SEP 2016

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the September 2016 edition of In the Boxing Ring

This month, Network Box USA's CTO Pierluigi Stella continues with part two of the series on **why you need WAF**. Previously, we touched upon the value of protecting one's webserver and the limitations of IPS against application vulnerabilities. Leading on from this, on pages 2–4 we detail the role of WAF, how it helps mitigate these threats, and its true value for one's webserver.

On page 5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, Network Box is pleased to announce that the company won *Best Managed Security Provider* at this year's **e-Brand Awards**, and Network Box Australasia was at the **UAC Expo & Seminar 2016**, to introduce the Network Box 5.3 Managed Security Service Platform. In addition, a new feature has been added to the *Network Box Dashboard*, this enhancement allows users to manually configure the network setup of their hardware.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
September 2016

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
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

Why you need WAF

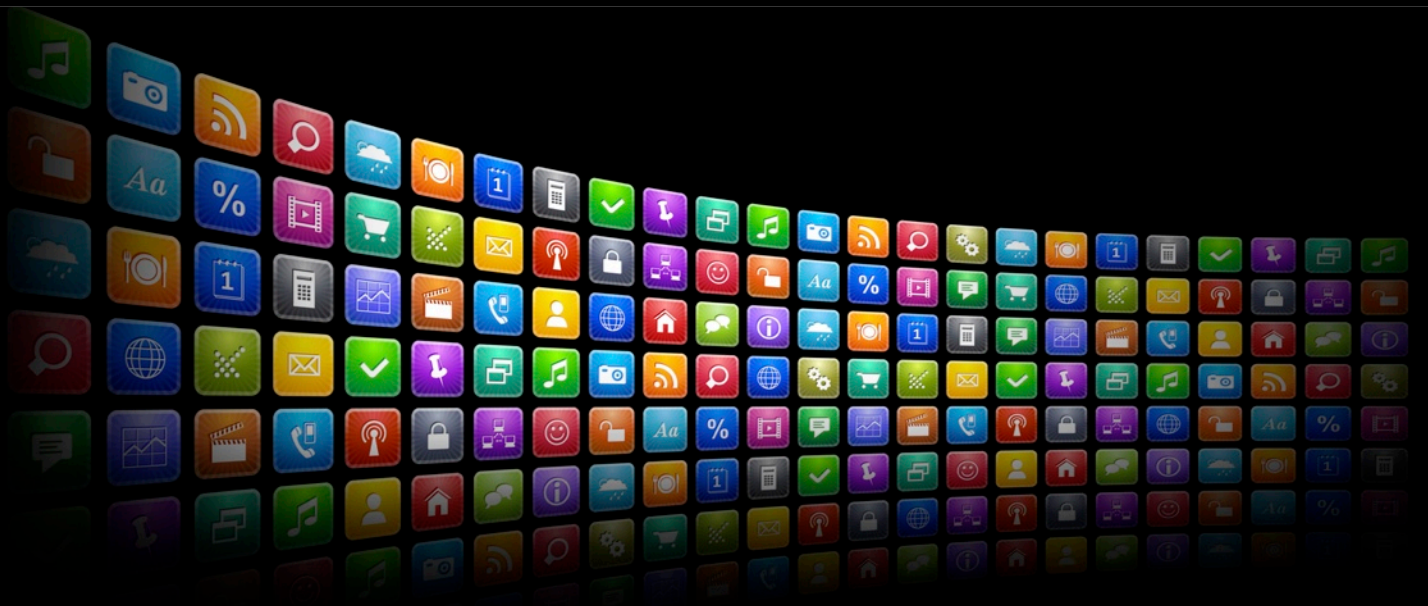
(part 2 of 3)

by Pierluigi Stella

Chief Technology Officer
Network Box USA

In the last article, we touched on the critical value of protecting one's web server, and the various way to do just that such as the setting up of a DMZ or the creation of an IPS. We also introduced the fact that while a good idea, establishing an IPS in line with firewall as a means to intercept malicious traffic, was limiting. Continuing from that, we will focus on the specific role of WAF and what this really means to your webserver.

NETWORK BOX



As explained previously, an IPS cannot be effective against all potential application vulnerabilities.

Typically, an IPS ends up producing too many false positives, which in turn yield two possible reactions – either:

1. *it delays application response time and incorrectly interferes with the application; or*
2. *it allows attacks as normal behavior in an attempt to reduce false positives.*

An IPS looks at signatures and anomalies; a WAF looks at behavior and logic, analyzes traffic in both directions, looks at what is being requested, and what is being returned.

A Web Application Firewall's main task is to protect web applications by inspecting the semantics of the flowing traffic and also inspecting HTTP/HTTPS for typical attacks at layer 7 such as:

- SQL Injections
- Buffer Overflow
- Cross Site Scripting (XSS)
- File Inclusion
- Cookie Poisoning
- Schema Poisoning
- Defacements
- and many more...

To obtain a better understanding of the topic, a good source of information is found at this link:

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP

The Open Web Application Security Project

OWASP is an open software security community collecting, among other things, the list of top attacks against web servers. Any WAF on the market today will have to at least protect web applications and servers from the OWASP top 10.

Another aspect of using a WAF is called SSL offloading. The internet is headed towards complete encryption. Increasingly, websites are using HTTPS, even when there is no confidential data to be protected. If the website runs an application that requires confidential data to be entered, such as your online banking portal, the choice of HTTPS is obvious. But there are plenty of examples of sites that are using HTTPS even though in principal they wouldn't need to, because there is no private data to be protected.

Soon after the NSA scandal of 2014, Google.com chose to use HTTPS for all their pages. Yahoo! has done the same. And the examples are countless. Encryption is adopted not just to hide searches, but to also guarantee the authenticity of a website. Too many attacks are conducted by spoofing the looks of other websites, and the mechanism of private/public key/cert inherent to the HTTPS protocol is likely the last bastion against a widespread diffusion of such attacks.

For instance, when you go to https://www.network-box.com/, the certificate on that website (published and guaranteed by a certificate authority) tells your browser that you have indeed reached the intended site, and not some hacked, spoofed site that might try to collect information to, in turn, conduct an attack against you.

NETWORK BOX

What does this really mean for one's webserver?

If the server capacity was designed for HTTP and suddenly every single transaction is encrypted, the CPU load can become such that the server itself may not be able to handle it. One feature where a WAF can help is HTTPS offloading – the certificates are placed on the WAF, the encrypted connection is terminated on the WAF. Between this and your servers, the traffic does not necessarily need to be encrypted, thus "offloading" the function to the WAF. This allows control over which version of TLS to use. That said, given that every version of SSL has now been compromised, so in reality, no one should really be using that for their HTTPS protocol. Yet we still see many websites that have not been updated and corrected, likely because the software version cannot be updated (for the reasons explained earlier). The WAF can easily enforce the use of the appropriate TLS version, without the need to touch anything at all on the web server.

Because the WAF decouples the traffic between web server and internet, and the browsers are no longer connecting directly to the webserver, a WAF is an inbound proxy. Once we consider this, we see how it is possible to deploy other technologies commonly applied to outbound proxies to a WAF, such as AV and access control. Applying AV rules to an inbound proxy may sound like a stretch because of possible performance limitations, and there are certainly issues with this; but it is vital to remember that in this case, we are not protecting a workstation.

We are protecting a very specific technology; so the applied AV can be limited to only signatures and heuristics that are relevant to a web server; there is really no need to run 11 million signatures to protect a web server. And this can make running an AV more plausible.

At this juncture, it is also worth mentioning what WAFs do not do.

A WAF will not enforce access control in the traditional meaning of the term. Do not be confused by the term "firewall" present in the name of this technology. A WAF only protects the server farm behind it, adopting signature based or anomaly detection algorithms but, unlike a network IPS, it will focus only on the HTTP and HTTPS protocols. A WAF is a layer 7 technology, not layer 3.

Some Web Application Firewalls will also provide layer 7 protection against DDoS attacks, although most vendors separate the 2 types of protection, offering specific DDoS protection as a different service or appliance. However, since this article pertains to WAF, we will not dwell on the details of DDoS attacks against web servers and why protection against such attacks is equally necessary.

Gartner's magic quadrant for WAFs says:

- Protect web applications against hackers' attacks, to monitor access to the web applications, and to collect access logs for compliance/auditing and analytics
- Primary WAF benefit: providing protection for custom web applications that would otherwise go unprotected by other technologies that guard only against known exploits and prevent vulnerabilities in off-the-shelf web application software
- WAF technology
  - Maximizes the detection and catch rate for known and unknown threats
  - Minimizes false alerts (false positives) and adapts to continually evolving web applications
  - Ensures broader adoption through ease of use and minimal performance impact

There is another aspect to WAF technology that must not be underestimated. A web server runs 2 'applications' – the web server itself (be it Apache or IIS or something else) and the user application (what you see when you go to that website). And in between, there are the tools used to develop the user application itself. These could be PHP, Wordpress templates, Java, ASP, you name it.

Each of these layers can have vulnerabilities. Apache has its own and plenty of them; IIS does as well. But these are often known, announced, patched and therefore, made irrelevant after a while. Aside from that, once they are known, it is often possible to create IPS signatures that can protect the web server itself.

The real issues, the ones that can cost an organization its entire database, are those caused by the user level application and tools used to develop it. Whether it is an off-the-shelf product or one developed in-house (which is most often the case), software invariably has errors, which leads to vulnerabilities. It is not a matter of if, but how many, and how exploitable.

For example, PHP and Java have vulnerabilities. But these aren't tools you can always update as this (act) could break the actual application. As such, these tools are often not updated, vulnerabilities are not patched, and they cause the application to be, well, laid bare and open to attacks.

Next month, in our third and final installment, we will discuss the inherent security pitfalls in the applications we use.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th September 2016, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
September 2016

This month, for Network Box 5, these include:

- Allow administrators to clear non-administrator entity attributes
- Add bandwidth limit to network utilisation line chart in admin web portal
- Improve validation of IP addresses on setting IPv4 attribute in admin web portal
- Provide a 'Reset' button for filters in admin and user web portals
- Improve widget container resizing for different screen sizes in admin and user web portals
- Introduce administrative notification messages when configuration changes are synced from/to box
- Introduce a Network Setup Guide for admin web portal
- Enhance display of mail message body size in admin web portal
- Enhancements to firewall behaviour for IPSEC VPN connections
- Enhancements to firewall behaviour for PPTP VPN connections
- Enhancements to firewall behaviour for SSL VPN connections
- Updates to administration guide for network-frontline
- Improve entity address learning configurability
- Introduce support for RFC-6238 (TOTP) Multi factor authentication
- Provide an option to use centralised authentication service helpers for admin web portal authentication
- Provide support for NXLOG system log events from windows activate directory servers
- Provide support for entity creation and IP address attribute learning, from windows active directory server login/logoff events
- Provide a configuration option to optionally rescan eMail before quarantine release on admin web portal
- Enhance 'bulk' classification to no longer classify Message Disposition Notifications as bulk
- Improvements to entity identification and logging in mail scanning, even if envelope verification is not enforced
- SSL Mitigation for SWEET32
- E-16000i box model support
- Regular update to IP geolocation accuracy
- Permit configuration of ethernet interface MTU size
- Allow custom connection tracking limits to survive a box reboot
- Provide protection for CVE-2016-5696 Linux Kernel challenge ACK side window vulnerability

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 SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

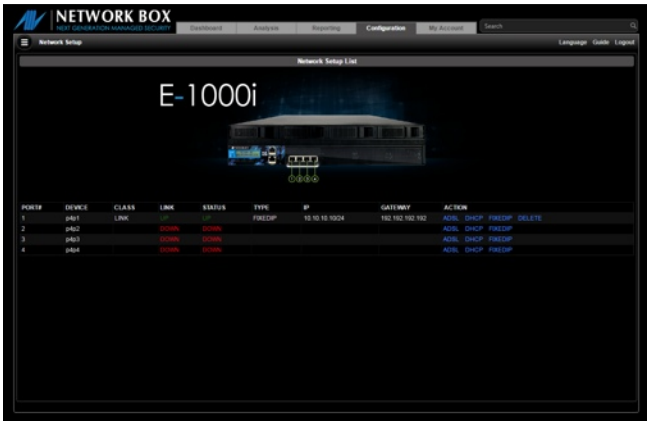
NETWORK BOX

Network Box Hardware Configuration: Network Setup

To help with accessibility, you can now manually make configuration changes to network configuration of your hardware, via the Network Box Dashboard.

Using this method, you can configure and set your device to use the following options:

- ADSL
- DCHP
- FIXED IP



This is particularly useful for instances where you may have changed your Internet service provider, and have forgotten to inform the Network Box SOC.

e-Brand Awards 2016
Best Managed Security Provider

Network Box won the **Best Managed Security Service Provider 2016**, at the 2016 *e-brand awards*. Many of the world's top IT brands were at the event, winning awards in their respective categories, including Amazon Web Services, Lenovo, HP Enterprise, ASUS, Microsoft, DELL, Seagate, CISCO, intel, NETGEAR, Canon, Epson, SAP, Fuji Xerox, and Oracle.

Network Box Australasia
UAC Expo & Seminar 2016

Network Box Australasia was at the **UAC Expo and Seminar 2016**, held in Christchurch, New Zealand, to introduce Network Box's latest Network Box 5.3 Managed Security Service Platform and key features.

UAC
UNDERWRITING AGENCIES COUNCIL

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box UK** **Network Box USA** Contributors	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 2736-2083 Fax: +852 2736-2778 www.network-box.com

NETWORK BOX