CHAPTER 4

Mass-Mailing-Based Threats

Revised: June 13, 2011, OL-24181-01

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

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).

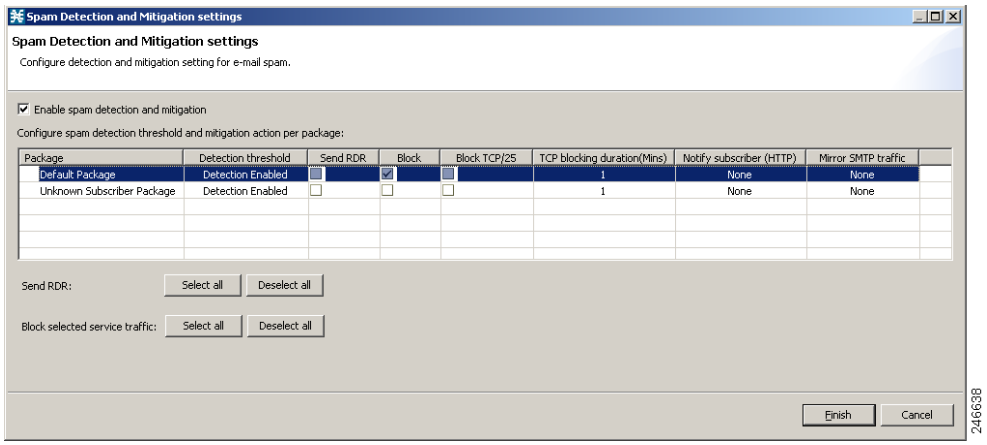
Configuration is based on the following stages:

- 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



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