Puertos e IP necesarios para el análisis de malware seguro

Contenido

Introducción

Este documento describe las configuraciones de red esenciales que necesita implementar en su firewall para garantizar un funcionamiento sin problemas de Secure Malware Analytics.

Colaboración de los ingenieros del TAC de Cisco.

Nubes de análisis de malware seguras

Nube de EE. UU. (Estados Unidos)

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

Hostname	IP	Puerto	Detalles
panacea.threatgrid.com	63.97.201.67 63.162.55.67	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	Ventana de interacción de ejemplo
glovebox.rcn.threatgrid.com	63.97.201.67	443	Ventana de interacción de ejemplo
glovebox.scl.threatgrid.com	63.162.55.67	443	Ventana de interacción de ejemplo

fmc.api.threatgrid.com	63.97.201.67 63.162.55.67	443	Servicio de análisis de archivos FMC/FTD

Nube de la UE (Europa)

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

Hostname	IP	Puerto	Detalles
panacea.threatgrid.eu	62.67.214.195 200.194.242.35	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	62.67.214.195	443	Ventana de interacción de ejemplo
glovebox.fam.threatgrid.eu	200.194.242.35	443	Ventana de interacción de ejemplo
fmc.api.threatgrid.eu	62.67.214.195 200.194.242.35	443	Servicio de análisis de archivos FMC/FTD

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

Nube de CA (Canadá)

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

Hostname	IP	Puerto	Detalles
panacea.threat.ca	200.194.240.35	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threat.ca	200.194.240.35	443	Ventana de interacción de ejemplo
fmc.api.threat.ca	200.194.240.35	443	Servicio de análisis de archivos FMC/FTD

Nube AU (Australia)

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

Hostname	IP	Puerto	Detalles
panacea.threatgrid.com.au	124.19.22.171	443	Para Secure Malware Analytics Portal y dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	124.19.22.171	443	Ventana de interacción de ejemplo

fmc.api.threatgrid.com.au	124.19.22.171	443	Servicio de análisis de archivos FMC/FTD

Dispositivo de análisis de malware seguro

A continuación se indican las reglas de firewall recomendadas por interfaz de Secure Malware Analytics Appliance.

Interfaz sucia

Las máquinas virtuales las utilizan para comunicarse con Internet, de modo que las muestras puedan resolver DNS y comunicarse con servidores de comando y control (C&C)

Permiso:

Dirección:	Protocolo	Puerto	Destino	Hostname	Detalles
Salientes	IP	CUALQUIERA	CUALQUIERA		Se recomienda, excepto cuando se especifique en la sección **Denegar** aquí. Se utiliza para permitir la conectividad para el análisis.
Salientes	TCP	22	54.173.231.161 1 63.97.201.98 2 63.162.55.98 2	support-snapshots.threatgrid.com	Se utiliza para cargas de diagnóstico de soporte automático Nota: requiere la versión de software 1.2+
Salientes	TCP	22	54.173.181.217 1 54.173.182.46 1 63.162.55.97 2 63.97.201.97 2	appliance-updates.threatgrid.com	Actualizaciones de dispositivos
Salientes	TCP	19791	54.164.165.137 1 34.199.44.202 1 63.97.201.96 2 63.162.55.96 2	rash.threatgrid.com	Soporte remoto/Modo de soporte de dispositivo
Salientes	TCP	22	54.173.124.172 1 63.97.201.99 2 63.162.55.99 2	appliance-licensing.threatgrid.com	Administración de licencias

[1]Estas IP se desactivarán en un futuro próximo.

[2]Estas son las IP que reemplazarían a las de [1]. Sugerimos agregar ambas IP hasta que la comunicación sobre los cambios de IP se realice en un futuro próximo.

Salida de red remota

Utilizado por el dispositivo para tunelizar el tráfico de VM a una salida remota antes conocida como tg-tunnel.

Dirección:	Protocolo	Puerto	Destino
Salientes	TCP	21413	173.198.252.53
Salientes	TCP	21413	163.182.175.193 **
Salientes	TCP	21417	69.55.5.250
Salientes	TCP	21415	69.55.5.250
Salientes	TCP	21413	76.8.60.91

Nota: la salida remota 4.14.36.142 se ha eliminado y ya no está en producción. Asegúrese de agregar todas las direcciones IP mencionadas a la lista de excepciones del firewall.

** La salida remota 163.182.175.193 se sustituirá por 173.198.252.53

Denegar:

Dirección:	Protocolo	Puerto(s)	Destino	Detalles
Salientes	SMTP	CUALQUIERA	CUALQUIERA	Para evitar que el malware envíe spam.
Entrante	IP	CUALQUIERA	Interfaz sucia de Secure Malware Analytics Appliance	Se recomienda, excepto cuando se especifique en la sección **Permitir** anterior. Se utiliza para permitir la comunicación para el análisis.

Limpiar interfaz

Utilizado por varios servicios conectados para enviar muestras, así como acceso a la interfaz de usuario para los analistas.

Permiso:

Dirección:	Protocolo	Puerto(s)	Destino	Detalles
Entrante	TCP	443 y 8443	Interfaz limpia de Secure Malware Analytics Appliance	Acceso a WebUI y API
Entrante	TCP	9443	Interfaz limpia de Secure Malware Analytics Appliance	Se utiliza para guantera
Entrante	TCP	22	Interfaz limpia de Secure Malware	Acceso TUI de administración sobre SSH

			Analytics Appliance	
Salientes	TCP	19791	**Host:** rash.threatgrid.com 54.164.165.137 [1] ,34.199.44.202 [1] 63.97.201.96 [2] , 63.162.55.96 [2]	Modo de recuperación para el soporte de Secure Malware Analytics.

[1]Estas IP se desactivarán en un futuro próximo.

[2]Estas son las IP que reemplazarían a las de [1]. Sugerimos agregar ambas IP hasta que la comunicación sobre los cambios de IP se realice en un futuro próximo.

Interfaz de administración

Acceso a la interfaz de administración.

Permiso:

Dirección:	Protocolo	Puerto(s)	Destino	Detalles
Entrante	TCP	443 y 8443	Interfaz de administración de Secure Malware Analytics Appliance	Se utiliza para configurar el hardware y las licencias.
Entrante	TCP	22	Interfaz de administración de Secure Malware Analytics Appliance	Acceso TUI de administración sobre SSH

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).