Welcome to the November 2012 edition of In the Boxing Ring

This month, as background for our Application Firewall, Identification, Control and Monitoring engine, APP-Scan; we talk in detail about Application Identification.

Today, for the firewall settings in most companies, all inbound protocols and ports are blocked by default and only those specifically required permitted. For outgoing data, all protocols and ports are open and traffic is restricted only on specific protocols and ports.

The problem comes when trying to impose policy control over what application users in the LAN are running and how they are using (or abusing) the shared resource that is the Internet link.

We look at how Application Identification addresses this issue and discuss in further detail: what it is, what it isn’t and what it can be used for.

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
November 2012
Application Identification

What is it?

Historically, firewalls have worked by blocking/permitting access to defined protocols and ports.

For incoming data (Internet -> LAN or DMZ), in the early days of computer security the firewall would be ‘open’ to all and only specific ports were blocked (e.g.; telnet and other administrative ports). That was quickly found to be problematic, and the industry moved to the model most commonly found today – that in which all protocols and ports are blocked by default and only those specifically required permitted. If you have a web server in your DMZ listening on port tcp/80, then opening that port to the Internet (at the firewall) will permit web application traffic to your web server.

For outgoing data (LAN or DMZ -> Internet), the situation today is still (in my opinion) in the dark ages of computer security – with a large proportion of users operating firewall policies allowing all protocols and ports open outbound, and trying to restrict traffic only on specific protocols and ports.

Looking at the bigger security picture (keeping your organisation’s data systems secure – keeping the bad guys out while allowing the good guys to do their jobs), outbound controls are perhaps 5% of the picture – with inbound security threats still making up 95% of the problem. So, perhaps it is not so bad to have a lax outbound security policy?

The problem comes when focussing on that 5% and trying to impose policy control over what those users in the LAN are doing. What applications they are running and how they are using (or abusing) the shared resource that is the Internet link.

Application identification tries to address this problem, by looking at the data passing through the network and trying to identify the application not by protocol/port (i.e. http web traffic on tcp/80) but by traffic signatures and behavioural analysis (i.e. http web traffic on any port). The application identification approach is to initially allow the traffic through, so as to be able to look at it and discover what it is. At that point, the application is identified and the decision made as to what to do with it.

What isn’t it?

I think it is pretty clear that Application Identification is not really a security tool.

For inbound traffic (95% of the security problem) it is of zero use as you already know what services you are running on your own network. For outbound traffic (5% of the security problem), an effective outbound policy coupled with content filtering controls can already adequately address the problem – with almost zero false positives.
What can it be used for?

I would say that the clearest and most sensible use of Application Identification is to further analyse traffic on permitted outbound ports, so as to improve the granularity of policy enforcement.

Once the application has been identified, policy decisions can be made – such as to permit/deny the traffic, or apply quality of service and other bandwidth controls.

Levels of Application Identification

Aplication Identification systems can be classified as operating at up to seven levels of sophistication:

1. **Session analysis**
   - Determining sessions (and related sessions) from raw network data.

2. **Encapsulating Application**
   - Identification: Identifying the application or protocol used to encapsulate an application's data.

3. **Application-within-application Identification**
   - Identifying an application tunneling within another application or protocol.

4. **Terminated Decryption Support**
   - The ability to decrypt protected data terminated on the application identification device, to identify the application within the encrypted stream.

5. **Man-in-the-Middle Decryption Support**
   - The ability to decrypt protected data as it passes the application identification device, to identify the application within the encrypted stream without affecting the receiver of the data (which still receives it encrypted).

6. **Meta Data Extraction**
   - The ability to extract meta data related to the application. Examples of this would include email addresses for SMTP mail, the URL for HTTP requests, and the type of transaction (chat, file transfer, etc) for Skype.

7. **Content Extraction**
   - The ability to extract content transfers related to the application. Examples of this would include the eMail message itself in an SMTP session, the web page content for an HTTP session, and the file being transferred in an MSN chat session.

NBR-3 Support

NBR-3 supports application identification at up to sophistication level 4 in the left table. It can identify popular applications, at the network traffic level, so that firewall, router, QOS and other policy based controls can be applied to the traffic. It can even do this for data in encrypted tunnels terminated on the NBR-3 network box itself.

NBR-5 Support

NBR-5 supports application identification at up to the full sophistication level 7 in the left table. It can identify popular applications, at the network traffic level, so that firewall, router, QOS and other policy based controls can be applied to the traffic. It can even do this for data in encrypted tunnels terminated on the NBR-3 network box itself.

Most importantly, application identification is at the core of all logging, analysis and other foundational systems in NBR-5. As well as reporting on users, NBR-5 can report on applications in the network.

Support for application identification within encrypted streams is supported in both terminated (vpn style) and man-in-the-middle (proxy style) approaches.

Both meta data and content extraction is supported for thousands of pieces of meta data, allowing sophisticated rules to be designed to implement policy. For example, as well as permitting / denying MSN, policy rules can control MSN chats to/from particular chat buddies. Coupled with the NBR-5 proxies providing in-depth and comprehensive protocol decodes and support, application identification content extraction in the generic proxy can provide for sophisticated scanning and control of hundreds of application protocols.

Conclusions

Application Identification technology has limited use in a security system, but offers a highly granular solution to the problem of outbound policy control. Coupled with the other policy control systems in Network Box devices, application identification is one of the most requested features of Network Box. It is something that we can support today, to some extent, in NBR-3, and will have comprehensive support for in the upcoming NBR-5 product.
November 2012 Features

On Tuesday, 6th November 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
- Minor fixes to the pdf weekly report system
- Support for the upcoming enhancements to the S-SCAN content filtering engine
- 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 MIDDLE EAST | New Security Operations Centre

Network Box is extremely pleased to announce that we will be opening an additional Network Box Security Response Center soon, at the heart of Dubai Silicon Oasis. This will be managed by our new team at Network Box Middle East, under the stewardship of a very well respected security industry veteran, Mohammad Abdul Kabeer.

Work is currently underway, and the centre should be operational before the end of the year. This latest Network Box Security Operations Centre, will be dedicated to providing world class Managed Security Services to new and existing Network Box customers across the Middle East and North Africa (MENA). Organizations in the MENA region wanting to contact Network Box Middle East, please feel free to contact us, we will be more than happy to put you in touch with them directly.

SEPTEMBER 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>472</td>
<td>-10.8</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>380,652</td>
<td>+16.6</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>905,377</td>
<td>-2.4</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>140,423</td>
<td>-5.1</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>12,848</td>
<td>-8.3</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>1,003</td>
<td>+32.8</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>160,989</td>
<td>-10.2</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>4,393,675</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.