

配置安全惡意軟體分析所需的IP和防火牆規則

目錄

[簡介](#)

[問題](#)

[環境](#)

[解析](#)

[安全惡意軟體分析裝置](#)

[管理員介面](#)

[清除介面](#)

[鑰介面](#)

[鑰介面出站](#)

[鑰介面傳入](#)

[安全惡意軟體分析雲](#)

[美國\(US\)雲端](#)

[歐洲（歐盟）雲端](#)

[加拿大\(CA\)雲](#)

[澳洲（澳洲）雲端](#)

[印度\(IN\)雲端](#)

[相關內容](#)

簡介

本檔案介紹思科安全惡意軟體分析（雲和裝置）所需的主機名、IP地址和埠。

問題

思科安全惡意軟體分析需要到特定主機名、IP地址和埠的出站和入站連線。如果阻止這些流量，門戶訪問、更新、許可、遠端支援和整合等功能可能會失敗。

環境



附註：請首先參閱本檔案，其中包括用於其他服務的附加IP和埠。

[Threat Grid所需的IP和埠](#)

本文檔包括基於裝置版本的其他服務的附加IP和埠。

請參閱安裝和升級指南檔案：[Threat Grid裝置安裝指南](#)

解析

裝置上游防火牆的防火牆規則：

*IP在發佈時是正確的。請通過nslookup在本地確認這些設定是否仍然正確。

安全惡意軟體分析裝置

管理員介面

來源	目的地	通訊協定	連接埠	方向	動作	備註
ANY	管理員介面	TCP	22	在	允許	SSH
ANY	管理員介面	TCP	80/443	在	允許	允許訪問管理GUI介面。
管理員介面	NFS伺服器IP	TCP	2049	外寄	允許	*必須開啟才能使用NFS備份或群集功能。

清除介面

來源	目的地	通訊協定	連接埠	方向	動作	備註
ANY	清除介面	TCP	80/443	在	允許	允許訪問Clean GUI介面。
ANY	清除介面	TCP	8443	在	允許	*必須開啟才能使用Admin over Clean功能。
ANY	清除介面	TCP	9443	在	允許	*必須開啟才能使用Glovebox功能示例。
清除介	已配置的電子郵件	TCP	25	外	允	裝置使用清除介面啟動與已配置郵件伺服

面	中繼伺服器			寄	許	器的SMTP連線。
清除介面	已配置乾淨DNS伺服器	TCP/UDP	53	外寄	允許	*可選，僅當配置了Clean DNS時才需要。
清除介面	已配置系統日誌伺服器	TCP/UDP	514	外寄	允許	允許連線到指定接收系統日誌消息和Threat Grid通知的伺服器。
清除介面	LDAP 伺服器	TCP/UDP	389/636	外寄	允許	*可選，僅當配置了LDAP時才需要。

髒介面

髒介面出站

來源	目的地	通訊協定	連接埠	動作	附註
髒介面	網際網路	ANY	ANY	允許	允許來自樣本的出站流量（可選擇通過思科資料中心代理）。 （要獲得準確的結果，必須允許惡意軟體使用它設計使用的任何埠和協定聯絡其命令和控制伺服器。）

髒介面傳入

來源	目的地	通訊協定	連接埠	動作	附註
ANY	髒介面的網際網路	ANY	ANY	拒絕	拒絕所有傳入連線。

來源	目的地	通訊協定	連接埠	動作	附註
髒介面	網際網路	TCP	22	允許	更新、支援快照和許可服務。
髒介面	網際網路	TCP/UDP	53	允許	允許出站DNS。

髒介面	網際網路	UDP	123	允許	允許出站NTP。
髒介面	網際網路	TCP	19791	允許	允許連線到安全惡意軟體分析支援。
髒介面	思科資安防護傘	TCP	443	允許	連線第三方檢測和富集服務。
髒介面	病毒總計	TCP	443	允許	連線第三方檢測和富集服務。
髒介面	TitaniumCloud	TCP	443	允許	連線第三方檢測和富集服務。



警告：所列的IP地址在2023年5月29日後保持活動狀態。

來源	目的地	通訊協定	連接埠	方向	主機名	詳細資料
髒介面	63.97.201.96 63.162.55.96	TCP	19791	外寄	rash.threatgrid.com	遠端支援/裝置支援模式
髒介面	63.97.201.97 63.162.55.97	TCP	22	外寄	appliance-updates.threatgrid.com	用於自動支援診斷上傳。  附註：需要軟體版本1.2+
髒介面	63.97.201.98 63.162.55.98	TCP	22	外寄	support-snapshots.threatgrid.com	用於自動支援診斷上傳。  附註：需要軟體版本1.2+
髒介面	63.97.201.99 63.162.55.99	TCP	22	外寄	appliance-licensing.threatgrid.com	授權管理

安全惡意軟體分析雲

美國(US)雲端

訪問URL:<https://panacea.threatgrid.com>

主機名	IP	連接埠	詳細資料
panacea.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6::6e	443	對於安全惡意軟體分析門戶和整合裝置 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	IPv4:200.194.241.35 IPv6: 2602:811:900f:6::6e	443	互動視窗範例
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6: 2602:811:9007:6::61	443	互動視窗範例
glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6: 2602:811:900b:6::6e	443	互動視窗範例

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 檔案分析服務
---	--	-----	----------------

歐洲 (歐盟) 雲端

訪問URL:<https://panacea.threatgrid.eu>

主機名	IP	連接埠	詳細資料
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	對於安全惡意軟體分析門戶和整合裝置 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	IPv4: 62.67.214.195 200.194.245.35 IPv6: 2602:811:900c:6::6e	3	互動視窗範例
glovebox.fam.threatgrid.eu	IPv4:	443	互動視窗範例

	200.194.242.35 IPv6: 2602:811:9006:6::6e		
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檔案分析服務

舊的IP 89.167.128.132已停用，請使用這些IP更新防火牆規則。

加拿大(CA)雲

訪問URL:<https://panacea.threatgrid.ca>

主機名	IP	連接埠	詳細資料
panacea.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	對於安全惡意軟體分析門戶和整合裝置 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	互動視窗範例

fmc.api.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:8111:900d:6::6e	443	FMC/FTD 檔案分析服務
---	--	-----	----------------

澳洲 (澳洲) 雲端

訪問URL:<https://panacea.threatgrid.com.au>

主機名	IP	連接埠	詳細資料
panacea.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:8111:900e:6::6e 2602:8111:9003:6::6e	443	對於安全惡意軟體分析門戶和整合裝置 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:8111:900e:6::6e 2602:8111:9003:6::6e	443	互動視窗範例
fmc.api.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35	443	FMC/FTD 檔案分析服務

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

印度(IN)雲端

訪問URL:<https://panacea.threatgrid.in>

主機名	IP	連接埠	詳細資料
panacea.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	對於安全惡意軟體分析門戶和整合裝置 (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	互動視窗範例
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	FMC/FTD 檔案分析服務

有關更多思科安全惡意軟體分析要求（如裝置），請參閱以下文章：

相關內容

有關最新要求，請參閱。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。