

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](#)

[安全恶意软件分析设备](#)

[脏接口](#)

[远程网络退出](#)

[清理接口](#)

[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的无缝操作。

由思科 TAC 工程师撰稿。

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	63.97.201.67 63.162.55.67	443	适用于安全恶意软件分析门户和集成设备 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	“示例交互”窗口
glovebox.rcn.threatgrid.com	63.97.201.67	443	“示例交互”窗口
glovebox.scl.threatgrid.com	63.162.55.67	443	“示例交互”窗口

fmc.api.threatgrid.com	63.97.201.67 63.162.55.67	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	62.67.214.195 200.194.242.35	443	适用于安全恶意软件分析门户和集成设备 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	62.67.214.195	443	“示例交互”窗口
glovebox.fam.threatgrid.eu	200.194.242.35	443	“示例交互”窗口
fmc.api.threatgrid.eu	62.67.214.195 200.194.242.35	443	FMC/FTD文件分析服务

旧的IP 89.167.128.132已停用，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	200.194.240.35	443	适用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	200.194.240.35	443	“示例交互”窗口
fmc.api.threatgrid.ca	200.194.240.35	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	124.19.22.171	443	适用于安全恶意软件分析门户和集成设备 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.sydney.threatgrid.com.au	124.19.22.171	443	“示例交互”窗口
fmc.api.threatgrid.com.au	124.19.22.171	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建议防火墙规则。

脏接口

虚拟机用于与互联网通信，以便样本可以解析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(但此处的拒绝部分中指定的除外)。 用于允许用于分析的连接。
出站	TCP	22	54.173.231.161 1 63.97.201.98 2 63.162.55.98 2	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	54.173.181.217 1 54.173.182.46 1 63.162.55.97 2 63.97.201.97 2	appliance- updates.threatgrid.com	设备更新
出站	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	远程支持/设备支持模式
出站	TCP	22	54.173.124.172 1 63.97.201.99 2 63.162.55.99 2	appliance-licensing.threatgrid.com	许可证管理


¹这些IP将在不久的将来被禁用。


²以下是将会替换¹中的IP地址。我们建议添加两个IP，直到在不久的将来完成有关IP更改的通信。

远程网络退出

设备用于将VM流量通过隧道传送到远程出口（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	21413	163.182.175.193 **
出站	TCP	21417	69.55.5.250
出站	TCP	21415	69.55.5.250
出站	TCP	21413	76.8.60.91

 **注意：**远程出口4.14.36.142已删除，并且不再生产。确保将提及的所有IP都添加到您的防火墙例外列表。

 **173.198.252.53将取代远程出口163.182.175.193

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脏界面	建议(但上面允许部分中指定的除外)。 用于允许通信进行分析。

清理接口

各种互联服务使用它来提交样本和分析专家的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安全接口	WebUI和API访问
入站	TCP	9443	安全恶意软件分析设备安全接口	用于Glovebox

入站	TCP	22	安全恶意软件分析设备安全接口	通过SSH进行管理员TUI访问
出站	TCP	19791	主机：rash.threatgrid.com 54.164.165.137 ¹ 、 34.199.44.202 ¹ 63.97.201.96 ² 、63.162.55.96 ²	安全恶意软件分析支持的恢复模式。

¹这些IP将在不久的将来被禁用。

²以下是将会替换¹中的IP地址。我们建议添加两个IP，直到在不久的将来完成有关IP更改的通信。

管理界面

访问管理UI。

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。
因布德	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）。