How do I opt a machine out of the MIT campus-network firewall using Moira?

Q: How do I opt a machine out of the MIT campus-network firewall using Moira?

On this page:

Overview
Context
Who Can Opt-Out?
Athena Workstation/Dialup Opt-Out Instructions
Web-based Opt-Out Instructions

Overview

This guide will describe how eligible members of the MIT community can opt systems out of the campus network firewall.

A general FAQ about the improvements to campus network security can be found here.

Context

Changes to MIT’s campus-network security model will be implemented in the month of June (2013), beginning no earlier than Monday, June 10th, 2013.

The changes will include the implementation of a stateful firewall that will block incoming network traffic that originates from outside of MIT’s various netblocks.

There may be a need for eligible members of the MIT community to opt certain machines out of the stateful firewall (e.g. email servers, web servers, etc.).

Functionality has been added to Moira to allow eligible members of the MIT community to opt machines out of the firewall policy.

In order to prevent interruptions to the community, IS&T is making this functionality available prior to the firewall's activation.

Who Can Opt-Out?

- If the Moira record for a machine lists an explicit owner, that named owner can opt out the machine. (You can use the command stella hostname to review the Moira record, and look for the "Owner" field.)
- If the Moira record for a machine lists an Account Number (Cost Object), the opt-out mechanism will also check whether you have Roles authorization to “Spend or Commit” on that cost object and checks that your own MIT affiliation is one of: Faculty, Sponsored Research Staff, Undergraduate Student, Graduate Student, or Other Academic Group (you can review this affiliation with stanley username). If so, you are allowed to opt-out.
  - Note that the rules for Account-number based Opt Out means that Staff or Administrative Staff (review with stanley username) have limited ability to opt machines out of the campus-network firewall. Staff who need to opt out machines may need to be get themselves listed explicitly as a machine owner, which may require approval.

In the past, the explicit "owner" field was mainly only used for residential computers. In the future, we expect more computers will use named owner field, since the opt-out system checks that field.

- please contact the IS&T Helpdesk if you need ownership permission assigned to a machine in your care

Some special-purpose networks on campus will be permanently firewalled or permanently open, and the rules listed above will not be relevant for machines that are not eligible for opt-out/opt-in. We’ll clarify this when we have more information, but the general rule is that private networks are not affected by the firewall, IS&T server networks are not affected by the firewall, and IS&T infrastructure networks are not eligible for opt-out.

Athena Workstation/Dialup Opt-Out Instructions

1. Log into an MIT dialup server or Athena workstation (e.g. ssh username@athena.dialup.mit.edu).
2. Run the following command:

```
stella hostname -optout -opcmt "Machine is an email server for Professor Doe."
```

   a. The command should all be one line.
   b. Replace `hostname` with the hostname of your computer.
   c. “opcmt” is a comment describing why your computer is opted out. Please be specific when indicating why the machine will be opted out of the campus-network firewall.

3. If you are returned to the $ prompt with no error messages, the machine has been successfully opted out of the campus-network firewall.

4. You can check the status of your machine by running the command `stella hostname` from an Athena workstation.

   a. Note: ‘Opt: 0’ means the machine is in the firewall; ‘Opt: 1’ (or higher) means the machine is NOT in the firewall, it’s opted out.

   ! Circumstantial evidence (Zephyr discussion and a handful of SN cases) suggests that ‘Opt: 0’ means “default status for that network” and ‘Opt: 1’ means “non-default status for that network”, i.e., on a network that is not firewalled by default, ‘Opt: 1’ will firewall that host. This, combined with nonobvious signs that a host is behind the firewall, can complicate troubleshooting and frustrate clients. More information is needed about how tools like `ping` and `traceroute` react to hosts that are behind the firewall.

Web-based Opt-Out Instructions

- A web-based method to opt machines out of the campus-network firewall is planned.
- This page will be updated with a link to the web-based opt-out page as soon as possible.