

Accessing the SRC-TMP

To access the SRC-TMP:

1. In your Web browser, enter the name or IP address of the host and the port number on which you installed the Threat Mitigation Application in the format:

`http(s)://<host>:<port>/thmp`

A Connect to dialog box appears.

2. In the Connect to dialog box, enter your username and password, and click **OK**. The default values are:

User name—admin

Password—secret

The Threat Mitigation Portal appears.

The screenshot shows the Juniper Threat Mitigation Portal. At the top is the Juniper Networks logo. Below it is a dark blue header bar with "Threat Mitigation Portal" on the left and "Home" on the right. A left sidebar contains a menu with five items: "Home", "Action Required", "Start Pending", "Stop Pending", and "Action Taken", each with a right-pointing arrow. The main content area has the title "Threat Mitigation Portal" followed by the text "Welcome to the Threat Mitigation Portal." Below this are four bullet points with links: "Action Required Attacks", "Action Start Pending Attacks", "Action Stop Pending Attacks", and "Action Taken Attacks". Further down are two input fields: "Display 20 attacks per page." and a checkbox labeled "Page refreshes every 30 seconds." At the bottom right of the main content area is the "Juniper yourNet" logo.

3. To modify the number of attacks displayed on each page from 20, enter the number in the Display attacks per page field.
4. To modify the page refresh rate, select the Page refreshes every 30 seconds check box, and enter the number of seconds in the text box.

You can manage the attacks that fall into these categories:

- Action Required—This page displays information about the attacks that require some action to be taken. See Managing Attacks Requiring Action.
- Start Pending—This page displays the attacks that are pending service activation. See Managing Attacks Pending Service Activation.

- Stop Pending—This page displays the attacks that are pending service deactivation. See [Managing Attacks Pending Service Deactivation](#).
- Action Taken—This page displays the attacks for which some action was taken. See [Managing Attacks with Activated Services](#).

The information provided about the attacks include attack ID, source and destination addresses, attack type, severity, first and last time the event was received, action that can be taken or action that was taken, and the time that the action was taken.