

安全惡意軟體分析所需的IP和埠

目錄

簡介

[安全惡意軟體分析雲](#)

[美國 \(美國\) 雲端](#)

[歐盟 \(歐洲\) 雲端](#)

[CA \(加拿大\) 雲](#)

[澳洲 \(澳洲\) 雲端](#)

[安全惡意軟體分析裝置](#)

[簡介](#)

[遠端網路退出](#)

[清除介面](#)

[管理員介面](#)

簡介

本文檔概述了需要在防火牆上實施的基本網路配置，以確保安全惡意軟體分析的無縫操作。

由Cisco TAC工程師貢獻。

安全惡意軟體分析雲

美國 (美國) 雲端

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

主機名	IP	連接埠	詳細資料
panacea.threatgrid.com	63.97.201.67中 ， 63.162.55.67	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	200.194.241.35	443	互動視窗範例
glovebox.rcn.threatgrid.com	63.97.201.67	443	互動視窗範例
glovebox.scl.threatgrid.com	63.162.55.67	443	互動視窗範例
fmc.api.threatgrid.com	63.97.201.67、	443	FMC/FTD 檔案分析服務

	63.162.55.67		
--	--------------	--	--

歐盟（歐洲）雲端

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

主機名	IP	連接埠	詳細資料
panacea.threatgrid.eu	62.67.214.195 , 200.194.242.35	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	62.67.214.195	443	互動視窗範例
glovebox.fam.threatgrid.eu	200.194.242.35	443	互動視窗範例
fmc.api.threatgrid.eu	62.67.214.195、 200.194.242.35	443	FMC/FTD 檔案分析服務

舊的IP 89.167.128.132已停用，請使用上述IP更新防火牆規則。

CA（加拿大）雲

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

主機名	IP	連接埠	詳細資料
panacea.threatgrid.ca	200.194.240.35	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	200.194.240.35	443	互動視窗範例
fmc.api.threatgrid.ca	200.194.240.35	443	FMC/FTD 檔案分析服務

澳洲（澳洲）雲端

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

主機名	IP	連接埠	詳細資料
panacea.threatgrid.com.au	124.19.22.171	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	124.19.22.171	443	互動視窗範例
fmc.api.threatgrid.com.au	124.19.22.171	443	FMC/FTD 檔案分析服務

安全惡意軟體分析裝置

以下是安全惡意軟體分析裝置每個介面的建議防火牆規則。

麟介面

虛擬機器用於與網際網路通訊，以便示例可以解析DNS並與命令和控制(C&C)伺服器通訊
允許:

方向	通訊協定	連接埠	目的地	主機名	詳細資料
出站	IP	ANY	ANY		建議使用，但在此處的Deny部分中指定的除外。 已使用 允許連線進行分析。
出站	TCP	22	54.173.231.161 1 63.97.201.98 2 63.162.55.98 2	support- snapshots.threatgrid.com	用於自動支援診斷上傳 注意：需要軟體版本1.2+
出站	TCP	22	54.173.181.217 1 中 , 54.173.182.46 1 63.162.55.97 2 63.97.201.97 2	appliance- updates.threatgrid.com	裝置更新
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	遠端支援/裝置支援模式
出站	TCP	22	63.97.201.99 63.162.55.99	appliance- licensing.threatgrid.com	授權管理

¹這些IP將在不久的將來被停用。


²以下是會取代第1個中的IP。我們建議新增這兩個IP，直到在不久的將來完成有關IP更改的通訊。

遠端網路退出

裝置用來將VM流量通道到遠端出口（以前稱為tg-tunnel）。

方向	通訊協定	連接埠	目的地
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

 註：遠端出口4.14.36.142已刪除，並且不再生產。請確保將提及的所有IP都新增到防火牆例外清單中。

拒絕：

方向	通訊協定	連線埠	目的地	詳細資料
出站	SMTP	ANY	ANY	防止惡意軟體傳送垃圾郵件。
傳入	IP	ANY	安全惡意軟體分析裝置不良介面	建議使用，但上面Allow部分中指定的除外。 用於允許用於分析的通訊。

清除介面

由各種連線的服務用來提交示例以及分析人員的UI訪問。

允許：

方向	通訊協定	連線埠	目的地	詳細資料
傳入	TCP	443和 8443	安全惡意軟體分析裝置清除介面	WebUI和API訪問
傳入	TCP	9443	安全惡意軟體分析裝置清除介面	用於Glovebox
出站	TCP	19791	主機：rash.threatgrid.com 54.164.165.137 ¹ , 34.199.44.202 ¹ 63.97.201.96 ² , 63.162.55.96 ²	安全惡意軟體分析支援的恢復模式。

¹這些IP將在不久的將來被停用。

²以下是會取代第1個中的IP¹。我們建議新增這兩個IP，直到在不久的將來完成有關IP更改的通訊。

管理員介面

對管理UI的訪問。

允許：

方向	通訊協定	連線埠	目的地	詳細資料
傳入	TCP	443和 8443	安全惡意軟體分析裝置管理介面	用於配置硬體和許可的設定。

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）。