AUG 2015

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the August 2015 edition of In the Boxing Ring

This month, we are proud to release the results of the unification of our ACLs and Rules engines across all components of our UTM+ platform. The ACL/Rules engine is the software component that implements policy decisions to allow or deny traffic. This unification brings important performance and functionality benefits, but most importantly standardises the way we treat ACLs and rules throughout the Network Box 5 system. This is discussed further on pages 2–3.

Back in 2006, we released the NBRS-3 (Network Box 3) platform, and since then it has been the core backbone for Network Box security appliances protecting thousands of our managed customer networks around the world. However, times have moved on, and the platform is now almost 10 years old and hard to keep up-to-date on modern hardware. Thus, as of 1st August 2015, we are announcing the sunset of the Network Box 3 platform. This, and our Sunset Policy, is discussed further on page 4.

On pages 5–6, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. Based on Sunset Policy, we will continue to support, Network Box 3 until at least late 2018.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2015

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:

Unification of ACLs and Rules Engine

This month, we are proud to release the results of the unification of our ACLs and Rules engines across all components of our UTM+ platform. This has been a long-term project for us here at Network Box Security Response, and this month marks the culmination as we release the final components of this important system.

The core purpose of a Network Box 5 appliance is to categorise traffic passing through the device, and then to allow policy decisions to be made based on those categories as well as other attributes of the traffic. We don't block spam, but instead we categorise an eMail message as 'spam' and then allow a policy decision to be defined to deny the traffic containing that message. This is a subtle, but important, distinction.

The ACL/Rules engine is the software component that implements those policy decisions. The configuration defines the security ACLs, as well as the rules, and the ACL/Rules engine implements that policy. The issue, up until now, is that our UTM+ appliances contain many components, and each component had its own rules engine. Today's release unifies all components of the Network Box 5 appliance to use the same core ACL/Rules engine. Previously, the configuration language had been unified. Now, today, the implementation of those rules is unified. This brings important performance and functionality benefits, but most importantly standardises the way we treat ACLs and rules throughout the Network Box 5 system.

ACL Types and wildcarding behaviour

Perhaps the biggest change with the release of the new ACL/Rules engine is the standardisation of ACL types and their wildcarding behaviour. We now support 51 different ACL types, and many support wildcarding behaviour.

In general, all ACL types are now case insensitive.

For those ACL types that support parts separated by delimiters (for example applications such as remote.citrix.ica where the parts are separated by "."), we support wildcarding at the delimiter level (so that for example "remote.*" would match "remote.citrix.ica"). In particular, this is true for application (application identifiers), domains (such as cloud.network-box.com), email addresses (user@domain), file content types (separated by delimiter "/"), file types (separated by space delimiters), http pathnames (separated by delimiter "/"), http hosts (similar to domains), http urls (with delimiters "/" and "." for the path and domain parts, respectively), http user agents (separated by space delimiters), ethernet mac addresses (with delimiter ":"), signature names (with delimiter "."), signature sets (with delimiter ":"), threat IDs (with delimitr "."), and waf tags (with delimiter "/').

For IP acls, we now support subnetting. So an acl containing 10.0.0.0/8 would match 10.1.2.3.

Policy Rules in Network Box 5

In Network Box 5, the configuration language for policy rules has been standardised. We now support rule subroutines, throughout the system, and the rules language has been extended to support many rich operators. In general, a rule is expressed as:

<action> { <term> } [with { <attributes> }]

An <action> is the final action of the rule. If all the terms are true, then that is the result of the rule. Examples of actions are 'permit', 'deny', etc.

A <term> is usually a three part <param> <operator> <value>.

1. The <param> is an attribute of the traffic to be checked (for example, the sourceip address, sender email address, or content classification).
2. The <operator> is one of the rich operators, and usually depends on the parameter (such as =, !=, >, <, >=, <=, inacl, notinacl, contains, startswith, endswith, inrange, notinrange).
3. The <value> is the value to be compared against. Each rule can list many terms, and all terms must be true for the entire rule to match and the specified action to be the result.

The "with <attributes>" are attributes to be set should all terms of the rule be true. Examples are flags to enable quarantining, whitelisting, specifying templates for alert messages, and changing eMail message subjects.

As multiple rules can be listed for each policy, the terms within one rule act like logical AND statements, and the individual rules themselves act like OR statements. In this way, the Rules have the power of a programming language, and this power allows a multitude of different policies to be specified and enforced.

Conclusion

With apologies for the technical nature of this article, we thought it would be good to provide a clear description of the technical implementation of this important component of the Network Box 5 platform. Our new ACL/Rules engine unifies the specification and implementation of security ACLs and policy Rules throughout the Network Box 5 system. Wildcarding and case-insensitivity is now treated uniformly throughout the system, and this should help both SOC engineers and customer administrators effectively define the security and organisational policies to be enforced by Network Box appliances.

NBRS-3 Sunset Announcement

We released the NBRS-3 (Network Box 3) platform back in 2006, and since then it has been the core backbone for Network Box security appliances protecting thousands of our managed customer networks around the world. However, times have moved on, and the Network Box 3 platform is now almost 10 years old and hard to keep up-to-date on modern hardware.

The replacement platform NBRS-5 (Network Box 5) was released almost two years ago. The situation today is that the majority of our customer base has already migrated to Network Box 5, and all new customer deployments for the past year or so have been on that newer platform.

Our ability to address emerging security threats, and take advantage of new hardware performance and reliability features, is dramatically better in Network Box 5 than in Network Box 3. In particular, the move towards SSL secured services, and Network Box 5's ability to enforce policy within SSL encrypted traffic, provides significant benefits for security policy enforcement.

Accordingly, we are announcing the sunset of the Network Box 3 platform as of 1st August 2015.

Sunset Policy

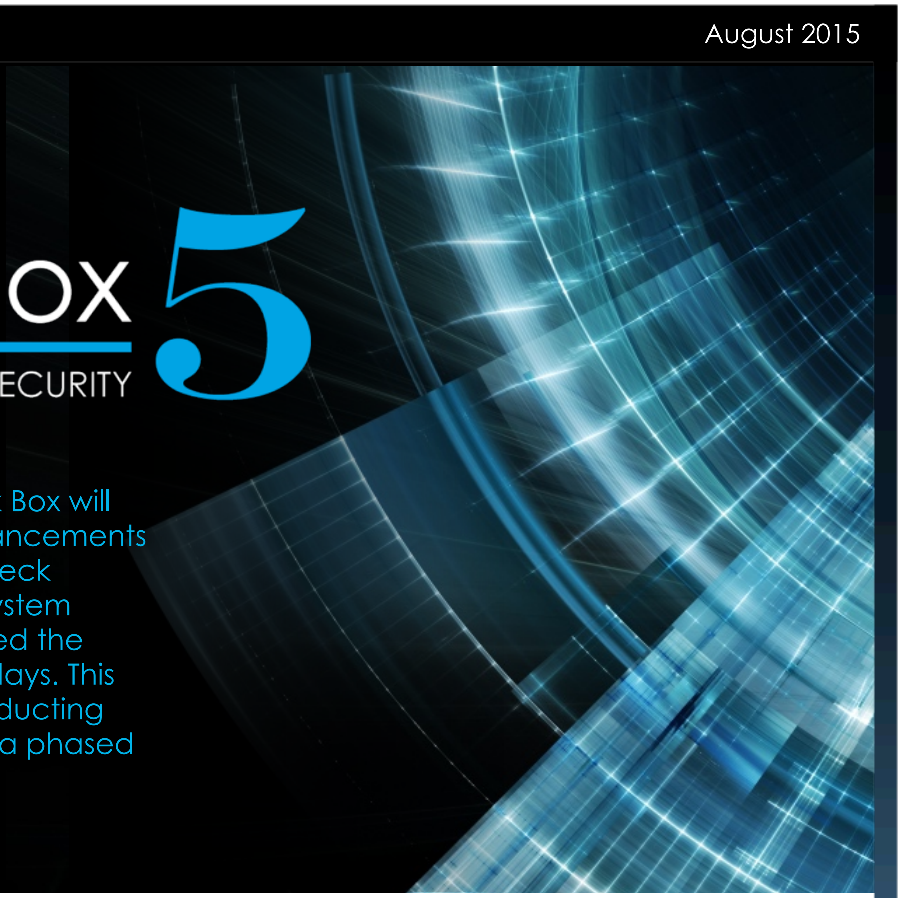
Upon Network Box's decision to start the sunset for a specific product version an announcement will be made with the following dates:

- Sunset Date
  Sunset Date of a product version (hardware or software) may be announced from time-to-time by Network Box Corporation Ltd.
- End-of-sale Date
  End-of-sale Date of a product version (hardware or software) will be six months from the date of the sunset announcement. The product version may be available after this date, subject to any remaining stock being available.
- End-of-support Date
  End-of-support Date of a product version (hardware or software) will be 3 years from the date of the sunset announcement. This is the date on which Network Box will cease to provide technical support, on-site support, helpdesk support, training and spare parts. Network Box may at its own discretion provide best endeavours support.

So, what does this mean? Firstly, it does not mean we are stopping support for Network Box 3 - far from it. It simply means that today we are announcing that the Network Box 3 platform is old - new customers should not use it, and existing customers should start planning for migration to Network Box 5. In six months time (1st February 2016), we will no longer sell the Network Box 3 platform. However, we will continue to provide support and security updates for Network Box 3 for 3 more years (until 1st August 2018), but our product development focus will be on Network Box 5 and its successors.

Network Box 5

NEXT GENERATION MANAGED SECURITY



On Tuesday, 4th August 2015, Network Box will release our patch Tuesday set of enhancements and fixes. Due to the configuration check requirements for the new ACL/Rules system released this month, we have increased the rollout window beyond the normal 7 days. This month, the regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features

August 2015

This month, for Network Box 5, these include:

- Improvements to on-line help system
- Introduction of a new box cluster sync service
- Updates and improvements to IP geolocation
- Add support for peripheral hot-plugging
- Enhanced support in quarantine system, for quarantined file export
- Change to GMS displays to show event date/time in local time zone
- Release of new ACL/Rules engine for all supported security modules
- Security updates to SSL protocol
- Fix to weekly KPI report template addressing duplicate network-infectedlan KPIs
- Improvements to IE11 compatibility in admin and user web portals
- Introduction of a facility for user to change his own password in user web portal
- Performance improvements in application identification policy control
- Improvements to mail alert messages to include threat details in the body of the alert message
- Improvements to live update suspension/resumption in admin and user web portals
- Enable Perfect Forward Secrecy ciphers in SSL proxy
- Improvements to international character support in PDF reporting
- New facility to support digital signing and acceptance of trust in incoming and quarantine released emails
- Optional policy control for IFRAME html sections in eMail, to categorise as executable
- Optional policy control for OBJECT html sections in eMail, to categorise as executable
- Optional policy control for SCRIPT html section in eMail, to categorise as executable
- Improvements to scanning of eMails with a large number of nested ZIP archives
- Add support for several new top level domains, in eMail 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 SOC will contact you to arrange this if necessary.

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

Network Box ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box 3 Features August 2015

On Tuesday, 4th August 2015, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs 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:

- Enhancements to Box Office and Response web sites.
- 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 SOC will contact you to arrange this if necessary.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
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 2736-2083
Fax: +852 2736-2778

www.network-box.com

Network Box Singapore
RSA Conference 2015

Network Box Singapore exhibited at the RSA Conference 2015, held on 22 - 24 July, at the Marina Bay Sands, Singapore.

LINK: http://www.network-box.com/sites/www.network-box.com/files/files/RSA%20Conference%202015-Asia%20Pacific.pdf

Network Box Hong Kong
Ferrari Junior - RED Charity Art Sale

Network Box supported the Ferrari Junior – RED Charity Art Sale, at the Ritz-Carlton, Hong Kong.

LINK: http://www.network-box.com/sites/www.network-box.com/files/files/Ferrari_Junior-RED_Chartity_Art_Sale.pdf

Network Box Germany
ZEG Trade Show

Network Box Germany exhibited at the The Zweirad Experten Gruppe (ZEG) Trade Show 2015 which took place on the 17th to the 20th July in Cologne, Germany.