Cisco Secure IPS − Excluding False Positive Alarms

Document ID: 13876

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
False Positive and False Negative Alarms
The Cisco Secure IPS Exclude Mechanism
Exclude a Host
Exclude a Network
Globally Disable Signatures
Related Information

Introduction

This document describes the exclusion of false positive alarms for Cisco Secure Intrusion Prevention System (IPS).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Secure Intrusion Prevention System (IPS) version 7.0 and Cisco IPS manager Express 7.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

False Positive and False Negative Alarms

Cisco Secure IPS triggers an alarm when a given packet or sequence of packets matches the characteristics of known attack profiles defined in the Cisco Secure IPS signatures. A critical IPS signature design criterion is to minimize the occurrence of false positive and false negative alarms.

False positives (benign triggers) occur when the IPS reports certain benign activity as malicious. This requires human intervention to diagnose the event. A large number of false positives can significantly drain resources, and the specialized skills required to analyze them are costly and difficult to find.

False negatives occur when the IPS does not detect and report actual malicious activity. The consequence of this can be catastrophic and signatures must be continuously updated as new exploits and hacking techniques are discovered. Minimizing false negatives is given a very high priority, sometimes at the expense of higher occurrences of false positives.

Due to the nature of the signatures that IPSs use to detect malicious activity, it is almost impossible to completely eliminate false positives and negatives without severely degrading the effectiveness of the IPS or severely disrupting the computing infrastructure of an organization (such as hosts and networks). Customized tuning when an IPS is deployed minimizes false positives. Periodic re−tuning is required when the computing environment changes (for example, when new systems and applications are deployed). Cisco Secure IPS provides a flexible tuning capability that can minimize false positives during steady−state operations.

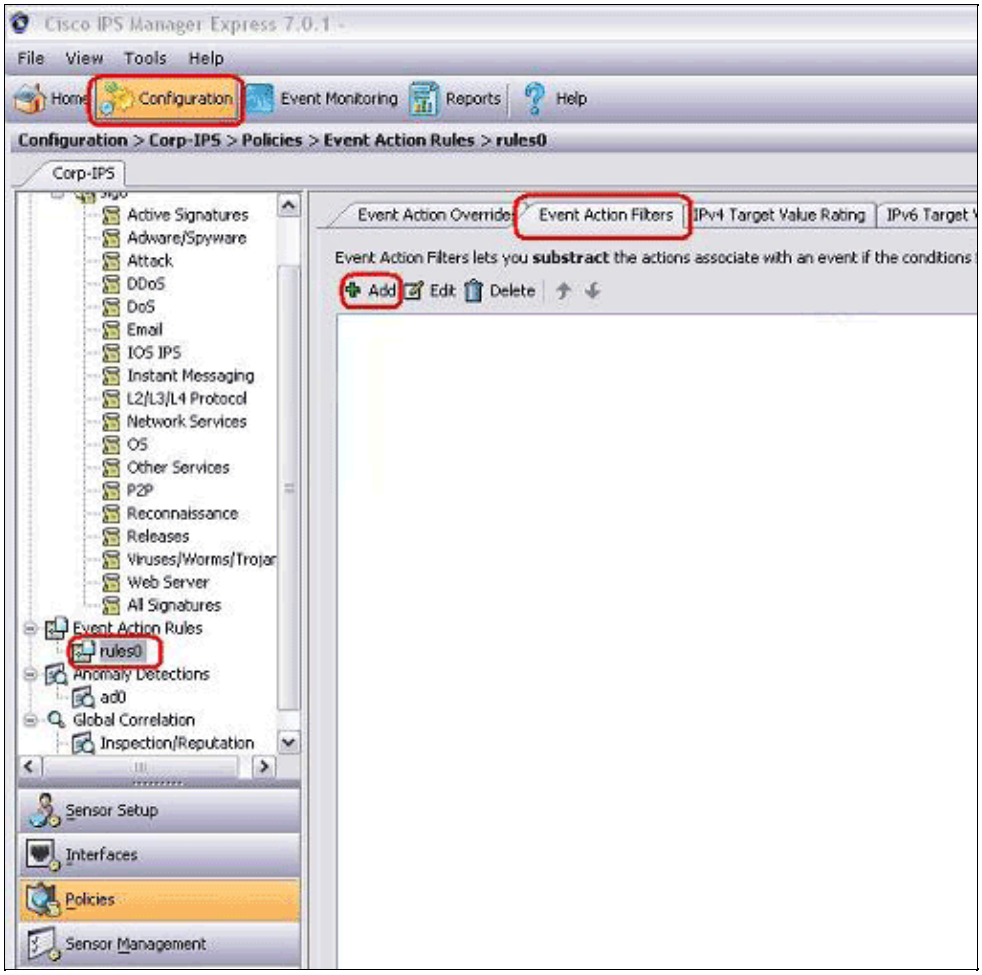
The Cisco Secure IPS Exclude Mechanism

Cisco Secure IPS provides the capability to exclude a specific signature from or to a specific host or network addresses. Excluded signatures do not generate alarm icons or log records when they are triggered from the hosts or networks that are specifically excluded through this mechanism. For example, a network management station might perform network discovery by running ping sweeps, which trigger the ICMP Network Sweep with Echo signature (signature ID 2100). If you exclude the signature, you do not have to analyze the alarm and delete it every time the network discovery process runs.

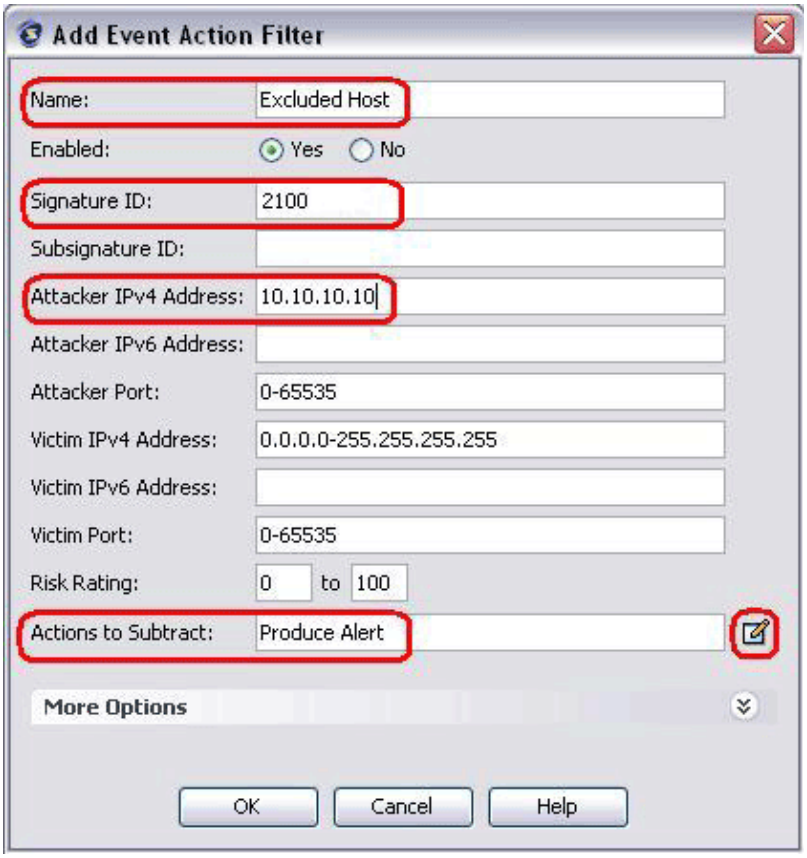
Exclude a Host

Complete these steps in order to exclude a specific host (a source IP address) from generating a specific signature alarm:

1. Choose **Configuration > Corp−IPS > Policies > Event Action Rules > rules0**, and click the **Event Action Filters** tab.



2. Click **Add**.
3. Type the filter name, signature ID, attacker's IPv4 address, and action to subtract in the appropriate fields, and then click **OK**.



Note: If you need to exclude multiple IP addresses from different networks, you can use the comma as a delimiter. However, if you use a comma, avoid the trailing space after the comma; otherwise, you might receive an error.

Note: In addition, you can use the variables defined in the Event Variables tab. These variables are useful when the same value must be repeated in multiple event action filters. You must use a dollar sign ($) as a prefix to the variable. The variable can be one of these formats:

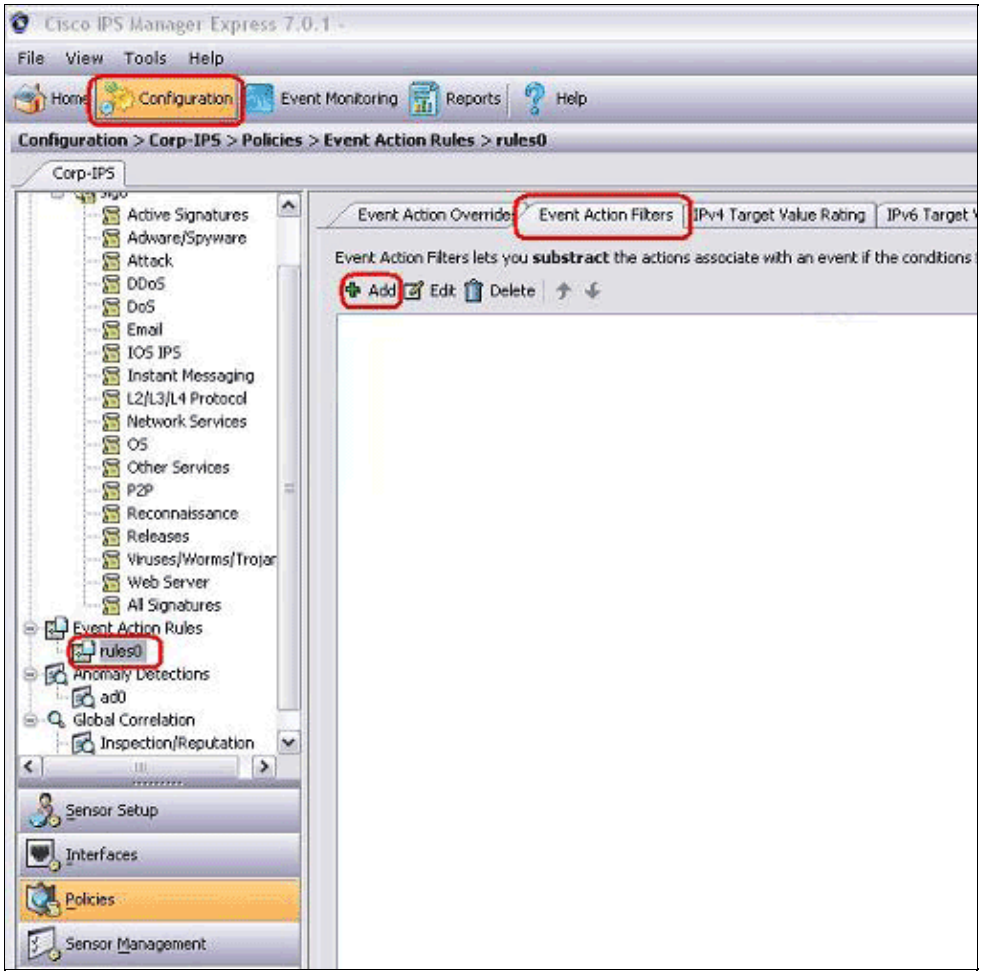
- Full IP address; for example, 10.77.23.23.
- Range of IP addresses; for example, 10.9.2.10−10.9.2.155.
- Set of range of IP addresses; for example, 172.16.33.15−172.16.33.100,192.168.100.1−192.168.100.11.

Exclude a Network

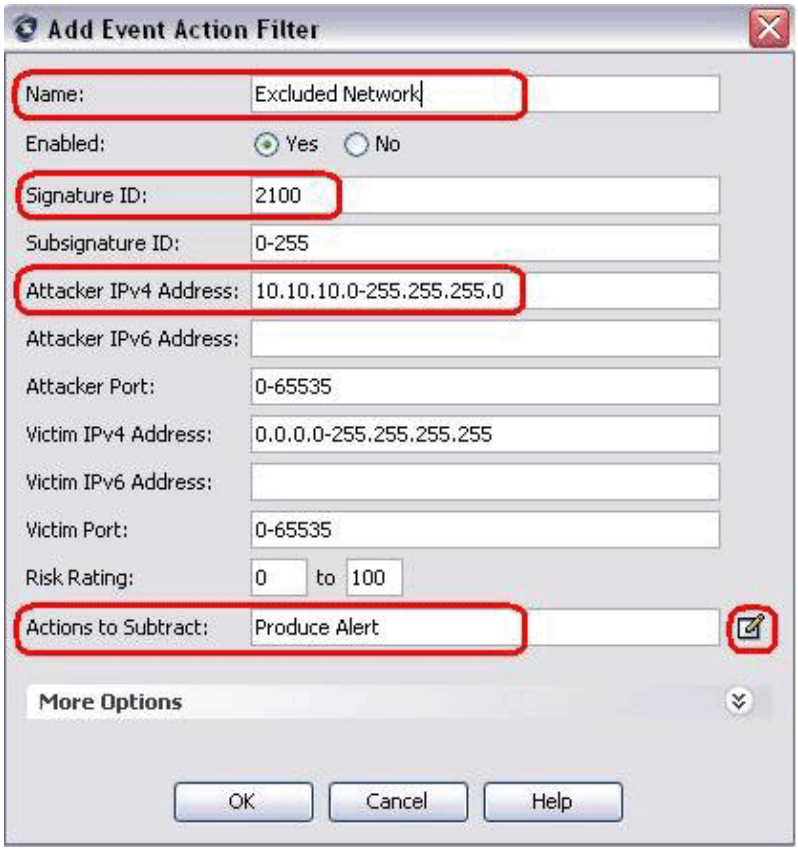
The Event Action Filter also excludes specific signatures to fire an alarm based on a source or destination network address.

Complete these steps in order to exclude a network from generating a specific signature alarm:

1. Click the **Event Action Filters** tab.



2. Click **Add**.
3. Type the filter name, signature ID, network address with subnet mask, and action to subtract in the appropriate fields, and then click **OK**.

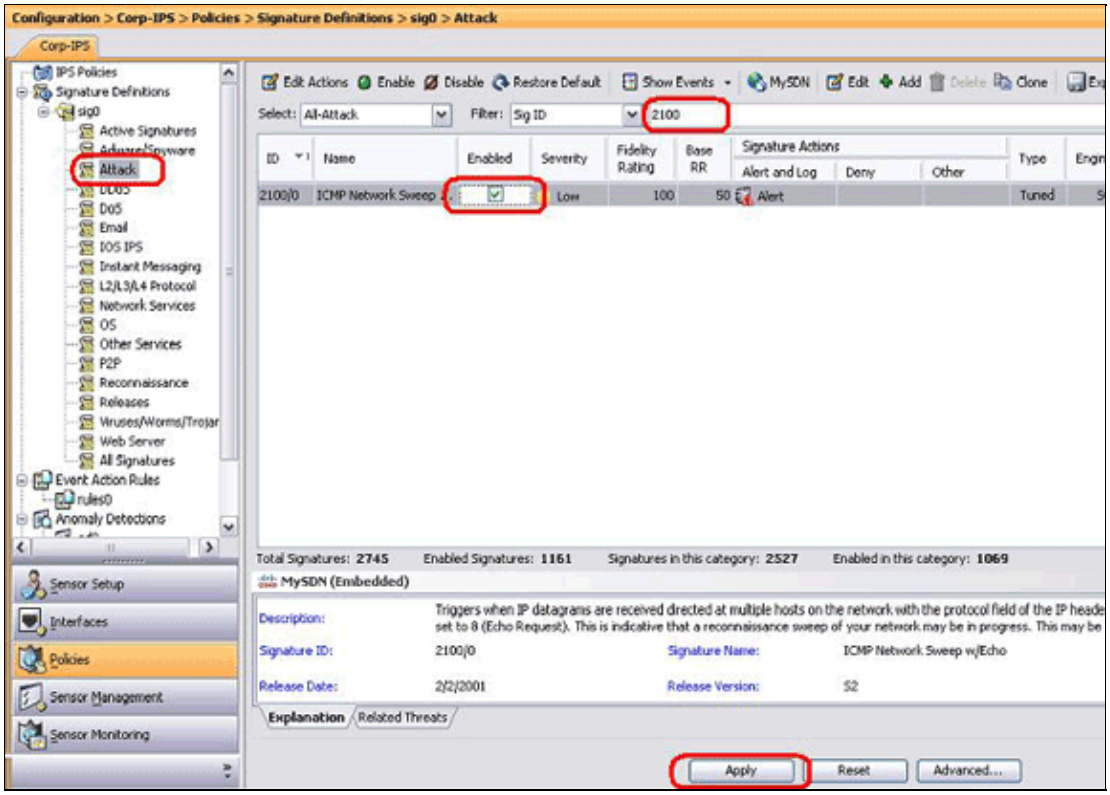


Globally Disable Signatures

You might want to disable a signature from alarming at any time. In order to enable, disable, and retire signatures, complete these steps:

1. Log in to IME using an account with Administrator or Operator privileges.
2. Choose **Configuration** > **sensor_name** > **Policies** > **Signature Definitions** > **sig0** > **All Signatures**.
3. In order to locate a signature, choose a sorting option from the Filter drop−down list. For example, if you are searching for a ICMP Network Sweep signature, choose **All Signatures** under sig0, then search by signature ID or name. The sig0 pane refreshes and displays only those signatures that match your sorting criteria.
4. In order to enable or disable an existing signature, choose the signature, and complete these steps:

    a. View the Enabled column to determine the status of the signature. A signature that is enabled has the check box checked.
    b. In order to enable a signature that is disabled, check the **Enabled** check box.
    c. In order to disable a signature that is enabled, uncheck the **Enabled** check box.
    d. In order to retire one or more signatures, choose the signature(s), right−click, and then click **Change Status To > Retired**.
5. Click **Apply** in order to apply your changes and save the revised configuration.



Related Information

- **End of Sale for the Cisco Secure IDS Director**
- **Cisco Secure Intrusion Detection Support Page**
- **Documentation for Cisco Secure Intrusion Detection System**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 26, 2009 Document ID: 13876
