Erforderliche IPs und Ports für sichere Malware-Analysen

Inhalt

Einleitung

In diesem Dokument werden die Netzwerkinformationen beschrieben, die Ihrer Firewall hinzugefügt werden müssen, damit Secure Malware Analytics ordnungsgemäß funktioniert.

Eingereicht von Cisco TAC-Technikern.

Sichere Clouds für Malwareanalysen

USA (USA) Cloud

Zugriffs-URL: https://panacea.threatgrid.com)

Hostname	IP	Anschluss	Details
panacea.threatgrid.com	63.97.201.67 4.14.36.148 63.162.55.67	443	Für Secure Malware Analytics-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)
glovebox.mtv.threatgrid.com	63.97.201.67 4.14.36.148	443	Beispiel-Interaktionsfenster
glovebox.rcn.threatgrid.com	63.97.201.67	443	Beispiel-Interaktionsfenster

glovebox.scl.threatgrid.com	63.162.55.67	443	Beispiel-Interaktionsfenster
fmc.api.threatgrid.com	63.97.201.67 4.14.36.148	443	FMC/FTD-Dateianalyse-Service

EU (Europa) Cloud

Zugriffs-URL: https://panacea.threatgrid.eu

Hostname	IP	Anschluss	Details
panacea.bedrohgrid.eu	89.167.128.132	443	Für Secure Malware Analytics-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bedrohgrid.eu	89.167.128.132	443	Beispiel-Interaktionsfenster
fmc.api.bedrohgrid.eu	89.167.128.132	443	FMC/FTD-Dateianalyse-Service

CA (Kanada) Cloud

Zugriffs-URL: https://panacea.threatgrid.ca

Hostname	IP	Anschluss	Details
panacea.bedrohgrid.ca	200.194.240.35	443	Für Secure Malware Analytics-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.bedrohgrid.ca	200.194.240.35	443	Beispiel-Interaktionsfenster
fmc.api.thregrid.ca	200.194.240.35	443	FMC/FTD-Dateianalyse-Service

Secure Malware Analytics Appliance

Dies sind die empfohlenen Firewall-Regeln pro Schnittstelle der Secure Malware Analytics Appliance.

Schmutzige Schnittstelle

Wird von VMs für die Kommunikation mit dem Internet verwendet, sodass Stichproben DNS auflösen und mit C&C-Servern (Command and Control Server) kommunizieren können
Zulassen:

Richtung	Protokolle	Anschluss	Ziel	Hostname	Details

Ausgehend	IP	BELIEBIGER	BELIEBIGER		Wird empfohlen, außer wenn im Abschnitt Verweigern hier angegeben. Verwendet , um Verbindungen für Analysen zuzulassen.
Ausgehend	TCP	22	54.173.231.161 1 63.97.201.98 2 63.162.55.98 2	support-snapshots.threatgrid.com	Wird für automatische Uploads von Support-Diagnosen verwendet Hinweis: Erfordert Softwareversion 1.2+
Ausgehend	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	Appliance-Updates
Ausgehend	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	Remote-Support/Support-Modus für Appliances
Ausgehend	TCP	22	63.97.201.99 63.162.55.99	appliance-licensing.threatgrid.com	Lizenzverwaltung

[1]Diese IP-Adressen werden in naher Zukunft deaktiviert.

[2]Dies sind die IPs, die diejenigen in [1] ersetzen würden. Wir schlagen vor, beide IPs hinzuzufügen, bis die Mitteilung über die IP-Änderungen in naher Zukunft erfolgt.

Remote-Netzwerkausgang

Wird von der Appliance verwendet, um VM-Datenverkehr in einen Remote-Ausgang zu tunneln, der früher als tg-tunnel bezeichnet wurde.

Richtung	Protokolle	Anschluss	Ziel
Ausgehend	TCP	21413	163.182.175.193
Ausgehend	TCP	21417	69.55.5.250
Ausgehend	TCP	21415	69.55.5.250
Ausgehend	TCP	21413	76.8.60.91

Hinweis: Remote Exit 4.14.36.142 wurde entfernt und wird nicht mehr produziert. Achten Sie darauf, dass alle genannten IPs Ihrer Firewall-Ausnahmeliste hinzugefügt werden.

Ablehnen:

Richtung	Protokolle	Port(s)	Ziel	Details
Ausgehend	SMTP	BELIEBIGER	BELIEBIGER	Um zu verhindern, dass Malware Spam versendet.
Eingehend	IP	BELIEBIGER	Secure Malware Analytics Appliance Dirty Interface	Empfohlen, außer wenn im Abschnitt Zulassen oben angegeben. Wird verwendet, um die Kommunikation für die Analyse zuzulassen.

Schnittstelle reinigen

Diese Funktion wird von verschiedenen verbundenen Services zum Einreichen von Stichproben sowie zum Zugriff auf die Benutzeroberfläche für Analysten verwendet.
Zulassen:

Richtung	Protokolle	Port(s)	Ziel	Details
Eingehend	TCP	443 8443	Secure Malware Analytics Appliance - Saubere Schnittstelle	WebUI- und API-Zugriff
Eingehend	TCP	9443	Secure Malware Analytics Appliance - Saubere Schnittstelle	Verwendet für Glovebox
Ausgehend	TCP	19791	Gastgeber: rash.threatgrid.com IP 54.164.165.137 [1] IP: 34.199.44.202 [1] IP: 63.97.201.96 [2] IP: 63.162.55.96 [2]	Wiederherstellungsmodus für Unterstützung von Secure Malware Analytics

[1]Diese IP-Adressen werden in naher Zukunft deaktiviert.

[2]Dies sind die IPs, die diejenigen in [1] ersetzen würden. Wir schlagen vor, beide IPs hinzuzufügen, bis die Mitteilung über die IP-Änderungen in naher Zukunft erfolgt.

Admin-Schnittstelle

Zugriff auf die Administrations-Benutzeroberfläche.
Zulassen:

Richtung	Protokolle	Port(s)	Ziel	Details
Eingehend	TCP	443 8443	Admin-Schnittstelle der Appliance für sichere Malwareanalyse	Wird verwendet, um Einstellungen für Hardware und Lizenzen zu konfigurieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.