IN THE BOXING RING

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

Welcome
Welcome to the August 2012 edition of ‘In the Boxing Ring’.
This month, on pages 2 and 3, we present details on the importance of direction.

When a security appliance trivially scans network traffic with a set of signatures, the
direction of the traffic is largely irrelevant. The appliance is just doing basic pattern
matching.

One of the most important contexts that we have is the direction of the traffic flow -
whether this is one of our LAN clients accessing an Internet server, or someone on the
Internet is accessing our DMZ web server, for instance. The protocol may be the same
(e.g.; HTTP in this example), but the traffic direction tells us about what is being done,
and allows us to accurately apply specific protection techniques, signatures and
heuristics to the particular problem.

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
          http://www.facebook.com/networkboxresponse
LinkedIn: http://www.linkedin.com/company/network-box-corporation-limited
Google+: https://plus.google.com/u/0/107446804085109324633/posts

Mark Webb-Johnson
CTO, Network Box Corporation
August 2012
The Importance of Direction

One topic that continually raises its head, when responding to customer requests, is the direction of traffic flows - and I’d like to spend some time this month discussing why it is so important.

Signatures vs Heuristics

When a security appliance trivially scans network traffic with a set of signatures, the direction of the traffic is largely irrelevant. The appliance is just doing basic pattern matching.

However, such basic signature-based pattern matching has been shown time-and-time again to be a largely ineffective security technique. Sure, an appliance with 10+ million signatures will do better than an appliance with 3,150 signatures, and will drastically reduce the amount of malware undetected, but sooner or later something will get through. It is a pure numbers game. The security appliance must succeed 100% of the time - the bad guys just have to win once.

So, how to win? Unlike in the movies, we cannot choose just not to play the game. Instead, Network Box introduces an extensive set of heuristics to its protection arsenal.

Unlike signatures, which are designed to precisely match just one particular threat, heuristics are much more broad and generally match a whole family of threats (both known samples, as well as future unknown variants of the same family). Sometimes, heuristics look for code exploiting known vulnerabilities. Sometimes, they are designed to detect unusual behaviour.

But, the important thing about heuristics is that they need to know the ‘context’ of the traffic, in order to be effective.

Contextual Hints

The context may be something as simple as file type (e.g.; a heuristic looking for self-decrypting behaviour should only be used in files that are executable in nature - running such a heuristic against raw data files would just lead to false positives).

One of the most important contexts that we have is the direction of the traffic flow - whether this is one of our LAN clients accessing an Internet server, or someone on the Internet is accessing our DMZ web server, for instance. The protocol may be the same (e.g.; HTTP in this example), but the traffic direction tells us about what is being done, and allows us to accurately apply specific protection techniques, signatures and heuristics to the particular problem.

Example #1 - Anti-Spam

As an example, let’s look at one of the most common requests we get regarding traffic direction. Customers often ask us to turn on anti-spam outbound.

On the face of it, this seems a ridiculous request. Why would the customer be concerned about spam leaving their network from their trusted users? Well, the answer is that the user’s machines may have been compromised and may be issuing spam, leading to blacklist of the customer’s IP address range.

The problem is that the Network Box SMTP mail scanning system is really two services in one - the first is protecting outbound mail clients sending to the Internet, and the second is protecting mail servers (and clients) from mail arriving from the Internet. The direction is the differentiator. For the two services, we employ different heuristics and protection algorithms. Turning anti-spam on outbound ruins a lot of the assumptions that are made, and requires that several protection engines and heuristics also be disabled inbound.

Revisiting the initial request to turn on anti-spam outbound, it is better to re-work it to solve the fundamental problem - detecting and blocking compromised hosts on the LAN/DMZ. Once we have that understanding, rather than blindly turning on anti-spam outbound (with all its undesirable consequences), a better solution is to apply rate-liming to the LAN/DMZ outbound connections. By limiting the number of outbound mail connections and mails that can be sent by LAN workstations, to a reasonable limit, we can detect possibly compromised hosts and deal with them appropriately.
Example #2 - Web Server Protection

Another example commonly raised is customers who instruct the NOC to turn on the HTTP anti-virus protection for their DMZ web servers.

The issue here is that the Network Box HTTP anti-virus system is implemented as a web proxy service and is designed to protect LAN/DMZ clients from compromised web servers on the Internet. It is not designed to protect customer web servers in the DMZ from malicious clients on the Internet. Quite apart from the intent and design of the protection mechanism, the security implications of opening up a web proxy to the Internet are daunting.

A better solution is to apply the NBIDPS IDS/IPS system to the problem. That system is specifically designed to protect DMZ web servers from malicious clients on the Internet.

Another solution, coming with NBRS-5, is to deploy a Web Application Firewall - a reverse proxy specifically designed for the problem.

Example #3 - Services open to the Internet

Traffic flow direction is often used to imply trust. For example, a connection to a DMZ RDP (Remote Desktop) service from a LAN workstation may be permitted. But, often NOCs receive requests from customers to open up such services to the Internet at large (so that roaming engineers can remotely access the servers they manage).

In general, that is a very bad idea. Every new DMZ/LAN service exposed to the Internet increases the chances of compromise by increasing the customer’s exposure. Some services have extremely poor track records with security vulnerabilities.

A better solution is to bring back ‘trust’ to connections from the Internet by the use of VPNs. By closing RDP to the Internet, but allowing it from VPN connections, we can restrict the exposure to only those Internet clients that have successfully established a VPN connection. Network Box offers PPTP, SSL and IPSEC VPN options, and any of those are an excellent solution to such a problem (with PPTP being the usual recommendation for such roaming engineers). Even an unencrypted GRE tunnel to a remote office is better than opening the service up to the world.

Remember that when you plug into the world it’s easy to forget the world is also plugged into you.

Conclusion

When making a request of the Network Box NOC supporting you, please take the time to explain your requirement, not just your request. Our NOCs are staffed by experienced security engineers dedicated to the task of keeping your networks secure, and can offer both advice and recommendations as to how best to mitigate the danger of network threats.
August 2012 Features

On Tuesday, 7th August 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
- Enhancements to mail scanning anti-spam, for recent emerging spam strains
- Further support for NBRS-5.0 in Box Office systems
- 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 CLOUD | Infrastructure Powered by 6fusion

With the move of more and more business critical applications to the cloud, you need to ensure you receive the best possible infrastructure protection and security. Network Box Managed Security Services gives you the ability to deliver award-winning Firewall, Intrusion Detection and Prevention (IDP) and Virtual Private Networking (VPN) services on the 6fusion Infrastructure as a Service (IAAS) platform.

Among cloud-computing security solutions, Network Box is the only one that is managed, automatically configuring and monitoring security - saving you time and resources. The combination of 6fusion and Network Box delivers on the benefits of cloud computing behind the security of an industry leading firewall. The Network Box Firewall has been certified and templated directly into the 6fusion platform, allowing solution providers to deploy security measures simply and easily. From 6fusion.

For more information, please see http://www.6fusion.com/?partner-programs/?alliance-partner/network-box/

JULY 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>635</td>
<td>+6.2</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>242,164</td>
<td>-2.7</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>888,490</td>
<td>-1.9</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>126,319</td>
<td>+2.3</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>13,089</td>
<td>-8.7</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>632</td>
<td>+93.9</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>175,734</td>
<td>-4.0</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>4,461,220</td>
<td>+2.9</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