Welcome to the October 2012 edition of In the Boxing Ring

This month, in our slightly extended edition, we talk in detail about Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on pages 2 to 4.

This has become a major issue these days as we see more and more attacks happening recently. It has moved from the middle pages of the technology post to front page news- it is relevant and happening today.

However, there is usually no way to completely stop an attack. The only solution is to mitigate the affects of the attack, so that there is little to no affect on the availability of your service to its intended users, at which point the attacker will usually go away and attack someone else.

There are two distinct forms of Denial of Service attacks: **Spoofed Source** and **Valid Source**. We talk more about defending against these forms of attacks and the NBRS-3.0 and NBRS-5.0 mitigation technology.

Page 5 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.

Mark Webb-Johnson  
CTO, Network Box Corporation  
September 2012
Denial of Service & Distributed Denial of Service

In computing, a Denial-of-Service attack (DoS attack) or Distributed Denial-of-Service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users (Wikipedia).

The real world equivalent would be getting a crowd of so many non-customers in front of a shop, that customers cannot even get to the shop’s front door, preventing the shop from doing any business.

Defending against DoS/DDoS Attacks

The first point to make is that there is usually no way to stop an attack. The only solution is to mitigate the affects of the attack, so that there is little to no affect on the availability of your service to its intended users, at which point the attacker will usually go away and attack someone else. Quite simply, defence is by making yourself a harder target than someone else - you don’t need to run faster than the lion, you just need to run faster than the guy next to you.

So, how to mitigate the attack? Well, the first step is to recognise that under the one umbrella term "Denial of Service", there are two distinct forms of attack:

1. **Spoofed Source** attacks occur when the attacker hides the identity of the attacking machine(s). He uses fake source addresses, generated at random, and attempts to flood your inbound bandwidth or resources handling simultaneous connections.

2. **Valid Source** attacks occur when the sender makes no attempt to hide the identity of the directly attacking machine(s). He, himself, hides behind those machines (usually compromised hosts not belonging to him). In such cases, the attacker uses real source addresses, on thousands (or hundreds of thousands) of real machines (a botnet) to flood your inbound and outbound bandwidth or resources handling simultaneous connections.

Historically, the first type (spoofed source) has been the most prevalent type of DOS/DDOS attack, but these are severely limited in the scope of attack, and we are now seeing fewer of these types of attacks. Because the source address is spoofed, the TCP/IP three-way handshake is unable to be completed, so higher-level TCP/IP services are inherently protected. The vulnerability here is the inbound bandwidth capacity itself, and resource capacity on the attacked servers handling the connections.

Nowadays, the second type (valid source) is by far the most prevalent, and web services (usually on tcp/80) are the most attacked. It is common for attackers to utilise botnets consisting of tens of thousands of compromised machines to flood the attacked servers with small HTTP GET requests retrieving large web pages. This effectively floods the outbound bandwidth and resources of the attacked servers.
Defending against Spoofed Source attacks

Defending against attacks where the attacker’s source IP addresses are spoofed involves a strict partitioning of the Internet from the attacked servers. The Network Box protection device, at the gateway to the Internet, handles all the initial connections from the Internet and applies protection techniques to identify the attacking traffic, and discard it before it reaches the protected servers. Such techniques include SYNcookies (for protocols such as TCP/IP), rate limiting and attack packet fingerprinting.

Only legitimate connections from verified non-spoofed source addresses are permitted to continue to the protected servers, and in this way the vast majority of such attacks can be mitigated (so long as the incoming bandwidth is sufficient to handle the attack).

DDoS (Distributed Denial of Service) Attacks
Prevention Method – Legitimate Users Access

**BOTNET**

The Botnet will attempt to attack and overwhelm the victim’s Web Server.

Whilst this is happening, the Anti-DDoS allows legitimate users to access the Web Server.

* During a DDoS attack, the attackers are mitigated using a variety of techniques whilst legitimate users are allowed normal access.
Defending against Valid Source attacks

Once Network Box knows that the source IP address of a particular connection has not been spoofed, we can permit that connection through to the customer servers, but continue to monitor the connection activity to see what the network client is doing. At this point, we are trying to separate legitimate requests from the requests coming from malicious attackers.

Network Box uses behavioural analysis, traffic signatures, rate limiting, and other such techniques to identify malicious traffic per source-address. Once we’ve identified a source of malicious traffic we blacklist it.

The Network Box networking stack consists of many layers of protection, from physical layer 1 all the way up to application protection at layer 7. Whitelists and blacklists of IP addresses are maintained very low down in this stack, and source traffic from addresses in the blacklists (but not in the whitelists) are blocked with the highest performance. Once an attack source has been identified, it is added to the blacklist, and further traffic from that source is either blocked for a certain time (the dynamic blacklists) or indefinitely (the permanent blacklists).

By identifying the sources of such attacks, and blacklisting them, the Network Box mitigates the attack within seconds of it starting, guarding the protected servers from overload, and providing accurate metrics and records for both the volume and specific sources of the attacks.

NBRS-3.0 and NBRS-5.0

This DOS/DDOS mitigation technology is in every Network Box. The difference is that in NBRS-5 we’ve greatly improved the performance of the protection mechanisms, and tightly integrated it to our Web Application Firewall and proxy systems. This allows NBRS-5 to apply automated heuristics and algorithms, coupled with an extensive signature and rule database of known web attacks, to identify and blacklist the attack sources.

It is this combination of Web Application Firewall and DOS/DDOS mitigation capabilities that brings NBRS-5 to the lead in Web Server protection.
Enhancements to various internal NOC systems
• Support for the upcoming enhancements to the S-SCAN content filtering engine
• Further support for NBRS-5.0 in Box Office systems
• Minor changes to some box health checking systems, to enhance box monitoring capabilities
• 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.

---

**October 2012 Features**

On Tuesday, 2nd October 2012, 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
- Support for the upcoming enhancements to the S-SCAN content filtering engine
- Further support for NBRS-5.0 in Box Office systems
- Minor changes to some box health checking systems, to enhance box monitoring capabilities
- 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.

---

**NETWORK BOX | Anti-DDoS WAF+ Global Launch Soon**

Network Box’s Anti-DDoS WAF+ (Anti-Distributed Denial of Service Web Application Firewall Plus) system, is a highly customizable managed security appliance (or alternatively virtual / cloud based device), which can apply a strict set of pre-configured rules to an HTTP / HTTPS conversation, in order to protect web facing servers against attack.

**Key features include:**

- Bandwidth and Network Optimization
- Distributed Denial of Service Mitigation
- Web Application Protection
- IPv4 - IPv6 / IPv6 - IPv4 Bridging
- Optimized Performance
- Adobe PDF Format Reporting

This is the first of a number of Network Box Version Five (NBRS-5.0) based systems which will be launched over the next few months.

---

**SEPTMBER 2012 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>529</td>
<td>-7.7</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>326,411</td>
<td>+12.14</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>927,429</td>
<td>+0.3</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>147,920</td>
<td>+4.9</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>14,006</td>
<td>+0.3</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>755</td>
<td>+5.6</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>179,202</td>
<td>+0.9</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>4,476,589</td>
<td>-1.9</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 © 2012 Network Box Corporation Ltd.