

Required IPs and Ports for Secure Malware Analytics

Contents

[Introduction](#)

[Secure Malware Analytics Clouds](#)

[US \(United States\) Cloud](#)

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

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

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

[Secure Malware Analytics Appliance](#)

[Dirty Interface](#)

[Remote Network Exit](#)

[Clean Interface](#)

[Admin Interface](#)

Introduction

This document outlines the essential network configurations you need to implement on your firewall to ensure seamless operation of Secure Malware Analytics.

Contributed by Cisco TAC Engineers.

Secure Malware Analytics Clouds

US (United States) 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	443	Sample Interaction window

	IPv6: 2602:811:900f:6::6e		
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

EU (Europe) Cloud

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

Hostname	IP	Port	Details
panacea.threatgrid.eu	62.67.214.195 200.194.242.35	443	For Secure Malware Analytics Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	62.67.214.195	443	Sample Interaction window
glovebox.fam.threatgrid.eu	200.194.242.35	443	Sample Interaction window
fmc.api.threatgrid.eu	62.67.214.195 200.194.242.35	443	FMC/FTD File Analysis Service

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

CA (Canada) Cloud

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

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

AU (Australia) Cloud

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

Hostname	IP	Port	Details
panacea.threatgrid.com.au	124.19.22.171	443	For Secure Malware Analytics Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	124.19.22.171	443	Sample Interaction window
fmc.api.threatgrid.com.au	124.19.22.171	443	FMC/FTD File Analysis Service

Secure Malware Analytics Appliance

The following are the recommended firewall rules per interface of the Secure Malware Analytics Appliance.

Dirty Interface

This is used by VMs to communicate with the internet so that samples can resolve DNS and communicate with command and control (C&C) servers.

Allow:

Direction	Protocol	Port	Destination	Hostname	Details
Outbound	IP	ANY	ANY		Recommended except where specified in the Deny section here. Used to allow connectivity for analysis.
Outbound	TCP	22	54.173.231.161 ¹ 63.97.201.98 ² 63.162.55.98 ²	support-snapshots.threatgrid.com	Used for automatic support diagnostic uploads Note: Requires software version 1.2+
Outbound	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
Outbound	TCP	19791	54.164.165.137 ¹	rash.threatgrid.com	Remote Support / Appliance Support Mode

			34.199.44.202 ¹ 63.97.201.96 ² 63.162.55.96 ²		
Outbound	TCP	22	54.173.124.172 ¹ 63.97.201.99 ² 63.162.55.99 ²	appliance-licensing.threatgrid.com	License Management


¹These IPs will be disabled in the near future.


²These are the IPs that would replace the ones in ¹. We suggest adding both IPs until the communication about the IP changes is made in the near future.

Remote Network Exit

This is used by the appliance to tunnel VM traffic to a remote exit formerly known as tg-tunnel.

Direction	Protocol	Port	Destination
Outbound	TCP	21413	173.198.252.53
Outbound	TCP	21413	163.182.175.193 **
Outbound	TCP	21417	69.55.5.250
Outbound	TCP	21415	69.55.5.250
Outbound	TCP	21413	76.8.60.91

 **Note:** Remote Exit 4.14.36.142 has been removed and is no longer in production. Ensure to have all IPs mentioned added to your firewall exception list.

 ** Remote Exit 163.182.175.193 will be replaced by 173.198.252.53

Deny:

Direction	Protocol	Port(s)	Destination	Details
Outbound	SMTP	ANY	ANY	To prevent malware from sending out spam.
Inbound	IP	ANY	Secure Malware Analytics Appliance Dirty Interface	Recommended except where specified in the Allow section above. Used to allow communication for analysis.

Clean Interface

This is used by various connected services to submit samples as well as UI access for analysts.

Allow:

Direction	Protocol	Port(s)	Destination	Details
Inbound	TCP	443 and 8443	Secure Malware Analytics Appliance Clean Interface	WebUI and API access
Inbound	TCP	9443	Secure Malware Analytics Appliance Clean Interface	Used for Glovebox
Inbound	TCP	22	Secure Malware Analytics Appliance Clean Interface	Admin TUI access over SSH
Outbound	TCP	19791	Host: rash.threatgrid.com 54.164.165.137 ¹ 34.199.44.202 ¹ 63.97.201.96 ² 63.162.55.96 ²	Recovery Mode for Secure Malware Analytics Support.

¹These IPs will be disabled in the near future.

²These are the IPs that would replace the ones in ¹. We suggest adding both IPs until the communication about the IP changes is made in the near future.

Admin Interface

This is used to access to the administration console or user interface.

Allow:

Direction	Protocol	Port(s)	Destination	Details
Inbound	TCP	443 and 8443	Secure Malware Analytics Appliance Admin Interface	Used to configure settings for hardware and licensing.
Inbound	TCP	22	Secure Malware Analytics Appliance Admin Interface	Admin TUI access over SSH