

StopIT for MAILsweeper™

WHAT StopIT DOES

StopIT for MAILsweeper™ for SMTP allows you to smooth out peaks in mail traffic volume and to protect internal mail systems from volume based denial of service attacks.

StopIT gives you all the benefits of MAILsweeper but with:

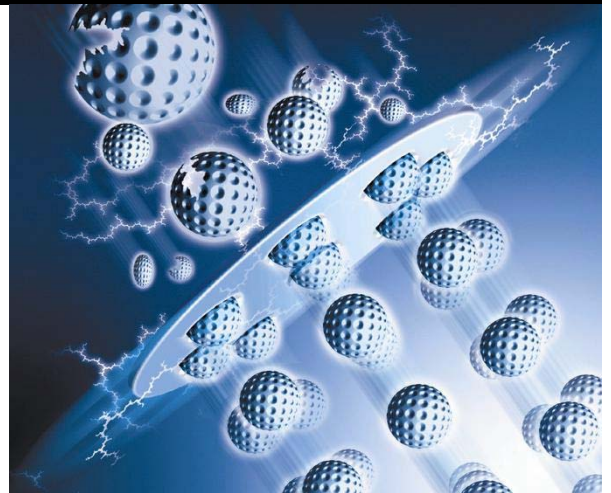
- **Improved Traffic Volume Management** by providing filtering based on volume and message numbers transmitted in nominated time intervals.
- **Increased Resilience** by providing management of incorrectly constructed SMTP transmissions.

StopIT can operate in Monitor Only mode.

Let StopIT monitor the traffic through your MAILsweeper SMTP gateway to establish accurate representative maxima for normal message volume and numbers for all sending users and domains. Then use this information to protect your site from abnormal traffic patterns.

Possible uses of StopIT are when:

- Your mail system users create very high volumes of low priority mail by mailing large messages to large mailing lists. StopIT can identify unusual volume patterns, tag messages for parking by MAILsweeper, and for release by MAILsweeper at off peak times.
- You want a report of the typical maximum volume or number of messages sent by a user or from a domain in a specified period of time (e.g. minute, hour, day).
- Macro virus infection at one of your business partner's sites results in large numbers of infected messages hitting your site, constituting an attempted denial of service attack.
- Your system suffers from mail loops as might occur if "out of office attendants" get chatting, or an internal recipient is automatically forwarding messages to an external account that fills up and generates error messages which are then sent back to the internal recipient.



WHERE TO GET StopIT

Who to Contact

Uwe Sommer
NetCon Unternehmensberatung
Soester Strasse 57
48155 Muenster
Telephone: 0251-1445950
e-mail: stopit@sommer-edv.de
web: <http://www.sommer-edv.de>

Licensing

StopIT is licensed on a per user basis.

The number of users licensed for StopIT must be the same as the number licensed for MAILsweeper.

HOW StopIT WORKS

StopIT examines every mail message received by MAILsweeper to determine the size and the address of origin. If a message conforms to StopIT's volume rules, then it is allowed to pass on for content checking by MAILsweeper.

StopIT allows you to set the maximum volume (in Mbytes) and maximum number of messages sent from an origin (a specific user or domain) in a nominated time period. This is known as a StopIT threshold for that origin. A specific user's number of messages and traffic volume can be included or excluded from the accumulated domain totals.

An example of a StopIT threshold is as follows:

first.last@domain.com can send a maximum of 100 messages, totalling no more than 50 Mbytes per 60 minutes and include in domain total.

When a StopIT threshold is exceeded, a single inform message is sent to the system administrator advising which threshold has been exceeded. Messages from the origin can be tagged and processed using standard MAILsweeper functions or can be detained.

StopIT continues to monitor message traffic and offers two options for action when volume drops below an exceeded threshold. It can allow mail from the origin to flow again without StopIT tagging or detaining it or it can keep blocking mail until an administrator intervenes.

StopIT is quite different to MAILsweeper's Park facility in two important respects; it operates on messages received over a period of time rather than on an individual message, and, it operates on message numbers not just size. Combine StopIT with MAILsweeper's Park facility to get better control.

© 2002 Scientific Software and Systems Limited. All rights reserved. MAILsweeper is a trademarks of Clearswift Corporation.

Software prerequisites

MAILsweeper for SMTP version 4.2 and above.

LDAPtIT is a product of:
Scientific Software and Systems Limited
New Zealand
Telephone +64 4 917-6670
e-mail: info@sss.co.nz
web: <http://www.sss.co.nz>

