Network Exit Configuration

This chapter describes the Network Exit feature and how to configure it.

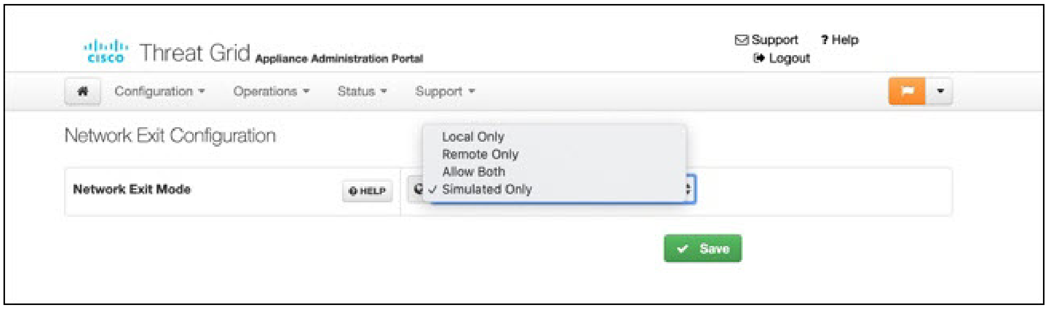
Configure Network Exit

Geographic location is often an important issue for malware analysis. Some types of malware behave differently depending on geographic location, while other types may target a specific area. Similar in concept to VPN, the **Network Exit** setting (v2.4.3 and later) makes any outgoing network that is generated during sample analysis appear to exit from that location. Configuration files are automatically distributed and there is no need for suport staff to manually install or update them.

Note If you were previously using tg-tunnel, you must allow outbound traffic to 4.14.36.142:21413 and 63.97.201.68:21413 before installing v2.4.3; otherwise, that traffic only needs to be permitted before enabling remote exit use.

Step 1 In the OpAdmin portal, click **Configuration** > **Network Exit**.

Figure 1: Network Exit Configuration



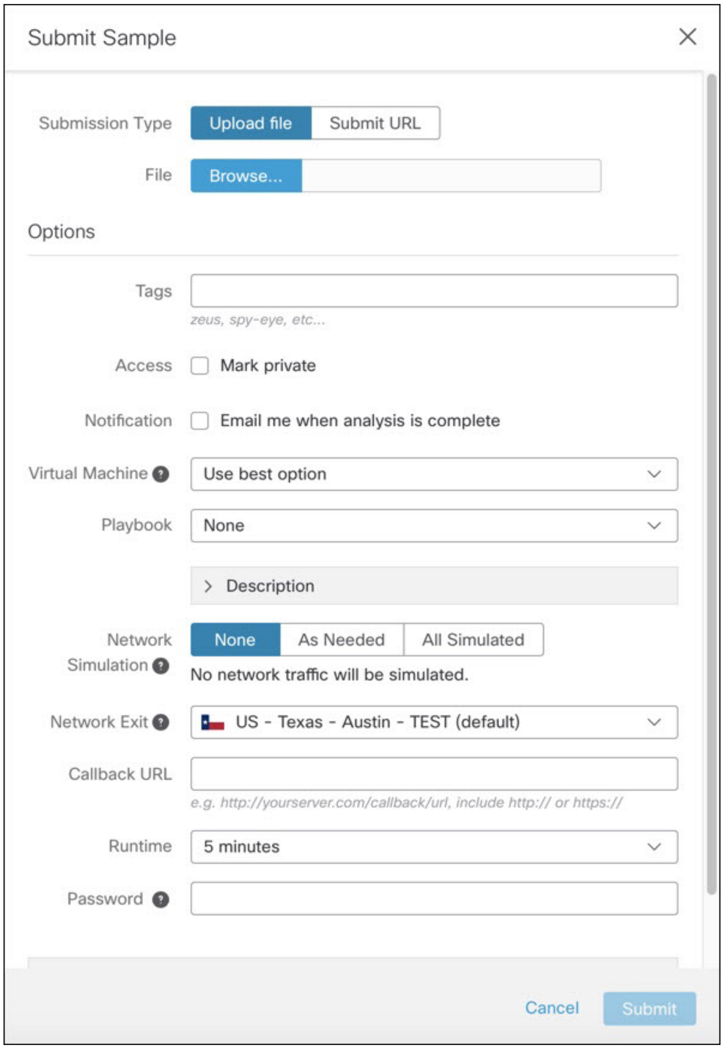
Step 2 In the **Network Exit Mode** field, choose **Local Only**, **Remote Only**, **Allow Both**, or **Simulated Only**. This field determines the **Network Exit** options that will be available in the application, such as when submitting samples in the UI.

If you select **Local Only** or **Remote Only**, the application only makes those options available to users.

If you select **Simulated Only**, the API and UI users cannot select any option to send network traffic from virtual machines to destinations outside of the local Threat Grid Appliance.

Accessing private networks, even for DNS lookup, is not allowed even for Network Exit. All malware traffic comes out of the Dirty interface, using the Dirty DNS server configured.

Figure 2: Submit Sample



Submit Sample

Submission Type: Upload file | Submit URL

File: Browse...

Options

Tags:
zeus, spy-eye, etc...

Access: □ Mark private

Notification: □ Email me when analysis is complete

Virtual Machine: Use best option

Playbook: None

> Description

Network Simulation: None | As Needed | All Simulated
No network traffic will be simulated.

Network Exit: US - Texas - Austin - TEST (default)

Callback URL:
e.g. http://yourserver.com/callback/url, include http:// or https://

Runtime: 5 minutes

Password:

Cancel Submit

Note Sometimes it may be necessary to simulate network connections during analysis. Network simulation provides analysts with a way to present network resources to malware samples that may otherwise be unavailable, and for other reasons. For example, you may want to select a network simulation option to simulate network connections when the upstream servers are not accessible; when they have been taken down; when their DNS records are gone; or if other restrictions on outbound connectivity apply in order to improve sample execution and convictions.

In addition, network simulation can provide at least some connectivity to air-gapped appliances and improve sample execution on them.

The **Network Simulation** option for sample analysis is available on Threat Grid Appliances v2.7.1 and later. See the Threat Grid portal UI online help topic for additional information.