In the Boxing Ring

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

Welcome to the May 2013 edition of In the Boxing Ring

This month, we talk in detail about Distributed Denial of Service (DDoS). With DDoS, as with most emergency situations (such as a successful hack attack, or web site defacement), the best thing you can do is to be prepared. We discuss how one can prepare for DDoS attacks.

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.

Note also that this month is the first month we are bringing NBRS-5.0 into our Patch Tuesday release cycle. Starting next month (June), we will be reporting NBRS-5.0 features and enhancements alongside those for NBRS-3.0.

Mark Webb-Johnson
CTO, Network Box Corporation
May 2013

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 ISSUE

2-3
How to be a Prepper
(aka How to Survive a DDoS Attack)

When asked about DDoS attacks and how Network Box can better help our customers, I always reply in the same way – “how prepared are you?” Being prepared is the best way to protect against DDoS attacks.

4
Awards & Events

Network Box won a PC3 Platinum Brand Award 2013.
Network Box exhibited at the International ICT Expo 2013.

4
April 2013 Features

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.
How to be a Prepper
(aka How to Survive a DDoS attack)

Distributed Denial of Service (DDoS): The unthinkable. The thing that puts terror into the heart of an IT administrator.

Preppers: Survivalists. Individuals or groups who are actively preparing for emergencies.

When asked about DDoS attacks and how Network Box can better help our customers, I always reply in the same way - “how prepared are you?”. With DDoS, as with most emergency situations (such as a successful hack attack, or web site defacement), the best thing you can do is to be prepared. To think through the possibilities of such an attack, put a written plan in place as to how to respond to such an attack, and then file it away for when the unthinkable actually happens. So, here we have “how to be a prepper” (aka How to survive a DDoS attack).

Source of the Attack

Most DDoS attacks are external to your network. The internal ones are relatively easy to handle (find the culprit and shut him down), but the external ones are harder to stop (because you can’t easily find the culprit, and it is very hard to shut him down when his attack is using 10,000 different machines across 100 countries). For an external attack, all you can really hope to do is (a) mitigate it (reducing the impact on the services your network provides), and (b) provide clues to identify the source to your upstream providers and (optionally) law enforcement.

External attacks can generally be divided into two classes:

1. Those that spoof the sender source addresses and try to overwhelm your incoming bandwidth or resources.
2. Those that do not attempt to spoof the sender source addresses and generally try to overwhelm your outgoing bandwidth or resources.

While the technology to defend against each type is very different, the general approach to plan for such attacks is similar.

Denial of Service by your ISP

The first step in any plan for DDoS mitigation is to talk to your Internet Service Providers (ISPs). The attack is coming in over their network on its way to attack you, and some ISPs are more concerned about their own networks than helping you. It is not unheard of for an ISP to implement upstream blocks (at their borders) for traffic destined to your network (effectively cutting you off from the Internet). If your ISP behaves like that, it does not matter what you do in your own network, your ISP is going to DoS you no matter what protections you put in place.

As an example, one popular ISP has the following stated policy:

- For a first-time DDoS, the attacked IP address will be blocked for a minimum of 1 day.
- For any subsequent DDoS, within 3 months from the date of first DDoS, the attacked IP address will be blocked for a minimum of 4 days (even if the attack has ceased).

This is the attacked IP address (i.e., the victim - you), not the attacker. If you used that ISP, the first time you were the victim of a DDoS attack, you would be cut-off for 1 day. If you got attacked again within 3 months, you would be cut-off for 4 days.
So, the first step in planning for DDoS is to talk to your ISPs and find out their policies surrounding DDoS attacks. Find the ISPs that explicitly state they will work with you in resolving the situation and will not block your IP address without express permission from you.

IP Addresses –
the more the merrier

The next step is to look at the IP addresses you have been assigned (or own yourself, if large enough), and what public services you offer on those addresses. Try to keep a large pool of addresses free, and keep the DNS TTL (time-to-live, expiry) records short for those services (to allow you to quickly switch IPs if necessary).

Often, DDoS botnets don’t correctly follow the Internet standards for caching of DNS records – they’ll continue to attack the same IP address long after you’ve switched to a different one.

Distribution of
Services

Next, try to distribute your services. Decide those which you must keep in-house and those which can be offloaded to a different network (or hopefully multiple different networks). By spreading your services across different data centers, you can increase the likelihood that you will have some availability when under attack. Simple services such as DNS are good candidates for distribution (and being UDP based, are very susceptible to spoofed source or reflection attacks).

Resource Planning

While being happy that your web server or firewall can cope with normal traffic with only 50% utilization, that 50% free capacity is likely to disappear very quickly when under DDoS attack. You need to put in sufficient equipment to deal with attack-level requests, not day-to-day level ones.

This can be expensive, so do the calculations to determine what is a reasonable level of incoming requests, and outgoing replies, to plan for. Base that on the bandwidth you have available and the complexity of the services you expose. Then, work back from those calculations to determine what resources you need to be able to serve that amount of requests.

It is not just
about the box

Planning for a DDoS attack is not just about the DDoS protection box you put in front of your network. Even the best DDoS mitigation appliances will be no good if your ISP cuts you off, or your upstream bandwidth is saturated.

The military has an adage called the 7 Ps - Proper Planning and Preparation Prevents Piss Poor Performance – adhering to such advise may just save you one day.

Once you have your plan in place, communicate it to your partners (ISPs, security and other service providers) as well as internally. Then, file it away in a place you can get to should the unthinkable happen.
May 2013 Features

On Tuesday, 7th May 2013, 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 NBRS-3.0, these include:

- Enhancements to various internal NOC systems
- Various (mostly internal) enhancements to Box Office and support systems
- Revision to reporting of network throughput in periodic PDF reporting system. Previously we reported on average network throughput, across all network interfaces, but this causes questions in cases where there are network interfaces configured but temporarily disconnected (with no data) - bringing down the averages. The change this month is to report on total usage of all interfaces in each class.

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.

Note also that this month is the first month we are bringing NBRS-5.0 into our Patch Tuesday release cycle. Starting next month (June), we will be reporting NBRS-5.0 features and enhancements alongside those for NBRS-3.0.

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

International ICT Expo 2013

13 – 16 April 2013

Network Box was at the International ICT Expo 2013. Network Box was heavily featured on the various HKICT Awards stands, because Network Box won the Best Business (Product) Gold Award 2013, Best Business Grand Award 2013, and the Award of the Year 2013; for the Network Box Anti-DDoS WAF+ system.

PC3 Platinum Brand Awards 2013

23 April 2013. Network Box won a PC3 Platinum Brand Award 2013. This was voted for by the public, using an on-line voting system.

APRIL 2013 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>654</td>
<td>+71.7</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>444,621</td>
<td>-7.2</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>951,342</td>
<td>+5.1</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>108,709</td>
<td>+1.7</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>16,347</td>
<td>+12.7</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>627</td>
<td>-30.7</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>175,867</td>
<td>-10.3</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>3,598,943</td>
<td>-8.4</td>
</tr>
</tbody>
</table>