Welcome

Welcome to the November 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 NBRS-5.0 High Availability, Load Balancing & Clustering. Network Box offers High Availability at the basic network level. But, then extends that to offer clustering and load balancing (which involves the distribution of individual workloads across a cluster of Network Boxes - to take advantage of the spare backup capacity).

High Availability and Load Balancing offer service continuity in the unlikely event of hardware failure, as well as scaling of traffic loads across two or more machines, at the network level. Clustering extends this at the application level, and IEEE 802.1D spanning tree support extends this to layer 2 bridged networks (including support for transparent deployments).

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
November 2011
The NBRS-5.0 High Availability, Load Balancing & Clustering

High Availability refers to the use of multiple hardware devices to provide for redundant backup in the event a primary device fails. The primary device (through which normal traffic flows) is called the MASTER and the others are the BACKUPs. Network Box offers High Availability at the basic network level. But, then extends that to offer clustering and load balancing (which involves the distribution of individual workloads across a cluster of Network Boxes - to take advantage of the spare backup capacity).

1. High Availability

Network Box NBRS-5.0 High Availability is built upon the industry-standard VRRP protocol.

VRRP (Virtual Router Redundancy Protocol) is a protocol used to negotiate the sharing of one or more IP addresses amongst a group of hosts, with only one host at any one time “holding” the addresses. The protocol allows Network Boxes to act as virtual routers, and to failover the role of router to another Network Box in the VRRP group (in the event the first box fails or is shutdown for maintenance). VRRP uses IP protocol #112 and multicast traffic on 224.0.0.18 to communicate amongst the different boxes in the VRRP group.

VRRP Monitors Interfaces and Reachability, Interface state (carrier, connection) is monitored and MASTER role is lost if an interface goes down (e.g.; unplugged, or switch/cable failure). The master and backup boxes continually broadcast VRRP packets amongst themselves, and should the backup boxes stop receiving VRRP packets from the master, they conduct an election (based on priority) to elect a new master. While the basic VRRP protocol allows for the definition of a group on a single interface, Network Box VRRP extends this to group interfaces together. With such an arrangement, a failure of one interface can also cause the relinquishment of master role on other associated interfaces.

As the basic VRRP protocol moves a virtual MAC address, it is limited to one VRRP group per interface. However, the Network Box implementation moves IP addresses (not MAC Addresses). Gratuitous ARPs (and other techniques) are used to broadcast the change of MAC address when a failover occurs, allowing multiple VRRP groups can thus operate on the same interface. Some networking equipment filter gratuitous ARPs, and this causes issues with the VRRP ARP switch that Network Box uses by to notify connected equipment. To work around this, NBRS-5.0 can also be configured to use direct broadcasts and other techniques to work around specific equipment limitations.

A typical High Availability configuration would have two Network Boxes, each with two interfaces (a NET and a LAN). Each interface would run a VRRP group, with the two interfaces grouped to provide a single seamless MASTER/BACKUP pair. Each Network Box would have its own IP addresses (on both LAN and NET), and in addition, one or more virtual IP addresses would be assigned to the VRRP pool. The workstations and router would use the VRRP pool to talk through the Network Box holding the MASTER role.

NBRS-5.0 includes an optional facility to synchronise connection tracking tables across the high-availability group, and in such cases, connections are not lost when switching box role. But, higher-level protocol states (such as proxy, vpn, etc) are not synchronised - as the overhead of synchronising those states far exceeds the benefits obtained (given the relative infrequent times that a box switch is required).
2. Load Balancing

Load Balancing typically works in the same way as High Availability, except that two VRRP groups are run on each interface (box #1 is master for one, box #2 is master for the other, and each box backs the other up), and an IBC (Inter-Box-Connect) network interface is established for the boxes to communicate over. Traffic is directed either by the workstations/servers/routers directing their traffic to specified virtual IP addresses, or by the network boxes balancing the traffic internally over the IBC (using a traffic director service and NAT on the master box). In either case, the traffic is load-balanced at the network level, so (for example) in the case of SMTP traffic, outbound SMTP traffic would be seen to leave the network via both boxes, in a load-balanced point of view.

Such Load Balanced deployments have a requirement for symmetry at the network traffic level. The network must be arranged such that traffic leaving one box must return back through the same box.

3. Clustering

In addition to High Availability and Load Balancing (which were both also offered with NBRS-3.0), NBRS-5.0 introduces a new technology called Service Level Clustering. While Load Balancing works at the network level, Clustering works at the application level (primarily for traffic scanning).

In such an arrangement, Service Jobs (such as scanning, policy enforcement, mail delivery, etc) are implemented in a clustered arrangement. Typically, a high-availability pair is used to handle the traffic at the network level (where performance is not an issue), and the scanning jobs themselves are offloaded to the cluster nodes.

The cluster nodes implement the service. They communicate amongst themselves to share service load levels, with jobs typically dispatched to the cluster node with the lowest load level. Around-robin allocation is also available to balance the load. Similar to Load Balancing configurations, an IBC is used to keep cluster traffic off the customer networks (both Internet and LAN sides). Back-to-back cables can be used for 2 node implementations, or redundant switches (or VLANs) for larger deployments.

4. Transparent Deployments and Bridging

A typical High Availability configurations works at level 3 of the network model, and, historically, techniques such as proxy-ARP (for transparent deployments) have not worked with High Availability or Load Balanced configurations. NBRS-5.0 supports layer 2 bridging, as an alternative for transparent deployments.

Network Box NBRS-5.0 layer 2 bridging supports the IEEE 802.1D Spanning Tree Protocol (STP), to permit High Availability style deployments to be built on layer 2 transparent networks. This is done in co-operation with switches also supporting the IEEE 802.1D standard. Transparent failover and traffic re-routing in High Availability and Load Balanced environments can now be supported by NBRS-5.0.

Conclusions

For routed networks, High Availability and Load Balancing offer service continuity in the unlikely event of hardware failure, as well as scaling of traffic loads across two or more machines, at the network level. Clustering extends this at the application level, and IEEE 802.1D spanning tree support extends this to layer 2 bridged networks (including support for transparent deployments).
November 2011 Features

On Tuesday, 1st November 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
- Revisions to box reporting of licensing status at contract renewal stage.
- Enhancements to the NTLM authentication system to add support for dual PPTP and web NTLM systems running chap v2 to the latest versions of Microsoft windows.
- Minor revisions to my.network-box.com administrative interface related to read-only administrators and firewall status.
- Various (mostly internal) enhancements to Box Office and 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.

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

Microsoft Active Protections Program (MAPP)

Network Box has been a member of the Microsoft Active Protections Program (MAPP) for security software providers for quite some time now. Members of MAPP, receive security vulnerability information from the Microsoft Security Response Centre (MSRC), in advance of Microsoft’s monthly update.

When MAPP partners receive vulnerability information early, they can provide updated protections to their customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. You can find out more information on MAPP at Microsoft’s MAPP site. Even with these protections, Microsoft recommends that customers deploy security updates to help prevent exploitation of vulnerabilities as quickly as possible.

Cyber security is an ‘arms race,’ the amount of time between the release of a Microsoft security update, and the release of exploit code for that update, continues to shorten. It is vital to stay at least one step ahead of the hackers, malware writers and other cyber criminals out there.

MAPP gives security software providers early access to vulnerability information. Before this program, security software providers had to wait until the public release of a security update before building protections. With MAPP, security software providers can deliver protection features to customers much more quickly. This is something Network Box has been doing for years.

We will soon be enhancing the Network Box Security Response Site, with real-time data on the most recently released Network Box MAPP security signatures. These security signatures will have been sent out to every active Network Box across the globe, using our award winning PUSH update technology.

---

SEPTMBER 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>576</td>
<td>-7.1</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>341,201</td>
<td>+3.8</td>
</tr>
<tr>
<td>Firewall Blocks / (box)</td>
<td>800,877</td>
<td>-1.2</td>
</tr>
<tr>
<td>IDP Blocks / (box)</td>
<td>116,054</td>
<td>-0.3</td>
</tr>
<tr>
<td>Spams / (box)</td>
<td>17,095</td>
<td>+1.6</td>
</tr>
<tr>
<td>Malware / (box)</td>
<td>503</td>
<td>-68.2</td>
</tr>
<tr>
<td>URL Blocks / (box)</td>
<td>180,156</td>
<td>+12.2</td>
</tr>
<tr>
<td>URL Visits / (box)</td>
<td>3,919,564</td>
<td>+1.8</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.