Welcome

Welcome to the September 2011 edition of ‘In the Boxing Ring’. Continuing on from April’s format changes, we have had a new look since June, as we continue 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 firewall. The Firewall is the core of any UTM+ device and is responsible for implementing the organisational policy at the network level. The NBRS-5.0 firewall is standalone, but holistically integrated with other security modules (such as Application Identification, Quality of Service, and Routing).

The firewall in NBRS-5.0 uses an atomic mechanism in the kernel to switch live running firewall rules in an instant (without loss of network connections). Access Control Lists and Rules are key features of NBRS-5.0, not just limited to firewalling but integrated to every module to extend the firewall throughout the system and allow for a holistic security policy to be applied.

Page 4 details the features and fixes to be released in this month’s 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
LinkedIn:  http://www.linkedin.com/company/network-box-corporation-limited

Mark Webb-Johnson
CTO, Network Box Corporation
September 2011
The NBRS-5.0 Firewall

For this month’s topic on NBRS-5.0, we’ll be presenting information on the firewall. The Firewall is the core of any UTM+ device and is responsible for implementing the organisational policy at the network level. The NBRS-5.0 firewall is standalone, but holistically integrated with other security modules (such as Application Identification, Quality of Service, and Routing).

A firewall designed for scalability

The NBRS-3.0 firewall, like many of its competitors, used a stop-start mechanism to apply firewall changes. This works fine with a reasonable number of rules, but becomes onerous when the number of rules increases into the thousands. The issue is the time taken to start the firewall, and that is purely related to the speed of the box and the number of rules to be loaded.

The firewall in NBRS-5.0 uses an atomic mechanism in the kernel to switch live running firewall rules in an instant (without loss of network connections). Internally, two firewall rule tables are maintained (the running set and the new set), and these are instantly and atomically switched (meaning either all or no rules are applied, depending if there were any errors in the rules) to apply the new rules. This allows us to scale NBRS-5.0 firewalls to tens of thousands of rules.

Access Control Lists and Rules

Access Control Lists and Rules are key features of NBRS-5.0, not just limited to firewalling but integrated to every module to extend the firewall throughout the system and allow for a holistic security policy to be applied.

As every security module implements the defined policies, duplication is eliminated and both routed and proxied traffic are controlled identically.

An Access Control List (ACL) is a typed list of objects. Examples would be lists of IP addresses, users, device IDs, etc. Having the list typed means that entries can be validated (eg; is 10.8.2.301 a valid IPv4 address?) and extended functionality provided (eg; 10.8.2.0/24 includes 10.8.2.99).

ACLs offer optimum performance (much faster than repeating rules). For example, consider the rules:

Permit LAN host 10.8.2.1 to call 10.8.9.99
Permit LAN host 10.8.2.65 to call 10.8.9.99
Permit LAN host 10.8.3.68 to call 10.8.9.99
(repeated for 100 LAN hosts)

It is much more efficient to put the 100 LAN hosts in an ACL and write one rule:

Permit LAN hosts in ACL goodusers to call 10.8.9.99
Rules build on ACLs to define the policy. They support boolean AND operations (across the terms of a rule - such as the ‘LAN host ... call ...’ in the above example) as well as boolean OR operations (down the ordered rules - the multiple rules in the above example). This ordering of rules, and Permit/Deny result, allow rules to reflect complex policies.

Access Control Lists and Rules are universal to NBRS-5.0 are the single mechanism to define policy across all security modules.

**Modular Integration**

The NBRS-5.0 firewall is standalone, but holistically integrated with other security modules. While the firewall runs in the kernel (to provide for optimum performance), various aspects are reflected into user-space for tight integration to high-level services such as:

- Connection and Packet marks (for packet and connection classification)
- Application Identification (allowing firewall rules to be based on identified application rather than merely protocol or port)
- IPS stream (to allow a connection stream to be sent for deep-packet analysis)
- Conditions (allowing various conditions, such as gateway down, High Availability mode, etc, to be shared between the firewall and other security modules providing or relying on those conditions)

**Conclusion**

The firewall in NBRS-5.0 is responsible for implementing the organisational policy at the network level. Standalone, but holistically integrated with other security modules (such as Application Identification, Quality of Service and Routing), it achieves this goal while optimising performance without sacrificing flexibility of configuration.
September 2011 Features

On Tuesday, 6th September 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 various internal NOC systems
- Fixes to the my.network-box.com display of custom LDAP web proxy policy groups, in the case where both a custom group and a LDAP group have the same name.
- Improvements to the my.network-box.com display of swap memory usage.
- Revisions to the Global Monitoring System to suspend monitoring updates for boxes intentionally taken offline.
- Improvements to the Global Monitoring System when monitoring the health of anti-virus systems.
- Introduction of a Global Monitoring System alert to report when a box has been rebooted.

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.

S-SCAN Content Filtering Engine

The Network Box ‘S-Scan’ engine is a high speed web content filtering system, designed to help organisations block undesirable web content from reaching their users.

When combined with ‘Google Safe Browsing’ there are sixteen categories of undesirable content, covering websites which might directly harm an organisation’s computer systems (websites compromised by malware), as well as websites which include subject matter that may be criminal in nature (hacking sites), cause offence (sexually explicit or hate sites), or otherwise harm users (spying or fraud).

Network Box S-Scan CF Engine won Computerworld Hong Kong Awards 2011 - Content Filtering / Anti-Spyware. “Network Box reinforces its world-class status. Over 40 international technology awards, clients around the world, including over 150 banks and credit unions in the US. Network Box has in the last 10 years risen to be a clear leader in the security space.” “On the issue of content filtering - is where Network Box won its award this year - the spate of security hacks has raised attention levels on how to protect data. Content filtering is a growing area as companies want to secure the flow of data in and out from the organisation”, said Chee-Sing Chan, Editor-in-chief of Computerworld Hong Kong.

For more information, please see http://www.network-box.com/s-scan

AUGUST 2011 NUMBERS

<table>
<thead>
<tr>
<th>Key Metric</th>
<th>#</th>
<th>% difference (since last month)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH Updates</td>
<td>649</td>
<td>+14.3</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>425,170</td>
<td>+14.0</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>823,945</td>
<td>+5.5</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>113,147</td>
<td>+4.2</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>12,591</td>
<td>-10.6</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>1,047</td>
<td>+202.7</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>163,382</td>
<td>+30.1</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>4,234,015</td>
<td>+18.5</td>
</tr>
</tbody>
</table>

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

Copyright © 2011 Network Box Corporation Ltd.