

In The Boxing Ring



Network Box Technical News from Mark Webb-Johnson, CTO Network Box

Welcome

Welcome to the February 2009 edition of 'In The Boxing Ring'. In this edition, I'll be devoting a page to talk about the third email relationship based system to be released by Network Box.

If you recall, Network Box email relationships are concerned with tracking the tuple of external sender, sender attribute and internal recipient - and using the resulting database to improve anti-virus and anti-spam accuracy. The first system released was the email relationship tracking engine itself (which analysed both incoming and outgoing emails in order to build up the relationship database). The second system released was the challenge/response system (to challenge emails without an established relationship). The third system, to be released this month, uses the relationship database to automatically adjust anti-spam scores based on relationship strength. More details on this new feature are on page #2 of this month's newsletter.

Turn to page 3 of this newsletter for an important discussion of two security policy problems that we see cropping up, across a large number of our customers, time and time again. The first is the practice of whitelisting the customer's own email domains (which leads to spam from forged senders getting through to user's mailboxes). The second is the lack of outbound firewall / content filtering policies (which allows for information leakage and difficulty enforcing adequate control on user behavior). Both of these problems are discussed in detail, and proposed solutions / workarounds presented. If this affects you, please consider revising your security policy.

As usual, if you have any feedback, or comments, it is always appreciated. You can contact us here at HQ via email (nbhq@network-box.com). Or, drop by our office next time you are in town.

Mark Webb-Johnson
CTO, Network Box Corporation
February 2009

IN THIS ISSUE

2. **RELATIONSHIP SPAM SCORE ADJUSTMENTS**

The third Network Box email relationships system to be released involves adjusting spam scores (whitelisting and/or blacklisting) based on relationship strength.

3. **WHITELISTING YOUR OWN DOMAIN**

A common problem of anti-spam whitelisting your own domain leads to spam (from forged senders) getting through to end-user mailboxes. There are alternatives to this, and we present them on page 3.

3. **OUTBOUND POLICIES**

A large number of Network Box customers have little or no outbound firewall / content-filtering policies in place. The benefit of an effective outbound policy will be discussed here.

4. **FEB 2009 FEATURES**

The ongoing deployment of our recently released features.

4. **PATCH TUESDAY**

Network Box has moved to a patch Tuesday form of software enhancement release mechanism.





Relationship Spam Score Adjustments

I am pleased to be able to announce that the third Network Box eMail Relationship system is now ready for general release. This new system uses the relationship database to automatically adjust anti-spam scores based on relationship strength. The rest of this article will discuss this system, how it works, and how it can be used to be (a) more aggressive towards known spam sources and (b) kinder to known good sources of non-spam mail.

I apologise for the technical description, below - but it is important for you to be able to see how the system works in determining the adjusted spam score.

Relationship Spam Score Adjustments are usually enabled for inbound SMTP email not coming via a backup MX server (ie; direct from the sender). The system will also not run if the email has already been specifically whitelisted or blacklisted.

For each message, it first determines (using envelope analysis and geographic IP location) some basic information on the sender, including:

- eMail address
- eMail domain
- IP address
- IP /16 address block
- Country hosting the IP

The system then queries the relationship database for matches of the following tuples, and produces an average total across matching relationship records:

- Sender email address, sender country, recipient (75% confidence for a specific recipient address match, 50% for a domain match).
- Sender email address, sender /16 network block, recipient (100%

confidence for a specific recipient address match, 75% confidence for a domain match).

- Sender email address, recipient (50% confidence for a specific recipient with a previous outbound relationship established).

The confidence figures given above are the weightings given to the match. For example, if we have relationship records for previous emails from a specific sender, from a specific country to a specific recipient, then we treat this as 75% confident it is the same sender.

The relationship database stores relationship scores in the range -100 to +100 (with -100 being 100% malicious and +100% being 100% non-malicious). The database stores these for each of trust, spam, malware and policy values.

In the final stages of anti-spam, scanning, the eMail Relationship Spam Score Adjustment system:

1. Takes the average relationship spam score, multiplies by the confidence (expressed as a percentage), to determine the adjusted spam weight (expressed as a percentage). For example, if relationship records gave +100 (ie; 100% not spam) with a 50% confidence, the adjusted spam weight would be 25% (ie; on the line 0=ham to 100=spam, we are half way below the mid-way point of 50=unknown).
2. Maps the adjusted spam weight onto a configurable sliding spam score scale to determine an adjustment spam score. For example, if the sliding spam scale was -7..+7, then an email whose relationship history indicated an adjusted spam weight of 25% would result in an adjusted spam score of -3.5 (ie; 25% of the way between -7 and +7).
3. Raises a spam test result, to adjust the total spam score up or down, depending on the adjusted spam

weight. This spam test is named NB_RELATIONSHIP_SSA.

The overall approach is to look at the history, and come up with weighted scores (for trust, spam, malware and policy) based on previous averages weighted by how confident we are of the sender. We can then use that to adjust our spam scores.

Note: there is an alternative mode (called 'percentage', rather than the default 'range' mode described above) that is not enabled by default, but is available. In 'percentage' mode, the stage 2 determination of the adjusted spam score is changed to not use a sliding scale but to use the actual current spam score. For example, a message currently scoring 10.0, and having an adjusted spam weight of 25%, would result in an adjusted spam score of -5.0 being raised (and the overall spam score thus being reduced to +5.0). This is considerably more aggressive than the default 'range' mode, so is not normally enabled.

The eMail Relationship Spam Score Adjustment system is extremely effective with messages in the 'border-line' zone (typically scoring between 5.0 and 9.0 before adjustment) and can 'tip the scale' to mark them spam / not spam. It adjusts the spam score of new messages by taking into account the previous relationship history of that sender and recipient pair, and has a confidence mechanism to attempt to authenticate the sender - even in the absence of sender authentication capability in the SMTP protocol itself.

The system is extremely configurable, and tunable, and can be configured to only adjust scores up or down by configuration of the adjustment range. Work is in progress to offer the same techniques for anti-virus and policy enforcement).

The code for this new feature is in the final stages of testing and defaults tuning. We have scheduled to release it to all NBRS-3.0 customers on February 23rd 2009 as a PUSHCODE update.



Whitelisting your own domain

Every Anti-Spam system available on the market today makes mistakes. While we strive for 100% accuracy in detection of spam, and 0 false positives (i.e.; a non-spam message inadvertently detected as spam), we can never be perfect (due to the ill-defined nature of spam itself). Examples of borderline cases include one person's spam being another person's newsletter, and if I forward spam to you, is it still spam? This last example is key to the problem of the consequences of whitelisting your own domain.

The Network Box uses several technologies to avoid the problem of your own internal eMail being inadvertently treated as spam, including:

1. Comprehensive differentiation between 'outbound' and 'inbound' email. The definition of outbound is that the sender is allowed to relay mail through the Network Box and is not related to the sender's email address or domain. Inbound email is that which is not, by definition, outbound. Relay ability can be obtained either by source IP address (for internal workstations/servers and VPN clients) or by SMTP authentication (for external users relaying through the Network Box).
2. By default, anti-spam is not active for 'outbound' email. This means that email from your workstations, servers, VPN clients and SMTP authenticated users can never be treated as spam.
3. For external offices using Network Box, outbound email is digitally signed as HAM (i.e.; not spam) and that, by default, will be accepted by the receiving Network Box and trusted. This means that email from external offices protected by Network Box will never be treated as spam.

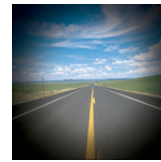
From the above list, you can see that if the network (and its users) are suitable configured, email from your fellow workers will never be treated as spam and there is zero chance of false positive.

So, why not just whitelist your own company domains, to make sure? The problem is that spammers work off lists of hundreds of millions of email addresses. They know your email address and they know the email addresses of your co-workers in the same domain. They do not know (in general) other domains you communicate with. There is no single standard for authenticating your email address and it is trivial for spammers to spoof you, or one of your co-workers, as the sender of spam.

During June 2008, Network Box Security Response conducted a forensic survey of spam emails and found that roughly 1% of spam had the envelope address sender domain the same as the recipient address domain. At that time, whitelisting your own domain would mean that 1% of spam would get through to your mailbox unblocked by Network Box (as you would have whitelisted it). However, in Dec 2008 a new wave of spam started hitting mailboxes (with MSN/YAHOO IM links and an invitation to chat) - with a high percentage of sender domain the same as recipient domain. For customers affected by this, we have seen upwards of 20% of spam being forged as coming from the customer themselves.

Sender Policy Framework (SPF) also offers a possible solution to this problem, and is supported by Network Box. With SPF, you ensure that all your outbound mail goes through defined gateways. You then publish a TXT record under your domain name DNS that lists those gateways. Receiving Mail Servers (including Network Box) can then verify this and detect spoofing of your name.

So, please avoid whitelisting your own domain names. There are several good alternatives available that can avoid the false-positive problem.



Outbound Policies

Many years ago, in the dawn of computer security, a firewall would typically be configured to allow all incoming connections but block only certain specified ports (such as telnet, rsh, etc). This was quickly found to be inadequate.

While it is common practice to now define the inbound security policy as 'block all ports except...' (as opposed to the historical 'allow all ports except...'), for a large number of our customers the same cannot be said for outbound policy.

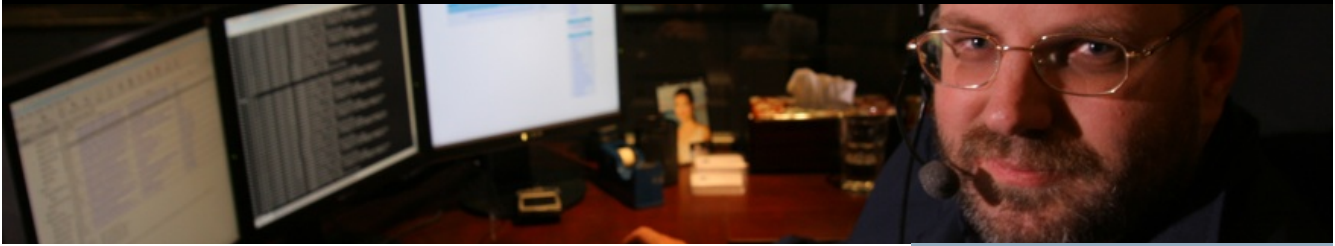
One of the most common requests we get is 'please block skype' or msn, or icq or some other protocol/application (rather than port).

The problem is that it is trivial to drill-through a firewall with open (unfiltered) outbound ports - either using tunneling software or by the application searching through all available ports until it finds one open.

The solution is to use the same approach to security policy outbound as inbound. Block all ports, and then allow (in a controlled manner) what is strictly required.

For most companies, the firewall can be configured to block all outbound connections except those to secure proxies on the Network Box (such as DNS, SMTP email, etc), and to force all web access through the Network Box Web Proxy (for control and policy enforcement) - with little or no negative impact on user productivity; but with huge improvements in security and control.

Once the default is 'block all', then fine-grained controls can be put in place (or even opened up for specific workstation addresses that require it). Please contact your local NOC for further assistance with this.



Feb 2009 Features



On Tuesday 3rd February 2009, we will be releasing several bug fixes and enhancements to the web proxy policy rating engine, including work on:

- Underscores, while technically illegal according to the DNS RFCs, are sometimes used in internal host names. We are therefore relaxing our validation for this and permitting them.
- An enhancement to allow the ‘suspicious url’ categorisation engine to be disabled / re-ordered if necessary.
- Revisions to the cache for policy categorisation, to timeout uncategorised results quicker than categorised.
- Fixes to the NBCP client-server engine to improve peer selection under high loading and/or poor Internet connectivity conditions.

The above changes will require a restart of the policy engine which will cause a few seconds pause in web proxy categorisation, but should not cause significant interruption to web browsing.

We will also be releasing extensions to our GMS monitoring packages to support ‘suppression’ of health problem alerts. In such a case, the Box Office Customer Portal will show a SUPPRESSED status for the sensor, but this will not be treated as an error. This will be used in cases where a known problem cannot be fixed by the NOC and requires customer involvement (such as high system utilisation, overload, and environmental issues).

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

February Hint

A hint for February - remember your computer room environment. For those of you in the southern hemisphere, this is the height of summer, and for those in the north, summer is just a few months away (although it might not feel like it at the moment).

Large rack-mount computers typically consume 100 - 300 watts of electricity, and that is all converted into noise, light and heat (with the vast majority being heat). Put 3 or 4 large computers together and you’ve got the equivalent of a 1KW fan heater.

With the holidays over, now would be a good time to check your air conditioning capacity. Is there still enough peak capacity after you added those couple of servers recently? Is it being regularly maintained? Are you monitoring it? etc etc.

Hint: You can check the temperature of the inside of your Network Box case remotely using the my.network-box.com interface - choose BOX/STATUS/HEALTH and look for “Sys Temp”. On some models you can also see this on the front-panel display.

Conclusions

Thank you for your support of Network Box, and the continued entrustment of your network security to our managed service. I hope you find this communication useful – if you have any suggestions, they are most appreciated, and should be directed towards your local NOC or account manager; please don't hesitate to contact us for assistance.

Mark Webb-Johnson
 CTO, Network Box Corporation
 February 2009

JAN 2009 NUMBERS

Key Metric	#
PUSH Updates	1,223
Signatures Released	356,745
Firewall Blocks (/box)	564,463
IDP Blocks (/box)	139,502
Spams (/box)	69,146
Malware (/box)	753
URL Blocks (/box)	48,300
URL Visits (/box)	2,144,895

NEWSLETTER STAFF

Mark Webb-Johnson
 Editor

Michael Gazeley
Jasmine Arif
Jason Law
 Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK
 Contributors

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com
 or via mail at:

Network Box Corporation
 16th Floor, Metro Loft,
 38 Kwai Hei Street,
 Kwai Chung, Hong Kong
 Tel: +852 2736-2078
 Fax: +852 2736-2778
www.network-box.com

Copyright © 2009
 Network Box Corporation Ltd.