CHAPTER 2

Functionality Overview

Revised: March 28, 2010, OL-22190-01

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 are 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 L7 signatures, but rather 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 SMTP session rates for individual subscribers. It uses the SCE platform's subscriber-awareness 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: either mail-based viruses or spam-zombie activity.
- Signature based detection—The SCE platform provides stateful L7 capabilities that can be used to detect malicious activity that 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 this are 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 using reports that are based on information collected for malicious activity that was detected, or using SNMP traps that can detect malicious activity using the anomaly detection module.

Block—Automatically block malicious activity that has been detected by the SCE platform 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