Required IP and Ports for Threat Grid

Contents

Introduction

This document describes the Hostnames, IP addresses and Ports that are required in order to enable the Threat Grid (Cloud and Appliance) product to operate as per design. In order to complete the operations successfully, your firewall must allow connectivity to the required Hostnames, IP addresses and Ports.

Threat Grid Cloud

NAM Cloud

(https://panacea.threatgrid.com)

Hostname	IP	Port	Details
panacea.threatgrid.com	63.97.201.67, 4.14.36.148	443	For Threat Grid Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)
glovebox.mtv.threatgrid.com	63.97.201.67, 4.14.36.148	443	Sample Interaction window
glovebox.rcn.threatgrid.com	63.97.201.67	443	Sample Interaction window
fmc.api.threatgrid.com	63.97.201.67, 4.14.36.148	443	FMC/FTD File Analysis Service

EU Cloud

(https://panacea.threatgrid.eu)

Hostname	IP	Port	Details
panacea.threatgrid.eu	89.167.128.132	443	For Threat Grid Portal and Integrated Devices (ESA/WSA/FTD/ODNS/Meraki)
glovebox.threatgrid.eu	89.167.128.132	443	Sample Interaction window
fmc.api.threatgrid.eu	89.167.128.132	443	FMC/FTD File Analysis Service

Threat Grid Appliance

These are the recommended firewall rules per interface of the ThreatGrid appliance.

Dirty Interface

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(s)	Destination	Details
Outbound	IP	ANY	ANY	• Recommended except where specified in the **Deny** section here. • This is to allow connectivity for analysis.
Outbound	TCP	22	Host: support-snapshots.threatgrid.com IP: 54.173.231.161	Used for automatic support diagnostic uploads Note: Requires software version 1.2+
Outbound	TCP	22	Host: appliance-updates.threatgrid.com IP: 54.173.181.217 IP: 54.173.182.46	Appliance Updates
Outbound	TCP	19791	Host: rash.threatgrid.com IP: 54.173.124.172 IP: 54.164.165.137	Remote Support / Appliance Support Mode

Remote Network Exit

Used by the appliance to tunnel VM traffic to remote exit formerly known as tg-tunnel.

Direction	Protocol	Port	Destination
Outbound	TCP	21413	163.182.175.193
Outbound	TCP	21417	69.55.5.250
Outbound	TCP	21415	69.55.5.250

Note: Remote Exit ` 4.14.36.142` has been removed and no longer in production. Please make sure to have all IPs mentioned above added in your firewall exception list.

Deny:

Direction	Protocol	Port(s)	Destination	Details
Outbound	SMTP	ANY	ANY	To prevent malware to send out the spam.
Inbound	IP	ANY	ThreatGrid appliance Dirty Interface	• Recommended except where specified in the **Allow** section above. • To allow communication for

analysis.

Clean Interface

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 8443	ThreatGrid appliance Clean Interface	WebUI and API access
Inbound	TCP	9443	ThreatGrid appliance Clean Interface	Used for Glovebox
Outbound	TCP	19791	Host: rash.threatgrid.com IP: 54.164.165.137 IP: 54.173.124.172	Recovery Mode for Threatgrid Support.

Admin Interface

Access to the administration UI.

Allow:

Direction	Protocol	Port(s)	Destination	Details
Inbound	TCP	443 8443	ThreatGrid appliance Admin Interface	Used to configure settings for hardware and licensing.