

Managing Attacks with Activated Services


To manage attacks for which some action was taken:

1. In the Threat Mitigation Portal navigation pane, click **Action Taken**.

The Action Taken page displays all attack records whose status is action taken.

Action Taken Attacks

Sorted By Ordered By

Attack ID	Source	Destination	Attack Type	Severity	First Received	Last Received	Repeat Count	Action 	Action Taken Time	
20060404:33	joe@thma	hactar.kanlab.jnpr.net	ICMP EXPLOIT FLOOD	minor	Thursday, April 27, 2006 6:32:13 PM	Thursday, April 27, 2006 6:32:13 PM	1	Block Attack	Thursday, April 27, 2006 12:24:50 PM	<input type="button" value="Stop"/> <input type="button" value="Force Cleanup"/>
20051222:2	116.3.2.79	116.3.1.45	TROJAN AUTOPROXY INFECTED-HOST	critical	Thursday, December 22, 2005 7:20:57 AM	Thursday, December 22, 2005 7:20:57 AM	4	Block Attacker	Friday, December 30, 2005 11:46:35 AM	<input type="button" value="Stop"/> <input type="button" value="Force Cleanup"/>
20051222:1	116.3.1.22	116.3.3.193	FTP USER ROOT	minor	Thursday, December 22, 2005 7:18:58 AM	Thursday, December 22, 2005 7:19:58 AM	84	Block Attack	Wednesday, January 11, 2006 3:39:28 PM	<input type="button" value="Stop"/> <input type="button" value="Force Cleanup"/>



The Attack ID is linked to the Attack Details page, which displays more information about the attack record.

The help button provides information about the possible actions that can be taken in response to an attack. For example, the Help could recommend blocking the attack, blocking the attacker, or slowing the attacker.

2. To sort the attacks by a different category, select another category from the **Sorted By** drop-down list, and click **Sort**.
3. To sort the attacks in a different order, select the order from the **Ordered By** drop-down list, and click **Sort**.
4. To cancel the action, click **Stop** in that row to update the state and deactivate the service that represents the action that was taken.

If the attack is no longer in the same state as when you clicked **Stop**, the action is aborted, and a message explains that the attack has been handled. Otherwise, the result depends on whether the service is deactivated.

- If a service is deactivated, the attack is moved to the Action Required page.
 - If a service is waiting to be deactivated, the attack record is placed in a pending state and appears in the Stop Pending page.
5. To delete the attack, click **Force Cleanup** in the row for the attack.

You are responsible for ensuring that the service is deactivated. The SRC-TMP does not try to deactivate the service in this case.

- Related Topics**
- Managing Attacks Requiring Action
 - Managing Attacks Pending Service Activation
 - Managing Attacks Pending Service Deactivation
 - Configuring Attack Types in the Database
 - Enabling Actions from NetScreen-Security Manager