In The Boxing Ring

IN THIS ISSUE

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

Welcome

Welcome to the March 2011 edition of 'In the Boxing Ring'. In this edition, we focus on Data Leakage Prevention and outbound policy scanning.

On page 2, we present a new feature of Network Box NBRS-3.0 - Outbound Data Leakage Prevention. While Network Box has historically provided extensive inbound anti-virus, anti-spam and policy enforcement, in the outbound direction we relied on URL content filtering and Intrusion Prevention. Some customers have asked us to turn on anti-spam outbound, and define anti-spam rules to enforce data leakage prevention policy rules, but that is not an ideal solution. Today, we are pleased to be able to announce the availability of a new outbound policy engine in NBRS-3.0. This new engine applies the same award-winning Network Box anti-spam technology to SMTP mail in the outbound direction and allows complex rules to be defined and policy blocks to be enforced.

Page 3 details the usual monthly features summary and March hint.

This will be the last month for this format of In The Boxing Ring Newsletter. With development of NBRS-5.0 making good progress, next month we will start a series of articles on individual features of the NBRS-5.0 platform. The newsletter will thus be split between coverage of the existing NBRS-3.0 platform as well as the upcoming NBRS-5.0.

You can contact us here at HQ via eMail (nbhq@network-box.com). Or, drop by our office next time you are in town. You can also keep in touch by following our Network Box Security Response twitter feed at

twitter.com/networkbox

Mark Webb-Johnson

CTO, Network Box Corporation

March 2011

NETWORK BOX

DLP - Data Leakage Prevention

Background

A large number of our customers have asked us, over the years, to enforce policy blocks on outbound content. Examples include such things as specific words, document files, credit card numbers, social security numbers, etc. These customers have often asked us to turn on anti-spam outbound so they could configure such rules in the anti-spam system.

The problem is that the anti-spam system is designed to detect inbound spam, not outbound. It is designed to protect the customer from Internet spam, not the Internet from customer spam, and has not facilities for policy enforcement or notification.

The Network Box DLP Engines

We are pleased to announce the immediate availability (in the Network Box March 2011 Patch Tuesday release) of a new outbound policy engine in NBRS-3.0, for Data Leakage Prevention (DLP).

Implemented in two parts, this new engine applies the same award-winning Network Box anti-spam technology to policy on SMTP mail in the outbound direction and allows complex rules to be defined and policy blocks to be enforced.

1. The 'dlp_rules' engine uses the same core technology as our anti-spam engine 'as_rules' (including complex pattern matching, content analysis, and heuristics) to scan outbound smtp emails and set 'tests' (similar to anti-spam tests) to record that certain rules (or sets of rules) have matched.

2. The 'policy_dlp' engine checks dlp tests and applies policy blocks for those tests that have triggered (and that it has been configured to block).

By splitting the scanning and enforcement phases, we get a very flexible implementation that can be selectively enabled and disabled on a per-user basis.

'dlp_rules' engine

The 'dlp_rules' engine runs at policy scanning stage (after anti-virus and anti-spam). This can be configured to only run outbound (the default), inbound, or bi-directionally.

The engine goes through each section of the unpacked eMail message and runs its rule-set against each such section. The rules include the ability to perform sophisticated pattern-matching scans, examine content headers (such as derived content type, and the results of previous scan stages), and apply boolean and arithmetic logic to previously triggered tests. Any rule that matches results in a named 'dlp test' being set.

Examples of such rules are:

- A VISA credit card number.
- An AMEX credit card number.
- Either a VISA or an AMEX credit card number (boolean logic).
- A validated social security card number.
- The MD5 checksum of a message matching a restricted set of documents to be blocked.

'policy_dlp' engine

The 'policy_dlp' engine is configured with a list of direction, named dlp tests and thresholds. This permits sophisticated policy enforcement rules to be configured. Examples of this include:

- Block outbound emails with more than 5 credit card numbers in them.
- Block outbound emails containing specific attachments (identified by md5 hash).
- Block outbound emails containing encrypted ZIP files.
- Block inbound emails containing Microsoft Excel documents.

As you can see, such facilities exceed those provided by most common Data Leakage Prevention systems.

Customisation

The 'dlp_rules' and 'policy_dlp' engines have today been released, along with a framework set of signatures, for all Network Box NBRS-3.0 customers. The engines, by default, do not run and will not impact performance or throughput of customers not using this facility.

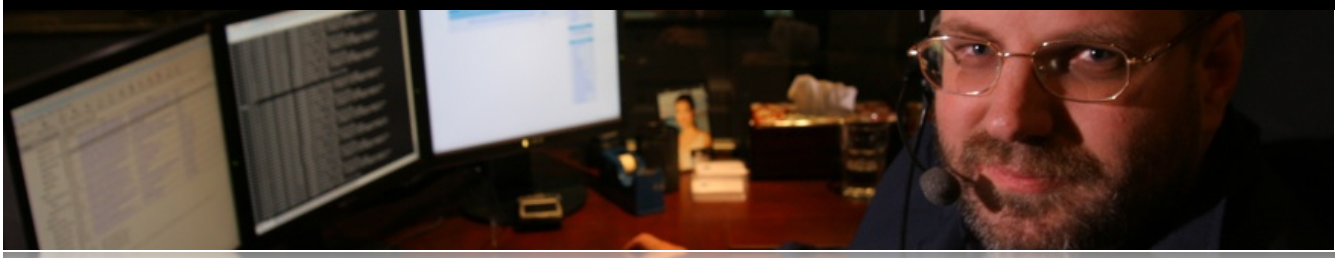
Data Leakage Prevention systems often required extensive customisation, which is beyond the scope of the standard managed services agreement Network Box has with most of our customers. No two customer requirements are the same, and the rule sets and policies must usually be designed, developed and configured on an individual customer basis.

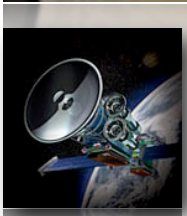
However, the availability of the engines and sophisticated rules language should greatly speed-up such customisation (and reduce costs appropriately).

Most importantly, this can be done with little impact on the existing anti-virus and anti-spam phases of scanning - and without the confusions caused by using the wrong tool for the job.

Conclusion

If you have a requirement for this technology, please discuss with your local Network Box account manager or support centre. We'll examine how closely your requirements match our capabilities and advise as appropriate.





March 2011 Features

On Tuesday, 1st March 2011, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Enhancements to the Global Monitoring System (GMS), and improved performance and functionality in the ticketing of GMS issues.
- Enhancements to the Global Monitoring System (GMS) reachability heuristics to better detect and identify reachability events and report them in a unified manner.
- Fixes to the Kaspersky v8 anti-virus engine to add support for newer formats of the winzip '.zipx' archive format, and address concerns with scanning of some very large archives.
- Release of the outbound mail Data Leakage Prevention and policy enforcement engines for mail scanning.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

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

March 2011 Hint

Box Office Notifications have been available since November 2011, but still only a limited number of customers are using them to their fullest extent.

The Notifications system offers a sophisticated facility to notify users of changes and events they need to know about. This is configured using My Account (and the Users Module) within Network Box Office. Notifications can be configured for individual classes and types of events (such as ticket updates) and sent as eMail, Apple iOS APNS (Push Notifications), Mail-to-SMS or SMS messages. You can even configure different boxes to have different notifications sent to different contact points (such as email addresses) and limit notifications to certain times of the day (eg; SMS after 6pm, email before).

Configuring this system correctly will allow us to notify you of the events regarding your devices under management, and will most importantly allow you to control how and when you want to be contacted. It can also be used for audit and management control of the service.

The manual for how to configure this is on-line and reached via the 'HELP' link at the top right of Network Box Office.

The March 2011 hint is that you investigate the Notifications facility within Network Box office, and help us to help you to configure it best.

Mark Webb-Johnson,

CTO, Network Box Corporation

FEBRUARY 2011 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	611	-33.7
Signatures Released	281,321	-38.6
Firewall Blocks (/box)	738,795	+0.2
IDP Blocks (/box)	100,142	+0.1
Spams (/box)	25,220	+8.2
Malware (/box)	705	+66.7
URL Blocks (/box)	119,637	+29.7
URL Visits (/box)	3,939,024	+0.1

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jasmine Arif
Nick Jones
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