## CISCO SERVICE CONTROL SOLUTION GUIDE

# Cisco Service Control Service Security:

# Outgoing Spam Mitigation Solution Guide, Release 5.0.x

Published: July 30, 2014

**Note** This document supports all 5.0.x releases.

# 1 Introduction and Scope

The need for protection from various attacks and malicious traffic that originate from the Internet has gained attention. Denial of Service (DoS) and distributed DoS (DDoS) attacks, worms, viruses, malicious HTTP content, and multiple types of intrusions are common.

Deep Packet Inspection (DPI) platforms, and specifically the Cisco Service Control Engine (Cisco SCE), are deployed inline and are stateful and programmable. These features position the Cisco SCE platform to detect and mitigate the effect of malicious traffic on service providers and their customers.

The Cisco Service Control Application for Broadband (Cisco SCA BB) includes service security functionality comprising anomaly detection, spam and mass-mailing detection, and signature detection. These detection features allow the Cisco SCE platform to address threats that exist in current networks.

The Cisco SCA BB 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 describes the specific ways of detecting and mitigating outgoing spam and mass-mailing based threats. For a full description of the service security functionality and relevant management modules, see the Cisco SCA BB user guides.

# 2 Functionality Overview

The Cisco SCE platform uses the mass-mailing activity detection approach to detect and mitigate outgoing spam.

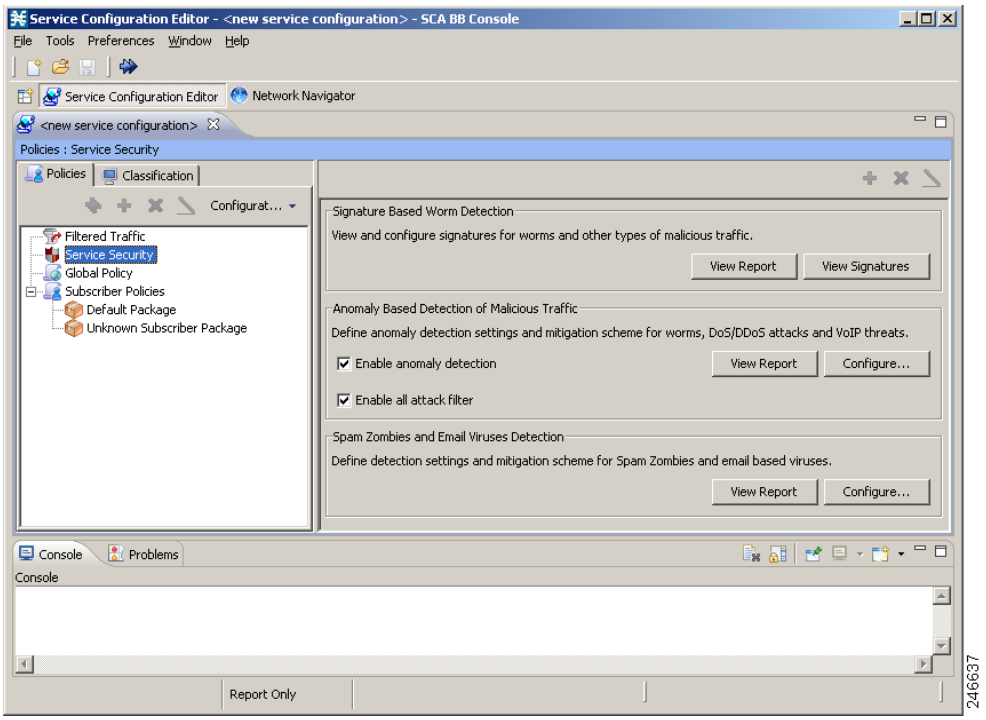
Simple Mail Transfer Protocol (SMTP) is a protocol used for sending e-mail. An excessive rate of such sessions originating from an individual subscriber is usually indicative of malicious activity involving sending e-mail, either mail-based viruses or spam-zombie activity. This mass-mailing activity detection approach is based on monitoring SMTP session rates, e-mail recipients count, email harvesting, and protocol compliance for individual subscribers. It uses the subscriber awareness of the Cisco SCE and can work in subscriber-aware or anonymous subscriber mode.

This detection approach provides operators with several possible courses of action to be implemented based on their business needs:

- Monitor—Inspects the network for malicious activity detected by this method. This can be done by using reports that are based on information collected for the malicious activity that is detected.
- Block—Automatically blocks malicious activity that is detected by the Cisco SCE platform to avoid threat propagation and adverse effects to the network.
- Notify—Notifies subscribers that they are detected as being involved in malicious activity by redirecting their web sessions to a captive portal.

Operators have flexibility in customizing the detection methods and actions to be taken based on their specific needs. The Cisco SCA BB Security Dashboard GUI application (see Figure 1) provides a front end for configuring and monitoring security functionality.

*Figure 1 Cisco SCA BB Security Dashboard*




# Mass-Mailing Detection Process

The mass-mailing detection process is based on session quotas and the number of messages or e-mail recipients.

The quota is a number of sessions for a given time interval.

The number of messages or e-mail recipients can be defined for a given time interval, for a specific SMTP session, or based on the percentage of message failures in an SMTP session.

This is an overview of the mass-mailing detection process, based on session quotas for given time interval, after the configuration is complete:

1. The time interval begins with the first session.
2. When a second session is opened, if the time is still within the first interval, the session is counted within the first interval. If the time is beyond the first interval, the second interval begins at that point.
3. If subscribers send more sessions than allotted within the time interval, they have exceeded their quota, and are marked as spammers. From that point on, all traffic sent from the subscriber is handled as spam, and the defined action (send Raw Data Record [RDR], block, notify, or mirror) is applied.

**Note** The action is applied only from that point on, and does not apply to any sessions that are still open from before the subscriber was marked as a spammer.

4. The subscribers are marked as a spammers until an interval elapses without the sessions exceeding the configured quota.

For example, the quota is defined as six sessions in ten seconds. The ten seconds begin when the first session is opened. If five more sessions are sent within ten seconds, from that point on, the subscriber is marked as a spammer and the defined action (RDR, block, notification, or mirror) is applied.

When the next session is sent at, for example, 12 seconds, the time interval begins again at 0 and the sessions are again counted. If the subscriber sends fewer than six sessions in the ten-second interval, the subscriber is no longer considered a spammer and the specified action is removed. An RDR is sent to the Collection Manager indicating that the subscriber is no longer a spammer.

### SMTP Message Counting Over All SMTP Sessions

This is an overview of the mass-mailing detection process based on the number of email-recipients in all SMTP sessions for a given time interval:

1. The time interval begins with the first session, with the count of email-recipients.
2. When a second session is opened, if the time is still within the first interval, the email-recipients is counted within the first interval. If the time is beyond the first interval, the second interval begins at that point.
3. If the session sent by subscribers has more email-recipients than allowed within the time interval, the subscribers have exceeded the quota, and are marked as spammers. From that point on, all traffic sent from the subscribers are handled as spam, and the defined action (send RDR, block, notify, or mirror) is applied.
4. The subscribers are marked as a spammers until an interval elapses without the email-recipients count exceeding the configured quota.

**Note** Mass-mailing detection based on session count and e-mail-recipients count in all SMTP sessions have two different time intervals. If both are configured, which ever threshold is breached first is considered for mass-mailing detection. The same interval is considered while relieving the subscriber as a spammer.

### SMTP Message Counting For a Specific SMTP Session

Cisco SCE counts the number of email recipients in an SMTP session. If the number of recipients exceeds the defined threshold, then the subscriber is marked as a spammer. All traffic sent from the subscriber is handled as spam, and the defined action (send RDR, block, notify, or mirror) is applied. The subscribers are marked as spammers until an SMTP session that has email-recipients count less than the defined threshold is identified.

### SMTP Anti-Harvesting

E-mail harvesters try to find out valid email address by sending a chunk of email names. Cisco SCE detects the success percentage of the e-mails in large email list destined in a single SMTP session. If the percentage of invalid e-mails crosses the configured percentage, then the subscriber is marked as a harvester or spammer. Cisco SCE marks the subscriber as a spammer until it receives an SMTP session with less percentage of invalid e-mails than the configured value.

### SMTP Protocol Compliancy

Cisco SCE checks for the valid SMTP sessions by verifying the commands and responses from the SMTP client and SMTP server. If the commands do not follow the proper sequence, then the session is considered as non-compliant to SMTP Protocol. The subscriber is marked as a spammer, and continues to be a spammer until Cisco SCE receives an SMTP session with proper command sequence.

### SMTP Blocking TCP Port 25

Instead of blocking the SMTP as a classified service, after the subscriber context is identified as spammer, TCP port 25 (SMTP) is blocked for the subscriber for a specific period.

For details on configuring the spam detection, see the "Configuring Outgoing Spam Detection Settings" section on page 5.

# 3 Mass-Mailing-Based Threats

This module describes how to monitor SMTP session rates, email recipients count, email harvesting, and protocol compliance for individual subscribers. The approach uses the Cisco SCE platform subscriber-awareness and can work in subscriber-aware or anonymous subscribers mode.

## Configuring Mass-Mailing Detection

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

For the functionality to operate correctly, you must configure the system to subscriber-aware or anonymous subscriber mode. This allows the Cisco SCE platform to accurately count the number of SMTP sessions generated by each subscriber.

Configuring mass-mailing detection consists of these stages:

- Define the quota to be used for indicating anomalous e-mail activity. The quota is defined as:
  - Number of sessions for a given period—Number of sessions and period length are both configurable
  - Number of messages for a given period in all SMTP sessions—Number of messages and period length are configurable
  - Number of messages in a single session—Number of messages is configurable
  - Percentage of messages failure or wrong usernames out of minimum configurable email recipients count in an SMTP session—Percentage of message failures or wrong usernames, and the minimum number of e-mail recipients are configurable.

  We recommend that you base the values for these fields on some baseline monitoring of subscriber activity.
- Define the action to be taken upon detecting mass-mailing activity. The actions to be taken can be:
  - Send RDR—Cisco SCE sends an RDR to the Collection Manager, and sends a second RDR when the status of the subscriber 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.

**Note** For the send RDR action, the Cisco SCE sends one RDR when the subscriber is marked as a spammer and sends a second RDR after the subscriber is no longer considered a spammer. However, when using the block and mirror actions, the action begins when the subscriber is marked as a spammer and is maintained until the subscriber is no longer considered a spammer.

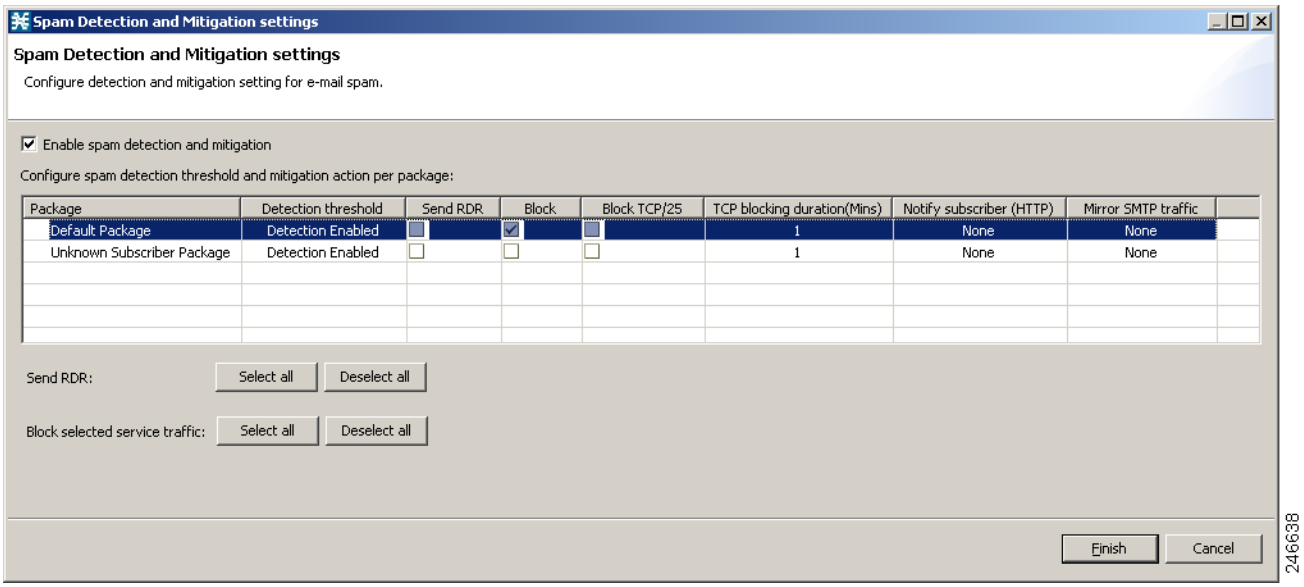
## Configuring Outgoing Spam Detection Settings

To configure the outgoing spam detections settings, complete these steps:

**Step 1** In the Service Security Dashboard, in the Spam Zombies and e-mail Viruses Detection pane, click **Configure**.

The Spam Detection and Mitigation settings window appears (see Figure 2).

*Figure 2 Spam Detection and Mitigation Settings*

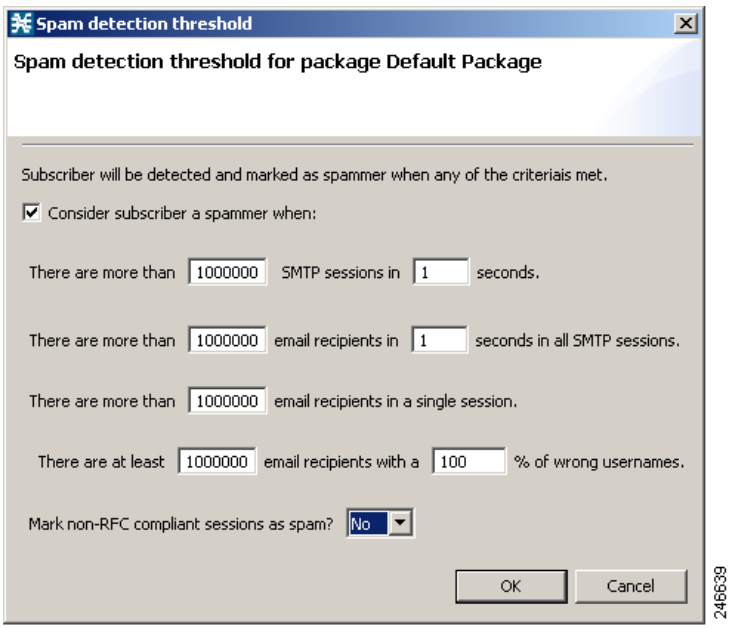



**Step 2** For each package, do these:

**a.** Define the quota to be used for indicating anomalous e-mail activity. We recommend that the values for these fields should be based on some baseline monitoring of subscriber activity.

- Click the Detection threshold column. A More ( ) button appears.
- Click the **More** button. The Spam Detection Threshold window appears (see Figure 3).

*Figure 3 Spam Detection Threshold*




- Define when to consider the subscriber as a spammer.
- Define whether to mark non-RFC compliant sessions as spam.
- Click **OK**.

**b.** Define one or more action to be taken upon detecting mass-mailing activity. Available actions are:

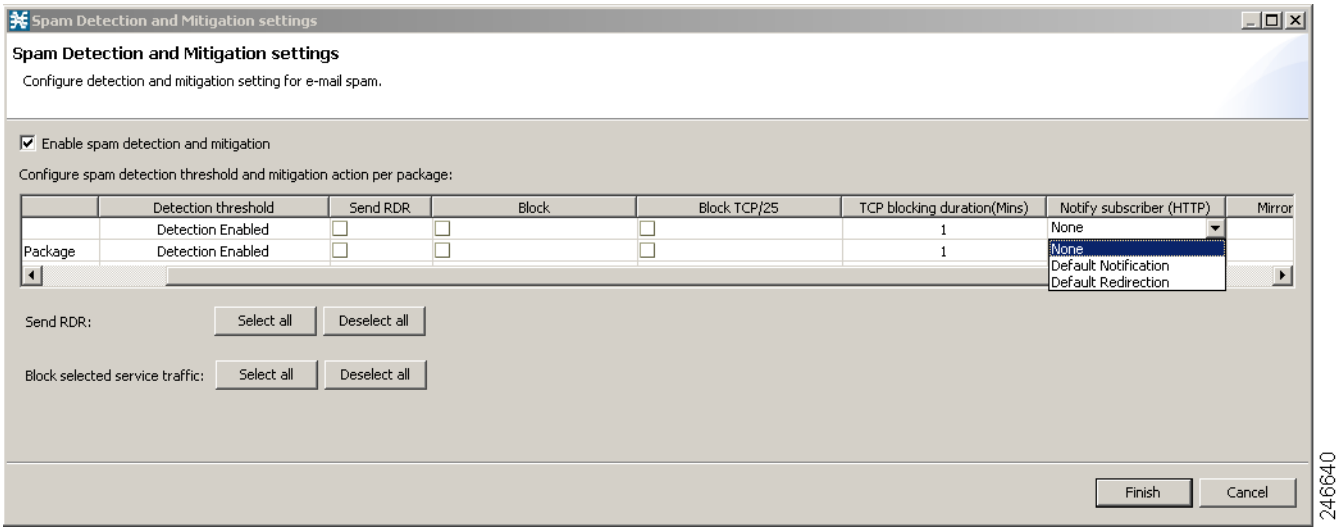
- **Send RDR**—Sends an RDR to the Collection Manager.

- **Block**—Blocks SMTP as a classified service.
- **Block TCP/25**—Blocks only TCP port 25.
- **TCP/25 Block Duration**—Defines the block duration for TCP port 25 in Minutes.
- **Notify Subscriber (HTTP)**—Redirects the subscriber browsing sessions to a captive portal presenting a message from the operator.
- **Mirror SMTP traffic**—Copies spam SMTP traffic to an inline spam detection service.

**Note** Block SMTP Traffic and Mirror SMTP traffic cannot both be selected. If you select one, the other is disabled.

To perform the Notify Subscriber (HTTP) action, choose or enter a notify subscriber (see Figure 4).

***Figure 4 Spam Detection and Mitigation Settings—Notify Subscriber***




To perform the Mirror SMTP traffic action, choose a Server Group.

**Step 3** Click **Finish**.

**Step 4** Apply the service configuration to the Cisco SCE platform.

**a.** From the toolbar, click the **Apply Service Configuration to SCE Devices** ( ) icon.
A Password Management dialog box appears.

**b.** Enter the username and password for managing the Cisco SCE and click **Apply**.
The service configuration is applied to the Cisco SCE platform.

For details on monitoring mass-mailing activity, see the "Monitoring Mass-Mailing Activity" section on page 8.

## Configuring Outgoing Spam Mitigation Settings per Package from Subscriber Policies

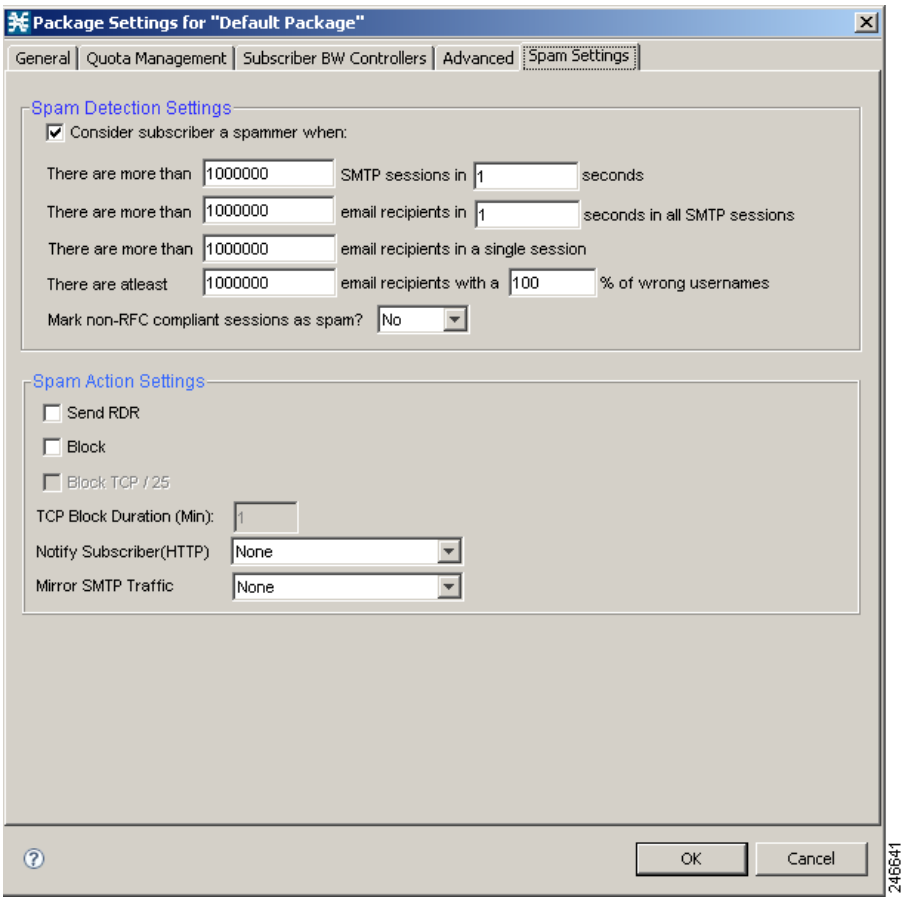
To configure the outgoing spam mitigation settings per package from subscriber policies, complete these steps:

**Step 1** In the Service Configuration Editor Policies tab, select a Package from the **Subscriber Policies**.

**Step 2** Right-click on the Package and select **Edit Package**. The Package Settings window appears (see Figure 5).

**Step 3** Click Spam Settings tab to view the Spam Detection Settings and Spam Action Settings.

*Figure 5 Package Settings for Default Package—Spam Settings*




**Step 4** Select the **Consider Subscriber a spammer when:** check box to enable the spam detection.

**Step 5** Define when to consider the subscriber a spammer and the actions to be taken.

**Step 6** Click **OK**.

## Disabling Outgoing Spam Detection

**Step 1** In the Service Security Dashboard, in the Spam Zombies and e-mail Viruses Detection pane, click **Configure**.
The Spam Detection and Mitigation settings window appears.

**Step 2** Uncheck the **Enable Spam detection and mitigation** check box. All other fields are disabled.

**Step 3** Click **Finish**.

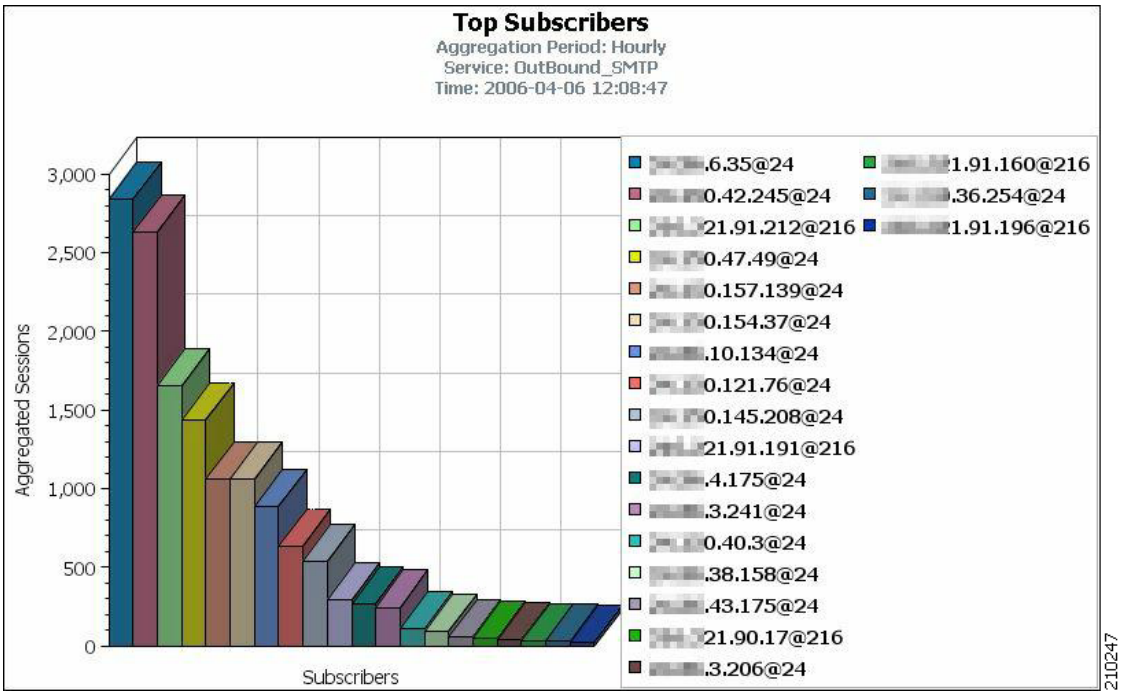
# Monitoring Mass-Mailing Activity

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 report (see Figure 6). This report is generated by running the Top Subscribers report with Metric=Aggregated Sessions.

The Top Subscribers report is generated for the service that is used for mass e-mail detection. This report can be used to identify the IDs of subscribers most likely to be involved in mass-mailing activity.

*Figure 6 Top Subscribers Report*




These are examples of two commonly used reports:

- Global Daily Usage Sessions per Service report—Shows the distribution of sessions among the different service usage counters defined in the system, grouped by day.
- Global Hourly Usage Sessions per Service report—Shows the distribution of sessions among the different service usage counters defined in the system, grouped by hour.

The Global Hourly Spam Sessions report is generated for the service that is used for mass e-mail detection. Figure 7, Figure 8, and Figure 9 shows the Global Hourly Spam Sessions report generated by using Cisco Insight.

*Figure 7 Global Hourly Spam Sessions Report Generated by Using Cisco Insight*

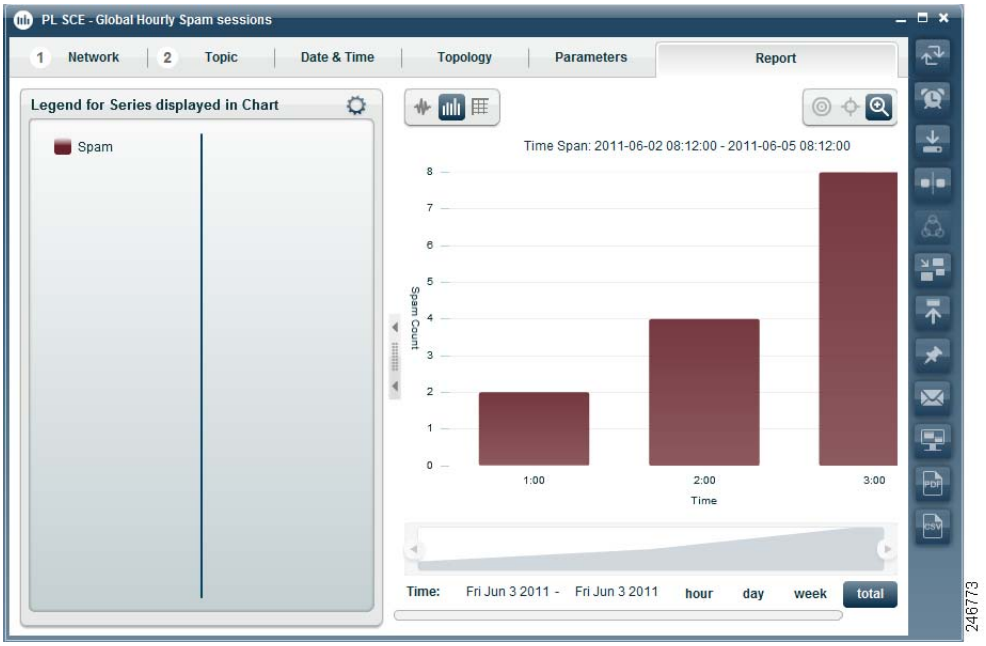


***Figure 8 Global Hourly Spam Sessions Report Generated by Using Cisco Insight***

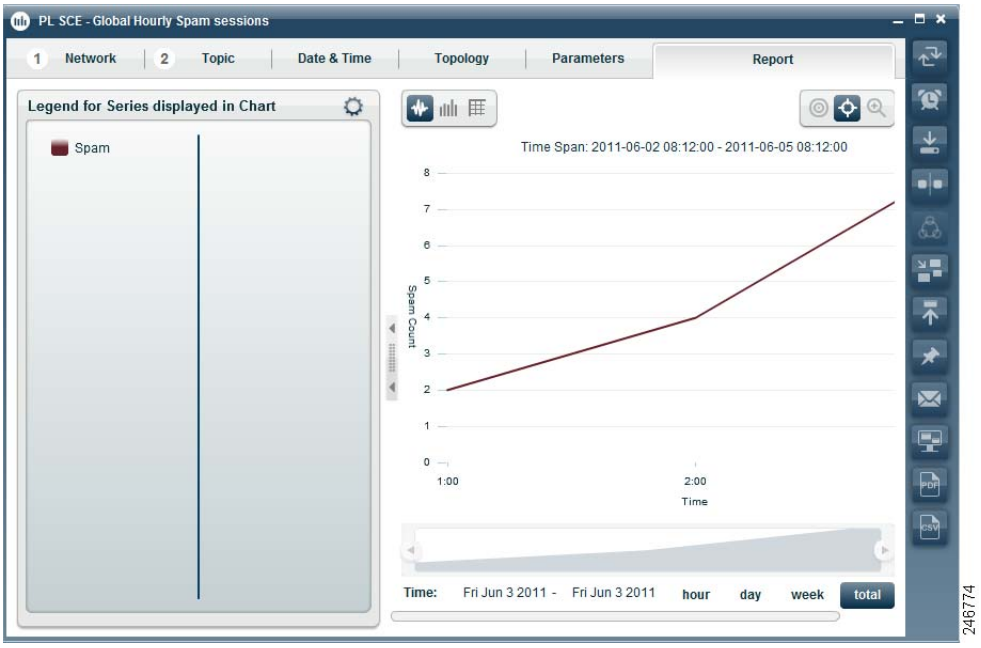
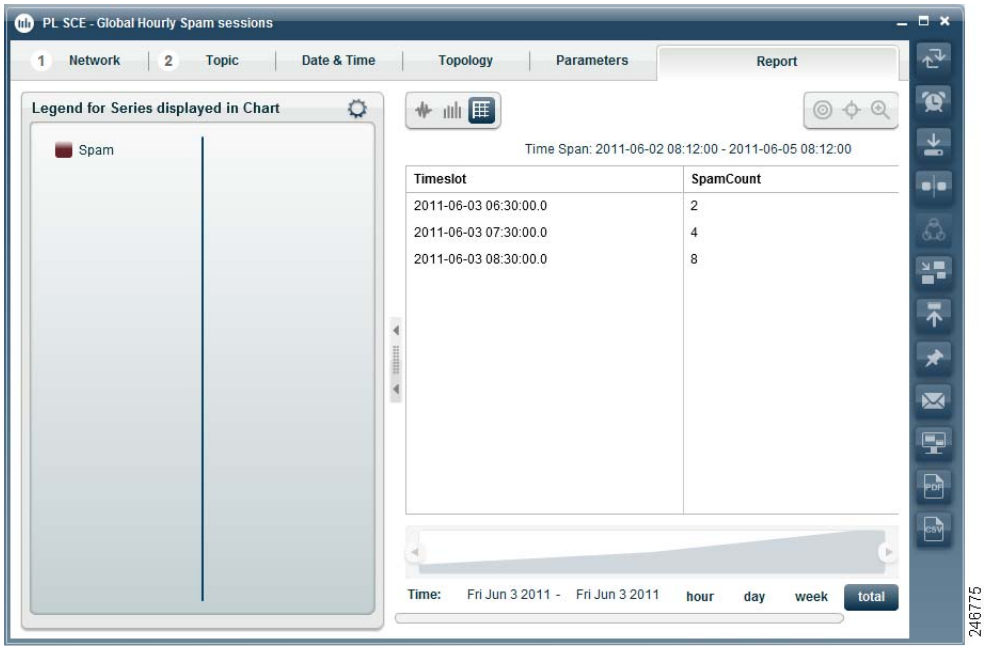



***Figure 9 Global Hourly Spam Sessions Report Generated by Using Cisco Insight***




The Top Spammers report is generated for the service that is used for mass e-mail detection. This report can be used to identify the top spammers during a certain period of time. Figure 10, Figure 11, and Figure 12 shows the Top Spammers report generated by using Cisco Insight.

*Figure 10 Top Spammers Report Generated by Using the Cisco Insight*

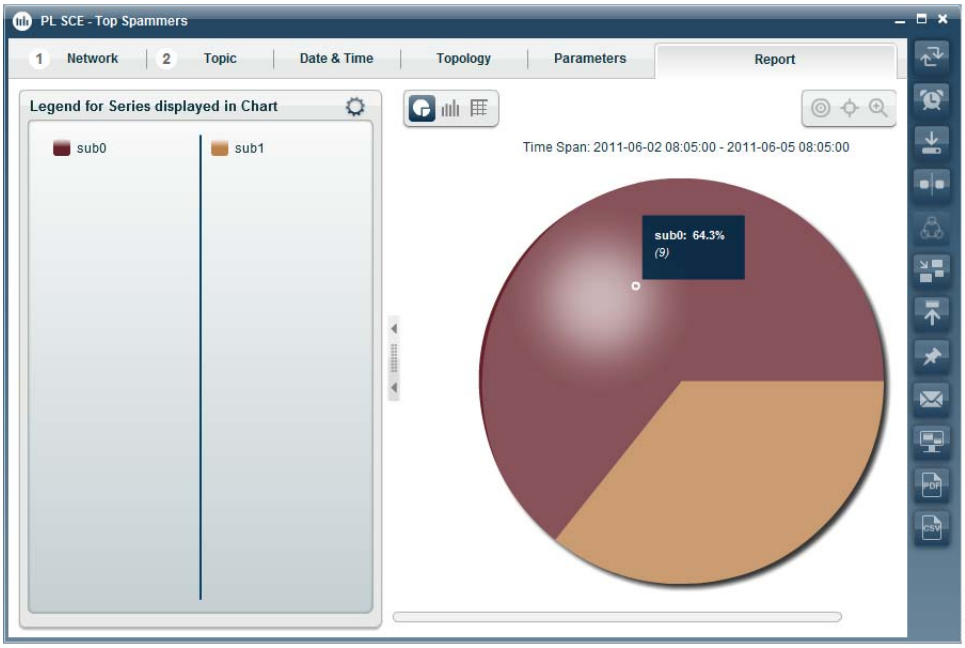



*Figure 11 Top Spammers Report Generated by Using the Cisco Insight*

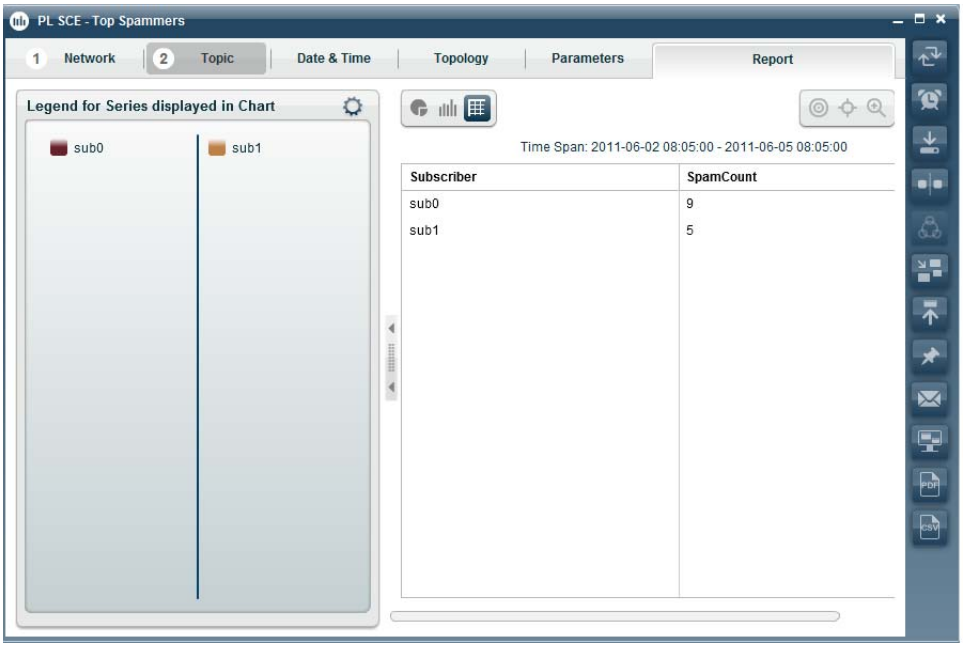
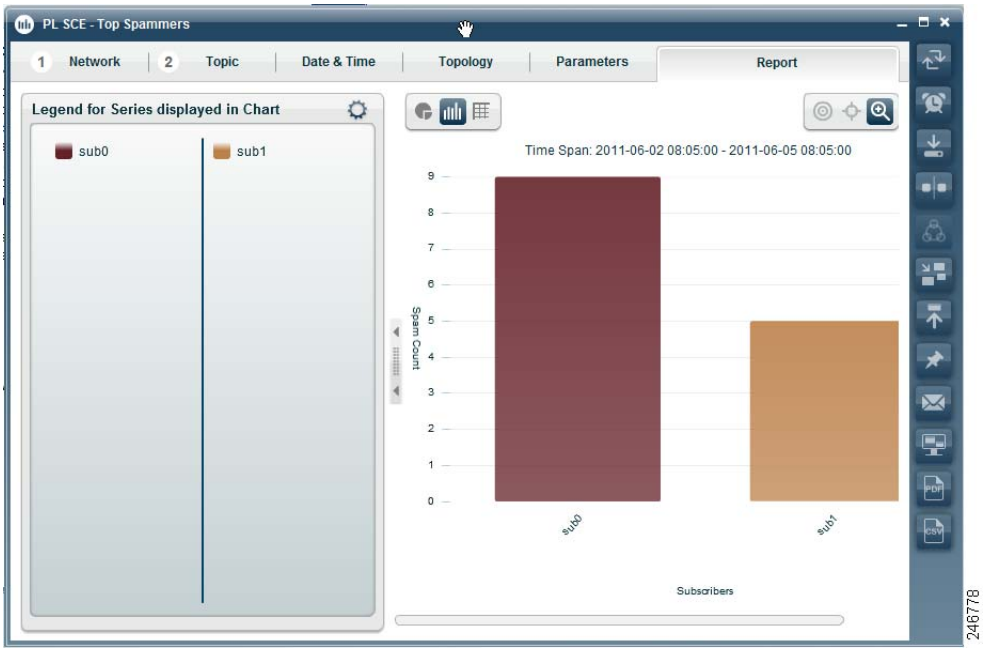


*Figure 12 Top Spammers Report Generated by Using the Cisco Insight*




## Viewing a Service Security Mass-Mailing Report Using Cisco Insight

For details on viewing the service security mass-mailing reports using Cisco Insight, see the *Cisco Insight Reporter User Guide*.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

---

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. 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 used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
The Netherlands

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**.