Configure Secure Malware Analytics Required IPs and Firewall Rules

Contents

Introduction

Issue

Environment

Resolution

- Secure Malware Analytics Appliance
  - Admin Interface
  - Clean Interface
  - Dirty Interface
- Dirty Interface Outbound
- Dirty Interface Inbound
- Secure Malware Analytics Cloud
- United States (US) Cloud
- Europe (EU) Cloud
- Canada (CA) Cloud
- Australia (AU) Cloud
- India (IN) Cloud

Related Content

Introduction

This document describes the hostnames, IP addresses, and ports required for Cisco Secure Malware Analytics (cloud and appliance).

Issue

Cisco Secure Malware Analytics requires outbound and inbound connectivity to specific hostnames, IP addresses, and ports. If these flows are blocked, features such as portal access, updates, licensing, remote support, and integrations can fail.

Environment

Note: Please first refer to this document, which includes additional IPs and ports for other services. Required IPs and ports for Threat Grid

This document includes additional IPs and ports for other services based on the appliance version.

Please refer to the Install and Upgrade Guides documentation: Threat Grid Appliances Installation Guides

Resolution

Firewall rules for the firewall upstream to the device:

*IPs were correct at the time of publishing. Please confirm locally via nslookup that these are still correct.

Secure Malware Analytics Appliance

Admin Interface

Source	Destination	Protocol	Port	Direction	Action	Notes
ANY	Admin Interface	TCP	22	IN	Allow	SSH
ANY	Admin Interface	TCP	80/443	IN	Allow	Allow access to Admin GUI Interface.
Admin Interface	NFS Server IP	TCP	2049	OUT	Allow	*Must be open to use NFS Backup or Clustering feature.

Clean Interface

Source	Destination	Protocol	Port	Direction	Action	Notes
ANY	Clean Interface	TCP	80/443	IN	Allow	Allow access to Clean GUI Interface.
ANY	Clean Interface	TCP	8443	IN	Allow	*Must be open to use Admin over Clean Feature.
ANY	Clean Interface	TCP	9443	IN	Allow	*Must be open to use sample Glovebox Feature.

Clean Interface	Configured Email Relay Server	TCP	25	OUT	Alllow	The appliance uses de clean interface to initiate SMTP connections to the configured mail server.
Clean Interface	Configured Clean DNS Server	TCP/UDP	53	OUT	Allow	*Optional, only required if Clean DNS is configured.
Clean Interface	Configured Syslog Server	TCP/UDP	514	OUT	Allow	Allow connectivity to server designated to receive Syslog messages and Threat Grid notifications.
Clean Interface	LDAP Server	TCP/UDP	389/636	OUT	Allow	*Optional, only required if LDAP is configured.

Dirty Interface

Dirty Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	ANY	ANY	Allow	Allow outbound traffic from samples, optionally proxied through Cisco datacenters. (To get accurate results, it is required that malware be allowed to contact its command and control server using whatever port and protocol it is designed to use.)

Dirty Interface Inbound

Source	Destination	Protocol	Port	Action	Note
ANY	Dirty Internet	ANY	ANY	Deny	Deny all incoming connections.

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	TCP	22	Allow	Update, support snapshot, and licensing services.

Dirty Interface	Internet	TCP/UDP	53	Allow	Allow outbound DNS.
Dirty Interface	Internet	UDP	123	Allow	Allow outbound NTP.
Dirty Interface	Internet	TCP	19791	Allow	Allow connectivity to Secure Malware Analytics support.
Dirty Interface	Cisco Umbrella	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	VirusTotal	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	TitaniumCloud	TCP	443	Allow	Connect with third-party detection and enrichment services.



Warning: The IP Addresses listed remain active after May 29th, 2023.

Source	Destination	Protocol	Port	Direction	Hostname	Details
Dirty Interface	63.97.201.96 63.162.55.96	TCP	19791	OUT	rash.threatgrid.com	Remote Support / Appliance Support Mode
Dirty Interface	63.97.201.97 63.162.55.97	TCP	22	OUT	appliance-updates.threatgrid.com	Used for automatic support diagnostic uploads.  **Note**: Requires software version 1.2+
Dirty Interface	63.97.201.98 63.162.55.98	TCP	22	OUT	support-snapshots.threatgrid.com	Used for automatic support diagnostic uploads.  **Note**: Requires software version

						1.2+
Dirty Interface	63.97.201.99 63.162.55.99	TCP	22	OUT	appliance-licensing.threatgrid.com	License Management

Secure Malware Analytics Cloud

United States (US) Cloud

Access URL: https://panacea.threatgrid.com

Hostname	IP	Port	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	For Secure Malware Analytics Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	IPv4: 200.194.241.35 IPv6: 2602:811:900f:6::6e	443	Sample Interaction window
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6: 2602:811:9007:6::61	443	Sample Interaction window

glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6: 2602:811:900b:6::6e	443	Sample Interaction window
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 File Analysis Service

Europe (EU) Cloud

Access URL: https://panacea.threatgrid.eu

Hostname	IP	Port	Details
panacea.threatgrid.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	For Secure Malware Analytics Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	IPv4: 62.67.214.195 200.194.245.35 IPv6: 2602:811:900c:6::6e	3	Sample Interaction window

glovebox.fam.threatgrid.eu	IPv4: 200.194.242.35 IPv6: 2602:811:9006:6::6e	443	Sample Interaction window
fmc.api.threatgrid.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/FTDFile Analysis Service

The old IP 89.167.128.132 has been retired, please update your firewall rules with these IPs.

Canada (CA) Cloud

Access URL: https://panacea.threatgrid.ca

Hostname	IP	Port	Details
panacea.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	For Secure Malware Analytics Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	Sample Interaction window
fmc.api.threatgrid.ca	IPv4:	443	FMC/FTD File Analysis Service

	200.194.240.35 IPv6: 2602:811:900d:6::6e		

Australia (AU) Cloud

Access URL: https://panacea.threatgrid.com.au

Hostname	IP	Port	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	For Secure Malware Analytics Portal and Integrated Devices (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	Sample Interaction window
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	FMC/FTD File Analysis Service

India (IN) Cloud

Access URL: https://panacea.threatgrid.in

Hostname	IP	Port	Details
panacea.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	For Secure Malware Analytics Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.threatgrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	Sample Interaction window
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	FMC/FTD File Analysis Service

For more Cisco Secure Malware Analytics requirements, such as appliances, please see this article:

Related Content

For the latest requirements, see .