Sorting the mail

How many e-mail filters sort through your messages with genuine intelligence? iomart's NetIntelligence MailFilter Edition has real brains!

BY DICK BEDDOE

Spam spam spam spam spam and spam. It seems everything these days comes with spam. Frankly, it's getting me down. My guess is that it's also proving a major source of irritation for a lot of you and, more importantly, your users. The fact is, we really do need some sort of a solution. On that note let me present one of the new products on the antispam block.

From the iomart Group stable comes a new service called NetIntelligence Mail Filter Edition. The basic idea is simple: all your e-mail is forwarded to an e-mail server run by NetIntelligence and is preprocessed for spam, e-mail-borne viruses, inappropriate e-mail (read 'porn') and any other e-mail that you see fit to filter. E-mail that passes the tests is then forwarded on from the NetIntelligence servers directly to your own boundary (Exchange) server(s) as inbound e-mail. Outbound mail is also passed through the same checking mechanism so that you may rest assured that your e-mail is not passing viruses out to valuable clients – who generally do not appreciate being fed a virus from their vendors!

However, this brief description is something of an oversimplification of NetIntelligence MailFilter and its clever, sophisticated interface that allows the client to configure the filtering settings to their own requirements.

I had a test account set up by the support team at NetIntelligence so that I could check out the management interfaces and get an idea of how it all works. The management process is controlled through an authenticated web-based interface. Once logged in, you may set up a series of policies that control the level of filtering applied (**Figure 1**). The objective here is to balance the requirement for filtered spam e-mail with the risk of filtering a genuine e-mail – after all, someone in your organisation may actually be interested in herbal Viagra… you never know! On a more serious note, the issue of what is termed 'false positives' is real and there is a fine balance between filtering to the nth degree and losing genuine e-mails. This product puts the responsibility where it should be, in your hands, controlling the level of filtering through policies. They could have gone further, though – a means of weighting the rules would have been a useful enhancement.

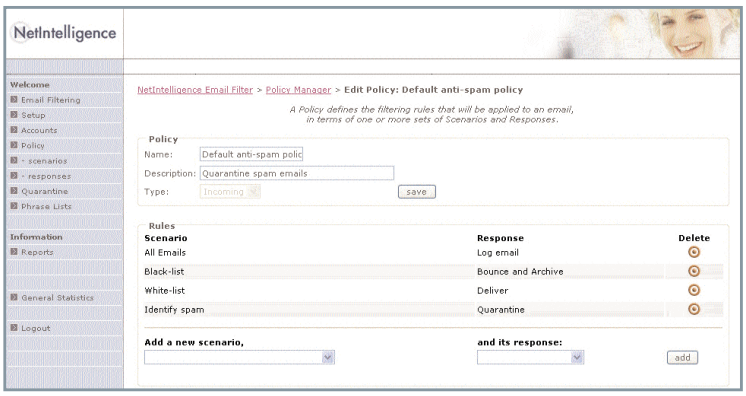

Figure 1: The web-based policy editor allows specific conditions to be defined

Having spent some time navigating around the management interface my conclusion is that it is basically very straightforward. The configuration is fairly self-explanatory and if there is any confusion there is a very useful help guide. To monitor the results of NetIntelligence MailFilter a series of reports are generated (**Figure 2**). These are easily interpreted and comprehensive and may be downloaded in PDF format or viewed on the screen.

Spam is not the only issue

Virus checking is a crucial component of mail filtering. To that end iomart has incorporated two of the leading virus checkers in the process. Trend Micro and Kapersky are run in sequence so that each e-mail is checked twice. Both of these virus checkers have online updates that ensure the latest IDE signature files are incorporated into the check. This clearly takes a huge strain off your shoulders. The only concern I have here is the risk of the latest 'fix' only being available on another scanner when a major virus outbreak is detected. NetIntelligence MailFilter also includes a proprietary 'zero-day-threat' detection mechanism to spot new virus outbreaks in the period before pattern updates are available for the antivirus checkers. This sounds like an interesting piece of technology, although I was unable to test its effectiveness.

Content handling is a very sensitive issue. NetIntelligence MailFilter has a sophisticated engine for a structural and heuristics analysis that comprises four major sections. First, online blocking lists identify

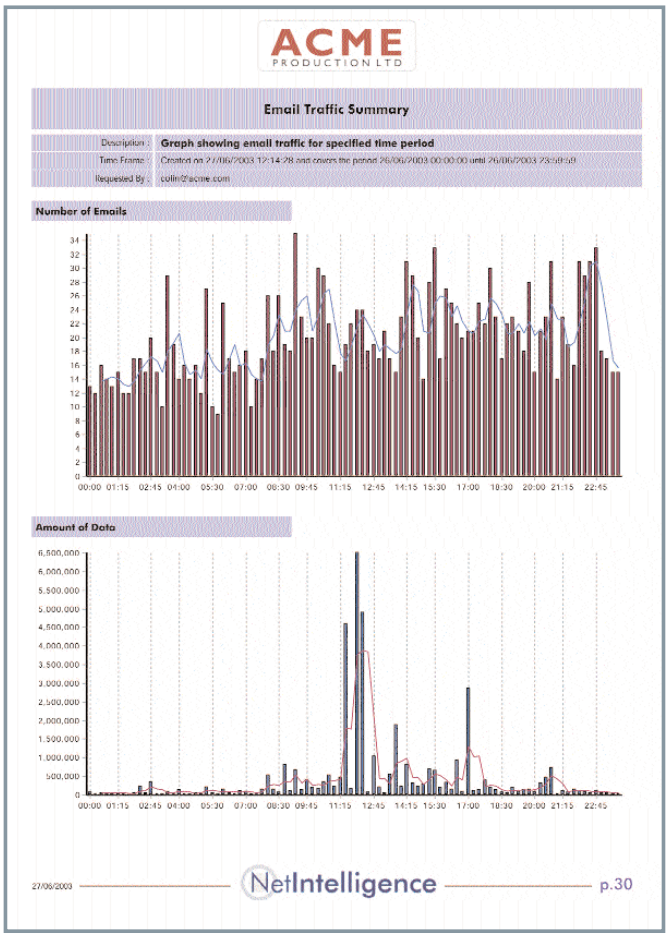

Figure 2: Reports are downloaded in pdf format. This is a sample mail flow report

known addresses. Secondly, there's a full P1 envelope subject line text analysis for keywords. Thirdly, attachments are checked for inappropriate images and files, and finally a textual content checker runs against the P2 message body (including checks on embedded URLs or flags).

Blocking lists are fully configurable; if you know of particular addresses that are causing a problem for your organisation these may be added through the management interface. The default list covers a large number of known sources of spam.

The blocking function is very important. It is not just a simple matter of blocking the obvious spam e-mails. The blocking needs to take account of other more subtle invalid messages. A classic tactic of the spammer is to use a valid address as the sender for the millions of messages sent. This results in vast numbers of non-delivery reports going back to the sender address – which might be yours. Clearly, you don't want to be receiving these messages. Happily, NetIntelligence MailFilter is easily configured to trash these messages.

In subject line analysis, the lexical engine picks up on keywords and phrases as another means of sifting inappropriate e-mail. The lexical analysis engine has been developed at NetIntelligence and is constantly being updated.

The human touch

The issue of attachments is common enough. A known e-mail address can be plagued by messages with a range of attachments from the ridiculous and funny through to the downright dangerous. At NetIntelligence a database of over 30 million examples has been built up over the past six years containing files, references to web sites, image files and other inappropriate material. This is never going to stand still and the NetIntelligence team are constantly adding new material at a reported rate of over 100,000 per week.

Finally, the lexical scanner tests the message body itself for word patterns and content. This is, of course, an essential component.

To support the operation, NetIntelligence runs a department whose job it is to monitor and add new and offending e-mail sources. A key feature of the service is this use of 'real' people who judge contentious web sites and attachments and decide which are inappropriate. The fact is , not everything can be analysed by a system.

(I have to say, when I heard about this department it did make me think: what sort of a job is this? I mean, how would you reply to folk at a party when asked what you do for a living? "Err… well, I look at porn all day!")

I discussed a whole range of issues about the e-mail filtering service with Iain Richardson, the technical bod at NetIntelligence, including the hardware platform and software used. It was no surprise to me that this is a Linux-based system; the SMTP service under Linux is extremely fast and efficient. To give complete resilience and failover, NetIntelligence runs multiple sites across the UK and the US, each supporting a series of NetIntelligence MailFilter servers. There is a failover mechanism so that in the unlikely event of a hardware failure the next server will pick up the cudgel and carry on processing.

The sheer scale of the task of e-mail checking on this level is impressive. The volume of data that is involved and the throughput required means that this sort of undertaking is a very serious business indeed. NetIntelligence is putting a lot of effort and investment into this product and the testimonials show they are doing the right thing. Managing e-mail is becoming a very tricky business and anything that makes the job easier has got to be good news. Junk mail in its broadest sense is probably the biggest headache we have at the moment. NetIntelligence Mail Filter is going to make your life easier. <

Dick Beddoe, ESM Exchange editor, is an IT consultant and instructor specialising in Microsoft Exchange and Windows NT/2000. He is an MCSE, author of the Learning Tree course on Exchange Server and director of an IT consultancy based in Surrey. You can reach him at dick.beddoe@esmag.co.uk

System requirements

None required as this is a hosted service.

UK supplier

NetIntelligence
E-mail enquiries@netintelligence.com
Web www.netintelligence.com

Cost

50p to £2 per mailbox per month depending on volume and particular service/feature set chosen.

Bottom line

Pros Simple to configure, extensive reference database and effective filter for spam.
Cons Can't weight the rules engine. Only two virus engines are supported – no choice.