

Sichere Malware-Analysen konfigurieren

Erforderliche IPs und Firewall-Regeln

Inhalt

[Einleitung](#)

[Problem](#)

[Umwelt](#)

[Auflösung](#)

[Secure Malware Analytics Appliance](#)

[Admin-Schnittstelle](#)

[Schnittstelle reinigen](#)

[Schmutzige Schnittstelle](#)

[Dirty Interface - ausgehend](#)

[Eingehende schmutzige Schnittstelle](#)

[Sichere Malware-Analyse-Cloud](#)

[USA \(USA\) Cloud](#)

[Europa \(EU\) Cloud](#)

[Kanada \(CA\) Cloud](#)

[Australien \(AU\) Cloud](#)

[Indien \(IN\) Cloud](#)

[Verwandte Inhalte](#)

Einleitung

In diesem Dokument werden die Hostnamen, IP-Adressen und Ports beschrieben, die für Cisco Secure Malware Analytics (Cloud und Appliance) erforderlich sind.

Problem

Cisco Secure Malware Analytics erfordert ausgehende und eingehende Verbindungen zu bestimmten Hostnamen, IP-Adressen und Ports. Wenn diese Datenflüsse blockiert werden, können Funktionen wie Portalzugriff, Updates, Lizenzierung, Remote-Support und Integration fehlschlagen.

Umwelt

 Anmerkung: Lesen Sie zunächst dieses Dokument, das zusätzliche IPs und Ports für andere Services enthält.
[Erforderliche IPs und Ports für Threat Grid](#)

Dieses Dokument enthält zusätzliche IPs und Ports für andere Dienste, die auf der Appliance-Version basieren.

Weitere Informationen finden Sie in der Dokumentation zu Installation und Upgrade: [Threat Grid Appliances - Installationsanleitungen](#)

Auflösung

Firewall-Regeln für die Firewall, die dem Gerät vorgelagert ist:

* IPs waren zum Zeitpunkt der Veröffentlichung korrekt. Bitte bestätigen Sie lokal via nslookup, dass diese weiterhin korrekt sind.

Secure Malware Analytics Appliance

Admin-Schnittstelle

Quelle	Ziel	Protokolle	Anschluss	Richtung	Aktion	Hinweise
BELIEBIGER	Admin-Schnittstelle	TCP	22	IN	Zulassen	SSH
BELIEBIGER	Admin-Schnittstelle	TCP	80/443	IN	Zulassen	Erlauben Sie den Zugriff auf die Admin-GUI-Schnittstelle.
Admin-Schnittstelle	NFS-Server-IP	TCP	2049	Aus	Zulassen	* Muss offen sein, um die NFS-Backup- oder Clustering-Funktion zu verwenden.

Schnittstelle reinigen

Quelle	Ziel	Protokolle	Anschluss	Richtung	Aktion	Hinweise
BELIEBIGER	Schnittstelle reinigen	TCP	80/443	IN	Zulassen	Zugriff auf saubere GUI-Schnittstelle zulassen.
BELIEBIGER	Schnittstelle reinigen	TCP	8443	IN	Zulassen	* Muss offen sein, um die Funktion "Admin over Clean" verwenden zu können.
BELIEBIGER	Schnittstelle reinigen	TCP	9443	IN	Zulassen	* Muss offen sein, um eine Beispiel-Glovebox-Funktion zu verwenden.
Schnittstelle reinigen	Konfigurierter E-Mail-Relayserver	TCP	25	Aus	Zulassen	Die Appliance verwendet eine de-clean-Schnittstelle, um SMTP-Verbindungen zum konfigurierten Mail-Server zu initiieren.
Schnittstelle reinigen	Sauberer DNS-Server konfiguriert	TCP/UDP	53	Aus	Zulassen	* Optional, nur erforderlich, wenn Clean DNS konfiguriert ist.
Schnittstelle reinigen	Konfigurierter Syslog-Server	TCP/UDP	514	Aus	Zulassen	Verbindung mit dem Server zulassen, der für den Empfang von Syslog-Meldungen und Threat Grid-Benachrichtigungen eingerichtet ist.
Schnittstelle reinigen	LDAP-Server	TCP/UDP	389/636	Aus	Zulassen	* Optional, nur erforderlich, wenn LDAP konfiguriert ist.

Schmutzige Schnittstelle

Dirty Interface - ausgehend

--	--	--	--	--	--	--

Quelle	Ziel	Protokolle	Anschluss	Aktion	Hinweis
Schmutzige Schnittstelle	Internet	BELIEBIGER	BELIEBIGER	Zulassen	Ausgehender Datenverkehr aus Stichproben, optional über Cisco Rechenzentren, zulassen. (Um genaue Ergebnisse zu erhalten, muss es der Malware gestattet sein, ihren Command-and-Control-Server über einen beliebigen Port und ein beliebiges Protokoll zu kontaktieren.)

Eingehende schmutzige Schnittstelle

Quelle	Ziel	Protokolle	Anschluss	Aktion	Hinweis
BELIEBIGER	Schmutziges Internet	BELIEBIGER	BELIEBIGER	Ablehnen	Alle eingehenden Verbindungen ablehnen.

Quelle	Ziel	Protokolle	Anschluss	Aktion	Hinweis
Schmutzige Schnittstelle	Internet	TCP	22	Zulassen	Update-, Support-Snapshot- und Lizenzierungs-Services
Schmutzige Schnittstelle	Internet	TCP/UDP	53	Zulassen	Ausgehenden DNS zulassen.
Schmutzige Schnittstelle	Internet	UDP	123	Zulassen	Ausgehendes NTP zulassen.
Schmutzige Schnittstelle	Internet	TCP	19791	Zulassen	Verbindung zulassen, um Unterstützung für Secure Malware Analytics zu erhalten.
Schmutzige Schnittstelle	Cisco Umbrella	TCP	443	Zulassen	Nutzen Sie Services zur Erkennung und Anreicherung von Bedrohungen durch Drittanbieter.
Schmutzige	VirusInsgesamt	TCP	443	Zulassen	Nutzen Sie Services zur

Schnittstelle					Erkennung und Anreicherung von Bedrohungen durch Drittanbieter.
Schmutzige Schnittstelle	TitanCloud	TCP	443	Zulassen	Nutzen Sie Services zur Erkennung und Anreicherung von Bedrohungen durch Drittanbieter.



Warnung: Die aufgeführten IP-Adressen bleiben auch nach dem 29. Mai 2023 gültig.

Quelle	Ziel	Protokolle	Anschluss	Richtung	Hostname	Details
Schmutzige Schnittstelle	63.97.201.96 63.162.55.96	TCP	19791	Aus	rash.threatgrid.com	Remote-Support/Support-Modul für Appliances
Schmutzige Schnittstelle	63.97.201.97 63.162.55.97	TCP	22	Aus	appliance-updates.threatgrid.com	Wird für automatische Uploads von Support-Diagnosen verwendet.  Anmerkung: Softwareversion 1.2+ erforderlich
Schmutzige Schnittstelle	63.97.201.98 63.162.55.98	TCP	22	Aus	support-snapshots.threatgrid.com	Wird für automatische Uploads von Support-Diagnosen verwendet.  Anmerkung: Softwareversion 1.2+ erforderlich
Schmutzige Schnittstelle	63.97.201.99 63.162.55.99	TCP	22	Aus	appliance-licensing.threatgrid.com	Lizenzmanagement

Sichere Malware-Analyse-Cloud

USA (USA) Cloud

Zugriffs-URL: <https://panacea.threatgrid.com>

Hostname	IP	Anschluss	Details
panacea.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6:6e	443	Für Secure Malware Analytics-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	IPv4: 200.194.241.35 IPv6: 2602:811:900f:6:6e	443	Beispiel-Interaktionsfenster
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6: 2602:811:9007:6::61	443	Beispiel-Interaktionsfenster
glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6:	443	Beispiel-Interaktionsfenster

	2602:811:900b:6:6e		
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	FMC/FTD-Dateianalyse-Service

Europa (EU) Cloud

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

Hostname	IP	Anschluss	Details
panacea.bedrohgrid.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	Für Secure Malware Analytics-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.bedrohgrid.eu	IPv4: 62.67.214.195 200.194.245.35 IPv6: 2602:811:900c:6:6e	3	Beispiel-Interaktionsfenster
glovebox.fam.bedrohgrid.eu	IPv4:	443	Beispiel-Interaktionsfenster

	200.194.242.35 IPv6: 2602:811:9006:6:6e		
fmc.api.bedrohgrid.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/FTDF-Dateianalyse-Service

Die alte IP-Adresse 89.167.128.132 wurde entfernt. Bitte aktualisieren Sie Ihre Firewall-Regeln mit diesen IP-Adressen.

Kanada (CA) Cloud

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

Hostname	IP	Anschluss	Details
panacea.bedrohgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	Für Secure Malware Analytics-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.bedrohgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	Beispiel-Interaktionsfenster

fmc.api.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	FMC/FTD-Dateianalyse-Service
---	---	-----	------------------------------

Australien (AU) Cloud

Zugriffs-URL: <https://panacea.threatgrid.com.au>

Hostname	IP	Anschluss	Details
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	Für Secure Malware Analytics-Portal und integrierte Geräte (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	Beispiel-Interaktionsfenster
fmc.api.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6:	443	FMC/FTD-Dateianalyse-Service

	2602:811:900e:6:6e		
	2602:811:9003:6:6e		

Indien (IN) Cloud

Zugriffs-URL: <https://panacea.threatgrid.in>

Hostname	IP	Anschluss	Details
panacea.bedrohgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	Für Secure Malware Analytics-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.bedrohgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	Beispiel-Interaktionsfenster
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	FMC/FTD-Dateianalyse-Service

Weitere Informationen zu den Anforderungen von Cisco Secure Malware Analytics, z. B. Appliances, finden Sie in diesem Artikel:

Verwandte Inhalte

Die neuesten Anforderungen finden Sie unter .

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.