP 443
	主控台	console.apjc.amp.cisco.com	TCP 443
	管理伺服器	mgmt.apjc.amp.cisco.com	TCP 443
	事件伺服器	intake.apjc.amp.cisco.com	TCP 443
	政策	policy.apjc.amp.cisco.com	TCP 443
	連接器下載和更新	upgrades.apjc.amp.cisco.com	TCP 80 和 443
	錯誤報告	crash.apjc.amp.cisco.com	TCP 443
	端點 IOC	ioc.apjc.amp.cisco.com	TCP 443
	TETRA 更新伺服器	tetra-defs.apjc.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 和 443

	macOS 和 Linux Clam 定義	clam-defs.apjc.amp.cisco.com	TCP 80 和 443
	進階自訂偵測	custom-signatures.apjc.amp.cisco.com	TCP 443
	遠端檔案擷取	rff.apjc.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	行為保護	apde.apjc.amp.cisco.com	TCP 443
	裝置控制	endpoints.apjc.amp.cisco.com	TCP 443
Android 連接器	處置服務器	cloud-android-asn.apjc.amp.cisco.com	TCP 443
CSC/iOS 連接器	處置服務器	cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
思科安全端點: 私有 雲	上游 處置伺服器< v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	上游 Disposition Server > v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Yum 伺服器	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	支援會話	support-sessions.amp.cisco.com	TCP 22
面向網路的 AMP:Firepower	處置服務器	6.0 - 6.2.x:cloud-sa.apjc.amp.sourcefire.com（靜態IP） 6.3.x+:cloud-sa.apjc.amp.cisco.com	TCP 443
	活動	5.x - 6.2.x：export.apjc.amp.sourcefire.com	TCP 443

		6.3.x+:export.apjc.amp.cisco.com	
	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
	動態分析	亞太地區、日本及中國目前沒有 Threat Grid 資料中心， 因此必須使用歐洲或北美主機名稱。	TCP 443
ESA/WSA/SMA	檔案信譽 (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
	檔案分析 (ESA/WSA/SMA)	亞太地區、日本及中國目前沒有 Threat Grid 資料中心， 因此必須使用歐洲或北美主機名稱。	TCP 443
	API(ESA)	>= 15.x:api.apjc.amp.cisco.com < 15.x：不適用	TCP 443
	事件伺服器(ESA)	>= 15.x:intake.apjc.amp.cisco.com < 15.x：不適用	TCP 443
	管理伺服器(ESA)	>= 15.x:mgmt.apjc.amp.cisco.com < 15.x：不適用	TCP 443
SDWAN	處置伺服器	cloud-isr-asn.apjc.amp.cisco.com cloud-isr-est.apjc.amp.cisco.com	TCP 443

正確的 Cisco Secure Malware Analytics Cloud 存取所需的伺服器位址

有關安全惡意軟體分析雲和裝置的詳細資訊，請參閱以下文章： Required IPs and Ports for Secure

Malware Analytics

正確使用 Orbital 所需的伺服器位址

適用於 Orbital 1.7+ 的靜態 IP

北美 (NAM) 雲端

主機名	IP	連接埠
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
遠端資料存放區的 NAT IP		
	34.223.219.240 35.160.108.105 52.11.13.222	高度隨機連接埠號碼

如需更多資訊，請參閱 Orbital 說明指南：https://orbital.amp.cisco.com/help/

歐盟 (EU) 雲端

主機名	IP	連接埠
orbital.eu.amp.cisco.com	3.120.91.16 18.196.194.92	443

	3.121.5.209	
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
遠端資料存放區的 NAT IP		
	52.29.47.197 52.57.222.67 52.58.172.218	高度隨機連接埠號碼

如需更多資訊，請參閱 Orbital 說明指南：https://orbital.eu.amp.cisco.com/help/

亞太地區、日本、中國 (APJC) 雲端

主機名	**IP**	**連接埠**
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

遠端資料存放區的 NAT IP		
	52.194.143.206 52.69.138.67 54.95.9.136	高度隨機連接埠號碼

如需更多資訊，請參閱 Orbital 說明指南：https://orbital.apjc.amp.cisco.com/help/

靜態 IP 位址

如果防火牆封鎖連接埠 443 上的傳出 TCP 連接（屬於異常情形），您必須先變更防火牆設定，然後再更新原則。如果帳戶是在 2016 年 2 月之後建立，則您已經將靜態 IP 位址寫入標準原則。如果您的帳戶在2016年2月之前建立，您可以聯絡思科技術支援中心(TAC)，請求將策略遷移到靜態IP地址。

註：為確保操作的連續性，並確保在兩個Firepower管理中心上檢測到的檔案惡意軟體處置相同，主要和次要管理中心都必須能夠訪問本文檔中列出的伺服器。

註：思科安全終端控制檯不使用靜態IP，必須通過DNS訪問。

北美的靜態 IP 位址	歐洲的靜態 IP 位址	亞太地區、日本及中國的靜態 IP 位址
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 52.4.151.41 52.4.245.162 52.4.246.178 52.5.92.125 52.6.103.57	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 52.17.211.190 52.17.233.49 52.18.9.153 52.18.28.229 52.18.79.226	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 52.196.247.47 52.196.185.158 52.197.74.4 52.69.39.127 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	52.18.202.103	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		52.68.1.146
54.227.247.102		54.248.107.84
107.20.158.55		54.248.109.124
107.20.203.8		54.248.126.98
		54.248.236.127

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 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	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	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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。