

## Overview of the Threat Mitigation Application

---

The Threat Mitigation Application helps administrators detect and respond to attacks on the network. The Threat Mitigation Application can be customized based on customer-supplied data to control the description and recommended actions for each type of attack. If the user chooses to take an action, the Threat Mitigation Application activates a service for the source address of the event. The Threat Mitigation Application includes the ability to log all user operations to provide an audit trail of actions.

You can use the Threat Mitigation Application to respond to threats on the network by:

- Executing a script for Juniper Networks NetScreen-Security Manager that posts information about the attack to the SRC Threat Mitigation Portal (SRC-TMP)
- Managing attacks with the SRC-TMP that provides information about the nature of the attack and possible actions
- Applying policies to the interfaces to manage problem traffic, such as applying policies that reduce the amount of available bandwidth or that block the threat

The Threat Mitigation Application deals with threats in an SRC-managed environment by providing a solution that involves using:

- Juniper Networks Intrusion Detection and Prevention (IDP) sensors to detect the threats.

IDP sensors are IDP hardware appliances that run the IDP sensor software. The sensors monitor network traffic to detect suspicious or anomalous traffic and respond as configured. IDP monitors network traffic to detect potentially detrimental traffic and responds to problem incidents to prevent damage to the network.

- Juniper Networks NetScreen-Security Manager to manage the IDP sensors and to signal the SRC-TMP when a threat is detected.

NetScreen-Security Manager is software that enables you to integrate and centralize management of your Juniper Networks security environment. NetScreen-Security Manager delivers integrated, policy-based security and network management for all Juniper Networks security devices. NetScreen-Security Manager is used for its elaborate authorization and auditing functionality, which provides more detailed reporting and analysis.

- The SRC-TMP to display detailed information about the threat and the recommended actions to the administrator.

The SRC-TMP is the user interface for the Threat Mitigation Application that enables administrators to manage threats and act on them. The administrator can react to the threat by activating a service in the SAE. The service activation can result in pushing policies, for the originating IP address, to the upstream JUNOS routing platforms in the core network or to the JUNOS edge routers, depending on the configuration.

