IP et ports requis pour Secure Malware Analytics

Table des matières

Introduction

Clouds Secure Malware Analytics

- Cloud US (États-Unis)
- Cloud UE (Europe)
- Cloud CA (Canada)
- AU (Australie) Cloud
- IN (Inde) Cloud

Appliance Secure Malware Analytics

- Interface sale
- Sortie du réseau distant
- Nettoyer l'interface
- Interface Admin

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.

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	IPv4: 63.97.201.67 63.162.55.67 IPv6 : 2602:811:9007:6::61	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)

	2602:811:900b:6::6e		
glovebox.chi.threatgrid.com	IPv4: 200.194.241.35 IPv6 : 2602:811:900f:6::6e	443	Exemple de fenêtre Interaction
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6 : 2602:811:9007:6::61	443	Exemple de fenêtre Interaction
glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6 : 2602:811:900b:6::6e	443	Exemple de fenêtre Interaction
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	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	IPv4: 62.67.214.195	443	Pour le portail Secure Malware Analytics et les périphériques intégrés

	200.194.242.35 200.194.245.35 IPv6 : 2602:811:9006:6::6e 2602:811:900c:6::6e		(ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threat.eu	IPv4: 62.67.214.195 200.194.245.35 IPv6 : 2602:811:900c:6::6e	3	Exemple de fenêtre Interaction
glovebox.fam.threat grid.eu	IPv4: 200.194.242.35 IPv6 : 2602:811:9006:6::6e	443	Exemple de fenêtre Interaction
fmc.api.threat.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/FTDFervice d'analyse de fichiers

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	IPv4: 200.194.240.35 IPv6 : 2602:811:900d:6::6e	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threat.ca	IPv4: 200.194.240.35 IPv6 : 2602:811:900d:6::6e	443	Exemple de fenêtre Interaction
fmc.api.threat.ca	IPv4: 200.194.240.35 IPv6 : 2602:811:900d:6::6e	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	IPv4: 200.194.246.35 200.194.247.35 IPv6 : 2602:811:900e:6::6e 2602:811:9003:6::6e	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	IPv4:	443	Exemple de fenêtre Interaction

	200.194.246.35 200.194.247.35 IPv6 : 2602:811:900e:6::6e 2602:811:9003:6::6e		
fmc.api.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6 : 2602:811:900e:6::6e 2602:811:9003:6::6e	443	Service d'analyse de fichiers FMC/FTD

IN (Inde) Cloud

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

Nom de l'hôte	IP	Port	Détails
panacée.mengrid.in	IPv4: 200.194.244.35 IPv6 : 2602:811:9001:6::6e	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.threat.grid.in	IPv4: 200.194.244.35 IPv6 : 2602:811:9001:6::6e	443	Exemple de fenêtre Interaction
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35	443	Service d'analyse de fichiers FMC/FTD

	IPv6 : 2602:811:9001:6::6e		

Appliance Secure Malware Analytics

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

Interface sale

Elle est utilisée 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	63.97.201.98 63.162.55.98	support-snapshots.threatgrid.com	Utilisé pour les téléchargements de diagnostics de support automatique. Remarque : Version logicielle 1.2+ requise.
Sortant	TCP	22	63.162.55.97 63.97.201.97	appliance-updates.threatgrid.com	Mises à jour
Sortant	TCP	19791	63.97.201.96 63.162.55.96	rash.threatgrid.com	Support à distance / Mode de support des appareils
Sortant	TCP	22	63.97.201.99	appliance-licensing.threatgrid.com	Gestion des licences

			63.162.55.99		

Sortie du réseau distant

Il est utilisé par l'appliance pour tunnelliser le trafic de la machine virtuelle vers une sortie distante anciennement appelée tg-tunnel.

Direction	Protocol	Port	Destination
Sortant	TCP	21413	173.198.252.53
Sortant	TCP	21417	69.55.5.250
Sortant	TCP	21415	69.55.5.250
Sortant	TCP	21413	38.123.149.87

Remarque : Depuis le 25 juillet 2026, les adresses IP de sortie à distance suivantes ont été remplacées :
- 163.182.175.193 a été remplacé par 173.198.252.53
- le 76.8.60.91 est remplacé par le 38.123.149.87

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

Il est 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 63.97.201.96 63.162.55.96	Mode de récupération pour prise en charge Secure Malware Analytics

Interface Admin

Utilisez cette option pour accéder à la console d'administration ou à l'interface utilisateur. 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.