

# Direcciones de servidor necesarias para las operaciones adecuadas de análisis de malware de Cisco Secure Endpoint &

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Direcciones de servidor necesarias para Cisco Secure Endpoint Operations adecuado](#)

[Ubicaciones del servidor](#)

[América del Norte](#)

[Europa](#)

[Asia Pacífico, Japón, China](#)

[Direcciones de servidor necesarias para el correcto acceso a la nube de Cisco Secure Malware Analytics](#)

[Direcciones de servidor necesarias para un uso orbital adecuado](#)

[Nube de Norteamérica \(NAM\) Nube](#)

[Nube europea \(UE\)](#)

[Asia Pacífico, Japón, China \(APJC\) Nube](#)


[Direcciones IP estáticas](#)

---


## Introducción

Este documento describe los servidores necesarios para habilitar el producto Cisco Secure Endpoint (anteriormente Cisco AMP) y el producto Cisco Secure Malware Analytics (anteriormente Threat Grid) para comunicarse y completar actualizaciones, búsquedas e informes. Para completar las operaciones correctamente, el firewall debe permitir la conectividad desde el conector/dispositivo a los servidores necesarios.

---

 Precaución: todos los servidores utilizan un esquema de direcciones IP de ordenamiento cíclico para el balanceo de carga, la tolerancia a fallos y el tiempo de actividad. Por lo tanto, las direcciones IP podrían cambiar, y Cisco recomienda que el firewall se configure con CNAME en lugar de una dirección IP.

---

 Precaución: el tráfico que llega a los servidores de Cisco no puede estar sujeto al descifrado de TLS.

---

# Prerequisites

## Requirements

Este artículo de Tech Zone se aplica a los siguientes productos de Cisco que se integran con el producto Cisco Secure Endpoint (AMP) y el análisis de malware (Threat Grid):

- Terminales seguros para redes de Cisco (Firepower Management Center y sensores)
- Cisco Secure Endpoint Private Cloud
- Nube pública de terminales seguros de Cisco
- Cisco Secure Email Appliance y Cisco Email Security (ESA y CES)
- Dispositivo Cisco Secure Web Appliance (WSA)
- Cisco Secure Malware Analytics Cloud o Appliance (Threat Grid)
- SDWAN/IOS-XE

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

## Direcciones de servidor necesarias para Cisco Secure Endpoint Operations adecuado

### Ubicaciones del servidor

Los servidores Cisco Secure Endpoint y Cisco Secure Malware Analytics se encuentran en tres ubicaciones diferentes:

- Norteamérica (Cisco Secure Endpoint y Cisco Secure Malware Analytics)
- Europa (Cisco Secure Endpoint y Cisco Secure Malware Analytics)
- Japón (solo para terminales seguros de Cisco)

### América del Norte

Esta tabla enumera las ubicaciones del servidor para Norteamérica. Según la fecha de creación de la cuenta, las direcciones del servidor pueden ser diferentes:

Categoría	Propósito	Servidor	Puerto
Terminal seguro de Cisco: nube pública	Servidor de disposición	cloud-ec-asn.amp.cisco.com	TCP 443

		cloud-ec-est.amp.cisco.com enrolment.amp.cisco.com	
	Consola	console.amp.cisco.com	TCP 443
	Servidor de administración	mgmt.amp.cisco.com	TCP 443
	Servidor de eventos	intake.amp.cisco.com	TCP 443
	Políticas	policy.amp.cisco.com	TCP 443
	Descargas y actualizaciones de conectores	upgrades.amp.cisco.com	TCP 80 y 443
	Informe de errores	crash.amp.cisco.com	TCP 443
	IOC de terminales	ioc.amp.cisco.com	TCP 443
	Servidor de actualización de TETRA	tetra-defs.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 y 443
	Definiciones de clam para macOS y Linux	clam-defs.amp.cisco.com	TCP 80 y 443
	Detecciones personalizadas avanzadas	custom-signatures.amp.cisco.com	TCP 443
	Captura remota de archivos	rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Protección del comportamiento	apde.amp.cisco.com	TCP 443
	Control de dispositivos	endpoints.amp.cisco.com	TCP 443
Conector para Android	Servidor de disposición	cloud-android-asn.amp.cisco.com	TCP 443
Conector CSC/iOS	Servidor de disposición	cloud-ios-asn.amp.cisco.com cloud-ios-est.amp.cisco.com	TCP 443
Cisco Secure Endpoint: nube	Servidor de disposición ascendente <v2.4	cloud-pc-est.amp.cisco.com	TCP 443

privada		cloud-pc-asn.amp.cisco.com	
	Servidor de disposición ascendente >v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Servidor Yum	packages-v2.amp.sourcefire.com	TCP 443
		pc-packages.amp.cisco.com	TCP 443
Sesión de asistencia	support-sessions.amp.cisco.com	TCP 22	
AMP para redes: Firepower	Servidor de disposición (desde FMC)	6.0 - 6.2.x: cloud-sa.amp.sourcefire.com 6.3.x +: cloud-sa.amp.cisco.com	TCP 443
	Eventos (desde FMC)	5.x - 6.2.x: export.amp.sourcefire.com 6.3.x +: export.amp.cisco.com	TCP 443
	API (de FMC)	5.x - 6.2.x: api.amp.sourcefire.com 6.3.x +: api.amp.cisco.com Y api.amp.sourcefire.com	TCP 443
	Análisis dinámico (desde el sensor)	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com Y fmc.api.threatgrid.com  *Dependiendo de la versión de la revisión 6.x, se puede utilizar cualquier URL	TCP 443
ESA/WSA/SMA	Reputación de archivos (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
	Análisis de archivos (ESA/WSA/SMA)	panacea.threatgrid.com	TCP 443
	API (ESA)	>= 15.x: api.amp.cisco.com  < 15,x: N/D	TCP 443

	Servidor de eventos (ESA)	>= 15.x: intake.amp.cisco.com < 15,x: N/D	TCP 443
	Management Server (ESA)	>= 15.x: mgmt.amp.cisco.com < 15,x: N/D	TCP 443
Meraki	Servidor de disposición	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
SDWAN	Servidor de disposición	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

## Europa

Esta tabla enumera las ubicaciones de servidor para Europa. Según la fecha de creación de la cuenta, las direcciones del servidor pueden ser diferentes:

Categoría	Propósito	Servidor	Puerto
Terminal seguro de Cisco: nube pública	Servidor de disposición	cloud-ec-asn.eu.amp.cisco.com cloud-ec-est.eu.amp.cisco.com enrolment.eu.amp.cisco.com	TCP 443
	Consola	console.eu.amp.cisco.com	TCP 443
	Servidor de administración	mgmt.eu.amp.cisco.com	TCP 443
	Servidor de eventos	intake.eu.amp.cisco.com	TCP 443
	Políticas	policy.eu.amp.cisco.com	TCP 443
	Descargas y actualizaciones de conectores	upgrades.eu.amp.cisco.com	TCP 80 y 443
	Informe de errores	crash.eu.amp.cisco.com	TCP 443
	IOC de terminales	ioc.eu.amp.cisco.com	TCP 443
	Servidor de actualización de TETRA	tetra-defs.eu.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 y 443

	Definiciones de clam para macOS y Linux	clam-defs.eu.amp.cisco.com	TCP 80 y 443
	Detecciones personalizadas avanzadas	custom-signatures.eu.amp.cisco.com	TCP 443
	Captura remota de archivos	rff.eu.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Protección del comportamiento	apde.eu.amp.cisco.com	TCP 443
	Control de dispositivos	endpoints.eu.amp.cisco.com	TCP 443
Conector para Android	Servidor de disposición	cloud-android-asn.eu.amp.cisco.com	TCP 443
Conector CSC/iOS	Servidor de disposición	cloud-ios-asn.eu.amp.cisco.com cloud-ios-est.eu.amp.cisco.com	TCP 443
Cisco Secure Endpoint: nube privada	Servidor de disposición ascendente <v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Servidor de disposición ascendente >v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Servidor Yum	packages-v2.amp.sourcefire.com	TCP 443
		pc-packages.amp.cisco.com	TCP 443
Sesión de asistencia	support-sessions.amp.cisco.com	TCP 22	
AMP para redes: Firepower	Servidor de disposición (desde FMC)	6.0 - 6.2.x: cloud-sa.eu.amp.sourcefire.com 6.3.x+: cloud-sa.eu.amp.cisco.com	TCP 443
	Eventos (desde FMC)	5.x - 6.2.x: export.eu.amp.sourcefire.com 6.3.x+: export.eu.amp.cisco.com	TCP 443
	API (de FMC)	5.x - 6.2.x: api.amp.sourcefire.com Y api.eu.amp.sourcefire.com	TCP 443

		6.3.x+: api.amp.sourcefire.com Y api.eu.amp.cisco.com	
	Análisis dinámico (desde el sensor)	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.eu Y fmc.api.threatgrid.eu Dependiendo de la versión del parche 6.x, se puede utilizar cualquier URL	TCP 443
ESA/WSA/SMA	Reputación de archivos (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
	Análisis de archivos (ESA/WSA/SMA)	panacea.threatgrid.eu	TCP 443
	API (ESA)	>= 15.x: api.eu.amp.cisco.com < 15,x: N/D	TCP 443
	Servidor de eventos (ESA)	>= 15.x: intake.eu.amp.cisco.com < 15,x: N/D	TCP 443
	Management Server (ESA)	>= 15.x: mgmt.eu.amp.cisco.com < 15,x: N/D	TCP 443
SDWAN	Servidor de disposición	cloud-isr-asn.eu.amp.cisco.com cloud-isr-est.eu.amp.cisco.com	TCP 443

## Asia Pacífico, Japón, China

Esta tabla enumera las ubicaciones de servidor para Asia Pacífico, Japón y China:

Categoría	Propósito	Servidor	Puerto
Terminal seguro de Cisco: nube pública	Servidor de disposición	cloud-ec-asn.apjc.amp.cisco.com	TCP 443
		cloud-ec-est.apjc.amp.cisco.com enrolment.apjc.amp.cisco.com	
	Consola	console.apjc.amp.cisco.com	TCP 443

	Servidor de administración	mgmt.apjc.amp.cisco.com	TCP 443
	Servidor de eventos	intake.apjc.amp.cisco.com	TCP 443
	Políticas	policy.apjc.amp.cisco.com	TCP 443
	Descargas y actualizaciones de conectores	upgrades.apjc.amp.cisco.com	TCP 80 y 443
	Informe de errores	crash.apjc.amp.cisco.com	TCP 443
	IOC de terminales	ioc.apjc.amp.cisco.com	TCP 443
	Servidor de actualización de TETRA	tetra-defs.apjc.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 y 443
	Definiciones de clam para macOS y Linux	clam-defs.apjc.amp.cisco.com	TCP 80 y 443
	Detecciones personalizadas avanzadas	custom-signatures.apjc.amp.cisco.com	TCP 443
	Captura remota de archivos	rff.apjc.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Protección del comportamiento	apde.apjc.amp.cisco.com	TCP 443
	Control de dispositivos	endpoints.apjc.amp.cisco.com	TCP 443
Conector para Android	Servidor de disposición	cloud-android-asn.apjc.amp.cisco.com	TCP 443
Conector CSC/iOS	Servidor de disposición	cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
Cisco Secure Endpoint:	Servidor de disposición ascendente < v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443



Nube privada	Upstream Disposition Server > v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Servidor Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	Sesión de asistencia	support-sessions.amp.cisco.com	TCP 22
AMP para redes: Firepower	Servidor de disposición	6.0 - 6.2.x: cloud-sa.apjc.amp.sourcefire.com (IP estática) 6.3.x+: cloud-sa.apjc.amp.cisco.com	TCP 443
	Events	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 AND api.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com Y api.apjc.amp.cisco.com	TCP 443
	Análisis dinámico	Actualmente no hay Data Centers de Threat Grid en APJC, por lo que el Se deben utilizar nombres de host europeos o norteamericanos.	TCP 443
ESA/WSA/SMA	Reputación de archivos (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
	Análisis de archivos (ESA/WSA/SMA)	Actualmente no hay Data Centers de Threat Grid en APJC, por lo que el Se deben utilizar nombres de host europeos o norteamericanos.	TCP 443

API (ESA)

		>= 15.x: api.apjc.amp.cisco.com < 15,x: N/D	TCP 443
	Servidor de eventos (ESA)	>= 15.x: intake.apjc.amp.cisco.com < 15,x: N/D	TCP 443
	Management Server (ESA)	>= 15.x: mgmt.apjc.amp.cisco.com < 15,x: N/D	TCP 443
SDWAN	Servidor de disposición	cloud-isr-asn.apjc.amp.cisco.com cloud-isr-est.apjc.amp.cisco.com	TCP 443

## Direcciones de servidor necesarias para el correcto acceso a la nube de Cisco Secure Malware Analytics

Para obtener más información sobre Secure Malware Analytic Cloud and Appliance, consulte este artículo: [IP y puertos necesarios para el análisis de malware seguro](#)

## Direcciones de servidor necesarias para un uso orbital adecuado

IP estáticas para Orbital 1.7+

### Nube de Norteamérica (NAM) Nube

Hostname	IP	Puerto
orbital.amp.cisco.com	54.71.115.87	443
	54.68.234.245	
	54.200.174.54	
ncp.orbital.amp.cisco.com	52.88.16.211	443
	52.43.91.219	
	54.200.152.114	
update.orbital.amp.cisco.com	54.71.197.112	443
	54.188.114.190	
	54.188.131.5	

IP de NAT para almacenamiento de datos remoto		
	34.223.219.240	Número de puerto aleatorio alto
	35.160.108.105	
	52.11.13.222	

Para obtener más información, consulte la guía de ayuda orbital:

<https://orbital.amp.cisco.com/help/>

## Nube europea (UE)

Hostname	IP	Puerto
orbital.eu.amp.cisco.com	3.120.91.16	443
	18.196.194.92	
	3.121.5.209	
ncp.orbital.eu.amp.cisco.com	18.194.154.159	443
	18.185.217.177	
	18.184.249.36	
update.orbital.eu.amp.cisco.com	3.123.83.189	443
	18.184.240.159	
	35.158.29.104	
IP de NAT para almacenamiento de datos remoto		
	52.29.47.197	Número de puerto aleatorio alto
	52.57.222.67	
	52.58.172.218	

Para obtener más información, consulte la guía de ayuda orbital:

<https://orbital.eu.amp.cisco.com/help/>

## Asia Pacífico, Japón, China (APJC) Nube

Hostname	IP	Puerto
orbital.apjc.amp.cisco.com	3.114.186.175 52.198.6.9 18.177.242.101	443
nep.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
IP de NAT para almacenamiento de datos remoto		
	52.194.143.206 52.69.138.67 54.95.9.136	Número de puerto aleatorio alto


Para obtener más información, consulte la guía de ayuda orbital:

<https://orbital.apjc.amp.cisco.com/help/>

## Direcciones IP estáticas

Si el firewall bloquea las conexiones TCP salientes en el puerto 443 (lo que normalmente no sucede), debe cambiar la configuración del firewall antes de actualizar las directivas. Si su cuenta se estableció después de febrero de 2016, ya tiene direcciones IP estáticas escritas en las políticas estándar. Si su cuenta se creó antes de febrero de 2016, puede ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) para solicitar una migración de las políticas a las direcciones IP estáticas.

---

 Nota: para garantizar la continuidad de las operaciones y garantizar que las disposiciones de malware de los archivos detectados sean las mismas en ambos Firepower Management Centers, tanto el principal como el secundario deben tener acceso a los servidores enumerados en este documento.

---



Nota: Cisco Secure Endpoint Console no utiliza IP estáticas y se debe acceder a ella a través de DNS.

Direcciones IP estáticas en Norteamérica	Direcciones IP estáticas en Europa	Direcciones IP estáticas en APJC
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
	46.137.99.242	52.69.16.172
50.16.242.171	52.16.63.115	13.112.137.80
50.16.244.193	52.16.95.58	52.198.208.254
	52.16.105.95	13.112.162.167
50.16.250.236	52.16.166.193	54.249.244.218
52.0.55.209	52.16.177.94	54.249.246.210
52.2.63.194	52.16.193.225	54.249.243.85
52.2.128.246	52.16.220.180	54.249.240.219
52.3.149.24	52.17.93.43	54.248.98.94
52.3.178.163	52.17.102.100	176.34.47.0
52.3.190.47	52.17.106.35	52.192.82.189
52.4.98.101	52.17.179.163	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
	54.228.250.255	52.198.202.24
54.204.8.61	54.246.88.192	52.198.221.53
54.221.210.7	54.247.189.117	52.198.223.169
54.221.255.190		52.198.225.221
54.225.226.117	54.74.229.75	52.198.226.104
54.225.227.9		52.198.26.36
54.225.227.30	107.21.250.31	52.198.94.104
54.225.227.45		52.199.124.11
54.225.227.105	107.21.236.143	52.199.127.80
54.225.228.145		52.199.92.142
54.225.228.166	52.2.128.246	52.68.1.146
54.225.228.244		54.248.107.84
54.227.247.102	52.18.202.103	54.248.109.124
107.20.158.55		54.248.126.98
107.20.203.8	52.18.119.87	54.248.236.127
107.20.229.191		54.248.236.141
107.20.234.220	192.111.5.0/24	54.248.236.144
107.21.212.157		54.248.236.151
107.21.217.202	34.249.48.182	54.248.237.93
107.21.218.60		54.249.246.7
128.177.8.0/24	34.248.52.55	54.250.127.131
174.129.203.65		
	99.81.233.22	
	3.123.83.189	192.111.6.0/24
54.161.128.60		
54.234.131.176	18.184.240.159	54.248.22.154
52.206.206.244		
34.225.208.192	35.158.29.104	18.178.184.79
52.22.120.193		
34.199.250.32	192.35.177.23	54.95.125.218
34.199.238.4	104.18.39.201	
34.194.224.132	172.64.148.55	192.35.177.23
34.198.112.150		104.18.39.201
34.224.236.198	104.18.4.5	172.64.148.55
52.20.233.31	104.18.5.5	
	52.3.48.165	18.180.25.43
192.111.4.0/24	52.6.245.67	54.95.253.127

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	34.120.67.236 34.98.122.109	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
--	--------------------------------	---

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).