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
- IN (India) 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.

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 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

EU (Europe) 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:	443	For Secure Malware Analytics Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)

	2602:811:9006:6::6e 2602:811:900c:6::6e		
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 above IPs.

CA (Canada) Cloud

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

Hostname	IP	Port	Details
panacea.threatgrid.ca	IPv4: 200.194.240.35 IPv6:	443	For Secure Malware Analytics Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)

	2602:811:900d:6::6e		
glovebox.kam.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	Sample Interaction window
fmc.api.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	FMC/FTD File Analysis Service

AU (Australia) 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:	443	FMC/FTD File Analysis Service

	200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6::6e		

IN (India) 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

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	63.97.201.98 63.162.55.98	support-snapshots.threatgrid.com	Used for automatic support diagnostic uploads. **Note**: Requires software version 1.2+.
Outbound	TCP	22	63.162.55.97 63.97.201.97	appliance-updates.threatgrid.com	Appliance Updates
Outbound	TCP	19791	63.97.201.96 63.162.55.96	rash.threatgrid.com	Remote Support / Appliance Support Mode
Outbound	TCP	22	63.97.201.99 63.162.55.99	appliance-licensing.threatgrid.com	License Management

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	21417	69.55.5.250
Outbound	TCP	21415	69.55.5.250
Outbound	TCP	21413	38.123.149.87



Note: As of **July 25, 2026**, the following Remote Exit IP addresses have been replaced:
- **163.182.175.193** was replaced by **173.198.252.53**
- **76.8.60.91** was replaced by **38.123.149.87**

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 63.97.201.96 63.162.55.96	Recovery Mode for Secure Malware Analytics Support

Admin Interface

Use this to access 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