PERFTECH

Abuse Sentry Application

Highlights:

No changes required to the sub-scriber's software or configuration

All outbound email is controlled whether through the provider's server or direct SMTP

Subscriber's privacy is protected; Subscriber email abuse containment is immediate and decisive

Subscribers are immediately notified of the action by on-screen alerts with a click-to-fix button

Subscriber's abuse attempts are monitored and the block is automatically removed when fixed

Provider can specify parameters that trigger the abuse flag, actions taken

---

The Abuse Sentry Application from PerfTech® offers Internet Providers a fully automated tool to detect, measure, and prevent outbound email abuse (spam).

Stop Spam without Alienating Subscribers
Abuse Sentry is like no other spam containment solution in that it notifies and offers self-remediation to abusers immediately and automatically without any human intervention, a process that not only provides substantial relief to provider call-center resources, but also maintains positive relations with abusing subscribers, most of whom are unaware that their machines are generating spam.

No Impact to Non-spamming Subscribers
Abuse Sentry does not force the subscriber to use a specific mail server; it detects and protects against spam sent through ISP servers, external servers, or directly to the Internet. Nor is there any requirement for changes to the email client. In essence, only those subscribers who are "infected," typically about 1% of the subscriber base, get the "treat-ment."

Abuse Sentry detects infected zombies—even in port 25 blocked networks—and will bring them to the anti-virus scrubber.
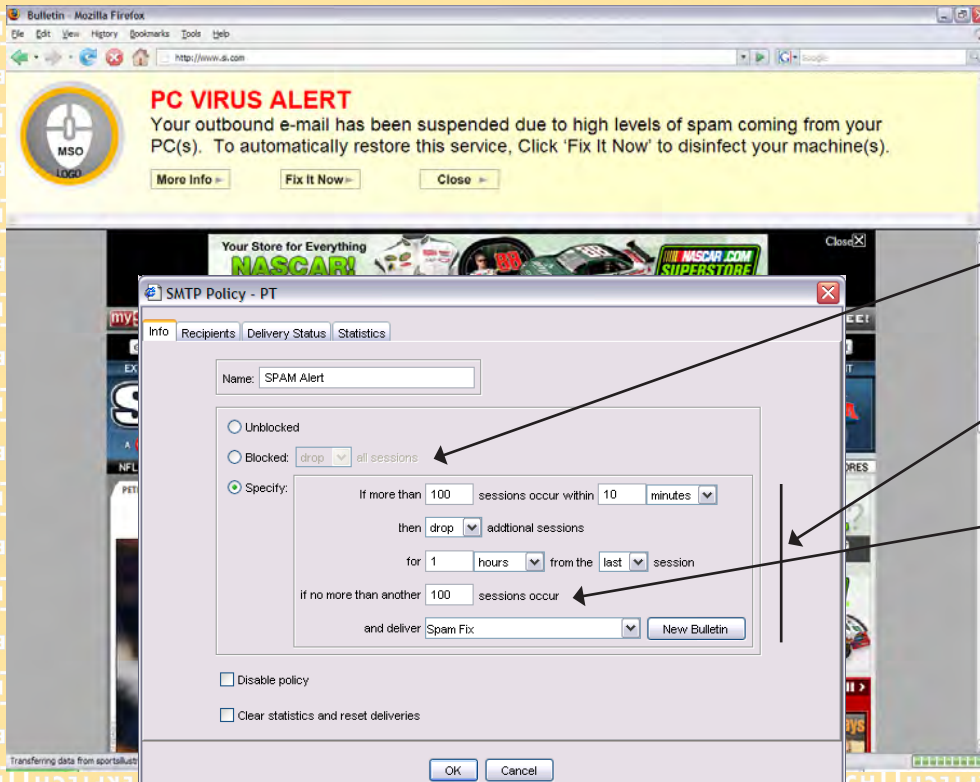
Subscriber Privacy Upheld
With Abuse Sentry, spam detection is based solely on traffic patterns typical of spam agents, and not on content. There is no examination or analysis of email content; thus, the process of spam detection remains objective, and subscriber privacy is not compromised.

Quick and Decisive Containment and Notification
Abuse Sentry is uniquely capable of coupling containment with notification, which is delivered immediately and automatically to the browser screen of abusing subscribers. The framed message does not overlay requested Internet content, informs the subscriber why his email is being temporarily blocked, and contains instructions for self-remediation. Simultaneously, outbound email from the offending machine, but not other Internet activity, is blocked until remediation occurs. Moreover, Abuse Sentry reduces the load on the abuse team by automatically eliminating outbound spam, which in turn eliminates abuse complaints and prevents blacklisting by other providers.

Abuse Sentry Thwarts Spam Yet Respects the Subscriber

PC VIRUS ALERT
Your outbound e-mail has been suspended due to high levels of spam coming from your PC(s). To automatically restore this service, Click 'Fix It Now' to disinfect your machine(s).

More Info ▶ Fix It Now ▶ Close ▶

SMTP Policy - PT
Info | Recipients | Delivery Status | Statistics

Name: SPAM Alert

○ Unblocked
○ Blocked drop all sessions
● Specify:
If more than 100 sessions occur within 10 minutes
then drop addtional sessions
for 1 hours from the last session
if no more than another 100 sessions occur
and deliver Spam Fix New Bulletin

□ Disable policy
□ Clear statistics and reset deliveries

OK Cancel

For Targeted Subscribers

Special group can be white-listed by subnet, list, or API

General network can be subject to specific thresholds, follow-on actions and communications

Automatic monitoring of abuse activity will remove block as soon as the abuse stops

Abuse Sentry activated:

The graph tells the story:
- ~1% of users are spamming at any given moment
- Spam accounts for ~90% of outbound email (SMTP) sessions
- 70% of users are remediating every week
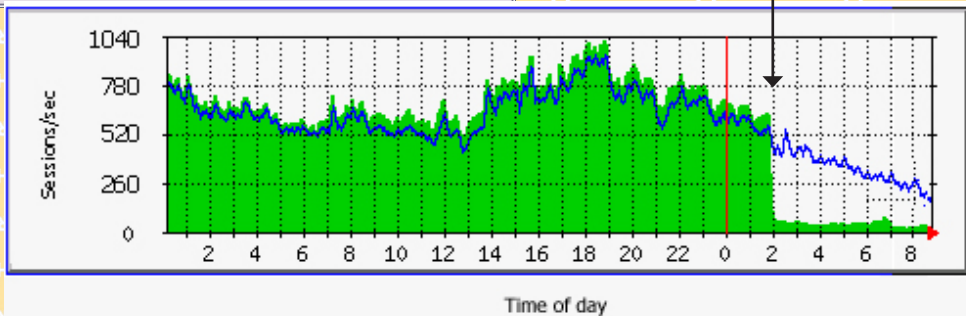
Blue line indicates spam level

Green line indicates total mail passed