# 配置安全恶意软件分析所需的IP和防火墙规则

## 目录


简介

问题

环境

分辨率

- 安全恶意软件分析设备
  - 管理界面
  - 清洁接口
  - 脏接口
- 出站脏接口
- 脏接口入站
- 安全恶意软件分析云
- 美国(US)云
- 欧洲（欧盟）云
- 加拿大(CA)云
- 澳大利亚(AU)云
- 印度(IN)云

相关内容


## 简介

本文档介绍思科安全恶意软件分析（云和设备）所需的主机名、IP地址和端口。

## 问题

思科安全恶意软件分析需要与特定主机名、IP地址和端口建立出站和入站连接。如果阻止这些流量，门户访问、更新、许可、远程支持和集成等功能可能会失败。

## 环境

注意：请首先参阅本文档，其中包括用于其他服务的附加IP和端口。
Threat Grid所需的IP和端口

本文档包括基于设备版本的其他服务的IP和端口。

请参阅《安装和升级指南》文档：Threat Grid设备安装指南

## 分辨率

设备上游防火墙的防火墙规则：

*IP在发布时是正确的。请通过nslookup在本地确认这些设置是否仍然正确。

### 安全恶意软件分析设备

管理界面

| 来源 | 目的地 | 协议 | 端口 | 方向 | 操作 | 备注 |
|---|---|---|---|---|---|---|
| ANY | 管理界面 | TCP | 22 | 配置 | 允许 | SSH |
| ANY | 管理界面 | TCP | 80/443 | 配置 | 允许 | 允许访问管理GUI界面。 |
| 管理界面 | NFS服务器IP | TCP | 2049 | OUT | 允许 | *必须打开才能使用NFS备份或群集功能。 |

清洁接口

| 来源 | 目的地 | 协议 | 端口 | 方向 | 操作 | 备注 |
|---|---|---|---|---|---|---|
| ANY | 清洁接口 | TCP | 80/443 | 配置 | 允许 | 允许访问Clean GUI Interface。 |
| ANY | 清洁接口 | TCP | 8443 | 配置 | 允许 | *必须打开才能使用Admin over Clean Feature。 |
| ANY | 清洁接口 | TCP | 9443 | 配置 | 允许 | *必须打开才能使用Glovebox功能示例。 |
| 清洁接 | 已配置的邮件中 | TCP | 25 | OUT | 允 | 设备使用安全接口发起到已配置邮件服务器 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 口 | 继服务器 | | | | 许 | 的SMTP连接。 |
| 清洁接口 | 已配置的安全DNS服务器 | TCP/UDP | 53 | OUT | 允许 | *可选，仅在配置了Clean DNS时需要。 |
| 清洁接口 | 已配置系统日志服务器 | TCP/UDP | 514 | OUT | 允许 | 允许连接到指定用于接收系统日志消息和Threat Grid通知的服务器。 |
| 清洁接口 | LDAP 服务器 | TCP/UDP | 389/636 | OUT | 允许 | *可选，仅在配置了LDAP时需要。 |

脏接口

## 出站脏接口

| 来源 | 目的地 | 协议 | 端口 | 操作 | 备注 |
|---|---|---|---|---|---|
| 脏接口 | 互联网 | ANY | ANY | 允许 | 允许来自示例的出站流量（可选择通过思科数据中心代理）。（要获得准确的结果，必须允许恶意软件使用它设计使用的任何端口和协议联系其命令和控制服务器。） |

## 脏接口入站

| 来源 | 目的地 | 协议 | 端口 | 操作 | 备注 |
|---|---|---|---|---|---|
| ANY | 肮脏的互联网 | ANY | ANY | 拒绝 | 拒绝所有传入连接。 |

| 来源 | 目的地 | 协议 | 端口 | 操作 | 备注 |
|---|---|---|---|---|---|
| 脏接口 | 互联网 | TCP | 22 | 允许 | 更新、支持快照和许可服务。 |
| 脏接口 | 互联网 | TCP/UDP | 53 | 允许 | 允许出站DNS。 |

| | | | | | |
|---|---|---|---|---|---|
| 脏接口 | 互联网 | UDP | 123 | 允许 | 允许出站NTP。 |
| 脏接口 | 互联网 | TCP | 19791 | 允许 | 允许连接到安全恶意软件分析支持。 |
| 脏接口 | 思科雨伞 | TCP | 443 | 允许 | 连接第三方检测和浓缩服务。 |
| 脏接口 | VirusTotal | TCP | 443 | 允许 | 连接第三方检测和浓缩服务。 |
| 脏接口 | Titanycloud | TCP | 443 | 允许 | 连接第三方检测和浓缩服务。 |

警告：所列的IP地址在2023年5月29日后保持活动状态。

| 来源 | 目的地 | 协议 | 端口 | 方向 | 主机名 | 详细信息 |
|---|---|---|---|---|---|---|
| 脏接口 | 63.97.201.96<br>63.162.55.96 | TCP | 19791 | OUT | rash.threatgrid.com | 远程支持/设备支持模式 |
| 脏接口 | 63.97.201.97<br>63.162.55.97 | TCP | 22 | OUT | appliance-updates.threatgrid.com | 用于自动支持诊断上传。<br>注意：需要软件版本1.2+ |
| 脏接口 | 63.97.201.98<br>63.162.55.98 | TCP | 22 | OUT | support-snapshots.threatgrid.com | 用于自动支持诊断上传。<br>注意：需要软件版本1.2+ |
| 脏接口 | 63.97.201.99<br>63.162.55.99 | TCP | 22 | OUT | appliance-licensing.threatgrid.com | 许可证管理 |

安全恶意软件分析云

## 美国(US)云

访问URL:https://panacea.threatgrid.com

| 主机名 | IP | 端口 | 详细信息 |
| --- | --- | --- | --- |
| panacea.threatgrid.com | IPv4:<br>63.97.201.67<br>63.162.55.67<br>IPv6:<br>2602:811:9007:6::61<br>2602:811:900b: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.chi.threatgrid.com | IPv4:200.194.241.35<br>IPv6:<br>2602:811:900f:6::6e | 443 | 示例交互窗口 |
| glovebox.rcn.threatgrid.com | IPv4:<br>63.97.201.67<br>IPv6:<br>2602:811:9007:6::61 | 443 | 示例交互窗口 |
| glovebox.scl.threatgrid.com | IPv4:<br>63.162.55.67<br>IPv6:<br>2602:811:900b:6::6e | 443 | 示例交互窗口 |
| fmc.api.threatgrid.com | IPv4: | 443 | FMC/FTD文件分析服务 |

| | | | |
|---|---|---|---|
| | 63.97.201.67<br>63.162.55.67<br>IPv6:<br>2602:811:9007:6::61<br>2602:811:900b:6::6e | | |

欧洲（欧盟）云

访问URL:https://panacea.threatgrid.eu

| 主机名 | IP | 端口 | 详细信息 |
|---|---|---|---|
| panacea.threatgrid.eu | IPv4:<br>62.67.214.195<br>200.194.242.35<br>200.194.245.35<br>IPv6:<br>2602:811:9006:6::6e<br>2602:811:900c: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.muc.threatgrid.eu | IPv4:<br>62.67.214.195<br>200.194.245.35<br>IPv6:<br>2602:811:900c:6::6e | 3 | 示例交互窗口 |
| glovebox.fam.threatgrid.eu | IPv4:<br>200.194.242.35<br>IPv6: | 443 | 示例交互窗口 |

| | | | |
|---|---|---|---|
| | 2602:811:9006:6::6e | | |
| fmc.api.threatgrid.eu | IPv4:<br>62.67.214.195<br>200.194.242.35<br>200.194.245.35<br>IPv6:<br>2602:811:9006:6::6e<br>2602:811:900c:6::6e | 443 | FMC/FTDF文件分析服务 |

旧的IP 89.167.128.132已停用，请使用这些IP更新您的防火墙规则。

## 加拿大(CA)云

访问URL:https://panacea.threatgrid.ca

| 主机名 | IP | 端口 | 详细信息 |
|---|---|---|---|
| panacea.threatgrid.ca | IPv4:<br>200.194.240.35<br>IPv6:<br>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:<br>200.194.240.35<br>IPv6:<br>2602:811:900d:6::6e | 443 | 示例交互窗口 |
| fmc.api.threatgrid.ca | IPv4:<br>200.194.240.35 | 443 | FMC/FTD文件分析服务 |

| | | | |
|---|---|---|---|
| | IPv6:<br>2602:811:900d:6::6e | | |

## 澳大利亚(AU)云

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

| 主机名 | IP | 端口 | 详细信息 |
|---|---|---|---|
| panacea.threatgrid.com.au | IPv4:<br>200.194.246.35<br>200.194.247.35<br>IPv6:<br>2602:811:900e:6::6e<br>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:<br>200.194.246.35<br>200.194.247.35<br>IPv6:<br>2602:811:900e:6::6e<br>2602:811:9003:6::6e | 443 | 示例交互窗口 |
| fmc.api.threatgrid.com.au | IPv4:<br>200.194.246.35<br>200.194.247.35<br>IPv6:<br>2602:811:900e:6::6e<br>2602:811:9003:6::6e | 443 | FMC/FTD文件分析服务 |

印度(IN)云

访问URL:https://panacea.threatgrid.in

| 主机名 | IP | 端口 | 详细信息 |
| --- | --- | --- | --- |
| panacea.threatgrid.in | IPv4:<br>200.194.244.35<br>IPv6:<br>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:<br>200.194.244.35<br>IPv6:<br>2602:811:9001:6::6e | 443 | 示例交互窗口 |
| fmc.api.threatgrid.com.in | IPv4:<br>200.194.244.35<br>IPv6:<br>2602:811:9001:6::6e | 443 | FMC/FTD文件分析服务 |

有关更多思科安全恶意软件分析要求（如设备），请参阅以下文章：

# 相关内容

有关最新要求，请参阅。

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）。