Welcome

Welcome to the May 2012 edition of ‘In the Boxing Ring’. In this edition, we focus on Network Box NBRS-5.0 Secure Sockets Layer (SSL).

This month, on pages 2 and 3, we present details on Network Box NBRS-5.0 the Secure Sockets Layer (SSL). The fundamental flaw is that SSL applications (such as web browsers) typically rely on the user to accept or reject certificate problems.

NBRS-5 can operate in one of two modes, for client protection: SSL Bypass Mode and Transparent SSL Intercept Mode. Most competing systems operate in mode 1 only, and are unable to protect SSL encrypted traffic. Those that offer mode 2 do so in only a limited fashion. Network Box NBRS-5 fully supports both modes and allows the selection of mode to be made on a very granular basis.

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
May 2012

2-3. Network Box NBRS-5.0 SSL
Network Box NBRS-5 includes extensive support for the Secure Sockets Layer (SSL) protocol. This protocol is at the core of secure Internet communications, is used by many higher-level protocols (such as HTTPS, SMTPS, POP3S, etc), but most implementations are fundamentally flawed.

4. Network Box Wins Multiple Awards
- PC3 Platinum Brand Award 2012
- BQJ Super Brand Award 2011
- Linux Pilot Editors’ Choice 2012

4. May 2012 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.
Network Box NBRS-5.0 Secure Sockets Layer (SSL)

Network Box NBRS-5 includes extensive support for the Secure Sockets Layer (SSL) protocol. This protocol is at the core of secure Internet communications, is used by many higher-level protocols (such as HTTPS, SMTPS, POP3S, etc), but most implementations are fundamentally flawed.

The “User” Problem

The fundamental flaw is that SSL applications (such as web browsers) typically rely on the user to accept or reject certificate problems. For example, if the user browses to a remote web server who’s SSL certificate has expired, the user is asked to accept/reject the connection. Or, if the remote web server name doesn’t match that signed in the certificate, the user is again asked to accept/reject the connection.

Study after study has shown that users will ignore these warning and press whatever button they think will get them to where they want to go. Real world results also show that the majority of users cannot even identify a secure browser connection when they see one, and most don’t even look at the Extended Validation (EV) certificate information designed to help protect against phishing attacks.

A good summary of the situation can be found in the Crying Wolf: An Empirical Study of SSL Warning Effectiveness study at http://lorrie.cranor.org/pubs/sslwarnings.pdf

The NBRS-5 Approach

NBRS-5 can operate in one of two modes, for client protection:

1. **SSL Bypass Mode** - SSL communications are left intact and bypass protection mechanisms.
2. **Transparent SSL Intercept Mode** - SSL communications are intercepted and transparently proxied, with the Network Box able to protect encrypted traffic and enforce certificate policy rules.

Most competing systems operate in mode 1 only, and are unable to protect SSL encrypted traffic. Those that offer mode 2 do so in only a limited fashion. Network Box NBRS-5 fully supports both modes and allows the selection of mode to be made on a very granular basis (for example; per-user, per-site-category, or per-site). Such a policy is an effective mechanism to deal with the privacy issues inherent in applying protection to SSL sessions.

Let’s look in detail at the Transparent SSL Intercept Mode of NBRS-5 and see how it can protect traffic.

**NBRS-5 Transparent Intercept Mode for SSL**

Diagram 1 shows a typical browser session for a web client protected by Network Box, when accessing a SSL protected server on the Internet. The connection originates at the web client on the LAN, is transparently proxied by the Network Box at the gateway, and targets a web server on the Internet. This communication normally occurs on port tcp/443, but with application identification, the initial SSL negotiation can be automatically identified for Transparent Interception and then the protocol itself determined from within the encrypted traffic stream.

Diagram 2 shows the flow of communications. The Network Box starts by intercepting the outbound tcp/443 call and transparently proxying it to the target server. The usual access policy checks can apply at this stage. Examining the communications between the client and the server, the Network Box determines that this is SSL communication. If configured for mode 2 Transparent SSL Intercept Mode, the Network Box first validates the certificate provided by the server with its own SSL policy check. Should the certificate be acceptable, the Network Box generates its own matching certificate, signed by a certificate authority on the Network Box itself and trusted by the client, to present to the client.
At this point, there are two SSL streams - one between the web client and the Network Box, encrypted and authenticated by Network Box itself, and the other between the Network Box and the remote web server. As a result of this arrangement, when encrypted traffic passes from the client to the Network Box, the Network Box has the ability to decrypt the traffic for protection, prior to re-encrypting it for onwards transmission to the server. Similarly, server responses can be decrypted by the Network Box for protection, then re-encrypted for onward transmission to the client.

The end-result of this is that:

a. The validation and decision whether to accept the remote server’s certificate is made at the Network Box - according to administratively defined policy.

b. Advanced certificate validation techniques can be implemented as a centralised policy.

c. The decision whether to perform mode 2 Transparent SSL Interception is made at the Network Box - again according to administratively defined policy.

d. Requests and responses to/from the remote server can be examined as unencrypted traffic and subject to full application identification.

e. Full protection (including anti-virus protection) can be offered, even for SSL-encrypted traffic, and policy/protection rules applied.

In particular, note that the application identification occurs both at the container (SSL) and content (decrypted plaintext traffic within the protected SSL sessions) levels. All this without compromising the security of the data passing over the network.

**NBR5-5 Protection of DMZ Web Servers**

As well as protecting web clients on the LAN from malicious content on SSL web servers in the Internet, NBR5-5 supports SSL in its Web Application Firewall (WAF) product for protecting web servers in the DMZ from malicious web clients on the Internet or LAN. It does this by SSL offload, as shown in diagram 3.

SSL Offload works by placing the SSL server certificates on the Network Box WAF device. The Network Box itself can then accept SSL connections from clients, and decrypt the incoming request for protection before passing on to the protected web servers. Similarly, replies from the DMZ web servers can be checked for policy conformance and other protection mechanisms, before being encrypted and sent on to the requesting client.

The administrator can choose whether to use SSL on the link between the Network Box and protected web servers in the DMZ. That decision can be made based on security vs performance vs administrative load.

Full WAF functionality is thus available, even for SSL secure connections, again without compromising the security of the data passing over the network.

**The Client Certificate Issue**

The problem with such SSL interception (either Transparent SSL Interception, or SSL Offload) approaches is the SSL client certificates require special handling. This is due to the design of the SSL protocol itself.

For SSL Offload, the Network Box can be configured either to bypass interception for SSL connections with client certificates, or it can accept and validate the client certificate itself before passing on the details as data in the request to the web server.

For Transparent SSL Interception, the Network Box can be configured to bypass interception of SSL connections with client certificates.

In the real world, SSL client certificates are normally used for close business partnerships, between trusted entities, and the above limitations are only required in a very small number of cases.

**Conclusions**

Network Box NBR5-5 includes extensive support for the SSL protocol. It allows the administrator to control the policy for SSL communications and provides effective mechanisms for identification, protection and policy enforcement of SSL traffic.
May 2012 Features

On Tuesday, 1st May 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
- 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 Wins Multiple Awards

PC3 Platinum Brand Award 2012

Network Box won the Platinum Brand Award 2012, in the Unified Threat Management category on 17th April 2012. This prestigious award is decided by the readers of PC3 Magazine, APPS Magazine and IT Pro Magazine, using an on-line vote.

BQJ Super Brand Award 2011

Network Box won the Best Super Brand Award, from the Business Quotient Journal on 14th April. The award was presented at the ICT Expo.

Linux Pilot Editors' Choice 2012

Network Box won the Linux and OSS Award 2012, for the Best Managed Security Service, from Linux Pilot magazine on 14th April 2012. The award also presented at the ICT Expo.

HKTDI International ICT Expo (13-16 Apr 2012)

The ICT Expo in Hong Kong is over for this year. A big thank you to everyone who came to visit us at our Booth. It was great to get the chance to tell people about our new Web Application Firewall, IPv6 bridging and Zero Day anti-virus technologies.

APRIL 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>599</td>
<td>+4.7</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>424,446</td>
<td>-6.4</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>896,789</td>
<td>+6.1</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>129,261</td>
<td>-11.3</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>14,276</td>
<td>-10.5</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>580</td>
<td>+174.9</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>160,154</td>
<td>+5</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>4,045,348</td>
<td>-1.3</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, Kowloon, Hong Kong
Tel: +852 2736-2078
Fax: +852 2736-2778
www.network-box.com

Copyright © 2012 Network Box Corporation Ltd.