

Configurar IP y reglas de firewall necesarias para el análisis de malware seguro

Contenido

[Introducción](#)

[Problema](#)

[Entorno](#)

[Resolución](#)

[Dispositivo de análisis de malware seguro](#)

[Interfaz de administración](#)

[Limpiar interfaz](#)

[Interfaz sucia](#)

[Interfaz Saliente Sucia](#)

[Interfaz entrante sucia](#)

[Nube de análisis de malware seguro](#)

[Nube de Estados Unidos \(US\)](#)

[Nube de Europa \(UE\)](#)

[Nube de Canadá \(CA\)](#)

[Nube de Australia \(AU\)](#)

[India \(IN\) Nube](#)

[Contenido relacionado](#)

Introducción

Este documento describe los nombres de host, las direcciones IP y los puertos necesarios para Cisco Secure Malware Analytics (nube y dispositivo).

Problema

Cisco Secure Malware Analytics requiere conectividad saliente y entrante con nombres de host, direcciones IP y puertos específicos. Si estos flujos se bloquean, las funciones como el acceso al portal, las actualizaciones, las licencias, el soporte remoto y las integraciones pueden fallar.

Entorno



Nota: Consulte primero este documento, que incluye IP y puertos adicionales para otros



servicios.

[IP y puertos necesarios para Threat Grid](#)

Este documento incluye direcciones IP y puertos adicionales para otros servicios basados en la versión del dispositivo.

Consulte la documentación de las guías de instalación y actualización: [Guías de instalación de dispositivos Threat Grid](#)

Resolución

Reglas de firewall para el flujo ascendente de firewall al dispositivo:

*Las direcciones IP eran correctas en el momento de la publicación. Confirme localmente a través de nslookup que estas siguen siendo correctas.

Dispositivo de análisis de malware seguro

Interfaz de administración

Fuente	Destino	Protocolo	Puerto	Dirección:	Acción	Notas
CUALQUIERA	Interfaz de administración	TCP	22	IN	Permiso	SSH
CUALQUIERA	Interfaz de administración	TCP	80/443	IN	Permiso	Permita el acceso a la interfaz GUI de administración.
Interfaz de administración	IP de servidor NFS	TCP	2049	FUERA	Permiso	*Debe estar abierto para utilizar la función de copia de seguridad o agrupación en clústeres de NFS.

Limpiar interfaz

Fuente	Destino	Protocolo	Puerto	Dirección:	Acción	Notas
CUALQUIERA	Limpiar interfaz	TCP	80/443	IN	Permiso	Permita el acceso a la interfaz gráfica de usuario limpia.
CUALQUIERA	Limpiar interfaz	TCP	8443	IN	Permiso	*Debe estar abierto para utilizar la función Admin over Clean.
CUALQUIERA	Limpiar interfaz	TCP	9443	IN	Permiso	*Debe estar abierto para utilizar la función de caja de guantes de muestra.
Limpiar interfaz	Servidor de retransmisión de correo electrónico configurado	TCP	25	FUERA	Permitir	El dispositivo utiliza una interfaz limpia para iniciar conexiones SMTP con el servidor de correo configurado.
Limpiar interfaz	Servidor DNS limpio configurado	TCP/UDP	53	FUERA	Permiso	*Opcional, solo se requiere si se ha configurado Clean DNS.
Limpiar interfaz	Servidor Syslog configurado	TCP/UDP	514	FUERA	Permiso	Permitir la conectividad con el servidor designado para recibir mensajes de Syslog y notificaciones de Threat Grid.
Limpiar interfaz	Servidor LDAP	TCP/UDP	389/636	FUERA	Permiso	*Opcional, solo se requiere si LDAP está configurado.

Interfaz sucia

Interfaz Saliente Sucia

Fuente	Destino	Protocolo	Puerto	Acción	Nota
Interfaz sucia	Internet	CUALQUIERA	CUALQUIERA	Permiso	Permitir el tráfico saliente de muestras, opcionalmente proxy a través de los Data Centers de Cisco. (Para obtener resultados precisos, es necesario que se permita que el malware se ponga en contacto con su servidor de comando y control mediante el puerto y protocolo que esté diseñado para utilizar.)

Interfaz entrante sucia

Fuente	Destino	Protocolo	Puerto	Acción	Nota
CUALQUIERA	Internet sucio	CUALQUIERA	CUALQUIERA	Denegar	Denegar todas las conexiones entrantes.

Fuente	Destino	Protocolo	Puerto	Acción	Nota
Interfaz sucia	Internet	TCP	22	Permiso	Servicios de actualización, instantáneas de soporte y licencias.
Interfaz sucia	Internet	TCP/UDP	53	Permiso	Permitir DNS saliente.
Interfaz sucia	Internet	UDP	123	Permiso	Permitir NTP saliente.
Interfaz sucia	Internet	TCP	19791	Permiso	Permita la conectividad a la compatibilidad con Secure Malware Analytics.
Interfaz sucia	Cisco Umbrella	TCP	443	Permiso	Conéctese con servicios de detección y enriquecimiento de terceros.

Interfaz sucia	TotalVirus	TCP	443	Permiso	Conéctese con servicios de detección y enriquecimiento de terceros.
Interfaz sucia	Nube de titanio	TCP	443	Permiso	Conéctese con servicios de detección y enriquecimiento de terceros.



Advertencia: Las direcciones IP que se muestran permanecen activas después del 29 de mayo de 2023.

Fuente	Destino	Protocolo	Puerto	Dirección:	Hostname	Detalles
Interfaz sucia	63.97.201.96 63.162.55.96	TCP	19791	FUERA	rash.threatgrid.com	Soporte remoto/Modo de soporte de dispositivo
Interfaz sucia	63.97.201.97 63.162.55.97	TCP	22	FUERA	appliance-updates.threatgrid.com	Se utiliza para cargas de diagnóstico de soporte automático.  Nota: Requiere la versión de software 1.2+
Interfaz sucia	63.97.201.98 63.162.55.98	TCP	22	FUERA	support-snapshots.threatgrid.com	Se utiliza para cargas de diagnóstico de soporte automático.  Nota: Requiere la versión de software 1.2+

Interfaz sucia	63.97.201.99 63.162.55.99	TCP	22	FUERA	appliance-licensing.threatgrid.com	Administración de licencias
-------------------	------------------------------	-----	----	-------	---	--------------------------------

Nube de análisis de malware seguro

Nube de Estados Unidos (US)

URL de acceso: <https://panacea.threatgrid.com>

Hostname	IP	Puerto	Detalles
panacea.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6:6e	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	IPv4: 200.194.241.35 IPv6: 2602:811:900f:6::6e	443	Ventana de interacción de ejemplo
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6: 2602:811:9007:6::61	443	Ventana de interacción de ejemplo
glovebox.scl.threatgrid.com	IPv4:	443	Ventana de interacción de ejemplo

	63.162.55.67 IPv6: 2602:811:900b:6:6e		
fmc.api.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6:6e	443	Servicio de análisis de archivos FMC/FTD

Nube de Europa (UE)

URL de acceso: <https://panacea.threatgrid.eu>

Hostname	IP	Puerto	Detalles
panacea.threatgrid.eu	IPv4: 62.67.214.195 200.194.242.35 200.194.245.35 IPv6: 2602:811:9006:6:6e 2602:811:900c:6::6e	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	IPv4: 62.67.214.195 200.194.245.35 IPv6:	3	Ventana de interacción de ejemplo

	2602:811:900c:6::6e		
glovebox.fam.threatgrid.eu	IPv4: 200.194.242.35 IPv6: 2602:811:9006:6:6e	443	Ventana de interacción de ejemplo
fmc.api.threatgrid.eu	IPv4: 62.67.214.195 200.194.242.35 200.194.245.35 IPv6: 2602:811:9006:6:6e 2602:811:900c:6::6e	443	Servicio de análisis de archivos FMC/FTDF

Se ha retirado la IP 89.167.128.132 antigua. Actualice las reglas del firewall con estas IP.

Nube de Canadá (CA)

URL de acceso: <https://panacea.threatgrid.ca>

Hostname	IP	Puerto	Detalles
panacea.threat.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threat.ca	IPv4: 200.194.240.35	443	Ventana de interacción de ejemplo

	IPv6: 2602:811:900d:6::6e		
fmc.api.threat.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	Servicio de análisis de archivos FMC/FTD

Nube de Australia (AU)

URL de acceso: <https://panacea.threatgrid.com.au>

Hostname	IP	Puerto	Detalles
panacea.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6:6e	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6:6e	443	Ventana de interacción de ejemplo
fmc.api.threatgrid.com.au	IPv4: 200.194.246.35	443	Servicio de análisis de archivos FMC/FTD

	200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6:6e		
--	--	--	--

India (IN) Nube

URL de acceso: <https://panacea.threatgrid.in>

Hostname	IP	Puerto	Detalles
panacea.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	Ventana de interacción de ejemplo
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	Servicio de análisis de archivos FMC/FTD

Para obtener más información sobre los requisitos de Cisco Secure Malware Analytics, como los dispositivos, consulte este artículo:

Contenido relacionado

Para conocer los requisitos más recientes, consulte .

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).