安全恶意软件分析所需的IP和端口

目录

简介

安全恶意软件分析云

- 美国（美国）云
- EU（欧洲）云
- CA（加拿大）云
- 澳大利亚（澳大利亚）云
- IN（印度）云

安全恶意软件分析设备

- 脏接口
- 远程网络退出
- 清洁接口
- 管理界面

简介

本文档概述了需要在防火墙上实施的基本网络配置，以确保安全恶意软件分析无缝运行。

安全恶意软件分析云

美国（美国）云

访问URL:https://panacea.threatgrid.com

主机名	IP	端口	详细信息
panacea.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61	443	对于安全恶意软件分析门户和集成设备(ESA/WSA/FTD/ODNS/Meraki)

	2602:811:900b:6::6e		
glovebox.chi.threatgrid.com	IPv4:200.194.241.35 IPv6: 2602:811:900f:6::6e	443	示例交互窗口
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6: 2602:811:9007:6::61	443	示例交互窗口
glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6: 2602:811:900b:6::6e	443	示例交互窗口
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	FMC/FTD文件分析服务

EU（欧洲）云

访问URL:https://panacea.threatgrid.eu

主机名	IP	端口	详细信息
panacea.threatgrid.eu	IPv4: 62.67.214.195	443	对于安全恶意软件分析门户和集成设备(ESA/WSA/FTD/ODNS/Meraki)

	200.194.242.35 200.194.245.35 IPv6: 2602:811:9006:6::6e 2602:811:900c:6::6e		
glovebox.muc.threatgrid.eu	IPv4: 62.67.214.195 200.194.245.35 IPv6: 2602:811:900c:6::6e	3	示例交互窗口
glovebox.fam.threatgrid.eu	IPv4: 200.194.242.35 IPv6: 2602:811:9006:6::6e	443	示例交互窗口
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	FMC/FTDF文件分析服务

旧的IP 89.167.128.132已淘汰，请使用上述IP更新您的防火墙规则。

CA（加拿大）云

访问URL:https://panacea.threatgrid.ca

主机名	IP	端口	详细信息
panacea.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	对于安全恶意软件分析门户和集成设备(ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	示例交互窗口
fmc.api.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	FMC/FTD文件分析服务

澳大利亚（澳大利亚）云

访问URL:https://panacea.threatgrid.com.au

主机名	IP	端口	详细信息
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	对于安全恶意软件分析门户和集成设备(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	示例交互窗口
fmc.api.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6::6e	443	FMC/FTD文件分析服务

IN（印度）云

访问URL:https://panacea.threatgrid.in

主机名	IP	端口	详细信息
panacea.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	对于安全恶意软件分析门户和集成设备(ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	示例交互窗口

fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	FMC/FTD文件分析服务

安全恶意软件分析设备

以下是安全恶意软件分析设备每个接口的推荐防火墙规则。

脏接口

VM用它与Internet通信，以便示例可以解析DNS并与命令和控制(C&C)服务器通信。允许:

方向	协议	端口	目的地	主机名	详细信息
出站	IP	ANY	ANY		建议使用，但此处的拒绝部分中指定的除外。 用于允许连接进行分析。
出站	TCP	22	63.97.201.98 63.162.55.98	support-snapshots.threatgrid.com	用于自动支持诊断上传。注意：需要软件版本1.2+。
出站	TCP	22	63.162.55.97 63.97.201.97	appliance-updates.threatgrid.com	设备更新
出站	TCP	19791	63.97.201.96 63.162.55.96	rash.threatgrid.com	远程支持/设备支持模式
出站	TCP	22	63.97.201.99 63.162.55.99	appliance-licensing.threatgrid.com	许可证管理

远程网络退出

设备使用此功能将VM流量通过隧道传输到远程出口，以前称为tg-tunnel。

方向	协议	端口	目的地
出站	TCP	21413	173.198.252.53
出站	TCP	21417	69.55.5.250
出站	TCP	21415	69.55.5.250
出站	TCP	21413	38.123.149.87

注意：截至2026年7月25日，已更换以下远程退出IP地址：
- 163.182.175.193被173.198.252.53取代
- 76.8.60.91被38.123.149.87取代

拒绝：

方向	协议	端口	目的地	详细信息
出站	SMTP	ANY	ANY	防止恶意软件发送垃圾邮件。
入站	IP	ANY	安全恶意软件分析设备不良界面	建议，但上面允许部分中指定的除外。 用于允许用于分析的通信。

清洁接口

各种连接的服务均使用此功能提交样本以及分析人员的UI访问。允许:

方向	协议	端口	目的地	详细信息
入站	TCP	443 和 8443	安全恶意软件分析设备全新界面	WebUI和API访问
入站	TCP	9443	安全恶意软件分析设备全新界面	用于Glovebox
入站	TCP	22	安全恶意软件分析设备全新界面	通过SSH进行管理员TUI访问

出站	TCP	19791	主机：rash.threatgrid.com 63.97.201.96 63.162.55.96	安全恶意软件分析支持的恢复模式

管理界面

使用此命令可访问管理控制台或用户界面。允许:

方向	协议	端口	目的地	详细信息
入站	TCP	443 和 8443	安全恶意软件分析设备管理界面	用于配置硬件和许可的设置
入站	TCP	22	安全恶意软件分析设备管理界面	通过SSH进行管理员TUI访问

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）。