



## **Cisco SCA BB Service Security Note**

Release 5.1.x  
March 12, 2015

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide.  
Addresses, phone numbers, and fax numbers  
are listed on the Cisco website at  
[www.cisco.com/go/offices](http://www.cisco.com/go/offices).

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

*Cisco SCA BB Service Security Note*

© 2015 Cisco Systems, Inc. All rights reserved.



**Preface 1**

- Introduction 1
- Document Revision History 2
- Organization 3
- Conventions 4
- Obtaining Documentation and Submitting a Service Request 5

---

**CHAPTER 1**

**Introduction and Scope 1-1**

- Introduction 1-1
- Introduction and Scope 1-1

---

**CHAPTER 2**

**Functionality Overview 2-1**

- Introduction 2-1
- Functionality Overview 2-1

---

**CHAPTER 3**

**Anomaly-Based Detection 3-1**

- Introduction 3-1
- Overview 3-2
- Configuring Anomaly Detection 3-3
  - General Concepts in Anomaly Detection Configuration 3-3
- Monitoring Malicious Traffic 3-14
  - Top Scanned or Attacked Ports 3-15
  - Global Scan or Attack Rate 3-16
  - Global DoS Rate 3-17
  - Infected Subscribers 3-18
  - Top Scanning or Attacking Hosts 3-19
  - Top Scanning or Attacking Subscribers 3-20
  - Top DoS Attacked Hosts 3-21
  - Top DoS Attacked Subscribers 3-22

---

**CHAPTER 4**

**Mass-Mailing-Based Threats 4-1**

- Introduction 4-1
- Mass-Mailing-Based Threats 4-1

Configuration of Mass-Mailing Detection 4-2  
Monitoring Mass Mailing Activity 4-3



# Preface

---

**Published: March 12, 2015**

## Introduction

This chapter describes who should read *Service Security Using the Cisco SCE Platform Application Note*, how it is organized, its document conventions, and how to obtain documentation and technical assistance. This guide assumes a basic familiarity with the concept of the Cisco Service Control solution, the Service Control Engine (SCE) platforms, and related components.

This document provides an introduction to Service Security using the Cisco SCE.

# Document Revision History

Table 1 lists the document revision history.

**Table 1**      **Document Revision History**

<b>Cisco Service Control Release and Date</b>	<b>Change Summary</b>
Supports all 5.0.x releases July 30, 2014	First release of the train.

# Organization

Table 2 provides the organization of the document.

**Table 2**      **Document Organization**

<b>Section</b>	<b>Title</b>	<b>Description</b>
1	<a href="#">Introduction and Scope</a>	This chapter provides an introduction to Service Security using the Cisco SCE.
2	<a href="#">Functionality Overview</a>	This chapter provides an overview of the service security functionality of the SCE platform.
3	<a href="#">Anomaly-Based Detection</a>	This chapter describes anomaly-based detection by using the Cisco SCE platform.
4	<a href="#">Mass-Mailing-Based Threats</a>	This chapter introduces the concept of mass-mailing based threats and how to protect against them by using the SCE.

# Conventions

Table 3 lists the conventions used in the document.

**Table 3** Document Conventions

Convention	Indication
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[ ]	Elements in square brackets are optional.
{ x   y   z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



**Note**

Means *reader take note*.



**Tip**

Means *the following information will help you solve a problem*.



**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



**Warning**

**Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**



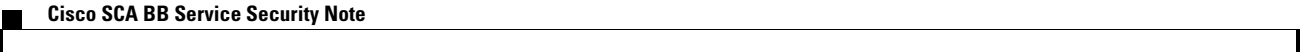
---

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





# Introduction and Scope

---

Published: March 12, 2015

## Introduction

This chapter provides an introduction to Service Security using the Cisco SCE.

## Introduction and Scope

The need for protection from various types of attacks and malicious traffic that originate from the Internet has gained focus in recent years. Denial of service (DoS) and distributed denial of service (DDoS) attacks, worms, viruses, malicious HTTP content, and various types of intrusions are becoming increasingly common.

Cisco SCE platforms are deployed inline and are stateful and programmable. These features position the SCE platform to detect and mitigate the effect of malicious traffic on service providers and their customers.

Cisco Service Control Application for Broadband (SCA BB) includes Service Security functionality comprising anomaly detection, spam or mass-mailing detection, and signature detection. This functionality allows the SCE platform to address many of the threats that exist in current networks.

The Cisco SCA BB solution is not an airtight solution against network threats. The solution is effective in providing an insight into malicious activity in an operator network, and in mitigating large-scale eruptions of malicious activity that might compromise overall network performance and degrade user experience.

This guide contains practical sections describing the specifics of configuration and reporting. The purpose is to explain and demonstrate the Service Security concepts. For a full operational description of the relevant management modules, see the Cisco SCA BB user guides.





# Functionality Overview

---

Published: March 12, 2015

## Introduction

This chapter provides an overview of the service security functionality of the SCE platform.

## Functionality Overview

The Cisco SCE platform uses three approaches for threat detection:

- Anomaly detection—This set of mechanisms monitors the rate of connections (successful and unsuccessful) to and from each host IP address. It detects malicious activity based on exceeding “normal” connection rates and on the ratio between successful and unsuccessful connections. Anomaly detection characteristics can indicate the following categories of malicious activity:
  - Scan/Sweep/Attack—Based on an indication that a host is generating an anomalous rate of connections.
  - DoS/DDoS—Based on an indication that a host is a target for an anomalous rate of connections.
  - DoS—Based on an indication that a pair of hosts is involved in an activity where one is generating, and the other one is a target, for an anomalous rate of connections.

The anomaly detection mechanism is effective in addressing zero-day threats—addressing threats as they appear, without the need for preliminary knowledge about their exact nature and Layer 7 signatures, based on the characteristics of their network activity.

For further details, see [Chapter 3, “Anomaly-Based Detection.”](#)

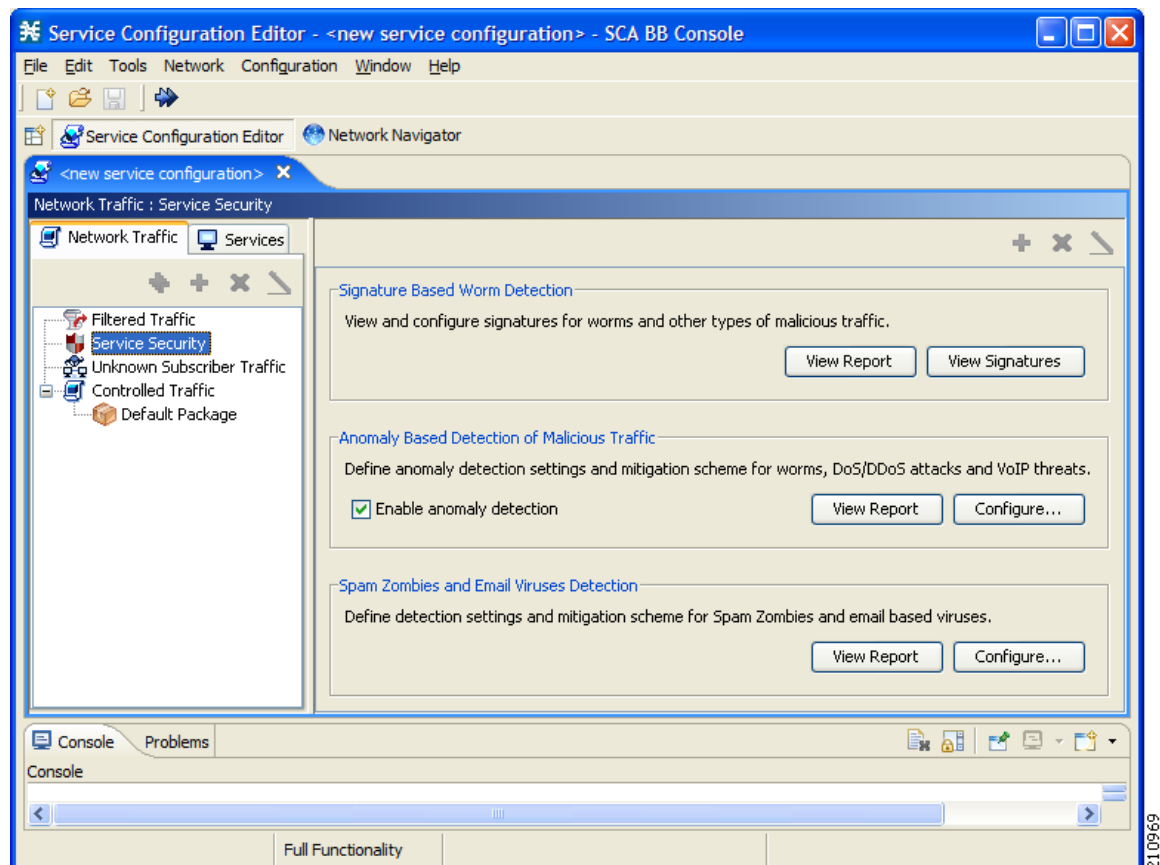
- Mass-mailing activity detection—This mechanism is based on monitoring Simple Mail Transfer Protocol (SMTP) session rates for individual subscribers. It uses the subscriber-awareness of the Cisco SCE platform and can work in subscriber-aware or anonymous subscribers mode. SMTP is a protocol used for sending email; an excess rate of such sessions originating from an individual subscriber is usually indicative of malicious activity involving sending email, that is, either mail-based viruses or spam-zombie activity.
- Signature-based detection—The SCE platform provides stateful Layer 7 capabilities that can be used to detect malicious activity, which is not easily detectable by the other mechanisms. A user can independently configure signatures for such threats, thus achieving a fast turnaround time in addressing threats. Details on signature-based detection is not covered in this document.

All three detection approaches provide operators with several possible courses of action to be implemented based on their business needs.

- **Monitor**—Inspect the network for malicious activity detected by each of these methods. This can be done by using reports that are based on information collected for malicious activity that was detected, or by using SNMP traps that can detect malicious activity using the anomaly detection module.
- **Block**—Automatically block malicious activity, that the SCE platform detected, to avoid threat propagation and adverse effects to the network.
- **Notify**—Notify subscribers that they have been detected as being involved in malicious activity by redirecting their web sessions to a captive portal.

Operators have a high level of flexibility in tuning the detection methods and actions to be taken based on their specific needs. The SCA BB Security Dashboard as shown in [Figure 2-1](#) is a GUI application that provides a simple front end for configuring and monitoring security functionality.

**Figure 2-1 SCA BB Security Dashboard**





# Anomaly-Based Detection

---

Published: March 12, 2015

## Introduction

This chapter describes anomaly-based detection by using the Cisco SCE platform. It consists of these sections:

- [Overview, page 3-2](#)
- [Configuring Anomaly Detection, page 3-3](#)
- [Monitoring Malicious Traffic, page 3-14](#)

# Overview

The most comprehensive threat detection module is the anomaly detection module. The module monitors successful (correctly established for TCP, bidirectional otherwise) and unsuccessful (uni-directional, also termed “suspected”) connection rates to and from any IP address viewed by the system. It triggers the detection of an anomaly based on one of the following criteria:

- Total connection rate exceeded a predefined threshold.
- OR
- Suspected connection rate exceeded a predefined threshold, and suspected-to-unsuspected connections ratio exceeded a predefined threshold.

The ratio metric is a robust indicator for malicious activity, and together with a rate qualifier, serves as a reliable identifier for malicious activity.

Anomaly detection is split into categories based on the directional nature of anomalies as described in the following subsections. The concepts used by the three methods are identical, but they differ in the role of the endpoint that is monitored for the anomaly.

Scan/Sweep/Attack is a category of malicious activity that is based on detecting an anomaly in the connection rate from an IP address. In this case, the module ignores the destination IP addresses involved.

The anomaly is detected based on the criteria specified in the previous paragraphs and can indicate one of the following:

- An attack—A host is participating in an attack on another host.
- A sweep—A host is sweeping the network in search of a vulnerable host. This activity is typical of network worms.
- A scan—A host is scanning the ports of other hosts to find out what services they are using and which ports are potentially vulnerable.

A DoS attack is detected based on an anomaly in the connection rate between a pair of hosts. One host is attacking the other. This attack can be either an isolated attack, or part of a larger scale DDoS attack.

A DDoS attack is detected based on an anomaly in the connection rate to an IP address. The module ignores the source IP addresses involved. A high connection rate indicates that the destination IP address is being attacked. The attack can be from either a single IP address (DoS) or multiple IP addresses (DDoS).

For many types of anomalies, flexibility is reflected in the ability to define detection thresholds and the action to be taken for each:

- Anomaly direction (subscriber/network)
- Protocol (TCP/UDP/ICMP/Other)
- Port uniqueness for TCP/UDP—Whether the anomaly threshold is applicable to a single port or the aggregate of ports.

The malicious traffic reports family in the reporter contains reports that allow monitoring different aspects of malicious activity.

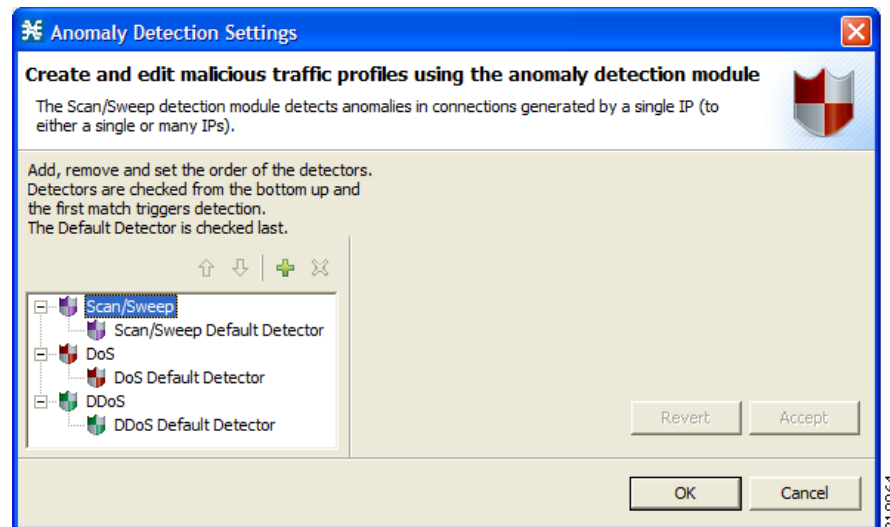


# Configuring Anomaly Detection

The configuration screen for anomaly detection shows the “tree” of various detectors (Figure 3-1). The tree comprises the three categories of anomalies.

The three categories are separate from a configuration perspective—Scan/Sweep, DoS, and DDoS.

**Figure 3-1** Configuring Anomaly Detection



210964

## General Concepts in Anomaly Detection Configuration

- [Detector Structure, page 3-3](#)
- [Configuring Detection Thresholds, page 3-5](#)
- [Configuring Actions, page 3-6](#)
- [Default Detector, page 3-6](#)
- [Additional Detectors, page 3-7](#)

### Detector Structure

The terms used in anomaly detection are described in this chapter. The term “related to” is used extensively; however, its meaning depends on the semantics of each anomaly and is mentioned in the description for each category of anomalies (Scan/Sweep/Attack, DoS, and DDoS).

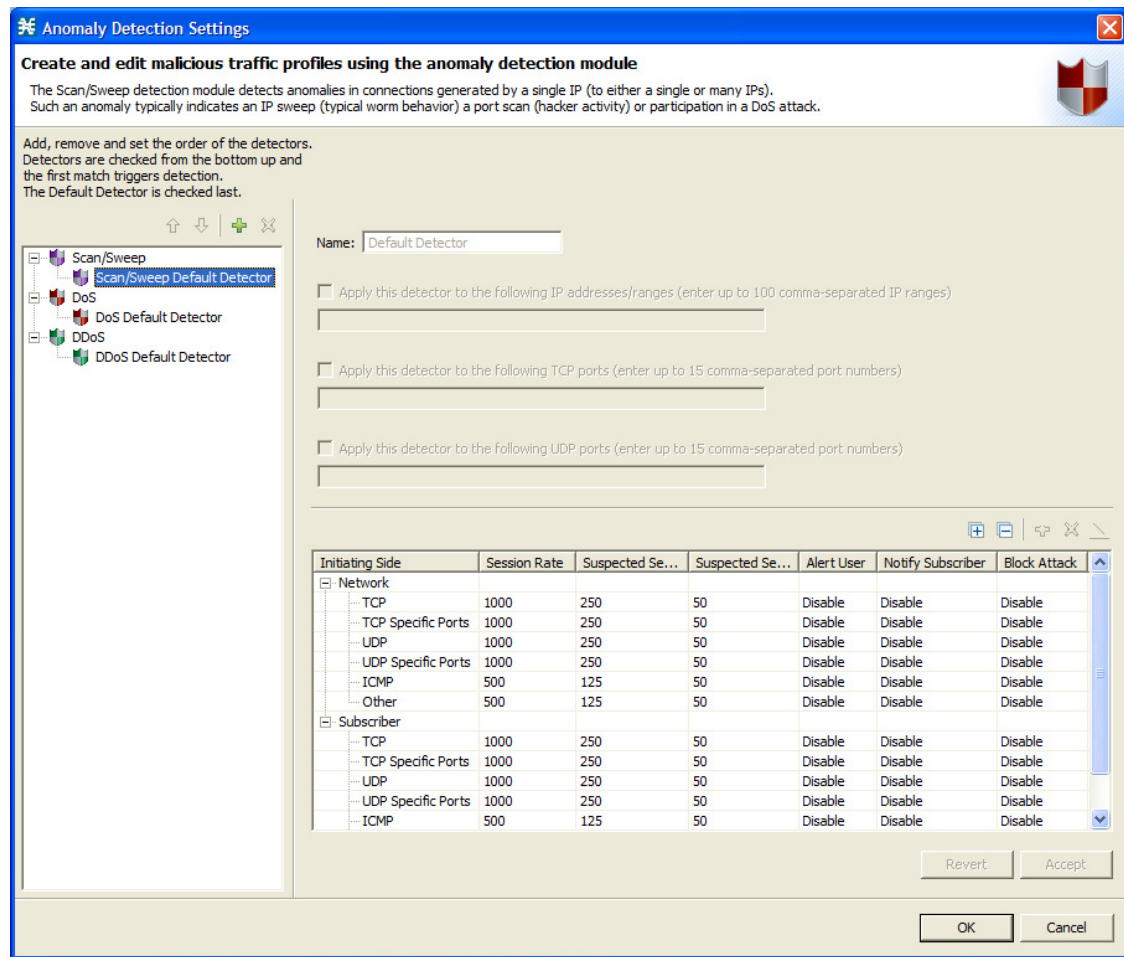
The first level of hierarchy within the detector contains two subcategories: Subscriber and Network. The Subscriber subcategory refers to malicious traffic related to IP addresses that are on the subscriber port. The Network subcategory refers to malicious traffic related to IP addresses that are on the network port.

These subcategories allow an operator to act on anomalies that are related to either the subscriber or network side (see Figure 3-2).

Under each subcategory, six further granular subcategories exist:

- TCP—Refers to anomalies in connection rate related to a host over any TCP destination port. The aggregate rate of connections on all TCP ports is applicable for matching this rule.
- TCP Specific—Refers to anomalies in connection rate related to a host over any specific TCP destination port. For example, the rate of connections related to a specific host on port 80 is applicable for matching this rule, as well as the rate of connections related to a host over each of the TCP ports 23, 25, 110 (and any specific TCP port).
- UDP—Refers to anomalies in connection rate related to a host over any UDP destination port. The aggregate rate of connections on all UDP ports is applicable for matching this rule.
- UDP Specific—Refers to anomalies in connection rate related to a host over any specific UDP destination port. For example, the rate of connections related to a host on port 53 is applicable for matching this rule, as well as the rate of connections generated by a host over each UDP port.
- ICMP—Refers to anomalies in the connection rate related to a host using Internet Control Message Protocol (ICMP).
- Other—Refers to anomalies in the connection rate related to a host using non-TCP/UDP/ICMP protocols.

**Figure 3-2** Detector Structure



210967

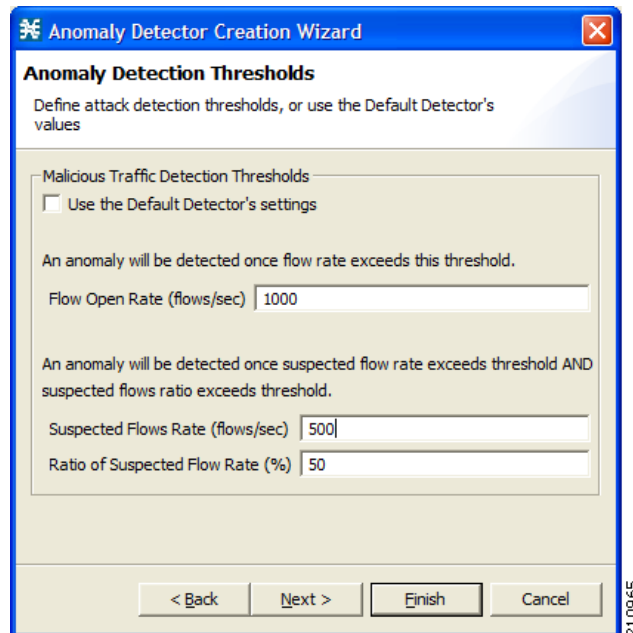
## Configuring Detection Thresholds

The configuration of specific detection parameters and related actions is carried out on a per subcategory basis (see [Figure 3-3](#)).

The configurable detection parameters for each anomaly subcategory are:

- Session Rate**—Refers to the threshold of session-rate (sessions per second for an IP address) that for itself would trigger the anomaly of this type.  
 For example, configuring the value 1000 on the session-rate for the TCP anomaly means that if a rate of 1000 TCP sessions per second (on any port) was detected from a host, the anomaly would be triggered.
- Suspected Session Rate**—Refers to the threshold of suspected-sessions-rate (suspected-sessions per second) that for itself would trigger the anomaly line item.  
 Suspected sessions are TCP sessions that were not properly established or unidirectional sessions for other protocols (UDP/ICMP/Other).  
 This parameter is used with the suspected-sessions ratio as an indicator of a traffic anomaly—a relatively high session-rate for which a large number do not respond typically indicates malicious activity.  
 For example, configuring the value 1000 suspected-sessions per second for the TCP anomaly means that if a rate of 1000 TCP suspected-sessions per second (on any port) was detected from a host, and the suspected connection-ratio crossed the predefined threshold, the anomaly would be triggered.
- Suspected Sessions Ratio**—The ratio between the suspected-sessions rate and the total session-rate. A high ratio indicates a high amount of “unresponsive” sessions, which indicates a malicious activity.

**Figure 3-3** Configuring Detection Thresholds



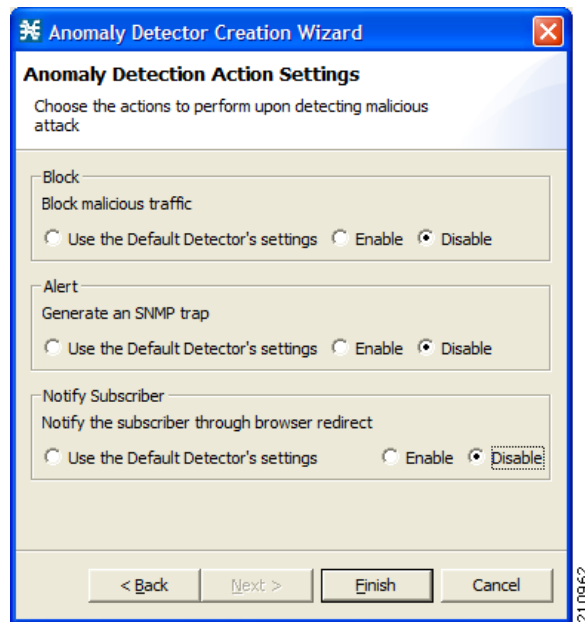
## Configuring Actions

Each anomaly subcategory also includes an option to define the action to be taken upon detection. It is not possible to configure, for each anomaly subcategory, logging to an on-device log file and to the Collection Manager database through SCE Raw Data Records (RDRs). To enable and disable RDRs for malicious traffic, from the Configuration menu, select RDR Settings (Figure 3-4).

There are three independent and not mutually exclusive actions that are configurable per item:

- **Alert**—Generate an SNMP trap (see Pcube proprietary MIB for details) indicating the beginning and end of such an attack.
- **Notify Subscriber**—Notify a subscriber of the malicious activity by redirecting the browsing sessions to a captive portal. To configure a subscriber notification, from the Configuration menu select **Subscriber Notifications**, then select **Network Attack Notification**. See the *Cisco Service Control Application for Broadband User Guide* for subscriber notification options.
- **Block**—Block the relevant session. Blocking is performed based on the specification of the malicious traffic that triggered the anomaly. For instance, if the anomaly detected is a port agnostic TCP scan from the subscriber side, all TCP sessions originating from the subscriber side is blocked. Blocking continues until the anomaly disappears. SCE removes the blocking intermittently and verifies whether the anomaly persists. If the subscriber notification is enabled for the anomaly, SCE does not block the port relevant for browsing (by default, TCP port 80).

**Figure 3-4** Anomaly Detection Action Settings



## Default Detector

For each category of malicious traffic, a default detector exists. You cannot remove this default detector. This default detector is preconfigured with factory defaults for thresholds and actions.

## Additional Detectors

For each category of malicious traffic (Scan/Sweep, DoS, DDoS), additional detectors can be defined under the default detector (see [Figure 3-5](#)). You can define a maximum of 100 detectors in the three categories combined.

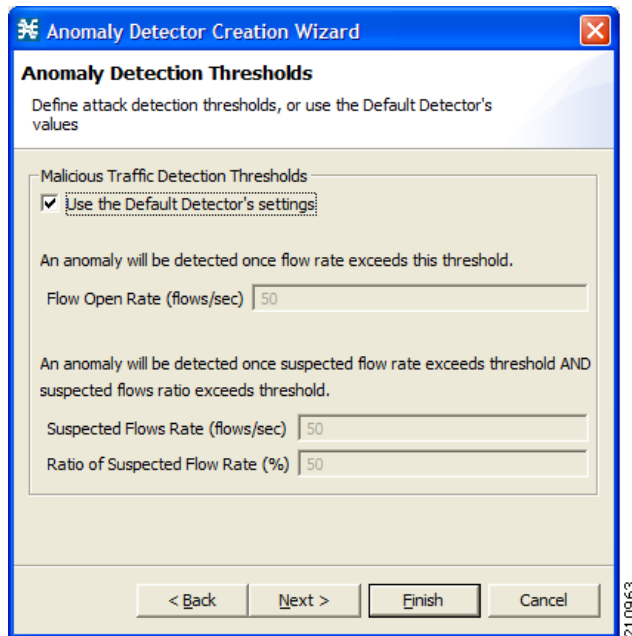
Such a detector applies to an IP Address list, a UDP port list, a TCP port list, or a combination of the three. The detector should contain different thresholds and different actions to be applied for anomalies that match the list.

For example, it is possible to have a DDoS detector, which corresponds to an IP address with no specific port, or to have another detector which monitors specific port attacks (for example, DNS or SMTP detectors). Another example is detectors that are targeted at a specific worm, and therefore, include a specific list of ports.

You can apply additional detectors to one or more of the subcategories of the anomaly. For example, if you create a DDoS detector for a specific IP list, and choose to apply it only for specific port attacks from the subscriber side. The new detector need not cover all “potential” subcategories of DDoS.

When creating a new anomaly subcategory, you must define the actions to take; but, you can choose to use custom detection thresholds, or to inherit detection thresholds from the default detector.

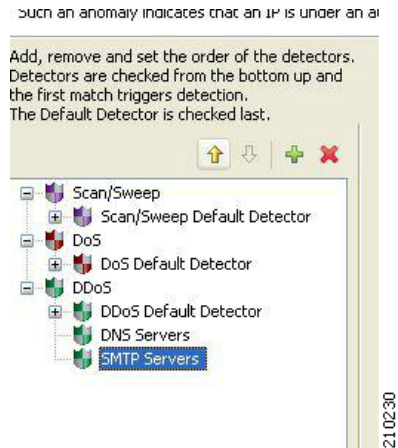
**Figure 3-5** Anomaly Detector Wizard



An anomaly can be triggered by exactly one detector. The order of detection is from the bottom of the list and up. The first detector that “matches” the anomaly threshold, together with the IP/Port list specification, sets the decision on the actions to take.

Use the up and down arrows above the anomaly tree window to arrange the detector in each category into the desired order (see [Figure 3-6](#)).

**Figure 3-6** Anomaly Tree



## Scan/Sweep Detector

The scan/sweep detector detects anomalies in connections generated by a host (see [Figure 3-7](#)). These anomalies include total-connection-rate, suspected-connections-rate, and suspected-connections-ratio.

A high ratio of suspected connections generated by a host, beyond some minimal rate, typically indicates the presence of a worm that tries to propagate by sweeping the network for vulnerable hosts. The presence of a worm is even more obvious when an anomaly is detected on a specific port over which the vulnerability exists—this would typically trigger the TCP/UDP-specific anomalies.

In addition, port scans and attacks performed by a host are also included in this category. Port scans are typically characterized by a high ratio of suspected connections, while host attacks can be either normal or suspected connections. Both types of malicious traffic could be detected by the non-port-specific anomaly detectors.

The first level of hierarchy within the detector contains two subcategories—Subscriber and Network. The Subscriber subcategory refers to scans, sweeps, and attacks that were detected from IP addresses that are on the subscriber port side. The Network subcategory refers to scans, sweeps, and attacks that were detected from IP addresses that are on the network port side.

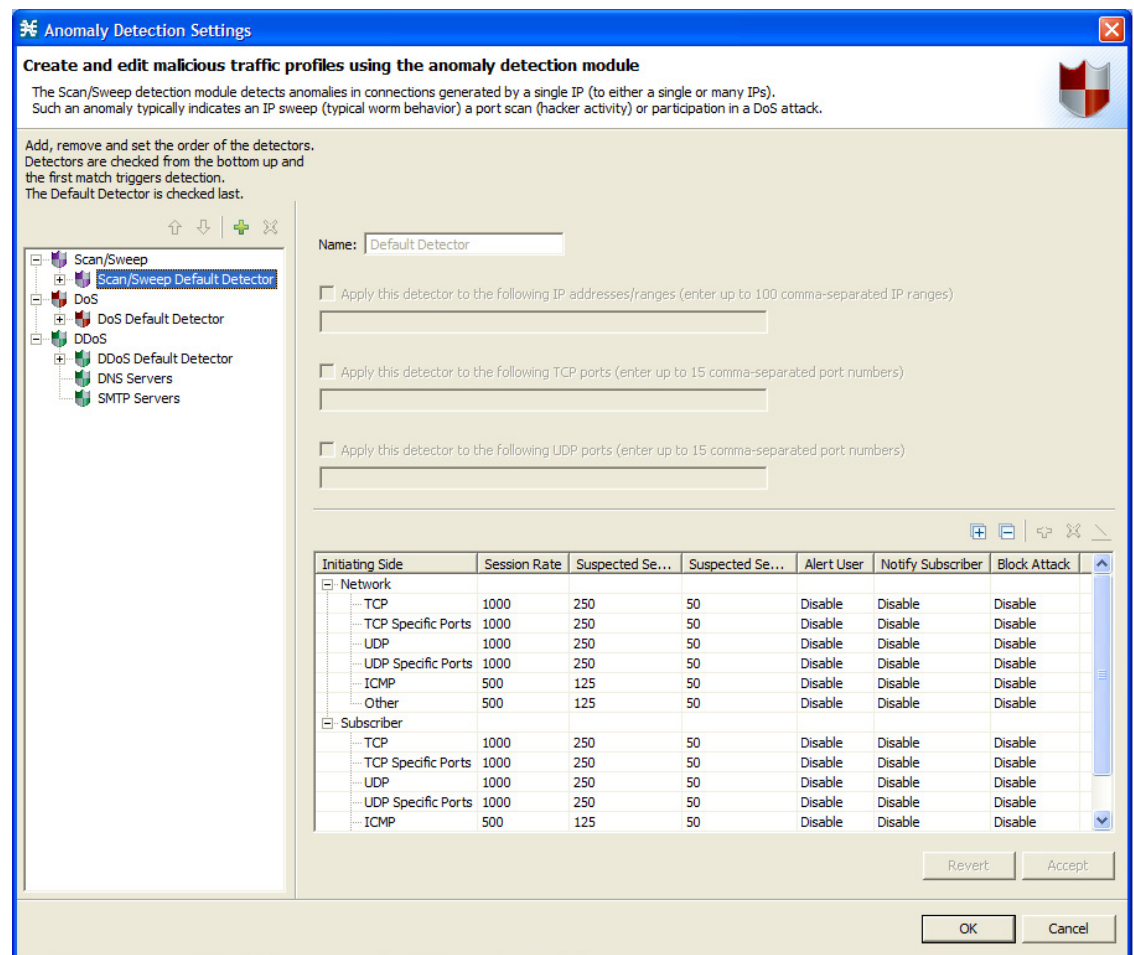
These subcategories allow an operator to act on Scan/Sweep/Attack anomalies that originate from either the subscriber or network side.(see [Figure 3-7](#)).

Under each subcategory, six further granular subcategories exist:

- **TCP**—Refers to anomalies in the aggregate connection rate generated by a host over all TCP destination ports. For example, the aggregate rate of connections generated by a host to ports 23, 25, 80, 110, and any other TCP port is applicable for matching this rule.
- **TCP Specific**—Refers to anomalies in the connection rate generated by a host to any specific TCP destination port. For example, the rate of connections generated by a host to port 80 is applicable for matching this rule, as well as the rate of connections generated by a host to any other individual TCP port.
- **UDP**—Refers to anomalies in the aggregate connection rate generated by a host to all UDP destination ports. For example, the aggregate rate of connections generated by a host to ports 53, 445, and any other UDP port is applicable for matching this rule.

- UDP Specific—Refers to anomalies in the connection rate generated by a host to any specific UDP destination port. For example, the rate of connections generated by a host to port 53 is applicable for matching this rule, as well as the rate of connections generated by a host to any other individual UDP port.
- ICMP—Refers to anomalies in the connection rate related to a host using Internet Control Message Protocol (ICMP).
- Other—Refers to anomalies in the connection rate related to a host using non-TCP/UDP/ICMP protocols

**Figure 3-7 Scan/Sweep Default Detector**



## DDoS Detector

The DDoS detector detects anomalies in connections for which a host is a destination (Figure 3-8). These anomalies include total-connection-rate, suspected-connections-rate, and suspected-connections-ratio.

A high rate of connections to an IP address indicates that the IP address is being attacked.

A better indicator that an IP is being attacked is when there is a high suspected-sessions rate, in addition to a high suspected-sessions ratio.

The DDoS detector module detects DoS and DDoS attacks without differentiating between them because the module does not track the IP addresses involved in generating the connection.

The first level of hierarchy within the detector contains two subcategories: Subscriber and Network. The Subscriber subcategory refers to attacks that were detected on IP addresses that are on the subscriber port side. The Network subcategory refers to attacks that were detected on IP addresses that are on the Network port side.

These subcategories allow an operator to act on anomalies that are towards either the subscriber or network side. (see [Figure 3-8](#)).

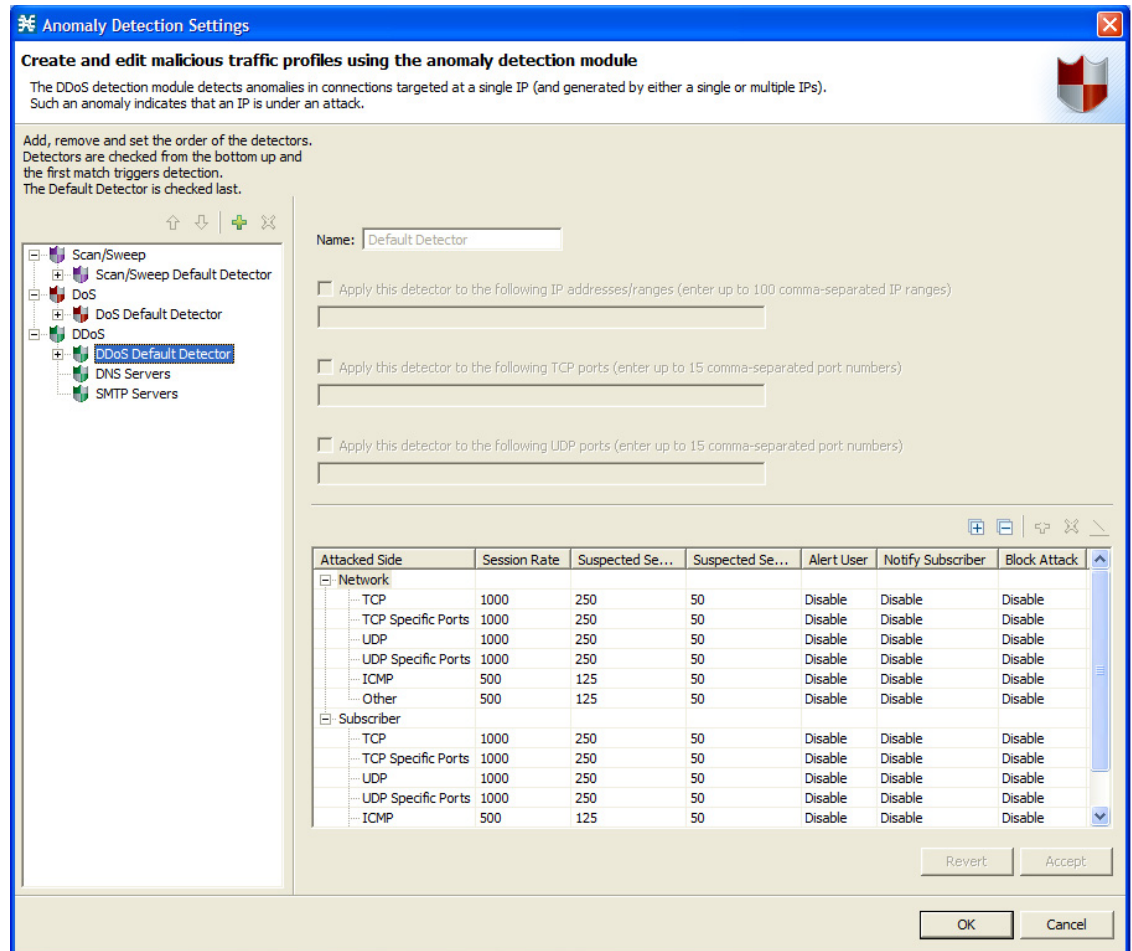
An operator might consider protecting subscribers from suspected attacks, while not doing this for network side activity, in order to not affect legitimate activity by subscribers who are falsely detected as participating in an attack.

Under each subcategory, six further granular subcategories exist:

- **TCP**—Refers to anomalies in the aggregate connection rate to a host over all TCP destination ports. For example, the aggregate rate of connections to ports 23, 25, 80, 110, and any TCP port is applicable for matching this rule.
- **TCP Specific**—Refers to anomalies in the connection rate to a host over any specific TCP destination port. For example, the rate of connections to a host on port 80 is applicable for matching this rule, as well as the rate of connections to a host on any other individual TCP port.
- **UDP**—Refers to anomalies in the connection rate to a host over all UDP destination ports. For example, the aggregate rate of connections to ports 53, 445, and any UDP port is applicable for matching this rule.
- **UDP Specific**—Refers to anomalies in the connection rate to a host over any specific UDP destination port. For example, the rate of connections to a host on port 53 is applicable for matching this rule, as well as the rate of connections to a host over any other individual UDP port.
- **ICMP**—Refers to anomalies in the connection rate related to a host using Internet Control Message Protocol (ICMP).
- **Other**—Refers to anomalies in the connection rate related to a host using non-TCP/UDP/ICMP protocols



Figure 3-8 DDoS Default Detector



## DoS Detector

The DDoS detector detects anomalies in connections between a pair of hosts. These anomalies include total-connection-rate, suspected-connections-rate, and suspected-connections-ratio. .

A high rate of connections between a pair of hosts may be an indicator that the source host is attacking the destination host.

A better indicator that one host is attacking the other is when there is a high suspected-sessions rate, with a high suspected-connections ratio.

This module monitors the rate of connections between a pair of hosts. This can include DoS and DDoS attacks without differentiating between them because there can be multiple hosts attacking the destination host, which the module may not explicitly detect.

The first level of hierarchy within the detector contains two subcategories—Subscriber and Network. The Subscriber subcategory refers to attacks that were detected from IP addresses that are on the subscriber port side. The Network subcategory refers to attacks that were detected from IP addresses that are on the Network port side.

These subcategories allow an operator to act on anomalies that are coming from either the subscriber or network side (see Figure 3-9).

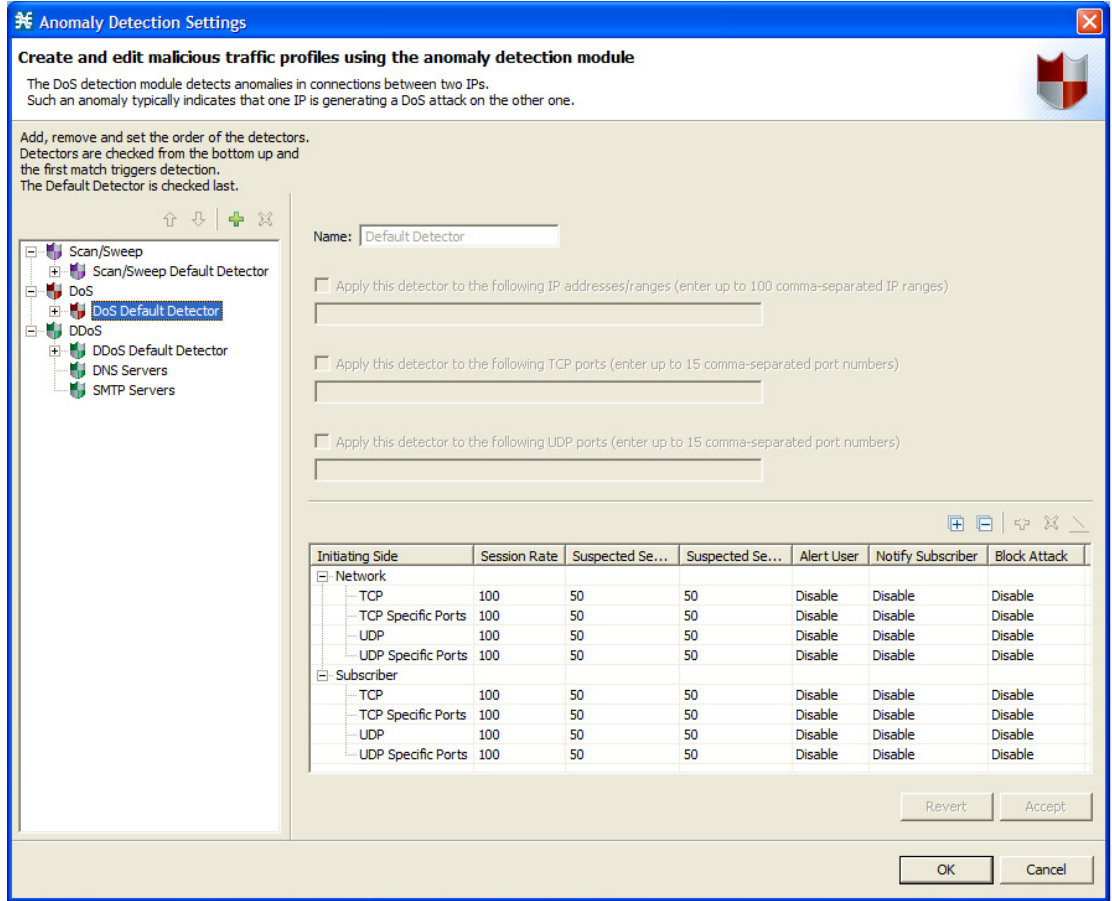
An operator might consider protecting subscribers from suspected attacks directed at them, but not doing this for network side activity, in order to not affect legitimate activity by subscribers who are falsely detected as participating in an attack.

Under each subcategory, four further granular subcategories exist:

- **TCP**—Refers to anomalies in the aggregate connection rate between a pair of hosts over all TCP destination ports. The aggregate rate of connections between a pair of hosts on ports 23, 25, 80, 110, and all other TCP ports is applicable for matching this rule.
- **TCP Specific**—Refers to anomalies in the connection rate between a pair of hosts over any specific TCP destination port. For example, the rate of connections between a pair of hosts on port 80 is applicable for matching this rule, as well as the rate of connections between a pair of hosts on any other individual TCP port.
- **UDP**—Refers to anomalies in the aggregate connection rate between a pair of hosts over all UDP destination ports. For example, the aggregate rate of connections between a pair of hosts on ports 53, 445, and all other UDP ports is applicable for matching this rule.
- **UDP Specific**—Refers to anomalies in the connection rate between a pair of hosts over any specific UDP destination port. For example, the rate of connections between a pair of hosts on port 53 is applicable for matching this rule, as well as the rate of connections between a pair of hosts over any other individual UDP port.

The ICMP category and the Other category do not exist for DoS detection because connections between a pair of hosts using these protocols cannot be distinguished from one another.

Figure 3-9 DoS Default Detector



210968

# Monitoring Malicious Traffic

Information about traffic anomalies detected using the scan/sweep and the DDoS modules is sent over RDRs and is stored in the Collection Manager database. This information can be used to find network trends, detect new threats, and track malicious hosts or subscribers.

Because the anomaly detection is based on session rate threshold breaches, the actual information stored in the database can vary, depending on the detection thresholds set.

For example, it is possible that scan/sweep reports generated for a system with thresholds set at 100 sessions per second would look notably different (much more loaded with events) than reports generated for a system with thresholds set at 1000 sessions per second (assuming traffic patterns are identical for both systems).

There are a number of reports dealing with malicious traffic.

Global or “trending” reports include:

- [Top Scanned or Attacked Ports, page 3-15](#)
- [Global Scan or Attack Rate, page 3-16](#)
- [Global DoS Rate, page 3-17](#)
- [Infected Subscribers, page 3-18](#)

Individual subscriber or host reports include:

- [Top Scanning or Attacking Hosts, page 3-19](#)
- [Top Scanning or Attacking Subscribers, page 3-20](#)
- [Top DoS Attacked Hosts, page 3-21](#)
- [Top DoS Attacked Subscribers, page 3-22](#)

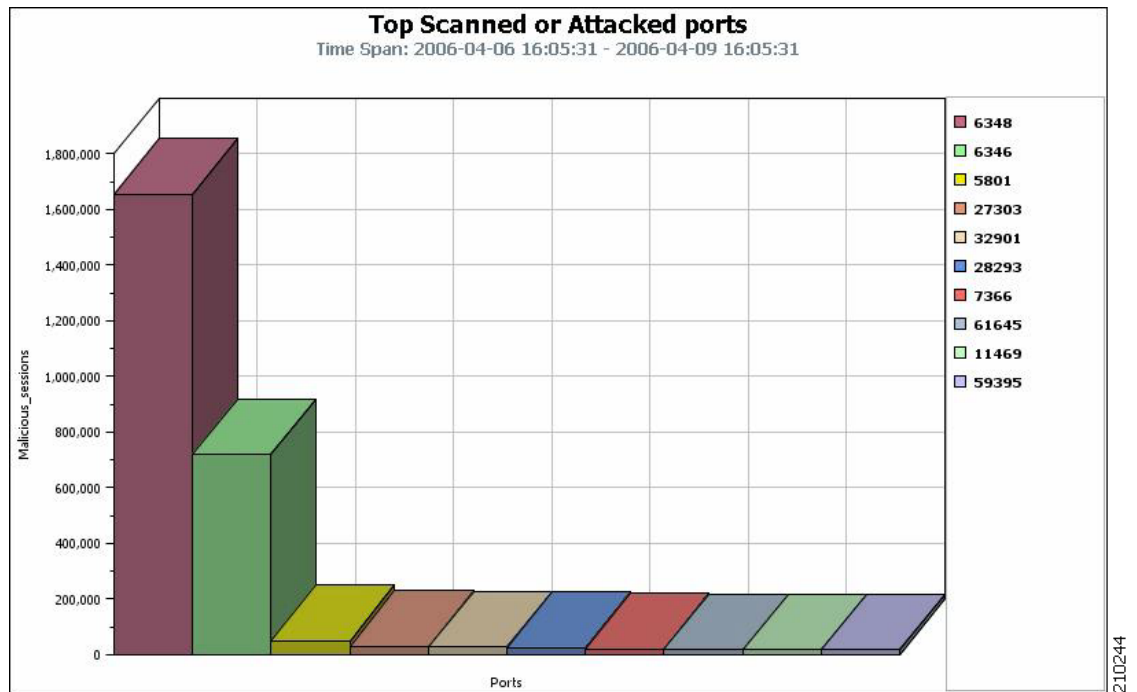
## Top Scanned or Attacked Ports

The Top Scanned or Attacked ports report is based on the records of sweep/attack activity detected by the SCE platform on a specific port (Figure 3-10).

The report presents the top ports over which such activity was detected. This provides a good indication of the current “vulnerable” ports being searched by worms, bots, and hackers.

The introduction of a new network worm is typically characterized by a rise in the number of sweeps on a specific port. Ongoing monitoring of the network by using this report would allow an operator to detect an outbreak of a new network threat based on a rise in the amount of malicious activity over some port.

**Figure 3-10** Top Scanned or Attacked Ports Report



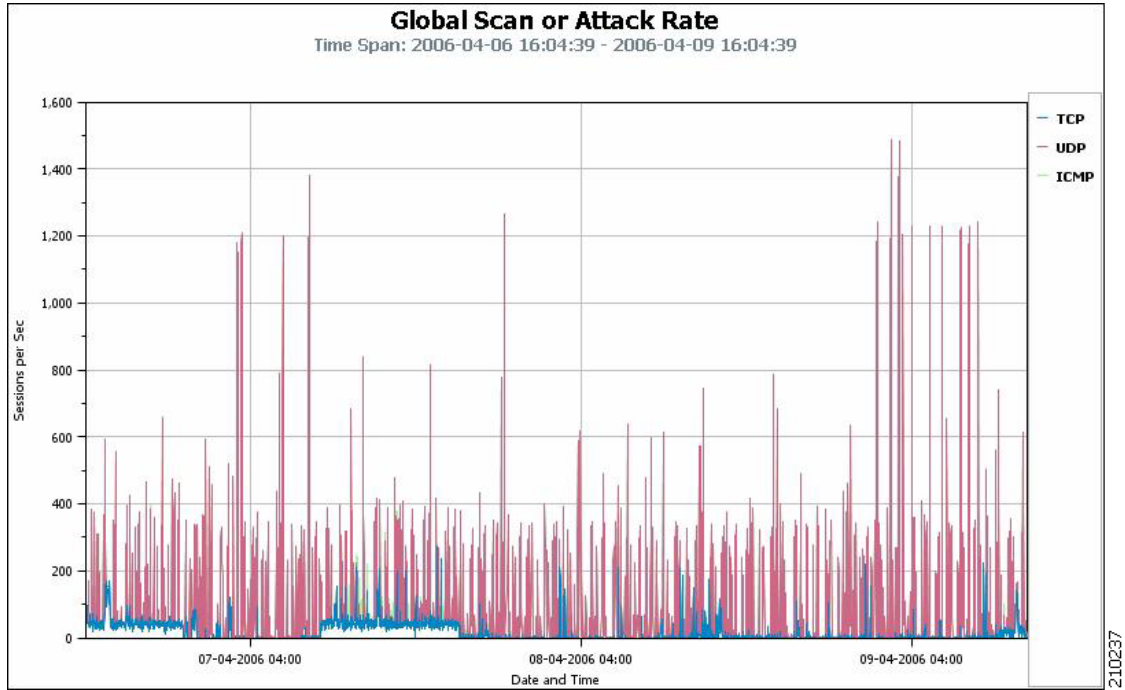
# Global Scan or Attack Rate

The Global Scan or Attack Rate report is based on the records of sweep/attack activity detected by the SCE platform, but not limited to a specific port (see [Figure 3-11](#)).

The report presents the global scan/attack rate over time, broken down by protocol. You can filter the report by the scan direction, that is, from the subscriber or from the network.

An outbreak of a network worm is typically reflected in a surge of scan activity, which this report can help detect.

**Figure 3-11** Global Scan or Attack Rate Report



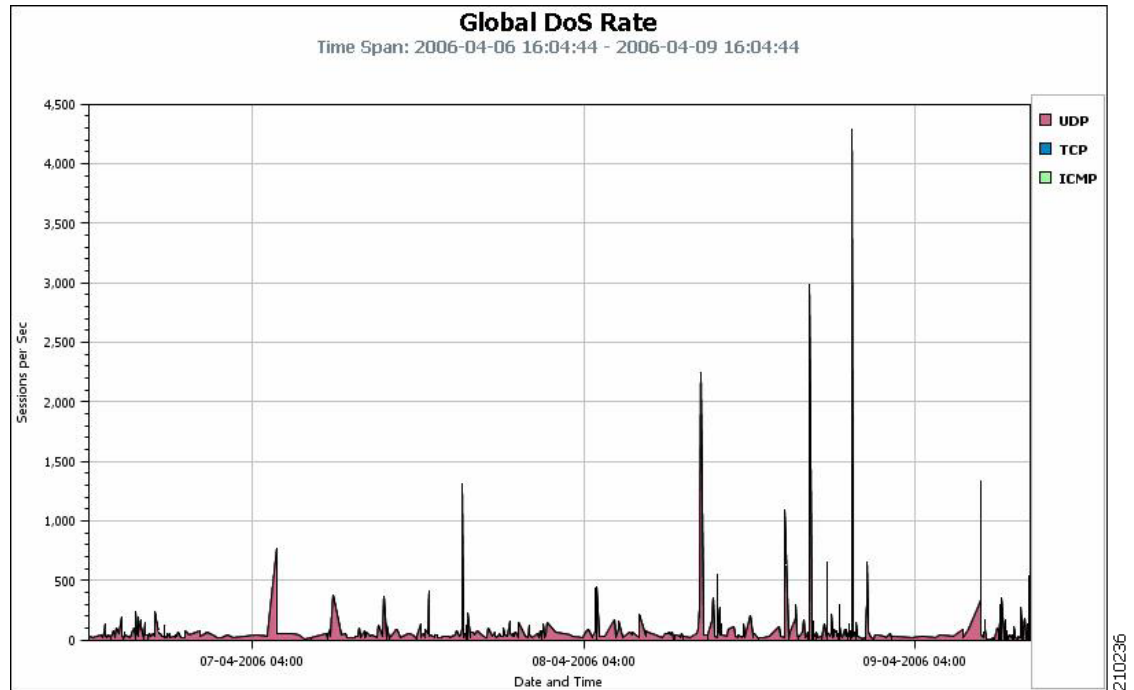
210237

# Global DoS Rate

The Global DoS Rate report is based on the records of DDoS activity detected by the SCE platform, but not limited to a specific port (see [Figure 3-12](#)).

This report presents the global DoS rate over time broken down by protocol. You can filter the report by the attack direction, that is, to the subscriber or to the network.

**Figure 3-12 Global DoS Rate Report**



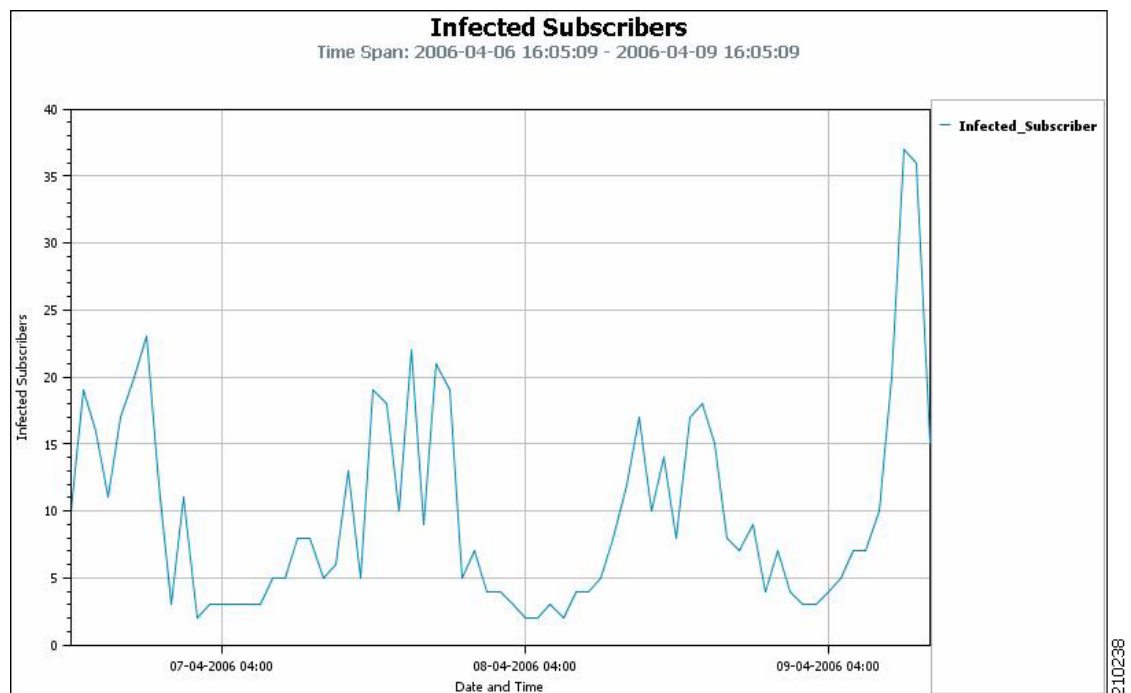
## Infected Subscribers

The Infected Subscribers report is based on the records of scan/attack activity detected by the SCE platform, but not limited to a specific port (see [Figure 3-13](#)).

The report estimates the number of infected subscribers over time (hourly time frames). This number represents the number of subscribers that were identified as generating malicious traffic during the hour in question. “Infected” reflects an assumption that some malicious agent on the subscriber host has generated the traffic.

The introduction of a new worm would typically trigger a considerable increase in the number of infected subscribers; therefore, this report is a good method of monitoring this activity.

**Figure 3-13** *Infected Subscribers Report*



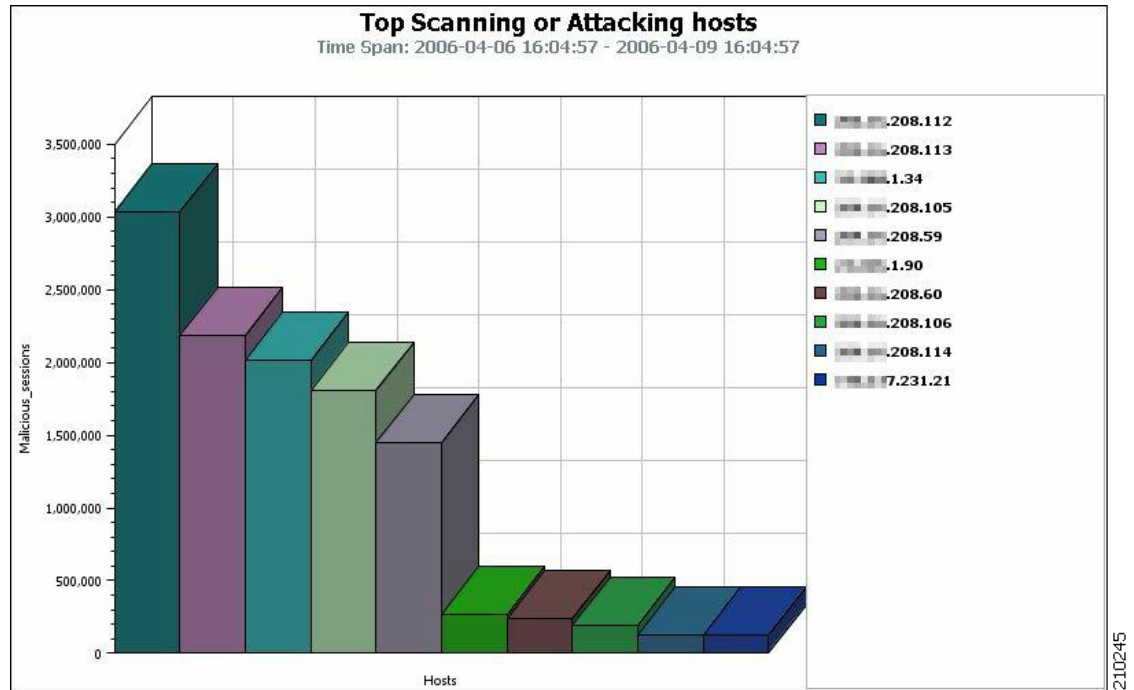


# Top Scanning or Attacking Hosts

The Top Scanning or Attacking hosts report is based on the records of scan/attack activity detected by the SCE platform, but not limited to a specific port (Figure 3-14).

The report presents the top *n* scanning or attacking hosts during the time frame specified. You can filter the report by subscriber or network, and by protocol.

**Figure 3-14** Top Scanning or Attacking Hosts Report



210245

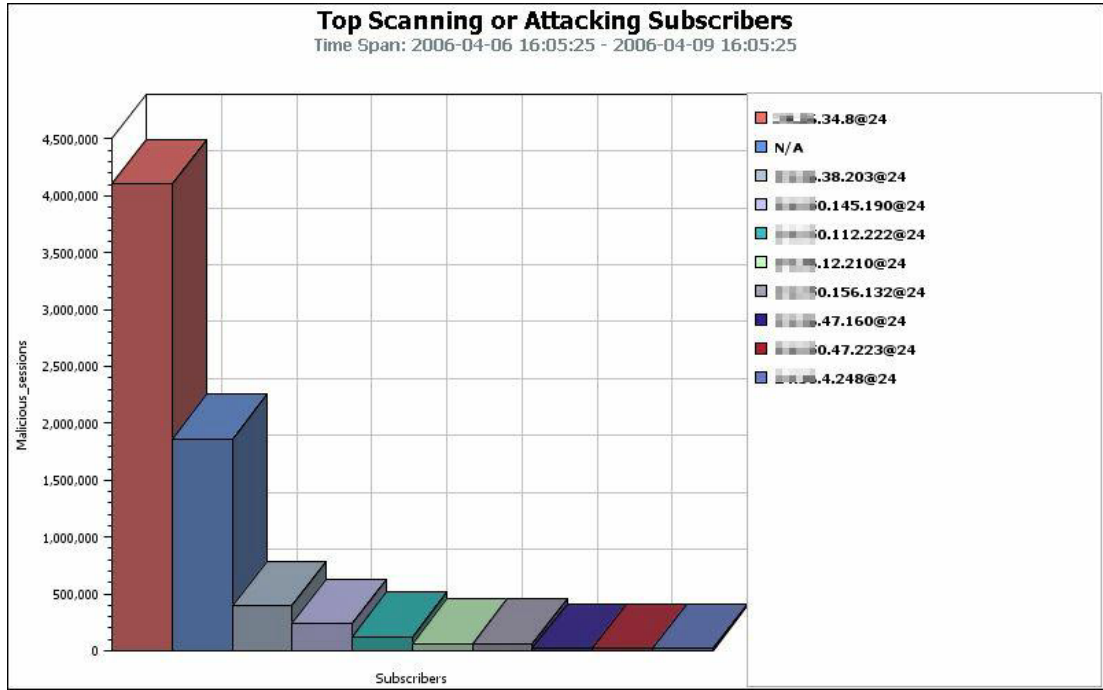
# Top Scanning or Attacking Subscribers

The Top Scanning or Attacking Subscribers report is based on the records of scan/attack activity detected by the SCE platform, but not limited to a specific port (Figure 3-15).

This report presents the top *n* scanning or attacking subscribers during the time frame specified. You can filter the report by protocol.

The N/A subscriber that typically exists in such a report is an aggregate of scan/attack traffic that could not be ascribed to a “named” subscriber—typically due to spoofing of the source IP address.

Figure 3-15 Top Scanning or Attacking Subscribers Report



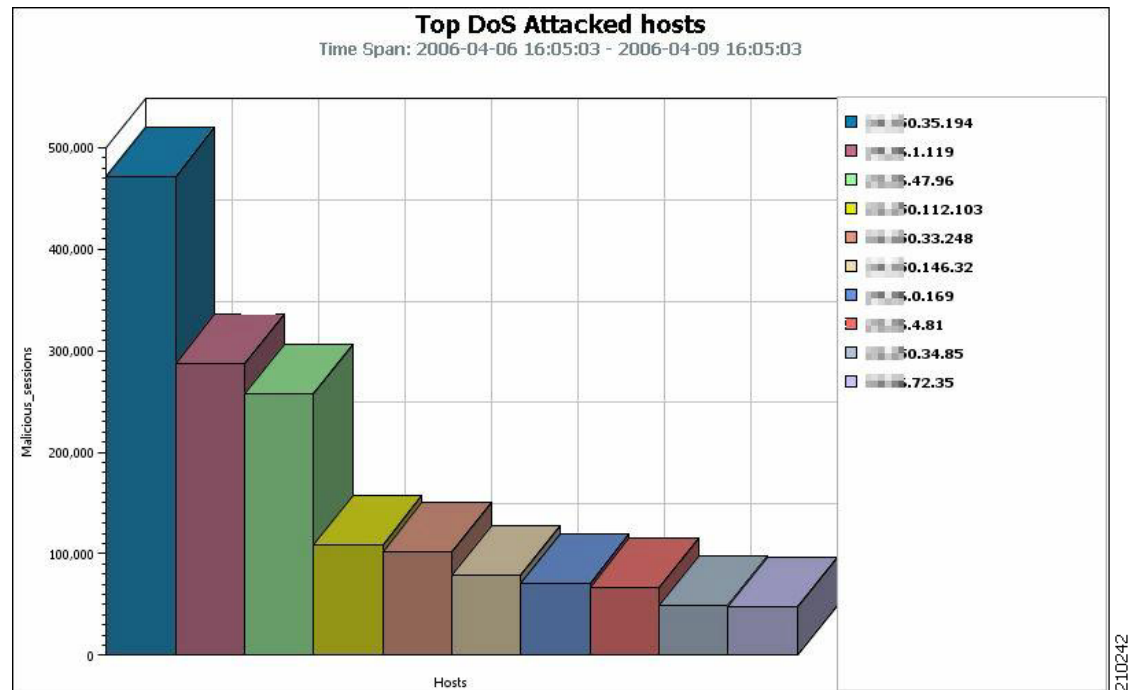
210246

## Top DoS Attacked Hosts

The Top DoS Attacked hosts report is based on the records of DDoS activity detected by the SCE platform, but not limited to a specific port (Figure 3-16).

This report presents the top *n* attacked hosts during the time frame specified. You can filter the report by subscriber or network, and by protocol.

**Figure 3-16** Top DoS Attacked Hosts Report

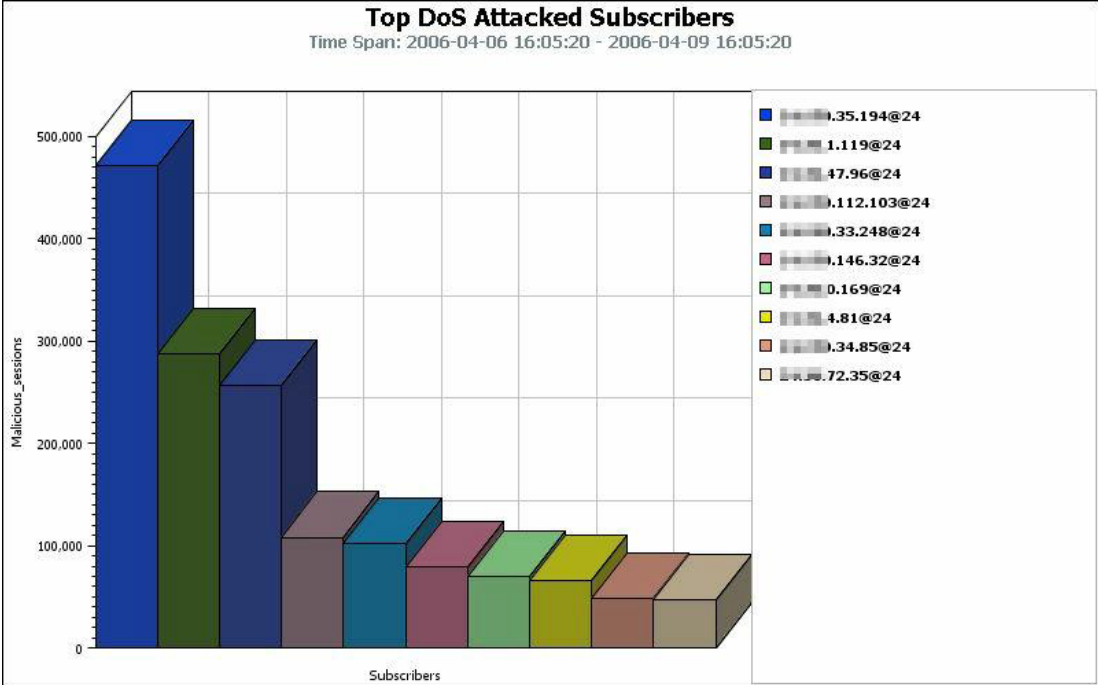


# Top DoS Attacked Subscribers

The Top DoS Attacked Subscribers report is based on the records of DDoS activity detected by the SCE platform, but not limited to a specific port (Figure 3-17).

This report presents the number of attacked subscribers over time (hourly time frames). This number represents the number of subscribers that were identified as being attacked during the hour in question. You can filter the report by protocol also.

Figure 3-17 Top DoS Attacked Subscribers Report



210243



# Mass-Mailing-Based Threats

---

Published: March 12, 2015

## Introduction

This chapter introduces the concept of mass-mailing-based threats and how to protect against them using the SCE.

## Mass-Mailing-Based Threats

The Mass-Mailing based threat detection module is based on monitoring SMTP session rates for individual subscribers. It uses the subscriber-awareness of the SCE platform and can work in subscriber-aware or anonymous subscribers mode.

SMTP is a protocol used for sending email. An excess rate of SMTP sessions from an individual subscriber is indicative of malicious activity involving sending email, that is, either mail-based viruses or spam-zombie activity.

- [Configuration of Mass-Mailing Detection, page 4-2](#)
- [Monitoring Mass Mailing Activity, page 4-3](#)

## Configuration of Mass-Mailing Detection

Mass-mailing detection is based on a subscriber breaching a predefined SMTP session quota.

For the functionality to work, the system must be configured to subscriber-aware or anonymous subscribers mode. This configuration allows the SCE platform to count the number of SMTP sessions generated by each subscriber accurately (see [Figure 4-1](#)).

Configuration is based on the following stages:

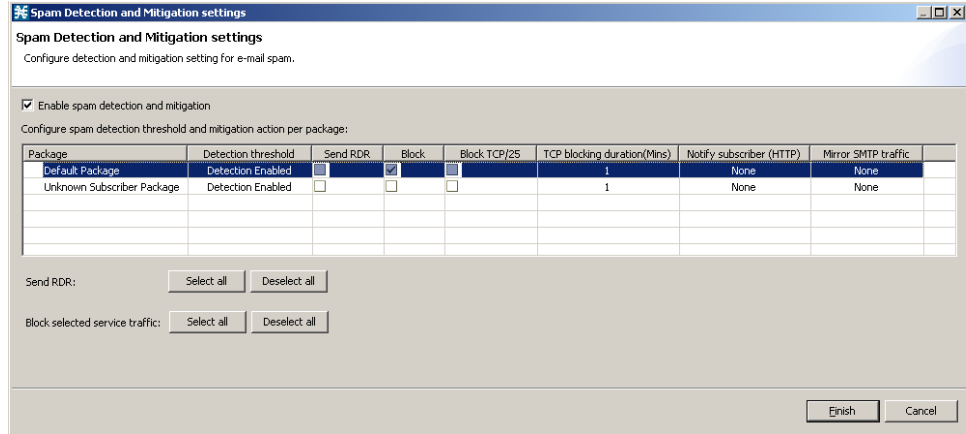
- Configuring the service for detection—You should configure the appropriate service, which should have been built before this stage, for mass-mailing detection. It is common to use a service that includes only the SMTP protocol.
- Define the quota to be used for indicating anomalous email activity. The quota is defined as:
  - a number of sessions for a given period—number of sessions and period length are both configurable
  - a number of messages for a given period in all SMTP sessions—number of messages and period length are configurable
  - a number of messages in a single session—number of messages is configurable
  - a percentage of messages failure rate over a period—percentage of messages and period length are both configurable.

It is recommended that you base the values for these fields on some baseline monitoring of subscriber activity. See the [“Monitoring Mass Mailing Activity”](#) section on page 4-3.

- Define the action to be taken upon detecting mass-mailing activity. The action to be taken can be:
  - Send RDR—SCE sends a Raw Data Record (RDR) to the Collection Manager, and sends a second RDR when the subscriber's status as a spammer is removed. The Collection Manager collects these RDRs in comma separated value (CSV) files for logging purposes. Alternatively, you can implement your own RDR collectors to receive these RDRs and respond in real-time.
  - Block—Blocks the SMTP traffic as a service.
  - Block TCP/25—Blocks only the TCP port 25.
  - Notify—Redirects the subscriber browsing sessions to a captive portal presenting a message from the operator. This action is performed using subscriber notification.
  - Mirror—Diverts spam SMTP traffic to an inline spam detection service.

For details on spam detection and mitigation, see the *Cisco Service Control Service Security: Outgoing Spam Mitigation Solution Guide, Release 3.7.x*.

Figure 4-1 Spam Setting Window



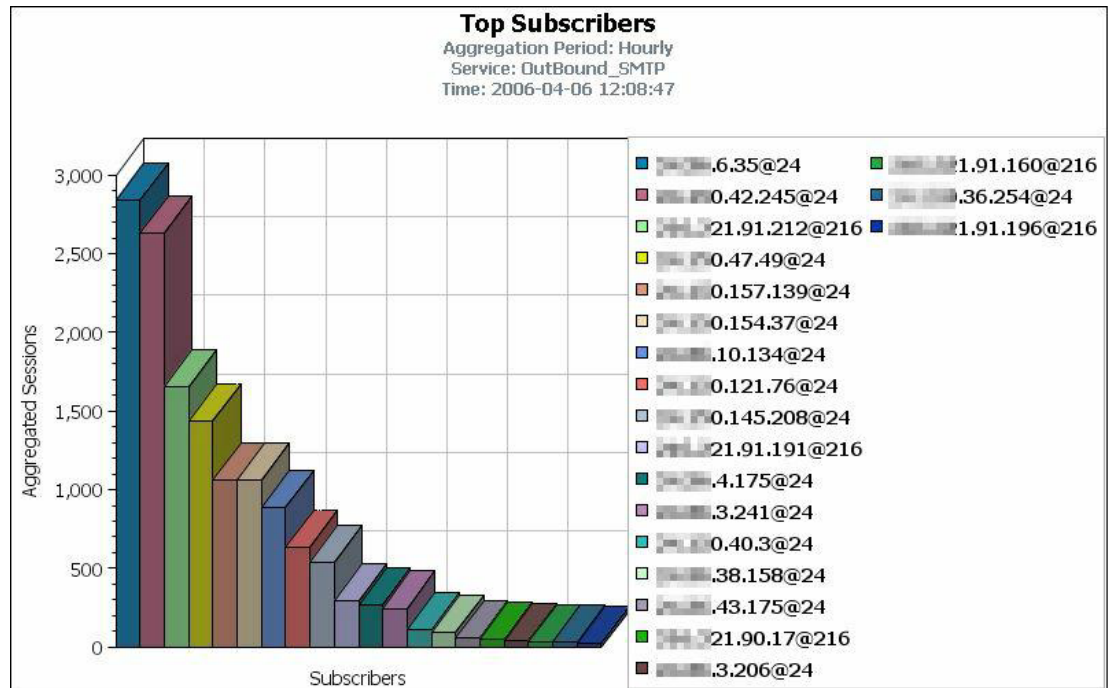
246638

## Monitoring Mass Mailing Activity

Mass mailing activity can be monitored based on information processed and stored in the Collection Manager database.

The most suitable report for detecting mass mailing activity by subscribers is the Top Subscribers by Sessions report. This report is generated for the service and is used for mass-email detection (SMTP or a more granular service if it was defined). The report would highlight the IDs of subscribers most likely to be involved in mass mailing activity (see Figure 4-2)

Figure 4-2 Top Subscribers Report



210247

