In The Boxing Ring

IN THIS ISSUE

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

Welcome

Welcome to the May 2011 edition of 'In the Boxing Ring'. Continuing on from last month's format changes, as we start the run-up to the release of NBRS-5.0. for the rest of this year, each month we will present one topic on NBRS-5.0 (the upcoming major Network Box firmware release). The monthly hint will go, and is replaced with an entire back page on the updates being released to the existing NBRS-3.0 product. This front page will remain, and summarise what is new and notable.

This month, on pages 2 and 3, we present details on the NBRS-5.0 configuration system. This new NBRS-5.0 system takes the NBRS-3.0 foundation and reworks it to provide full revision control, auditing, clustered replication and bi-directional syncing - all on a single unified base.

We've taken all the customer feedback from the past ten years of providing a managed service, and built it into a system capable of meeting the needs of our customers (as well as the regulatory and compliance requirements of their security auditors). The configuration system in NBRS-5.0 is a core foundational component for our new platform.

By unifying the configuration into a single store, and providing support for revision control, auditing, cluster replication and bi-directional sync, we've taken what we had with NBRS-3.0 and extended it from the NOC to the BOX.

Page 4 details the features and fixes to be released in this months patch Tuesday for NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years), and this page will be used to keep you informed as to what is happening with our core product.

You can contact us here at HQ by eMail (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch by several social networks:

Twitter: http://twitter.com/networkbox
Facebook: http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse
LinkedIn: http://www.linkedin.com/company/network-box-corporation-limited

Mark Webb-Johnson
CTO, Network Box Corporation
May 2011

The NBRS-5.0 Configuration System

For this month's topic on NBRS-5.0, we'll be presenting information on the design and use of our new configuration system, called NBCONFIG. The NBRS-3.0 configuration system offered us the most flexible configurations for any appliance available today (managed or otherwise), but brought with it complexity and suffered from lack of fundamental support for clustered configurations. The new NBRS-5.0 configuration system takes that foundation and reworks it to provide full revision control, auditing, clustered replication and bi-directional syncing - all on a single unified base.

This page describes the system from a technical perspective. Overleaf, we talk about it from the perspective of what it means to you.

NBRS-5.0 Foundational Storage Database

Have you ever tried to sync your mobile phone to a desktop computer and been presented with 'conflict' warnings or lost data? If so, you'll be aware of the problem caused by trying to synchronise different databases in different formats. With so many different objects (e.g.; emails, address book entries, calendar entries, etc) and no standard format, the necessary conversions and attempts to discover which object was modified first, cause endless frustration.

To avoid this issue, the NBRS-5.0 configuration system is backed by a single unified foundational storage database that stores all configuration parameters and their values in the same way. At its core, this is a parameter[instance]=value store (for example network.interface.ip.address[ethernet port 1]=192.168.1.1/24).

It doesn't matter if the configuration item is a network address, whitelisted sender or access control list - they are all stored in the same way to avoid any conversion conflicts.

The store itself is in two parts:

1. The first (smallest) part holds just the current values.
   It is this that is used for fast indexed lookup of the current configuration value (with one record for each parameter[instance]).

2. The second (larger) part holds a full history of revisions.
   It is this that is used for historical information and revision control (with one record for each revision of each parameter[instance])

Along with the revision timestamp (to determine which revision was first), the store holds information on who made the revision and why. As configuration changes are made, the data is written to both parts in the same transaction - giving us the foundations of revision control and auditing.

Cluster Synchronisation

Having a configuration store with records chronologically time stamped makes it relatively simple and straightforward to bidirectionally synchronise changes to the configuration amongst a cluster of boxes (along with all the revision control and auditing information that accompanies them). The problems of conflict resolution are solved (as the logical result is that the latest change is always the winner).

To support restricted cluster synchronisation, the store also includes information on the cluster level and order (and allows storage of different values for each such cluster level and order).

- The cluster level refers to a group of boxes (e.g.; `global', `Europe', `San Francisco Office', or a particular box).
- The cluster order controls how conflicts are resolved. Values can be configured to `Insert' (i.e.; override, or come first), `Append' (i.e.; provide a default, or come last), and can even be defined as override-able or not (for example to provide a regional setting that can never be overridden by a regional office).

To provide for the grouping of boxes into clusters, the synchronisation system can be configured to only synchronise configuration values at, or above, a certain cluster level.

The Configuration Service

The NBRS-5.0 configuration system is controlled by a configuration service running on each box. It is this service that is responsible for the storage and maintenance of the configuration, as well as synchronisation amongst members of the cluster. It also handles notifications and actions necessary whenever a particular configuration value is set (for example; setting the IP address on a network port when the corresponding configuration is changed).

The inclusion of revision control (a full history of changes), and synchronisation of configurations amongst the cluster, means that the backup and restore of configurations is automatically available. Individual box configurations can be replicated, to provide for redundancy and fast restore to a replacement device upon a hardware failure.

NBRS-5.0 Configuration: What this means to you

Having presented the technical aspects of the NBRS-5.0 configuration system, let's now have a look at the practical aspects - what this means to you.

The Box is a NOC

NBRS-3.0 (and its predecessor NBRS-1.1) had a clear separation between the BOX and its NOC. Configurations were maintained on the NOC (including full revision control, auditing, etc) and PUSHed to the boxes. This award-winning approach works fantastically (especially when a device fails and replacement hardware can be reconfigured and brought online in minutes).

However, there were some configuration items in NBRS-3.0 that were maintained by the customer on the box itself (such as email whitelists, content filtering customisations, etc), and those could not be bidirectionally synced to the NOC.

The NBRS-5.0 configuration system solves this by unifying all the configurations to be stored and synchronised in the same way. It doesn't matter if they are maintained on the box or on the NOC, in the web-based UI or on the command line, they are bidirectionally synced and both NOC and BOX benefit from full revision control and auditing.

In NBRS-5.0, the BOX is a NOC. One or more boxes can be configured to control the configurations of a cluster of boxes (dependent, of course, on ownership and access rights).

Clustered Configurations

The inclusion of support for clustered configurations in NBRS-5.0 will allow larger customers to benefit from a global configuration. A suitably authorised administrator can recategorise a web site at the global office level and that setting would automatically synchronise to all the organisations' boxes. These clusters of boxes can be configured at various levels (typically global, regional, office and box, for large organisations) and controls put in place to restrict which administrators can make changes at which levels.

Even for smaller customers operating just two boxes in a high-availability pair can arrange for the pair to operate as a cluster and for settings to automatically replicate between the two boxes (wherever the setting is changed). Should the primary box fail, and the secondary box take over its role, changes made on the secondary are automatically synchronised back to the primary when it recovers.

Whatever the size of organisation, NBRS-5.0 support for clustered configurations leads the industry by including this in the base foundation, and not requiring a separate management system / NOC (although you may, of course, choose to keep this separate).

Regulatory Support

As the configuration in NBRS-5.0 is unified and stored in one single place, it can be exported in a variety of formats, and used for both backup and regulatory compliance purposes. This has been the #1 request from customers around the world, and we are glad to be able to finally provide it in the format you require.

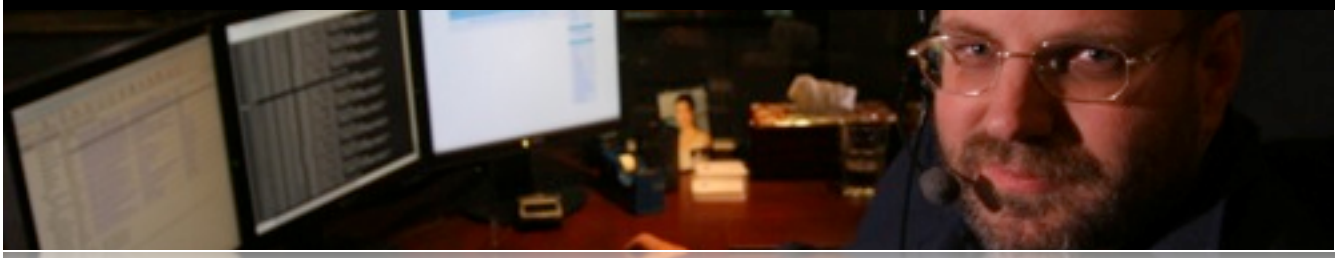
The inclusion of full audit support in the configuration (whether the change is made on the BOX or the NOC) provides a clear timeline of changes made to the configuration, who made them and why. This will meet the regulatory requirements, without having to merge two reports (one from the NOC and the other from the BOX) as is currently the case with NBRS-3.0.

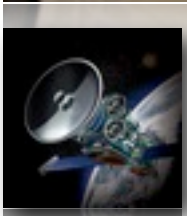
Conclusions

We've taken all the customer feedback from the past ten years of providing a managed service, and built it into a system capable of meeting the needs of our customers (as well as the regulatory and compliance requirements of their security auditors).

Full access control and auditing secure the configuration, both on the box and on the cluster.

The configuration system in NBRS-5.0 is a core foundational component for our new platform. By unifying the configuration into a single store, and providing support for revision control, auditing, cluster replication and bi-directional sync, we've taken what we had with NBRS-3.0 and extended it from the NOC to the BOX.





May 2011 Features

On Tuesday, 3rd May 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:

- The start of a phased deployment for configurable heuristic support in the Kaspersky anti-virus scanning engine. Support for this has been in internal beta for some time now, and we will be rolling this out to all customers during May 2011. The new configurable heuristic support allows the heuristic level within the Kaspersky anti-virus engine to be set, on a per-box basis, to Off, Shallow, Medium or Detailed (with individual settings for mail and http scanning).
- Minor enhancements to the health monitoring system.
- Performance enhancements to the web proxy policy engine (improving performance for boxes with many hundreds of users and dozens of web proxy policy rules).
- Various enhancements and minor fixes to the my.network-box.com administrative interface.

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.

Security Response on Facebook

This month, we have released a Facebook page for Network Box Security Response:

http://www.facebook.com/networkboxresponse

The new page is designed to give you a one-stop place to go for the latest security news from our Security Response engineers. We hope you like it.

With the aim of improving our transparency, we've also updated the main Security Response website with some new statistics an charts to show changes to the counts for key signature performance metrics. Now, you can see not only the current number of protection signatures we use, but also changes to those numbers over time. In April, we PUSHed 633 updates to our customers, and released almost a quarter of a million new protection signatures. All this, coupled with millions of signatures in our cloud-based protection systems such as Z-SCAN.

APRIL 2011 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	633	+34.1
Signatures Released	240,055	-16.6
Firewall Blocks (/box)	775,155	+9.2
IDP Blocks (/box)	141,943	+8.0
Spams (/box)	19,666	-7.4
Malware (/box)	932	+24.8
URL Blocks (/box)	115,658	+0.6
URL Visits (/box)	3,806,940	-2.5

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