Cisco Service Control Solution Guide

Cisco Service Control Service Security:

Outgoing Spam Mitigation Solution Guide, Release 3.6.x

Revised: March 28, 2010, OL-21077-01

Note This document supports all 3.6.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 (SCE), 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.

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

The 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 SCA BB user guides.

2 Functionality Overview

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

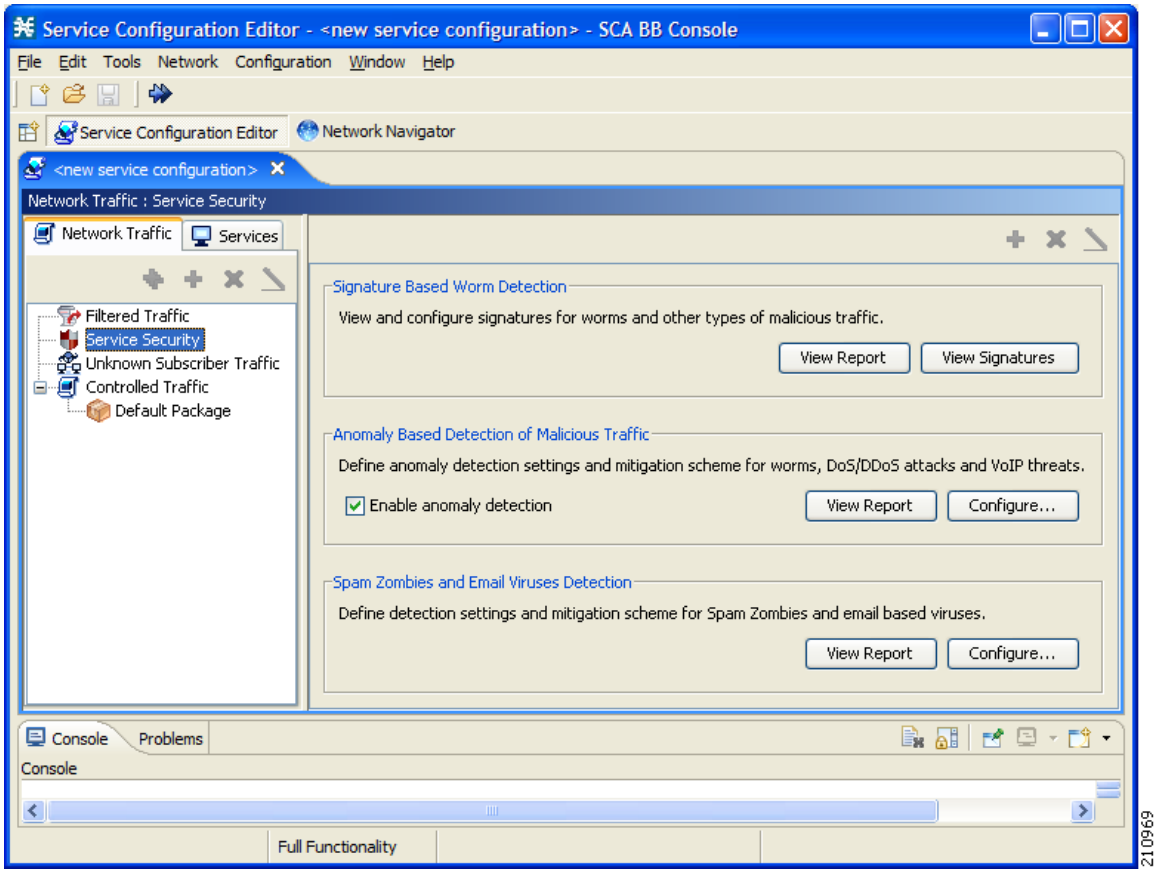
Simple Mail Transfer Protocol (SMTP) is a protocol used for sending e-mail. An excessive rate of such sessions originating from an individual subscriber is usually indicative of malicious activity involving sending e-mail, either mail-based viruses or spam-zombie activity. This mechanism is based on monitoring SMTP session rates for individual subscribers. It uses the SCE platform's subscriber awareness 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 using reports that are based on information collected for malicious activity that is detected.
- Block—Automatically blocks malicious activity that is detected by the 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 SCA BB Security Dashboard GUI application (see Figure 1) provides a front end for configuring and monitoring security functionality.

Figure 1 SCA BB Security Dashboard



Mass-Mailing Detection Process

The following is an overview of the mass-mailing detection process after configuration is complete.

The mass-mailing detection process is based on session quotas. The quota is a number of sessions for a given time interval.

1. The time interval begins with the first session.
2. When a second session is sent, 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, then 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, notification, or mirror) is applied.

Note The action is only applied 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.
5. For example, the quota is defined as six sessions in ten seconds. The ten seconds begin when the first session is sent. 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.

Note The actions are not applied to open sessions during which the subscribers were marked as spammers.

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.

Related Topics

- "Configuring Outgoing Spam Detection Settings" section on page 6

3 Mass-Mailing Based Threats

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

SMTP is a protocol used for sending e-mail; an excess rate of such sessions from an individual subscriber is usually indicative of malicious activity involving sending e-mail, (either mail-based viruses or spam-zombie activity).

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 SCE platform to accurately count the number of SMTP sessions generated by each subscriber.

Configuration is based on the following stages:

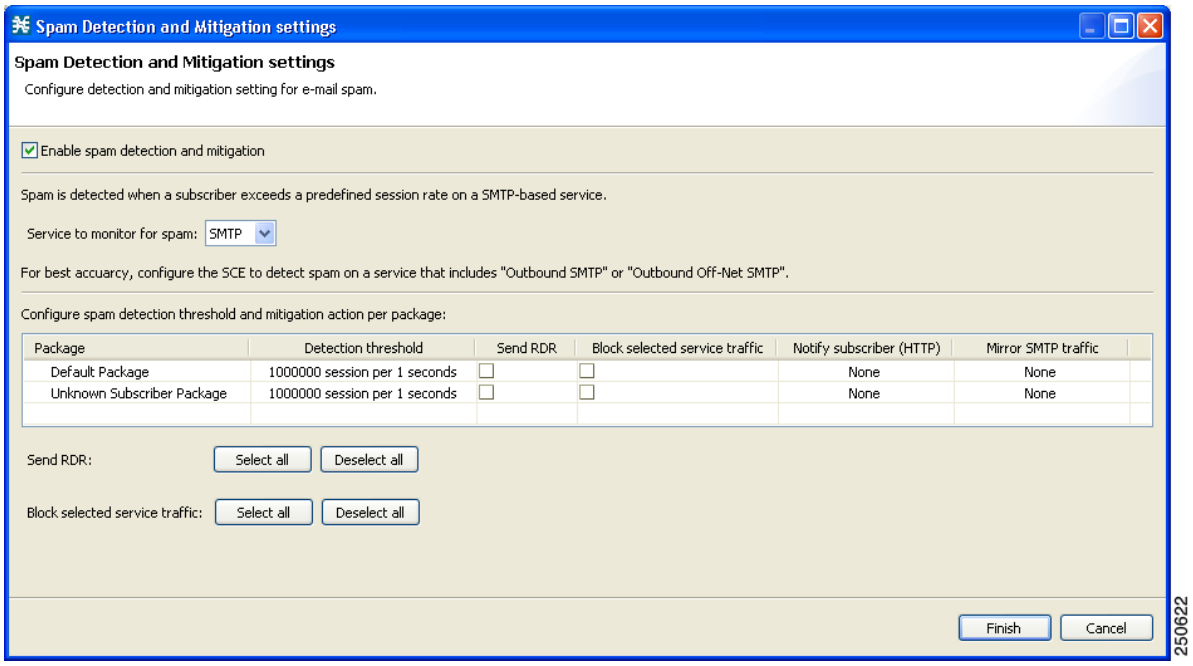
- Configure the service for detection—Configure the appropriate service, which should have been built before this stage, for mass-mailing detection. It is common to use a service that includes only the SMTP protocol. Refinements can be made to narrow the scope of detection and to potentially reduce the detection threshold.
  - "Outbound SMTP"—To account for only SMTP sessions generated by a subscriber. SMTP should not normally be seen as an inbound protocol because subscribers are not expected to run an SMTP server on their own premises. Inbound SMTP connections may represent other kinds of malicious activity. To build such a service, a user should include the "Subscriber-Initiated" attribute in the service definition.
  - "OffNet SMTP"—SMTP that is not targeted to a subscriber home SMTP server." Normal e-mail clients send e-mail through a home SMTP server, which later relays the e-mail to wherever needed. Limiting the service to offNet can avoid accounting for "legitimate" sessions; that is, sessions that subscribers conduct with the SMTP server of their ISP. One caveat is that prominent non-ISP e-mail providers provide an SMTP based service either for a fee, or free of charge. OffNet is no longer a suitable differentiator between "legitimate" and "non-legitimate" activity. To build such a service, you should define a Zone of IP ranges and then define a service that associates the SMTP protocol with the defined Zone.
  - A combination of the two.
- Define the quota to be used for indicating anomalous e-mail activity. The quota is defined as a number of sessions for a given period—number of sessions and period length are both configurable. It is recommended 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 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 spam SMTP traffic.
  - 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 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, notify, 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

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 Window



Step 2 From the Service to monitor for spam drop-down list, choose a service.

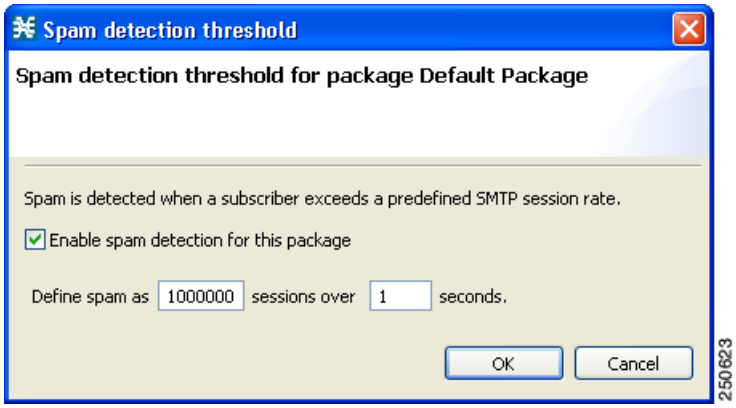
Note Leave the default value for the monitored service (SMTP), unless you have defined a more specific service, such as Outbound SMTP or OffNet SMTP.

Step 3 For each package, do the following:

a. Define the quota to be used for indicating anomalous e-mail activity. The quota is defined as a number of sessions for a given period—number of sessions and period length are both configurable. It is recommended 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 Window



- Define the threshold e-mail session rate for anomalous behavior.
- Click **OK**.

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

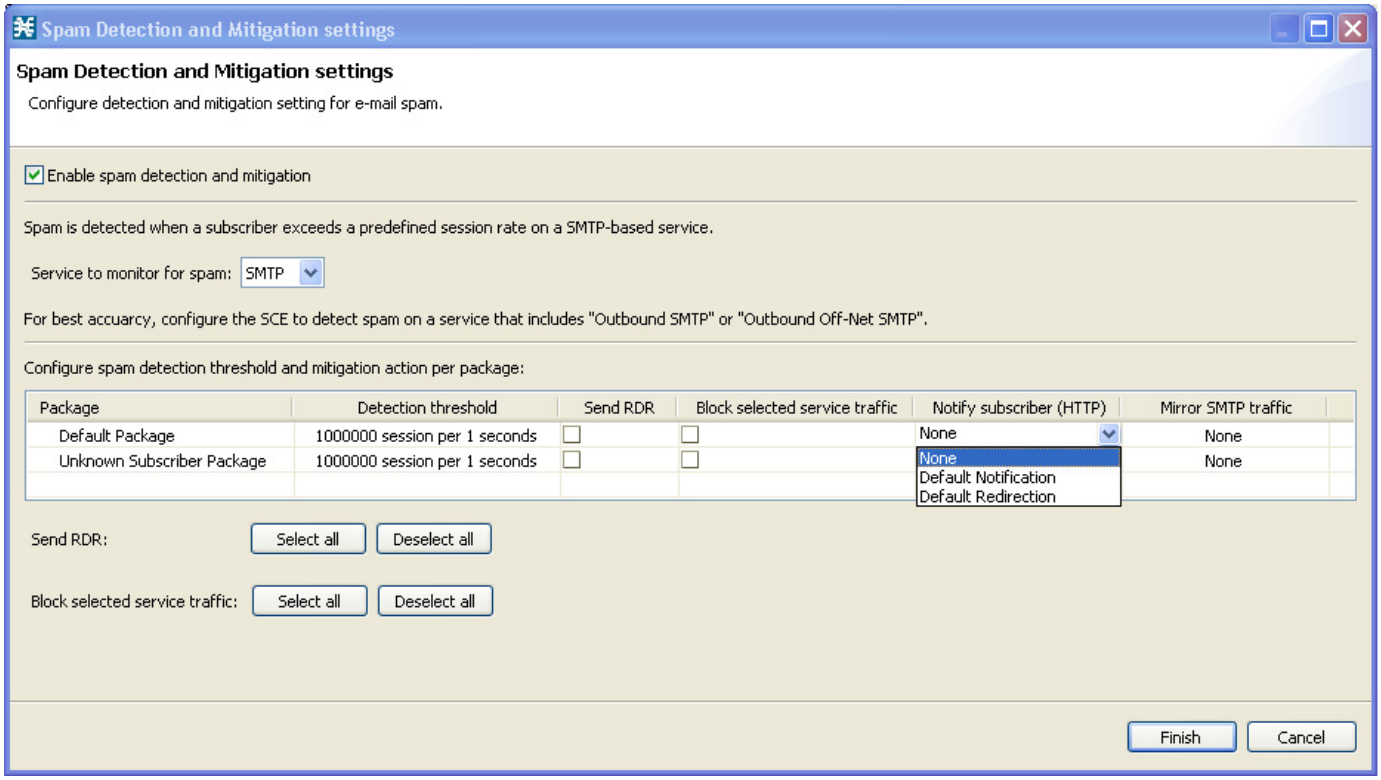
- **Send RDR**—SCE sends a Raw Data Record (RDR) to the Collection Manager, and sends a second RDR when the subscriber's status as a spammer is removed. The Collection Manager collects these RDRs in CSV files for logging purposes. Alternatively, you can implement your own RDR collectors to receive these RDRs and respond in real-time.
- **Block SMTP Traffic**—Blocks the spam SMTP traffic.
- **Notify Subscriber (HTTP)**—Redirects the subscriber browsing sessions to a captive portal presenting a message from the operator. This is performed using subscriber notification.
- **Mirror SMTP traffic**—Copies spam SMTP traffic to an inline spam detection service.

Note For the send RDR action, the 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, notify, 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.

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 Window—Notify Subscriber



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

Step 4 Click **Finish**.

Step 5 Apply the service configuration to the SCE platform.

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

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

Related Topics

- "Monitoring Mass Mailing Activity" section on page 9

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 dialog box appears.

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

Step 3 Click **Finish**.

Disabling Outgoing Spam Detection per Package

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 dialog box appears.

Step 2 In the row of the package for which you want to disable outgoing spam detection, click inside the Detection Threshold column. A More button ( ) appears.

Step 3 Click the **More** button. The Spam detection threshold dialog box appears.

Step 4 Uncheck the **Enable Spam detection for this package** check box. All fields are disabled.

Step 5 Click **OK**.

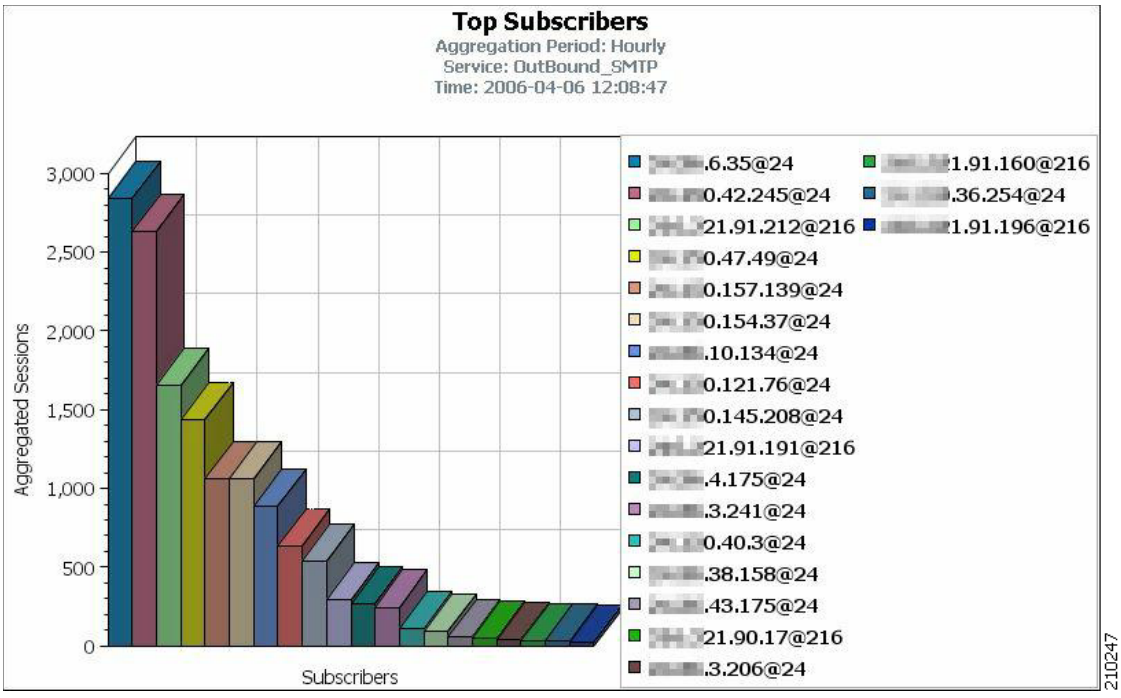
Monitoring Mass Mailing Activity

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 5). 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 (SMTP or a more granular service if it was defined). This report can be used to identify the IDs of subscribers most likely to be involved in mass mailing activity.

Figure 5 Top Subscribers Report



Following 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. (see Figure 6)
- 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. (see Figure 7)

Figure 6 Global Daily Usage Sessions per Service Report

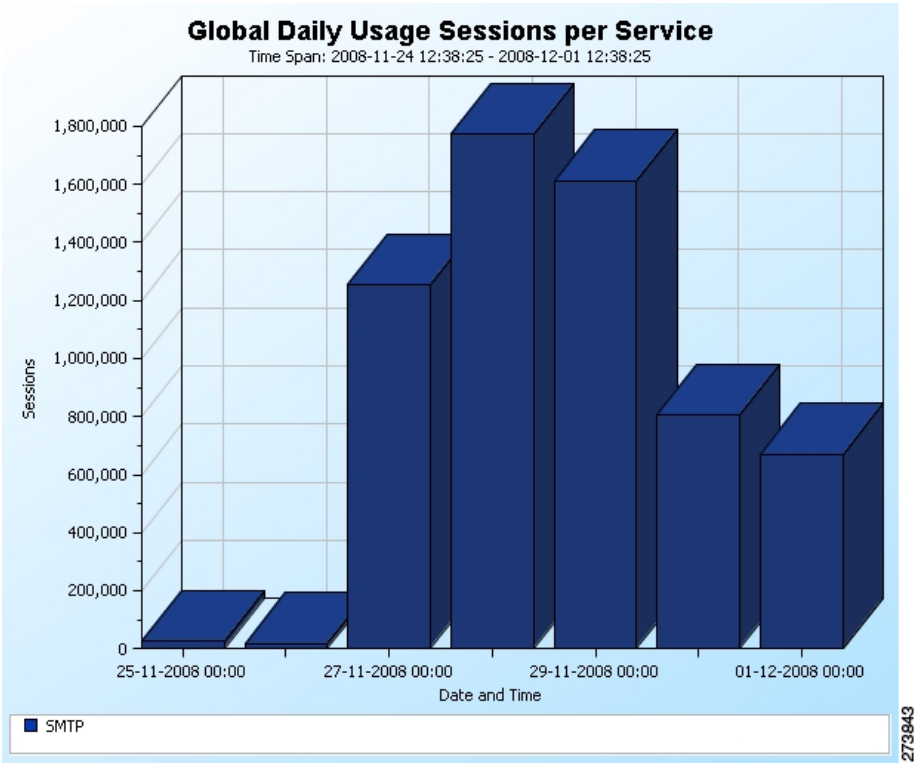
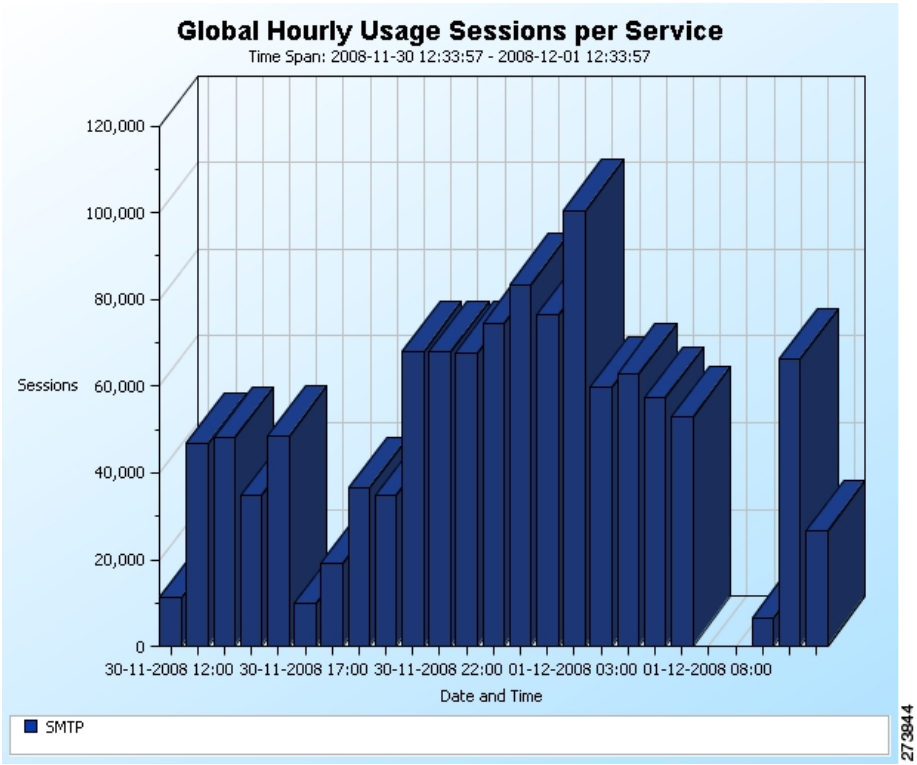


Figure 7 Global Hourly Usage Sessions per Service Report



Viewing a Service Security Mass Mailing Report

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

A Choose a report dialog box appears, displaying a tree of relevant reports.

Step 2 Choose a report from the report tree.

Step 3 Click **OK**. The Choose a report dialog box closes.

The Reporter tool opens in the Console, and displays the requested report.

Step 4 For information about manipulating and saving the report, see the "Getting Started" chapter of the *Cisco Service Control Application Reporter User Guide*.

4 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.

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**.

Printed in the USA on recycled paper containing 10% postconsumer waste.

OL-21077-01