عناوين IP والمنافذ المطلوبة لتحليلات البرامج الضارة الآمنة

المحتويات

المقدمة

يوضح هذا المستند التكوينات الأساسية للشبكة التي تحتاج إلى تنفيذها على جدار الحماية لديك لضمان التشغيل السلس لتحليلات البرامج الضارة الآمنة.

تمت المساهمة بواسطة مهندسو Cisco TAC.

سحب تحليلات البرامج الضارة الآمنة

الولايات المتحدة (الولايات المتحدة) السحابة

عنوان URL للوصول: https://panacea.threatgrid.com)

اسم المضيف	IP	المنفذ	التفاصيل
panacea.threatgrid.com	63.97.201.67, 63.162.55.67	443	لبوابة تحليلات البرامج الضارة الآمنة والأجهزة المدمجة (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	نافذة التفاعل العينة
glovebox.rcn.threatgrid.com	63.97.201.67	443	نافذة التفاعل العينة
glovebox.scl.threatgrid.com	63.162.55.67	443	نافذة التفاعل العينة

fmc.api.threatgrid.com	63.97.201.67, 63.162.55.67	443	خدمة تحليل ملفات FMC/FTD

سحابة الاتحاد الأوروبي (أوروبا)

عنوان URL للوصول: https://panacea.threatgrid.eu

اسم المضيف	IP	المنفذ	التفاصيل
شارب المدد	62.67.214.195, 200.194.242.35	443	بوابة تحليلات البرامج الضارة الآمنة والأجهزة المدمجة (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatened.eu	62.67.214.195	443	نافذة التفاعل العينة
glovebox.fam.threatened.eu	200.194.242.35	443	نافذة التفاعل العينة
fmc.api.threatened.eu	62.67.214.195, 200.194.242.35	443	خدمة تحليل ملفات FMC/FTD

تم إلغاء IP 89.167.128.132 القديم، يرجى تحديث قواعد جدار الحماية باستخدام عناوين IP الموجودة أعلاه.

سحابة CA (كندا)

عنوان URL للوصول:https://panacea.threatgrid.ca

اسم المضيف	IP	المنفذ	التفاصيل
شارب المدد.ca	200.194.240.35	443	بوابة تحليلات البرامج الضارة الآمنة والأجهزة المدمجة (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatened.ca	200.194.240.35	443	نافذة التفاعل العينة
fmc.api.threatened.ca	200.194.240.35	443	خدمة تحليل ملفات FMC/FTD

سحابة الاتحاد الأفريقي (أستراليا)

عنوان URL للوصول:https://panacea.threatgrid.au

اسم المضيف	IP	المنفذ	التفاصيل
panacea.threatgrid.com.au	124.19.22.171	443	بوابة تحليلات البرامج الضارة الآمنة والأجهزة المدمجة (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	124.19.22.171	443	نافذة التفاعل العينة

fmc.api.threatgrid.com.au	124.19.22.171	443	خدمة تحليل ملفات FMC/FTD

جهاز Secure Ware Analytics

فيما يلي قواعد جدار الحماية الموصى بها لكل واجهة لجهاز تحليلات البرامج الضارة الآمن.

قرذق ةهجاو

يستخدم من قبل VMs للاتصال بالإنترنت بحيث يمكن للعينات حل DNS والاتصال بخوادم الأوامر والتحكم (C&C)

سماح:

التفاصيل	اسم المضيف	الوجهة	المنفذ	البروتوكول	الاتجاه
يوصى به باستثناء المكان المحدد في قسم **الرفض** أدناه. يستخدم للسماح بالاتصال للتحليل.		أي	أي	IP	صادر
يستخدم لتحميل تشخيص الدعم التلقائي ملاحظة: يتطلب إصدار البرنامج 1.2+	support-snapshots.threatgrid.com	54.173.231.161 [1] 63.97.201.98 [2] 63.162.55.98 [2]	22	TCP	صادر
تحديثات الجهاز	appliance-updates.threatgrid.com	54.173.181.217 [1]، 54.173.182.46 [1] 63.162.55.97 [2] 63.97.201.97 [2]	22	TCP	صادر
وضع دعم / جهاز عن بعد	rash.threatgrid.com	54.164.165.137 [1]، 34.199.44.202 [1] 63.97.201.96 [2] و 63.162.55.96 [2]	19791	TCP	صادر
إدارة الترخيص	appliance-licensing.threatgrid.com	63.97.201.99 63.162.55.99	22	TCP	صادر

[1] سيتم تعطيل عناوين IP هذه في المستقبل القريب.

[2] هذه هي عناوين IP التي ستحل محل تلك في [1]. نقترح إضافة الكل بروتوكول الإنترنت (IP) حتى يتم إجراء الاتصال حول تغييرات IP في المستقبل القريب.

الخروج من الشبكة عن بعد

يستخدم بواسطة الجهاز لتنفق حركة مرور VM إلى مخرج بعيد كان يعرف سابقا باسم tg-tunnel.

الوجهة	المنفذ	البروتوكول	الاتجاه
163.182.175.193	21413	TCP	صادر
69.55.5.250	21417	TCP	صادر

صادر	TCP	21415	69.55.5.250
صادر	TCP	21413	76.8.60.91

ملاحظة: تمت إزالة Remote Exit 4.14.36.142 ولم يعد قيد الإنتاج. تأكد من إضافة جميع بروتوكولات IP المذكورة إلى قائمة إستثناءات جدار الحماية لديك.

رفض:

التفاصيل	الوجهة	المنفذ (المنافذ)	البروتوكول	إتجاه
لمنع البرامج الضارة من إرسال البريد العشوائي.	أي	أي	SMTP	صادر
مستحسن باستثناء المكان المحدد في قسم **السماح** أعلاه. يستخدم للسماح بالاتصال للتحليل.	الواجهة الظرفية لجهاز تحليلات البرامج الضارة الآمن	أي	IP	داخل

واجهة نظيفة

يستخدم بواسطة خدمات متصلة مختلفة لإرسال نماذج وكذلك وصول واجهة المستخدم للمحللين.

سماح:

التفاصيل	الوجهة	(المنافذ) المنفذ	البروتوكول	إتجاه
API و WebUI وصول	الواجهة الظرفية لجهاز التحليلات الآمنة للبرامج الضارة	8443 و 443	TCP	داخل
Glovebox يستخدم ل	الواجهة الظرفية لجهاز التحليلات الآمنة للبرامج الضارة	9443	TCP	داخل
وصول TUI للمسؤول عبر SSH	الواجهة الظرفية لجهاز التحليلات الآمنة للبرامج الضارة	22	TCP	داخل
وضع الاسترداد لدعم تحليلات البرامج الضارة الآمنة.	**المضيف:** rash.threatgrid.com 54،164،165،137 [1] 34،199،44،202 [1] 63،97،201،96 [2] 63،162،55،96 [2]	19791	TCP	صادر

[1] سيتم تعطيل عناوين IP هذه في المستقبل القريب.

[2] هذه هي عناوين IP التي ستحل محل تلك في [1]. نقترح إضافة كل بروتوكول الإنترنت (IP) حتى يتم إجراء الاتصال حول تغييرات IP في المستقبل القريب.

واجهة المسؤول

الوصول إلى واجهة مستخدم الإدارة.

سماح:

إتجاه	البروتوكول	المنفذ (المنافذ)	الوجهة	التفاصيل
داخل	TCP	8443 و 443	واجهة مسؤول جهاز تحليلات البرامج الضارة الآمنة	يستخدم لتكوين إعدادات الأجهزة والترخيص.
إنبوند	TCP	22	واجهة مسؤول جهاز تحليلات البرامج الضارة الآمنة	وصول TUI للمسؤول عبر SSH

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).