IP et ports requis pour Secure Malware Analytics

Table des matières

Introduction

Ce document présente les configurations réseau essentielles que vous devez mettre en oeuvre sur votre pare-feu pour assurer un fonctionnement transparent de Secure Malware Analytics.

Contribution des ingénieurs du TAC Cisco.

Clouds Secure Malware Analytics

Cloud US (États-Unis)

URL d'accès : https://panacea.threatgrid.com

Nom de l'hôte	IP	Port	Détails
panacea.threatgrid.com	63.97.201.67 63.162.55.67	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	Exemple de fenêtre Interaction
glovebox.rcn.threatgrid.com	63.97.201.67	443	Exemple de fenêtre Interaction
glovebox.scl.threatgrid.com	63.162.55.67	443	Exemple de fenêtre Interaction

fmc.api.threatgrid.com	63.97.201.67 63.162.55.67	443	Service d'analyse de fichiers FMC/FTD

Cloud UE (Europe)

URL d'accès : https://panacea.threatgrid.eu

Nom de l'hôte	IP	Port	Détails
panacea.threat.eu	62.67.214.195 200.194.242.35	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threat.eu	62.67.214.195	443	Exemple de fenêtre Interaction
glovebox.fam.threat grid.eu	200.194.242.35	443	Exemple de fenêtre Interaction
fmc.api.threat.eu	62.67.214.195 200.194.242.35	443	Service d'analyse de fichiers FMC/FTD

L'ancienne adresse IP 89.167.128.132 a été supprimée. Veuillez mettre à jour vos règles de pare-feu avec les adresses IP ci-dessus.

Cloud CA (Canada)

URL d'accès : https://panacea.threatgrid.ca

Nom de l'hôte	IP	Port	Détails
panacea.threat.ca	200.194.240.35	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threat.ca	200.194.240.35	443	Exemple de fenêtre Interaction
fmc.api.threat.ca	200.194.240.35	443	Service d'analyse de fichiers FMC/FTD

AU (Australie) Cloud

URL d'accès : https://panacea.threatgrid.com.au

Nom de l'hôte	IP	Port	Détails
panacea.threatgrid.com.au	124.19.22.171	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)

glovebox.syd.threatgrid.com.au	124.19.22.171	443	Exemple de fenêtre Interaction
fmc.api.threatgrid.com.au	124.19.22.171	443	Service d'analyse de fichiers FMC/FTD

Appliance Secure Malware Analytics

Voici les règles de pare-feu recommandées par interface de l'appliance Secure Malware Analytics.

Interface sale

Utilisé par les machines virtuelles pour communiquer avec Internet afin que les échantillons puissent résoudre le DNS et communiquer avec les serveurs de commande et de contrôle (C&C)

Allow:

Direction	Protocol	Port	Destination	Nom de l'hôte	Détails
Sortant	IP	TOUS LES MODÈLES	TOUS LES MODÈLES		Recommandé sauf indication contraire dans la section **Refuser** ici. Utilisé pour permettre la connectivité pour l'analyse.
Sortant	TCP	22	54.173.231.161 1 63.97.201.98 2 63.162.55.98 2	support-snapshots.threatgrid.com	Utilisé pour les téléchargements de diagnostics de support automatique Remarque : version logicielle 1.2+ requise
Sortant	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	Mises à jour
Sortant	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	Support à distance / Mode de support des appareils
Sortant	TCP	22	54.173.124.172 1 63.97.201.99 2 63.162.55.99 2	appliance-licensing.threatgrid.com	Gestion des licences

[1]Ces adresses IP seront désactivées dans un avenir proche.

[2]Il s'agit des adresses IP qui remplaceraient celles du [1]. Nous vous suggérons d'ajouter les deux adresses IP jusqu'à ce que la communication relative aux modifications apportées aux adresses IP soit effectuée dans un avenir proche.

Sortie du réseau distant

Utilisé par l'appliance pour tunnelliser le trafic des machines virtuelles vers une sortie distante anciennement appelée tg-tunnel.

Direction	Protocol	Port	Destination
Sortant	TCP	21413	173.198.252.53
Sortant	TCP	21413	163.182.175.193 **
Sortant	TCP	21417	69.55.5.250
Sortant	TCP	21415	69.55.5.250
Sortant	TCP	21413	76.8.60.91

Remarque : la sortie distante 4.14.36.142 a été supprimée et n'est plus en production. Assurez-vous que toutes les adresses IP mentionnées sont ajoutées à votre liste d'exceptions de pare-feu.

** La sortie distante 163.182.175.193 sera remplacée par 173.198.252.53

Refuser :

Direction	Protocol	Port(s)	Destination	Détails
Sortant	SMTP	TOUS LES MODÈLES	TOUS LES MODÈLES	Pour empêcher les programmes malveillants d'envoyer du spam.
Entrant	IP	TOUS LES MODÈLES	Secure Malware Analytics Appliance Dirty Interface	Recommandé, sauf indication contraire dans la section **Autoriser** ci-dessus. Utilisé pour permettre la communication pour l'analyse.

Nettoyer l'interface

Utilisé par divers services connectés pour envoyer des échantillons ainsi que l'accès à l'interface utilisateur pour les analystes.

Allow:

Direction	Protocol	Port(s)	Destination	Détails
Entrant	TCP	443 et 8443	Secure Malware Analytics Appliance Clean Interface	Accès WebUI et API
Entrant	TCP	9443	Secure Malware Analytics Appliance Clean Interface	Utilisé pour Glovebox

Entrant	TCP	22	Secure Malware Analytics Appliance Clean Interface	Accès TUI administrateur sur SSH
Sortant	TCP	19791	**Hôte :** rash.threatgrid.com 54.164.165.137 [1] ,34.199.44.202 [1] 63.97.201.96 [2] , 63.162.55.96 [2]	Mode de récupération pour prise en charge Secure Malware Analytics.

[1]Ces adresses IP seront désactivées dans un avenir proche.

[2]Il s'agit des adresses IP qui remplaceraient celles du [1]. Nous vous suggérons d'ajouter les deux adresses IP jusqu'à ce que la communication relative aux modifications apportées aux adresses IP soit effectuée dans un avenir proche.

Interface Admin

Accès à l'interface utilisateur d'administration.

Allow:

Direction	Protocol	Port(s)	Destination	Détails
Entrant	TCP	443 et 8443	Interface d'administration du dispositif Secure Malware Analytics	Utilisé pour configurer les paramètres du matériel et des licences.
Entrant	TCP	22	Interface d'administration du dispositif Secure Malware Analytics	Accès TUI administrateur sur SSH

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.