Planning

The Cisco Threat Grid Appliance is a Linux server with Threat Grid software installed by Cisco Manufacturing prior to shipment. Once a new Threat Grid Appliance is received, it must be set up and configured for your on-premises network environment.

This chapter includes the following information about the environmental, hardware, and network requirements that should be reviewed prior to configuration:

Supported Browsers

Threat Grid supports the following browsers:

- Google Chrome™
- Mozilla Firefox®
- Apple Safari®

Note Microsoft Internet Explorer is **not** supported.

Environmental Requirements

Threat Grid Appliance (v2.7.2 and later) is deployed on the Threat Grid M5 Appliance server. Before you set up and configure the Threat Grid Appliance, make sure the necessary environmental requirements for power, rack space, cooling, and other issues are met, according to the specifications in the *Cisco Threat Grid M5 Hardware Installation Guide*.

Hardware Requirements

The SFP+ form factor is used for the Admin interface. If you are clustering Threat Grid Appliances, each one will require an additional SFP+ module on the Clust interface.

Note The SFP+ modules must be connected *before* the Threat Grid Appliance is powered on for the session in which the configuration wizard is going to be run.

If there are no SFP+ ports available on the switch, or SFP+ is not desirable, then a transceiver for 1000Base-T can be used (for example, Cisco Compatible Gigabit RJ 45 Copper SFP Transceiver Module Mini -GBIC - 10/100/1000 Base-T Copper SFP Module).

Figure 1: Cisco 1000BASE-T Copper SFP (GLC-T)

You can attach a monitor to the server, or, if Cisco Integrated Management Controller (CIMC) is configured, you can use a remote KVM (on UCS C220-M3 and C220-M4 servers).

Note CIMC is not supported on the Threat Grid M5 Appliance server.

The Cisco UCS Power Calculator is available to get a power estimate.

Network Requirements

The Threat Grid Appliance requires three networks:

- **ADMIN** - The Administrative network must be configured to perform the Threat Grid Appliance setup.

- OpAdmin Management Traffic (HTTPS)
- SSH
- NFSv4 (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.)

- **CLEAN** - The Clean network is used for inbound, trusted traffic to the Threat Grid Appliance (requests), and integrated appliances such as the Cisco Email Security Appliance and Web Security Appliance; integrated applicances connect to the IP address of the Clean interface.

Note The URL for the Clean network interface will not work until the OpAdmin portal configuration is complete.

The following specific, restricted types of network traffic can be outbound from the Clean network:

- Remote syslog connections
- Email messages sent by the Threat Grid Appliance
- Disposition Update Service connections to AMP for Endpoints Private Cloud devices
- DNS requests (related to any of the above)
- LDAP

- **DIRTY** - The Dirty network is used for outbound traffic from the Threat Grid Appliance (including malware traffic).

Note To protect your internal network asses, we recommend using a dedicated external IP address (for example, the Dirty interface) that is different from your corporate IP.

For network interface setup information, see Network Interfaces.

DNS Server Access

The DNS server needs to be accessible via the Dirty network when used for purposes other than Disposition Update Service lookups, resolving remote syslog connections, and resolving the mail server used for notifications from the Threat Grid software.

By default, DNS uses the Dirty interface. The Clean interface is used for AMP for Endpoints Private Cloud integrations. If the AMP for Endpoints Private Cloud hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in the OpAdmin interface.

See the Cisco Threat Grid Appliance Administrator Guide for additional information.

NTP Server Access

The NTP server needs to be accessible via the Dirty network.

Integrations

Additional planning may be required if the Threat Grid Appliance is going to be used with other Cisco products, such as the Email Security Appliance, Web Security Appliance, or AMP for Endpoints Private Cloud. See the *Cisco Threat Grid Appliance Administrator Guide* for more information.

DHCP

If you are connected to a network configured to use DHCP, follow the instructions provided in the Using DHCP section of the *Cisco Threat Grid Appliance Administrator Guide*.

License

You will receive a license and password from Cisco Threat Grid.

For questions about licenses, contact support@threatgrid.com.

Rate Limits

The API rate limit is global for the Threat Grid Appliance under the terms of the license agreement. This affects API submissions ONLY, not manual sample submissions.

Rate limits are based on a window of rolling time, not to a calendar day. When the submission limit is exhausted, the next API submission will return a 429 error, plus a message about how long to wait before retrying. See the FAQs in the Threat Grid portal UI online Help for a detailed description.

Organization and Users

Once you have completed the Threat Grid Appliance setup and network configuration, you must create the initial Threat Grid organizations and add user account(s), so that people can login and begin submitting malware samples for analysis. This task may require planning and coordination among multiple organizations and users, depending on your requirements.

See the Create New Organization section in the *Cisco Threat Grid Appliance Administrator Guide*. See the Threat Grid portal Help for information about managing users.

Updates

The initial Threat Grid Appliance setup and configuration steps **must be completed** before installing any Threat Grid Appliance updates. We recommend that you check for updates immediately after completing the initial configuration (see Install Updates).

Threat Grid Appliance updates cannot be downloaded until the license is installed, and the update process requires that the initial appliance configuration is completed. Updates must be done in sequence.

Note Verify that SSH is specified for updates.

User Interfaces

After the server has been correctly attached to the network and powered up, there are several user interfaces available for configuring the Threat Grid Appliance.

Note LDAP authentication is available for TGSH Dialog and OpAdmin (v2.1.6 and later).

TGSH Dialog

The **TGSH Dialog** interface is used to configure the network interfaces. The TGSH Dialog is displayed when the Threat Grid Appliance successfully boots up.

Reconnecting to the TGSH Dialog

The TGSH Dialog remains open on the console and can be accessed either by attaching a monitor to the appliance or, if CIMC is configured, via remote KVM.

Note CIMC is not supported on the Threat Grid M5 Appliance server.

To reconnect to the TGSH Dialog, ssh into the Admin IP address as the user **threatgrid**.

The required password is either the initial, randomly generated password, which is visible initially in the TGSH Dialog, or the new Admin password you create during the first step of the OpAdmin Portal Configuration.

Threat Grid Shell (tgsh)

The Threat Grid Shell (tgsh) is an administrator's interface that is used to execute commands (including destroy-data and forced backup), and for expert, low-level debugging. To access tgsh, select **CONSOLE** in the TGSH Dialog.

Note OpAdmin uses the same credentials as the Threat Grid user, so any password changes/updates made via tgsh will also impact OpAdmin.

Caution Network configuration changes made with tgsh are not supported unless specifically directed by Threat Grid support; OpAdmin or TGSH Dialog should be used instead.

OpAdmin Portal

This is the primary Threat Grid GUI configuration tool. Much of the Threat Grid Appliance configuration can ONLY be done via OpAdmin, including licenses, email host, and SSL certificates.

Threat Grid Portal

The Threat Grid user interface application is available as a cloud service, and is also installed on Threat Grid Appliances. There is no communication between Threat Grid Cloud service and the Threat Grid Portal that is included with a Threat Grid Appliance.

Network Interfaces

The available network interfaces are described in the following table:

Interface	Description
Admin	• Connect to the Admin network. **Only inbound** from Admin network. • OpAdmin UI traffic • SSH (inbound) for TGSH Dialog • NFSv4 for backups and clustering (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.) Must be accessible from all cluster notes. **Note** The form factor for the Admin interface is SFP+. See Hardware Requirements.
Clust	The non-Admin SFP+ port is used for clustering. • Clust interface required for clustering (optional) • Requires an additional SFP+ module for direct interconnect. This interface does not require any configuration. Addresses are automatically assigned.

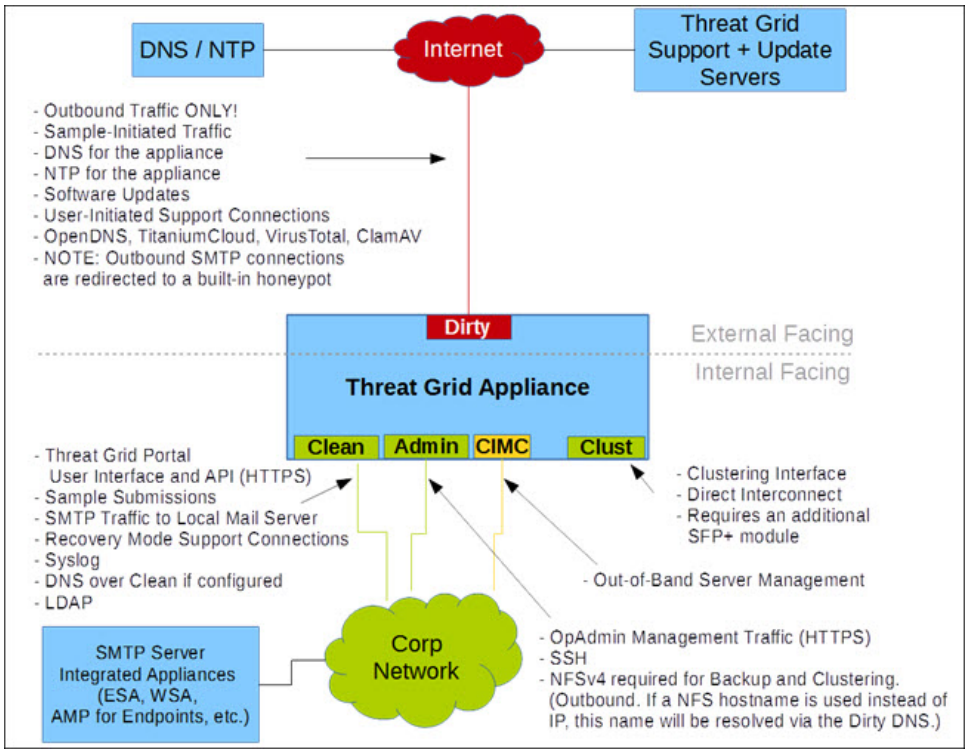
Interface	Description
Clean	• Connect to the Clean network. Clean must be accessible from the corporate network but requires no outbound access to the Internet. • UI and API traffic (inbound) • Sample submissions • SMTP (outbound connection to the configured mail server) • SSH (inbound for TGSH Dialog) • Syslog (outbound to configured syslog server) • ESA/WSA and CSA Integrations • AMP for Endpoints Private Cloud Integration • DNS optional • LDAP (outbound)
Dirty	Connect to the Dirty network; requires Internet access. Outbound Only. You should not use your own DNS (private IP) for the Dirty Interface because traffic sent to a private IP is dropped at the Network Exit Localization firewall. • DNS **Note** If you are setting up an integration with a AMP for Endpoints Private Cloud, and the AMP for Endpoints appliance hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in OpAdmin. • NTP • Updates • Support session in Normal operations mode • Support snapshots • Malware sample-initiated traffic • Recovery mode support session (outbound) • OpenDNS, TitaniumCloud, VirusTotal, ClamAV • SMTP outbound connections are redirected to a built-in honeypot **Note** Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.

Interface	Description
CIMC Interface	Recommended. If the Cisco Integrated Management Controller (CIMC) interface is configured, it can be used for server management and maintenance. For more information see the *Cisco Threat Grid Appliance Administrator Guide*. **Note** CIMC is not supported on the Threat Grid M5 Appliance server.

Network Interface Setup Diagram

This section describes the most logical and recommended setup for a Threat Grid Appliance. However, each customer's interface setup is different. Depending on your network requirements, you may decide to connect the Dirty interface to the inside, or the Clean interface to the outside with appropriate network security measures in place.

Figure 2: Network Interfaces Setup Diagram



Note In Threat Grid Appliance (v2.7.2 and later), the **enable_clean_interface**option is available but is disabled by default. This option (after applying configuration and rebooting) enables access to the administrative interface on port 8443 of the assigned clean IP.

Firewall Rules

This section provides suggested firewall rules.

Note Implementing a restrictive outgoing policy on the Dirty interface for ports 22 and 19791 requires tracking updates over time and spending more time maintaining the firewall.

Note Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.

Dirty Interface Outbout

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	ANY	ANY	Allow	Allow outbound traffic from samples. (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.

Clean Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Clean Interface	SMTP Servers	TCP	25	Allow	The appliance uses the clean interface to initiate SMTP connections to the configured mail server.

Clean Interface Outbound (Optional)

Source	Destination	Protocol	Port	Action	Note
Clean Interface	Corporate DNS Server	TCP/UDP	53	Allow	Optional, only required if Clean DNS is configured.

Source	Destination	Protocol	Port	Action	Note
Clean Interface	AMP Private Cloud	TCP	443	Allow	Optional, only required if AMP for Endpoints Private Cloud integration is used.
Clean Interface	Syslog Servers	UDP	514	Allow	Allow connectivity to server designated to receive Syslog messages and Threat Grid notifications.
Clean Interface	LDAP Servers	TCP/UDP	389	Allow	Optional, only required if LDAP is configured.
Clean Interface	LDAP Servers	TCP	636	Allow	Optional, only required if LDAP is configured.

Clean Interface Inbound

Source	Destination	Protocol	Port	Action	Note
User Subnet	Clean Interface	TCP	22	Allow	Allow SSH conectivity to the TGSH Dialog.
User Subnet	Clean Interface	TCP	80	Allow	Appliance API and Threat Grid user interface. This will redirect to HTTPS TCP/443.
User Subnet	Clean Interface	TCP	443	Allow	Appliance API and Threat Grid user interface.
User Subnet	Clean Interface	TCP	9443	Allow	Allow connectivity to the Threat Grid UI Glovebox.

Admin Interface Outbound (Optional)

The following depends on what services are configured.

Source	Destination	Protocol	Port	Action	Note
Admin Interface	NFSv4 Server	TCP	2049	Allow	Optional, only required if Threat Grid Appliance is configured to send backups to an NFSv4 share.

Admin Interface Inbound

Source	Destination	Protocol	Port	Action	Note
Admin Subnet	Admin Interface	TCP	22	Allow	Allow SSH connectivity to the TGSH Dialog.
Admin Subnet	Admin Interface	TCP	80	Allow	Allow access to the OpAdmin Portal interface. This will redirect to HTTPS TCP/443.

Source	Destination	Protocol	Port	Action	Note
Admin Subnet	Admin Interface	TCP	443	Allow	Allow access to the OpAdmin Portal interface.

Dirty Interface for Non Cisco-Validated/Recommended Deployment

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 Threat Grid 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.

Login Names and Passwords (Default)

The default login names and passwords are listed in the following table:

User	Login/Password
Web UI Administrator	Login: **admin** Password: **changeme**
OpAdmin and Shell User	Use the initial Threat Grid/TGSH Dialog randomly generated password, and then the new password entered during the first step of the OpAdmin configuration workflow. If you lose the password, see the Reset Administrator Password section in the of the *Cisco Threat Grid Appliance Administrator Guide*.
CIMC	Login: **admin** Password: **password**

Setup and Configuration Overview

The following setup and initial configuration steps are described in this guide:

- Initial Network Configuration
- OpAdmin Portal Configuration
- Installing Updates
- Testing Appliance Setup

Complete the remaining administrative configuration tasks (such as license installation, email server, and SSL certificates) in the OpAdmin Portal as documented in the *Cisco Threat Grid Appliance Administrator Guide*.

You should allow approximately 1 hour to complete the initial configuration steps.