



## Traffic Control with Spamhaus

### Overview

Spamhaus XBL is a real-time database of IP addresses for computers that have been hijacked into botnets. Spamhaus PBL is a database of end-user IP address ranges that are provided by ISPs for customer use, and should not be used to send email directly to other email servers. Traffic Control with Spamhaus XBL and PBL is an extension that allows the Sentrion Policy Engine to use these two third-party block lists in order to automatically reject email from rogue mail servers, botnets and other illegitimate sources.

### Audience

Companies that want to block unwanted and dangerous email from bad senders, but that are required to use government-approved block lists rather than a traditional IP reputation service (such as the Commtouch GlobalView service enabled by our IP Reputation Services application). This application is currently available only in Japan.

### Key Features and Functionality Overview

One of the most effective ways to prevent spam, phishing schemes and infected attachments from entering your network is to subscribe to a service that tracks global email traffic in real time, assigning reputation scores that identify risky senders based on their patterns of behavior. Our IP Reputation Service is one of the best in the business. But what if your company is subject to government regulations that prohibit the use of a proprietary sender reputation service? Do you just give up and let the spammers have their way?

With Spamhaus XBL and PBL, you can still fight a winning battle against spam. This extension to the Sentrion Policy Engine works with the Spamhaus exploits block list (XBL) and policy block list (PBL) to identify mail from illegitimate senders, using techniques that comply with regulations that ban reputation scoring technologies.

- **Spamhaus XBL** incorporates data from the CBL (Composite Block List at [cbl.abuseat.org](http://cbl.abuseat.org)) and the NJABL Open Proxy IPs list ([www.njabl.org](http://www.njabl.org)), along with Spamhaus' own refinements to increase efficiency and minimize false-positives. With your Spamhaus subscription and the Sentrion Traffic Control application, your enterprise can automatically query this database to determine whether incoming messages originate from desktops that have been compromised—including open proxies, malware with built-in spam engines, and other exploits.
- **Spamhaus PBL** is a list of IP ranges, including both static and dynamic IPs, that have been assigned to end-users by ISPs and should, according to ISP policy, send email only through the ISP's mail servers and never directly to third-party mail servers. Enterprises can query the PBL database to identify senders that are running illegal spam operations, or that have been unknowingly hijacked into a botnet for the purpose of sending spam.

Subscription to the Spamhaus block lists is eminently affordable. And our Traffic Control with Spamhaus application—delivered and configured to your policy needs by our expert Professional Services team—is the easiest way to tap into government-approved Spamhaus block lists. Working together, they block bad email traffic and prioritize good traffic at connection time to keep junk out of your network, protecting your employees from criminals who want to rob their privacy and productivity.