FILTERING APPLICATIONS

IP Reputation Services

Overview

IP Reputation Services provides a first line of defense against spam entering the corporation and consuming network resources. It uses a classification system to rate email senders based on the known behavior of connecting IP addresses. Implemented as a flow control mechanism, the application applies traffic-shaping policies based on each sender's reputation score.

Audience

Any company that wants to take advantage of global intelligence regarding the trustworthiness of sending IP addresses to prevent spam from entering the corporate network.

Key Features and Functionality Overview

The best way to fight spam through a series of solutions configured in a "funnel" that progresses from the least computationally intensive action to the most. IP Reputation Services serves as the first layer of defense in the security funnel, eliminating approximately 80% of inbound spam at connection time—before any resources are used to process the body of a message.

By blocking unwanted messages at the perimeter, you reduce the load on downstream processes to keep your email infrastructure free for optimum processing of legitimate traffic. You also reduce the number of machines required to handle inbound mail at the Internet gateway. That means lower capital, power, and IT expenses.

The IP Reputation Services application allows Sentrion to use the Commtouch GlobalView Mail Reputation Service. This network of globally distributed detection centers analyzes more than two billion Internet transactions per day to deliver real-time scoring of IP addresses according to actual traffic patterns and behaviors. Based on the risk scores in the GlobalView database at any given time, IP Reputation Services can instantly determine whether a connection request comes from an IP address that can be trusted, one that is known to send spam, or even one that has recently been taken over as a zombie and is now sending spam as part of a botnet.

The Sentrion Policy Engine uses GlobalView reputation scores to take the appropriate action for each connection attempt, for example:

- For a low-risk sender, allow normal traffic shaping—such as 10 concurrent connections and 1,000 envelopes per minute
- For a medium-risk sender, throttle traffic back to 5 concurrent connections and 50 envelopes per minute
- For a high-risk sender, throttle back to 1 connection and 5 envelopes per minute
- For a blacklisted sender, block the connection completely
- Of course, these are only examples, and the solution can be tailored to your email environment and traffic-shaping needs.

Many senders are neither entirely good nor entirely bad, and their behavior may change from day to day. Spammers are constantly attacking from a different angle. With IP Reputation Services, you have the automatic intelligence to respond in real time, rejecting the vast majority of junk before it can ever enter your network. And keeping the network clear for employee and customer messages is just one more way Sendmail helps advance your own good reputation.