FEB 2014

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the February 2014 edition of In the Boxing Ring

This month, we discuss in detail the concept of **entities**. In the realm of gateway threat protection, it is notoriously difficult to determine what a 'user' is. This could be a workstation, mobile device or a logged in user. Network Box addresses the problem with entities.

On pages 2-3 we talk about what these are, how they are used, and how they can help you monitor and control the policies of the user and resources on your network.

In our effort to provide accessibility, we are renaming NBRS-5.0 and NBRS-3.0 to **Network Box 5** and **Network Box 3** respectively. For clarity, this month we are referring to both names, however, starting next month we will be using the new rebranded names.

Please also note, starting this month, we are no longer publishing the monthly key metrics statistics. We will resume publishing these statistics later in 2014, once the percentage of Network Box 5 boxes deployed increases.

Finally, on pages 4-5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2014

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 with us 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

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

Entities

Network Box 5 introduces the concept of entities. This article discusses what these are, how they are used, and how they can help you monitor and control the policies of the users and resources on your network.

The 'user'
Problem

In the realm of gateway threat protection, it is notoriously difficult to determine what a 'user' is.

- Is it a workstation? But what if the workstation is shared and used by more than one person?
- Is it a logged in user? But what about servers (such as mail servers) handling messages for hundreds or thousands of different mail accounts?

Network Box 5 addresses the problem with the introduction of the concept of an *entity*.

The Entity
Solution

Put simply, a Network Box 5 entity is either a shared server (a network entity) or a person/automaton (a user entity). You would typically create individual entities for each of your shared servers, as well as for each user account on your system.

Every network session that passes through the Network Box 5 device is then allocated to a set of 4 entities:

1. A local network entity
2. A local user entity
3. A remote network entity
4. A remote user entity

The terms 'local' means belonging to the protected network, while 'remote' means external. In the case where one of the four entities cannot be determined (or is not tracked), a special entity #0 (others) is used.

In this way, we can track the server the session came from, the server it is going to, the user at the remote end, as well as the user at the local end.

To illustrate, let's look at an example:

> Let's say user Joe sends an eMail from his workstation to user Mary, delivered to the mail server.

1. A local network entity: Joe (his workstation)
2. A local user entity: Joe (the user)
3. A remote network entity: Mail Server
4. A remote user entity: Mary (the user)

Entity Attributes

To implement the entity system, Network Box 5 uses entity attributes. Each entity in the system is assigned an ID (a number) and is uniquely identified by a name. Entities can have one or more attributes assigned to it, and these attributes includes things such as:

- Passwords
- eMail addresses
- Host names
- IPv4 addresses
- IPv6 addresses
- MAC (hardware) addresses

Entity attributes are dynamically created and maintained by the system, both by synchronization (against such things as Active Directory or LDAP servers) and by learning behavior (based on transactions such as logins, logouts, DHCP allocations, verification, etc). In addition, entities and their attributes can be manually maintained and tuned from the administrative consoles.

What can be done with entities?

As each network stream is assigned to entities, and per-minute summary statistics are maintained on the network bandwidth used by entities, the first real use of entities is for reporting. With Network Box 5, you no longer need to report on network bandwidth usage by IP address, but can now focus on the users of the bandwidth.

As a result of the attribute system, you no longer need to worry how to group reports by user. A particular user may have multiple IP addresses at one time (for example his workstation, desktop VOIP phone, as well as mobile phone and tablet on wifi) – but each of these are attributes of the user's entity, so are automatically grouped by that user.

The entity system becomes a large on-the-box cache of information about the users of the network. Once built-up, this can be used for a multitude of security functions. A good example is envelope verification (verifying incoming eMail RCPT TO email addresses against the email attributes of entities on the system, and refusing email to non-existent addresses).

Entities can be used for problem tracing. When the user calls up complaining of a problem he is happening, the administrator can call up information on all that user's activity, across all his devices, and show all policy control blocks for that user (regardless of device or location).

And, entities can be used for control. The policy rules can now control entities, irrespective of the device they are associated with.

Summary

In summary, the entity system in Network Box 5 provides for grouping the activity of all the devices in your network, and assigning that activity to individual users. Comprehensive reporting and policy control facilities are then made available – all based on the users, not IP addresses, of your network.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 4th February 2014, 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.

Network Box 5 (NBRS-5.0) Features
February 2014

This month, for Network Box 5, our patch Tuesday set of enhancements and fixes include:

- Improvements to boot-time during initial power-up and reset of the device
- Performance enhancements in SMTP client/server protocol scanners
- Improvements to mail quarantine facility
- Enhancement to include support for import/export of periodic reports
- Support for showing detailed record information for Web Application Firewall blocks
- Enhancements to mail scanning systems for anti-spam and policy control
- Miscellaneous enhancements to VPN sub-systems
- Support for fine-grained control of mail policy based on classification confidence percentages
- Release of User Portal security modules
- Release of administration guides for new security modules
- Improvements to transparent proxying in bridging configurations
- Various security patches to core SSL protocol
- Support for option to prefix mail subjects with custom text (as an alternative to message quarantine)
- Support for option to control disposition (discard, defer or reject) for mail policies
- Support for pipelining in SMTP protocol

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.

NETWORK BOX

Network Box 3 (NBRS-3.0) Features February 2014

On Tuesday, 4th February 2014, 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, for Network Box 3, these include:

- Extensions to Box Office regarding device provisioning
- Extensions to Box Office to improve support for regional NOCs
- Various (mostly internal) enhancements to several internal support systems

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.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor	Network Box Corporation nbhq@network-box.com or via mail at:
Michael Gazeley **Nick Jones** **Kevin Hla** Production Support	**Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong
Network Box HQ **Network Box UK** **Network Box USA** Contributors	Tel: +852 2736-2078 Fax: +852 2736-2778 www.network-box.com

Network Box
South China Morning Post

Following the recent massive cyberattacks that hit large retailers Target and Neiman Marcus in the United States, Network Box Managing Director, Michael Gazeley was interviewed by the South China Morning Post.

"The biggest retail credit card breach in history has just happened, yet the vast majority of information-technology managers, and even well-known cybersecurity professionals, seem to be almost pathologically fixated on the last attack rather than the next attack."

Link: http://www.scmp.com/business/companies/article/1405804/rise-cybercrime-poses-risk-smaller-hong-kong-firms

Network Box HQ
Onsite Visit

JARING come together

Network Box welcomed our partners at JARING Communications and members of the IT department of Universiti Teknologi PETRONAS (UTP) to Network Box HQ. Those that were present were given a detailed overview of the Network Box 5 UTM+ and Anti-DDoS WAF+ engines. In addition, they were introduced to the new 64bit hardware.

NETWORK BOX USA
The Denver Post

THE DENVER POST

Network Box USA's CTO, Pierluigi Stella, was quoted in The Denver Post Business, in an article titled, "At CES, new data collection in gadgets raises interest, and eyebrows."

LINK: http://www.denverpost.com/business/ci_24880720/at-ces-new-data-collection-gadgets-attracts-interest

NETWORK BOX