Welcome to the February 2013 edition of In the Boxing Ring

This month, the two main topics being discussed are: DNS and SSL. The Domain Name System (DNS), as we know it, dates back to 1982. But, being designed back then, DNS has a core foundational problem – and that is it is built primarily on the UDP/IP protocol, which means responses must typically be restricted to 512 bytes or less. We discuss this further in page 2 and how Network Box has resolved this issue.

On page 3, Nick Jones, Network Box’s Head of R&D, discusses the Network Box Secure Socket Layer (SSL) Security Strategy. His first article in a series on SSL, talks about the TurkTrust Certificate Authority’s accidental issuing of an Intermediate Certificate to a client instead of a regular Website Certificate, compromising browsers to accept these certificates as perfectly valid. This incident not only highlights the delicate nature of SSL but also the material benefit that Network Box NBRS-5.0 can bring to customers.

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.

Mark Webb-Johnson
CTO, Network Box Corporation
February 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
Linkedin: http://www.linkedin.com/company/network-box-corporation-limited
Google+: https://plus.google.com/u/0/10744680485109324633/posts

IN THIS ISSUE

2
DNS, Mail and 512 bytes
A background discussion regarding a change to the Network Box store-and-forward mail server and “ANY” style DNS queries.

3
SSL Security Strategy
In the first of a multi-part series on Secure Sockets Layer (SSL), Network Box’s Head of Research & Development, Nick Jones, discusses issues surrounding its adoption.

4
NETWORK BOX Events
Network Box gave a talk about Zero Day Attacks, Zero Day Malware, and how to keep organizations’ computers and networks safe at the, “Tackling Targeted Cyber Attacks Event.” In addition, Network Box USA was at the TechMecca Expo in Forth Worth, Texas.

4
February 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.
DNS solves the core problem of associating a name with an IP address, but also goes beyond that by allowing the name to also retrieve other informational records (such as MX records for mail servers). Various conventions have arisen, over time, to extend the record types understood by DNS clients, and how they are interpreted. Nowadays, DNS is ubiquitous. It is the ‘telephone directory’ of the global Internet.

But, being designed back in 1982 for a very limited number of records, DNS has a core foundational problem – and that is it is built primarily on the UDP/IP protocol, which means responses must typically be restricted to 512 bytes or less. DNS clients can fall-back to TCP/IP to overcome this restriction, but that is comparatively very slow and problematic for some deployments (not to mention not universally enabled, and often firewall blocked). When DNS responses just consisted of a few short IP address records, this wasn’t a problem. Now, with MX records, A records, AAAA records, NS records, and most importantly DNSSEC, the responses are exceeding 512 bytes, and DNS is struggling.

Historically, it has been relatively common to permit UDP/53 (DNS over UDP) at the firewall level, but deny TCP/53 (DNS over TCP) as the TCP protocol was used for larger DNS zone transfers. Denying TCP/53 offered a simple approach to firewalling sensitive DNS zone transfers. Lately, some major DNS providers are going even further by restricting certain DNS query types (such as the “ANY” query used to ask a server for all records it has on a particular name). Both of these defensive approaches are violating the RFCs, and resulting in undeliverable eMail and general network connectivity problems.

Network Box has historically tried to balance the relatively high latency of the DNS system with efficiency, in order to enhance performance and optimize network usage. It is, quite simply, more efficient to send a single request for multiple record types in a single response, than to request each record type individually. Specifically, we have used DNS “ANY” queries when looking up mail server MX records (as it allows us to retrieve all relevant records with a single query). This approach, while fully standards-conformant, is becoming problematic when dealing with badly configured name servers, and their firewall protections, that don’t conform to the Internet standards. Network Box often receives the blame for such situations, even though it is clearly the remote DNS server that is at fault. The situation is only likely to get worse, as more and more sites adopt DNSSEC and DNS replies get larger.

With the February 2013 Patch Tuesday, Network Box is releasing a revised version of our SMTP store-and-forward server that no longer uses “ANY” style DNS queries. Instead, it will issue multiple individual record type queries, as needed. This will reduce the average response size of DNS packets (as only the record types specifically asked for will be returned), but with the drawback that more DNS queries (with associated slow latency) may be required to retrieve other record types. This approach is fully standards-compliant, and improves compatibility with existing non-compliant DNS servers – but at the expense of more DNS queries for some types of DNS server responses.

The Network Box Transparent SMTP system is not affected by this change, as it does not use DNS (instead relying on the DNS resolution of the host making the original TCP/53 SMTP mail service connection).

As always, should you have any questions or concerns, please feel free to contact your local Network Box NOC for assistance.
This is the first article in a series about the Network Box Secure Socket Layer (SSL) Security Strategy, or SSL Plus. SSL Plus encompasses certain technologies present in Network Box NBRS-5.0 and a set of business processes employed by Network Box Corporation, that add value to the essential security provided by the SSL.

This first article in the series was intended to be an introduction to some of the most important technologies falling under the umbrella of the term Secure Sockets Layer and SSL Plus, but in recent weeks an incident occurred that not only highlights the delicate nature of SSL but also the material benefit that Network Box NBRS-5.0 can bring to customers.

No time will be spent on definitions and explanations of the technologies mentioned in this article, they can wait until next month.

The incident in question is the TurkTrust Certificate Authority’s accidental issuing of an Intermediate Certificate to a client instead of a regular Website Certificate. The details of this incident, including the causes and the presence of any malice are not important, but what is important is the outcome that the runaway Intermediate Certificate was able to sign any Website Certificate and that browsers accepted these Website Certificates as perfectly valid. This incident once again demonstrates the weakness of Intermediate Certificates and indeed Certificate Authority as a whole, as well as the fact that Web Browsers place so much trust in Certificates until that trust is explicitly and ponderously removed.

The incident hit mass media at the beginning of January and it is only just now, a month later, that major Operating System vendors are releasing updates to remove trust in these Intermediate Certificates. Although some of the major Web Browser vendors were quicker to respond, the issue still remains that organizations and end users will not be anywhere near as quick to globally update their own software.

Let us now examine the case where an organization is using the Network Box NBRS-5.0 Web Client Scan product, that includes Client SSL Plus. One of the features of Client SSL Plus is it’s ability to inspect SSL connections on behalf of all Web Browsers in an organization, and apply administrator defined Access Control Rules to those connections at an organizational level, at the Network Gateway. If any secure connection is identified as having the runaway Intermediate Certificate in its chain of trust, then the Access Control Rule can have the connection blocked by the NBRS-5.0 Network Box. Because the Intermediate Certificate is identified using a globally unique SHA1 fingerprint, the Access Control Rule will have no affect on any other secure connections.

Upon learning of this incident, Network Box Regional SOC staff will communicate with a customer and approve the Access Control Rule rule for immediate activation on the customers NBRS-5.0 installation, thus protecting ONE Network Box customer in a matter of MINUTES.

Upon learning of this incident, Network Box Headquarters will initiate a procedure to install the Access Control Rule as a global default setting and using the NBRS-5.0 Configuration Synchronization, propagating that protective rule to all CURRENT Network Box customers in a matter of A FEW HOURS.

Upon learning of this incident, the Network Box Core Development Team will integrate the Access Control Rule into the NBRS-5.0 software set, essentially making it a fixed part of the NBRS-5.0 product. The software can then be released to Regional and Headquarters Engineering Teams so that all Network Box products delivered from that time forward contain the Access Control Rule, thus protecting all FUTURE Network Box customers in a matter of SEVERAL HOURS.

This first article in the series was intended to be an introduction to some of the most important technologies falling under the umbrella of the term Secure Sockets Layer and SSL Plus, but in recent weeks an incident occurred that not only highlights the delicate nature of SSL but also the material benefit that Network Box NBRS-5.0 can bring to customers.

Network Box
Secure Socket Layer Security Strategy
(SSL Plus)

by Nick Jones
Head of R&D, Network Box

Nick Jones
Head of R&D, Network Box
Nick brings depth of technology expertise to Network Box. He is an enthusiastic participant in the Free and Open Source Software community, which has led him into projects such as the Linux Kernel, OpenSSL and the ASIO networking library. He is also a contributor to the ISO C++ Standardization Committee Study Group for Networking.
February 2013 Features

On Tuesday, 5th February 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, these include:

- Enhancements to various internal NOC systems
- Minor fixes to my.network-box.com administrative web interface
- Revisions to mail service DNS resolution mechanism
- 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 I Cyber Security Event


Network Box USA I TechMecca 2013

21-22 January 2013. Network Box USA was at TechMecca 2013, held at the Omni Forth Worth Hotel, Forth Worth, Texas. TechMecca features dynamic general sessions led by industry experts who understand the fragile balance between technology, marketing and customer service.

JANUARY 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>692</td>
<td>+15.9</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>594,462</td>
<td>+6.2</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>982,050</td>
<td>+3.3</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>114,090</td>
<td>-7.1</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>12,020</td>
<td>-3.8</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>369</td>
<td>-54.3</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>169,784</td>
<td>+7.0</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>3,975,586</td>
<td>-4.6</td>
</tr>
</tbody>
</table>