

Spam protection in Teamware MIME Connector

In today's environment email systems are under frequent attacks by unsolicited commercial mail (spam). Without protection against these malicious attacks security of mission critical communication and organizational information is compromised. Teamware MIME Connector now includes features that offer basic spam protection capability. Teamware MIME Connector enables connection and message filter groups, which can restrict the amount of unwanted email being delivered to your users. The enhanced Teamware MIME Connector offers those customers who have the MIME Connector at the outer edge of their network an easy-to-configure solution against unsolicited commercial email.

Features

Connection filters

There are lists available of known spammers and one of the most effective ways of stopping them is to prevent them from connecting to your server in the first place. The MIME Connector supports IP filters and SMTP filters which give precise control over which SMTP hosts are able to connect to your server.

IP filters work by checking whether the IP address of the SMTP server attempting to connect to your server is allowed to do so. In addition, white lists, i.e. those addresses in a range of rejected addresses that are allowed to connect, are supported. Address ranges are specified using the CIDR (Classless Inter-Domain Routing) addressing scheme, which provides a flexible way to define IP address ranges. IP blacklists can easily be downloaded from the web and used by the MIME Connector.

SMTP filters work by checking the content of SMTP commands that are sent by the sending SMTP server when trying to deliver mail to your system. This enables the MIME Connector to reject or accept individual SMTP commands by matching the content of the command against a configured pattern.

Message filters

Message filters work by examining the message headers and checking for patterns in the header. If matches are found then a number of actions are supported. Any header can be matched in the message, including the content header and any headers in forwarded messages.

The supported actions are:

- Delete. The delete action causes the message to immediately be moved to the spam directory under the smtp directory. It will not be delivered to any recipients.
- Redirect. The redirect action allows the message to be redirected to a specific mailbox. It will not be delivered to any of the original recipient.
- Rewrite. The rewrite action allows some prefix text to be added to the Subject before the mail is delivered to the recipients. This allows administrators to put some advisory text in a message before delivery.