Configuration des adresses IP et des règles de pare-feu requises pour Secure Malware Analytics

Table des matières

- Introduction
- Problème
- Environnement
- Résolution
  - Appliance Secure Malware Analytics
    - Interface Admin
    - Nettoyer l'interface
    - Interface sale
  - Dirty Interface Outbound
  - Dirty Interface Inbound
  - Cloud Secure Malware Analytics
  - Cloud États-Unis (US)
  - Cloud Europe (UE)
  - Cloud Canada (CA)
  - Cloud Australie (AU)
  - Inde (IN) Cloud
- Autres informations utiles

Introduction

Ce document décrit les noms d'hôte, les adresses IP et les ports requis pour Cisco Secure Malware Analytics (cloud et appliance).

Problème

Cisco Secure Malware Analytics nécessite une connectivité sortante et entrante vers des noms d'hôtes, des adresses IP et des ports spécifiques. Si ces flux sont bloqués, des fonctionnalités telles que l'accès au portail, les mises à jour, les licences, l'assistance à distance et les intégrations peuvent échouer.

Environnement

Remarque : Veuillez d'abord vous reporter à ce document, qui inclut des adresses IP et des ports supplémentaires pour d'autres services.
IP et ports requis pour Threat Grid

Ce document inclut des adresses IP et des ports supplémentaires pour d'autres services en fonction de la version de l'appliance.

Reportez-vous à la documentation des guides d'installation et de mise à niveau : Guides d'installation des appliances Threat Grid

Résolution

Règles de pare-feu pour le pare-feu en amont du périphérique :

*Les adresses IP étaient correctes au moment de la publication. Veuillez confirmer localement via nslookup que ces informations sont toujours correctes.

Appliance Secure Malware Analytics

Interface Admin

Source	Destination	Protocol	Port	Direction	Action	Remarques
TOUS LES MODÈLES	Interface Admin	TCP	22	DANS	Allow	SSH
TOUS LES MODÈLES	Interface Admin	TCP	80/443	DANS	Allow	Autorisez l'accès à l'interface utilisateur Admin.
Interface Admin	IP du serveur NFS	TCP	2049	DEHORS	Allow	*Doit être ouvert pour utiliser la fonction de sauvegarde NFS ou de clustering.

Nettoyer l'interface

Source	Destination	Protocol	Port	Direction	Action	Remarques

TOUS LES MODÈLES	Nettoyer l'interface	TCP	80/443	DANS	Allow	Autoriser l'accès à l'interface utilisateur Clean.
TOUS LES MODÈLES	Nettoyer l'interface	TCP	8443	DANS	Allow	*Doit être ouvert pour utiliser la fonctionnalité Admin sur Clean.
TOUS LES MODÈLES	Nettoyer l'interface	TCP	9443	DANS	Allow	*Doit être ouvert pour utiliser l'exemple de fonction Glovebox.
Nettoyer l'interface	Serveur de relais de messagerie électronique configuré	TCP	25	DEHORS	Autoriser	La solution matérielle-logicielle utilise l'interface de nettoyage pour initier des connexions SMTP au serveur de messagerie configuré.
Nettoyer l'interface	Serveur DNS propre configuré	TCP/UDP	53	DEHORS	Allow	*Facultatif, uniquement requis si Clean DNS est configuré.
Nettoyer l'interface	Serveur Syslog configuré	TCP/UDP	514	DEHORS	Allow	Permettre la connectivité au serveur désigné pour recevoir les messages Syslog et les notifications Threat Grid.
Nettoyer l'interface	Serveur LDAP	TCP/UDP	389/636	DEHORS	Allow	*Facultatif, uniquement requis si LDAP est configuré.

Interface sale

Dirty Interface Outbound

Source	Destination	Protocol	Port	Action	Remarque

Interface sale	Internet	TOUS LES MODÈLES	TOUS LES MODÈLES	Allow	Autoriser le trafic sortant des échantillons, éventuellement transmis par proxy via les data centers Cisco. (Pour obtenir des résultats précis, le programme malveillant doit être autorisé à contacter son serveur de commande et de contrôle à l'aide du port et du protocole qu'il est conçu pour utiliser.)

Dirty Interface Inbound

Source	Destination	Protocol	Port	Action	Remarque
TOUS LES MODÈLES	Internet sale	TOUS LES MODÈLES	TOUS LES MODÈLES	Refuser	Refuser toutes les connexions entrantes.

Source	Destination	Protocol	Port	Action	Remarque
Interface sale	Internet	TCP	22	Allow	Services de mise à jour, de capture instantanée et de licence.
Interface sale	Internet	TCP/UDP	53	Allow	Autoriser les DNS sortants.
Interface sale	Internet	UDP	123	Allow	Autoriser NTP sortant.
Interface sale	Internet	TCP	19791	Allow	Permettre la connectivité au support Secure Malware Analytics.
Interface sale	Cisco Umbrella	TCP	443	Allow	Connectez-vous à des services de détection et d'enrichissement tiers.
Interface sale	TotalVirus	TCP	443	Allow	Connectez-vous à des services de détection et d'enrichissement tiers.
Interface sale	Nuage De Titane	TCP	443	Allow	Connectez-vous à des services de détection et d'enrichissement tiers.

Avertissement : Les adresses IP répertoriées restent actives après le 29 mai 2023.

Source	Destination	Protocol	Port	Direction	Nom de l'hôte	Détails
Interface sale	63.97.201.96 63.162.55.96	TCP	19791	DEHORS	rash.threatgrid.com	Support à distance / Mode de support des appareils
Interface sale	63.97.201.97 63.162.55.97	TCP	22	DEHORS	appliance-updates.threatgrid.com	Utilisé pour les téléchargements de diagnostics de support automatique. Remarque : Version logicielle 1.2+ requise
Interface sale	63.97.201.98 63.162.55.98	TCP	22	DEHORS	support-snapshots.threatgrid.com	Utilisé pour les téléchargements de diagnostics de support automatique. Remarque : Version logicielle 1.2+ requise
Interface sale	63.97.201.99 63.162.55.99	TCP	22	DEHORS	appliance-licensing.threatgrid.com	Gestion des licences

Cloud Secure Malware Analytics

Cloud États-Unis (US)

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 2602:811:900b:6::6e	443	Pour le portail Secure Malware Analytics et les périphériques intégrés (ESA/WSA/FTD/ODNS/Meraki)
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	443	Service d'analyse de fichiers FMC/FTD

	63.162.55.67 IPv6 : 2602:811:9007:6::61 2602:811:900b:6::6e		

Cloud Europe (UE)

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

Nom de l'hôte	IP	Port	Détails
panacea.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	Pour le portail Secure Malware Analytics et les périphériques intégrés (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.threatgrid.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 ces adresses IP.

Cloud Canada (CA)

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 :	443	Service d'analyse de fichiers FMC/FTD

	2602:811:900d:6::6e		

Cloud Australie (AU)

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: 200.194.246.35 200.194.247.35 IPv6 : 2602:811:900e:6::6e 2602:811:9003:6::6e	443	Exemple de fenêtre Interaction
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

Inde (IN) 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 IPv6 : 2602:811:9001:6::6e	443	Service d'analyse de fichiers FMC/FTD

Pour plus d'informations sur les exigences de Cisco Secure Malware Analytics, telles que les appareils, consultez cet article :

Autres informations utiles

Pour connaître la configuration requise la plus récente, reportez-vous à .

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.