In The Boxing Ring

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

Welcome

Welcome to the November 2010 edition of 'In the Boxing Ring'.

This month, we launch the M-385 model as direct replacement for our highly-successful M-380 model. Using Intel® Core™2 Duo CPU technology, 2GB RAM, 4GB of industrial flash memory, and a 320GB SATA hard drive, this model leads the performance in the Network Box M series of models. Turn to page 2 for details.

Also on page 2, we discuss a set of enhancements to the Global Monitoring System, including adding support for Box Office Ticketing based on GMS alerts, as well as integrating monitoring of external devices from the Network Box itself. These two new extensions to the Network Box Global Monitoring System allows us to expand the monitoring capability and improve our service to you.

On page 3, we present the release of the Network Box Office Notifications system, replacing the old 'want ticket mail' option.

Also on page 3, we present the new v3.3 of the Network Box iOS App, supporting APNS Push Notifications.

On page 4, we present our monthly hint (this month on the importance of monitoring box utilisation and workload), and outline the software updates delivered as part of this month's software release.

As usual, if you have any feedback, or comments, they are 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.

You can also keep in touch by following our Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
November 2010

NETWORK BOX

Network Box M-385 Model

Network Box M-385

Available today, the Network Box M-385 model is the direct replacement for our highly-successful M-380 model. Using Intel® Core™2 Duo CPU technology, 2GB RAM, 4GB of industrial flash memory, and a 320GB SATA hard drive, this model leads the performance in the Network Box M series of models.

As standard, the model comes with 1x 10/100 TX and 6x 10/100/1000 TX ethernet ports. It can be expanded with either (a) one 4x 10/100/1000 TX, or (b) one 4x Gbe SFP module; offering up to a total of 11 independent ethernet ports to cope with the most demanding of network requirements.

The Network Box M-385 is a member of the Network Box S-M-E product range, used to protect medium-sized organizations. It is designed to be 19 inch rack mounted with the included mounting kit. The Network Box M-385 has all of the same capabilities as the rest of the Network Box range. Updates to the systems are performed in real-time using PUSH technology. Whenever a new anti virus signature, security patch or software update is available, it is pushed out to every Network Box around the world, in an average of less than 45 seconds.

M-385 TECHNICAL SPECIFICATIONS

Processor	Intel® Core™2 Duo 3.0 GHz 6 MB Cache
RAM	2 GB
Flash	4 GB Industrial
Disk	320GB SATA HDD
Network	1x 10/100 TX 6x 10/100/1000 TX
Options	[A] Network Module (4x 10/100/1000 TX) [B] Network Module (4x Gbe SFP)

Global Monitoring System Ticketing and Device Monitoring

NOC staff generally work on two sorts of tickets with you - the first are service tickets and relate to configuration changes and general troubleshooting, while the second are tickets raised in response to issues detected by our health monitoring systems.

In order to streamline this process, this month we are releasing changes to Box Office to explicitly support both kinds of tickets. You, the customer, will see both types of tickets in a single unified interface, but the Box Office Notification system (released this month) treats the two ticket types as different, and allows you to control how you want to be notified about the two different sorts of problems. The new health tickets are directly connected to the Network Box Global Monitoring System, and allow NOC operators to associate device health problems with customer tickets, and to update those tickets in real-time as the GMS detects changes in the health of your devices.

Also released this month is a facility to allow a Network Box participating in the Global Monitoring System to monitor and report on the status of sub-devices. These may be other Network Boxes, customer devices, ISP devices, or other parts of the global Internet infrastructure. This allows, for example, a Network Box to monitor connected mail servers, DNS servers, etc, and to alert (via the standard GMS systems, as well as the new Box Office Notifications) both customers and Network Box NOCs as to problems found.

These two new extensions to the Network Box Global Monitoring System allows us to expand the monitoring capability and improve our service to you.
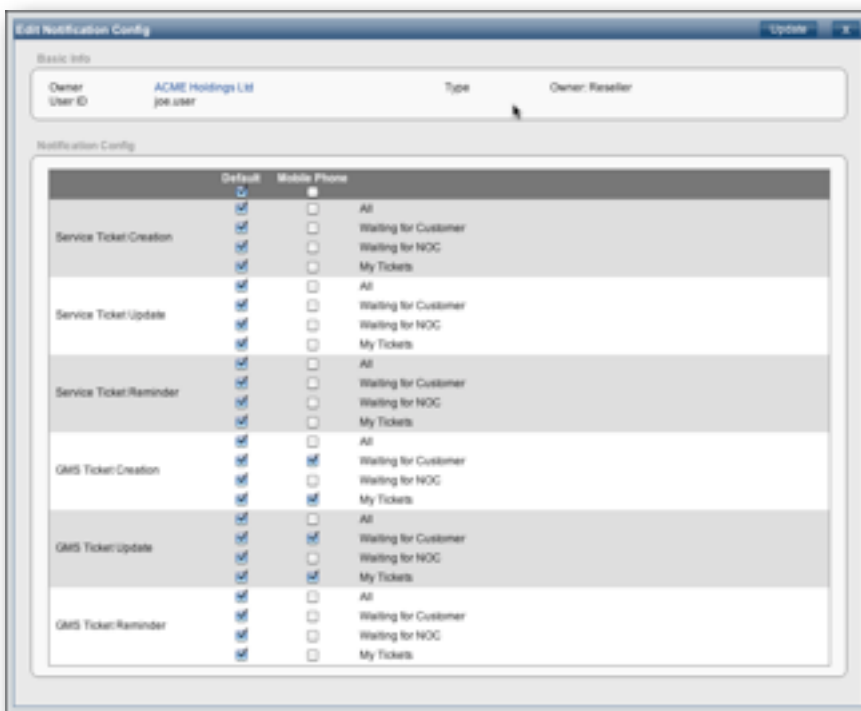
Network Box Global Monitoring System

Network Box Office Notifications

As presented in last month's In The Boxing Ring, the Box Office Notifications system is being released to all users, globally, on Tuesday 2nd November 2010.

The new Box Office Notification system replaces the old 'want ticket email' facility (which allowed users to receive simple emails whenever a Box Office ticket was changed). The new replacement 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 Box Office. To use the system, you firstly create Contact Types (which are methods you can be contacted at, and filters to define when and for what boxes these contact types should be used). Then, you update the Notification Config to let the system know which events you want to be notified on, and which contact types to use. The initial release of this system supports the following notification methods:

- Audit - to create an audit trail of notifications. This does not send out any notifications, but merely records a notifiable event in your notification list.
- Email - to notify you by SMTP eMail. You can choose an eMail template to use, and enter your eMail address that you want to receive the notifications on.
- iOS APNS - to notify you by the Apple Push Notification service (APNS). You pair your Apple iOS device (iPhone, iPad or iPod Touch) to the service using the Network Box App for the iPhone/iPad/iPodTouch.
- Mail-To-SMS - to notify you by Mail-To-SMS gateways. Your Mobile Phone Provider may provide such a service, whereby Network Box can send an eMail to your Mobile Phone Provider gateway, and they forward it on to you as an SMS.
- SMS - to notify you by SMS message to your mobile phone. You enter the mobile phone number that you wish to be notified using, and we deliver over the telephone network. Note that use of this notification method will require 'SMS credits' purchased from Network Box. Please contact your account manager for further information.

The old 'want ticket email' settings have already been migrated to the new system - which should be live and available for your use by the time you get this newsletter. The Box Office Customer Portal manual (downloadable by clicking HELP at the top right of Box Office) is also available for your reference.

When you plug into the world it's easy to forget that the world is also plugged into you

Copyright 2008 - 2010
Network Box Corporation Ltd.

One More Thing...

Version v3.3 of the Network Box iOS App (for Apple's iPhone, iPad and iPod Touch devices) has been submitted to the Apple App Store, and should be available for download within the next few days.

This version adds support for the Apple Push Notification Service, and is fully integrated with the new Box Office Notifications system. When you first run the new App, it will ask you for permission to send you notifications, and if you answer 'OK', it will automatically create you a Box Office Notification Contact Type tied to your Apple device, for you to manage the notifications. We have also added a Notifications tab, to allow you to see notification history.

Support has been added for new box models (including the M-385 released this month), and some welcome performance improvements have resulted in two-to-three times speed improvement in refresh of ticket and box status lists.

The App is a free download on the Apple iTunes App store. You can find it with a search for 'Network Box' in the business category.

As always, if you need assistance with this, please contact your local Network Box NOC.
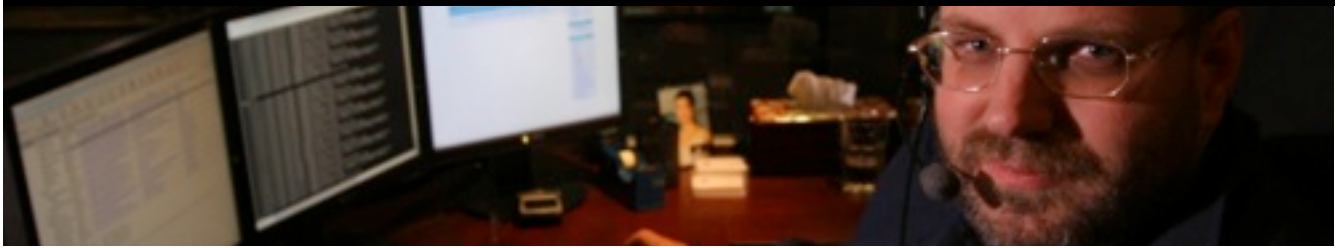
November 2010 Features

This month, we emphasise our work on Box Office, and there will be minimal changes to the box firmware itself. While the Box Office changes will be deployed on the Patch Tuesday itself, NOCs will be conducting staged releases of device firmware updates over the next 7 days. The changes include:

- Support for the new M-385 model.
- Global Monitoring System Ticketing.
- Global Monitoring System Device Monitoring.
- Box Office Notifications.
- Network Box iOS App v3.3.
- Revisions to the my.network-box.com and content policy filtering system to add support for new licensing options.
- Revisions to the Protected Service Proxy system addressing issues with accessing some custom websites.
- Minor revisions to the Global Monitoring System health checks on the Network Box itself, including foundational work for a new system kernel.

The above changes should not require a device restart, but may impact running services at some sites, so NOCs may contact affected customers to schedule a deployment timeframe.

The enhancement work will be handled by the regional NOCs and will not require any action on your part. Only minimal service interruption is expected to be required.

October Hint: Utilisation and Workload

Unfortunately, the workload of a perimeter security device such as Network Box has little to do with the number of users on the LAN, but has much more to do with what they are doing combined with malicious behavior on the Internet you are connected to.

A 100 user organisation who gets 5,000 HAM emails a day (50 per user per day), may also be getting 45,000 SPAM emails a day - leading to a workload of 50,000 emails a day. However, spam volumes fluctuate over time, so that same organisation may have to deal with anywhere from 25,000 to 95,000 emails, even though the HAM email figure of 5,000 stays constant. Average workload may half or double over time, and that is completely unrelated to what the users on the LAN are doing.

The Network Box Office BOXES module keeps track of actual box workload, and can present that as tables and charts. For more detailed information, the my.network-box.com administrative interface provided for detailed drill-down into box workload statistics.

It is important to keep an eye on box workload, as the behavior of both LAN users, and Internet malicious activity changes over time. Identifying trends early, and ensuring sufficient capacity, are vital to maintaining adequate service levels.

If you need assistance with capacity planning, or the many techniques Network Box can offer to reduce system workload, please talk to your local support NOC, who are there to help.

OCTOBER 2010 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	833	-20.2
Signatures Released	445,679	+76.5
Firewall Blocks (/box)	702,081	-0.8
IDP Blocks (/box)	128,466	+5.5
Spams (/box)	28,460	-23.7
Malware (/box)	831	+21.8
URL Blocks (/box)	127,338	+16.8
URL Visits (/box)	3,579,505	+1.5

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