Welcome to the December 2012 edition of In the Boxing Ring

This month, we are extremely proud to officially announce the launch of our new Anti-DDoS WAF+ (Anti-Distributed Denial of Service Web Application Firewall Plus) system, WAF-Scan. This is the first in a series of Network Box Version Five products and services that will be launched over the coming months.

In pages 2 to 4, Network Box’s Head of Research and Development, Nick Jones, introduces and gives a technical overview of the system; highlighting its Interception, Classification, Action and Translation methods.

As a special feature to mark what is arguably the most important launch for Network Box since the original Unified Treat Management Plus (UTM+) platform twelve years ago; we present a pictorial of the event in page 5.

Page 6 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
December 2012

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

IN THIS ISSUE

2-4
Anti-DDoS WAF+
Overview
Our new system is a multi level security solution, for the protection of Web Applications, the Servers that those applications are deployed on, and the Networks that those servers are connected to. It addresses a security problem that also exists at multiple levels, where attackers are combining precise Web Application and Server vulnerability attacks with Distributed Denial of Service attacks.

5
NETWORK BOX
Anti-DDoS WAF+
Global Launch
A special pictorial covering the launch of our new system. Managing Director, Michael Gazeley, gave a brief overview of Network Box’s key milestones; followed by an introduction and live demonstration by CTO Mark Webb-Johnson and Head of R&D Nick Jones.

6
December 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.
Anti-DDoS WAF+

Overview

Introduction

Anti-DDoS WAF+ is a multi level security solution, for the protection of Web Applications, the Servers that those applications are deployed on, and the Networks that those servers are connected to.

It addresses a security problem that also exists at multiple levels, where attackers are combining precise Web Application and Server vulnerability attacks with the scale and violence of Distributed Denial of Service attacks.

The Anti-DDoS WAF+ product provides protection against HTTP borne Web Application attacks with built in rules for the detection of common attack types such as: Cross Site Scripting, SQL Injection and the detection of Crawlers and Malware, as well as the ability to create more specific security rules for the protection of unique functions in custom Web Applications. It also provides Denial of Service protection in the form of IP (v4 and v6) address Black Lists, that can be dynamically updated when the Anti-DDoS WAF+ system identifies a DoS attack.

In addition, the Network Box Hybrid Firewall implementation, the component that captures traffic for security analysis, can perform transport and session protocol translation, allowing a NBRS-5.0 device to be a terminator for IPv6 and SSL.

As part of this issue of ‘In the Boxing Ring’, some of the key architectural components of the Anti-DDoS WAF+ and its most important features and benefits will be discussed.

Interception

The ideal method for deployment of an Anti-DDoS WAF+ device is as an inline, transparent interceptor of traffic, sitting in between an external, untrusted, Web Client and the customers’ Web Server.

Here, the Anti-DDoS WAF+ device will generally follow the Network Box philosophy for the design of security functions, and that is: ‘Do No Harm’. The original IP address of the Client, from the point of view of the Web Server, is preserved, and from the point of view of the Web Client, the IP address of the Web Server is preserved, maintaining an illusion of directness.

However, although ‘Do No Harm’ is the guiding principle for the treatment of benign traffic, the same will not be said for the enforcement of Security Policy against malicious traffic. Actions

On the 30th of November 2012, our Anti-DDoS WAF+ system, WAF-Scan was made generally available, and introduced to a number of our important customers at the official product launch ceremony.
taken against such traffic can range from outright blocking of all IP traffic to and from blacklisted Web Client addresses, to the protocol specific mangling and removal of transaction data and meta data deemed to be in violation of Security Policy.

To begin with, traffic from Web Clients is tested against IPv4 and IPv6 address blacklists at the time they first enter into the network stack of the Anti-DDoS WAF+ device. These blacklists contain the addresses of Clients previously deemed to be malicious by Anti-DDoS WAF+ Security Policy, in particular the DDoS Protection Policies.

This filtering process is performed at a level that is very close to the physical hardware of the device, before significant processing is carried out by the NBRS-5.0 host system, therefore decisions made at this level are fast, in the order of hundreds of thousands of packets per second, even on mid-range hardware such as the Network Box M-Series devices.

Following this, traffic is passed into the Interception layer, which is the Application Layer Proxy component of the NBRS-5.0 Hybrid Firewall. The Application Layer Proxy has hooks into lower layers of the Operating System network stack, and provides a ‘Best of Both Worlds’ service, by allowing full access to protocol level data streams for the purpose of Classification, but at the same time preserving original IP addresses in a style akin to IP level bridging.

The Translation functions, which are a key feature of the Anti-DDoS WAF+ product, are performed by the Application Layer Proxy. They will be discussed in detail in the Translation section, but to summarize, Web Client traffic is stripped of Transport and Session level encapsulations and presented as a stream of data to the Anti-DDoS WAF+ Classification layer.

Classification

A foundational design principle in NBRS-5.0 is the separation of Classification and Action.

The Classification process in NBRS-5.0 has the simple goal: ‘Determine as much about a given traffic flow as possible’. Each security module in NBRS-5.0 aims to perform this function in a unique context, to determine the nature of a given piece of data, whether that be the extraction and cataloguing of protocol specific meta data, or the identification of any Virus or Malware in a transaction payload. Therefore, behind the generic goal statement of the Classification layer lie implementation details that are anything but generic.

The purpose of the Web Firewall, which is the incarnation of the Classification component of the Anti-DDoS WAF+ security product, is to completely and utterly decompose the incoming HTTP protocol data into basic elements. Meta data is extracted, behaviors are observed and logged for future reference, and a
rules engine, powered by a Web Application Firewall specific rule language are applied to the de-constructed HTTP protocol information.

Due to its complexity and comprehensiveness, the Anti-DDoS WAF+ Web Firewall is a security subsystem unto itself, with a multi layered HTTP protocol parsing and extraction engine, as well as a rules based analysis engine utilizing a unique set of signatures, supported by Network Box in a dedicated maintenance and update cycle.

The results of the Classification phase are then interpreted by the Action phase.

**Action**

The Action phase involves many layers of the fundamental NBRS-5.0 architecture, from the unifying configuration management provided by NBCONFIG and NBCONSOLE, to the context specific components such as Anti-DDoS WAF+.

The first stage of the Action phase actually occurs long before Web Client and Web Server transactions begin. It is where Security Policy rules are defined using the NBCONSOLE system. The Anti-DDoS WAF+ plugs into the NBCONSOLE system, to make use of the enormous library of data types and network administration and security concepts already provided in NBRS-5.0, and at the same time add Web Application Firewall specific data types and concepts.

The Anti-DDoS WAF+ NBCONSOLE commands provide administrators with a means to define Security Policy and Rules that will be invoked with the meta data and analysis verdicts of the specific Anti-DDoS WAF+ Web Firewall, and interpret them as Actions to carry out against the transaction being analysed.

The DDoS Protection facet of the Anti-DDoS WAF+ product also provides similar enrichment to the NBCONSOLE environment, by adding a few unique network administration concepts.

The DDoS Protection module also allows the Administrator to interpret the analysis and meta data of HTTP transactions as being evidence of a DDoS attack. Such DDoS verdicts will result in special actions being taken by the Anti-DDoS WAF+ system, namely the updating of the dynamic IP address blacklists to provide immediate and responsive rejections of subsequent connections from DDoS clients.

**Translation**

The translation layer of the Anti-DDoS WAF+ product provides an important function to the core Classification component, that is, to isolate incoming protocol data regardless of low level Transport Layer or Secure Encapsulation (SSL).

By giving Network Administrators access to these translation features for incoming data, and allowing them perform similar translations to the outgoing data, an Anti-DDoS WAF+ device can become a powerful translation tool. Two key use cases for this feature is the efficient and near transparent translation between IPv6 and IPv4 networks, as well as the termination of SSL encryption before the transactions reach the internal Web Servers.

One key benefit of the IP translation services are: Removing the need to directly engage internal Web Server Operating Systems with an IPv6 Internet, or even with an IPv6 network, saving cost and complexity for customers. However, customer Web Applications and Web Server software should be updated to sensibly handle IPv6 client addresses, in particular for the purpose of logging.

For SSL Translation and Termination. The benefits are two fold: Firstly, a customer may enjoy the added performance gained by removing the CPU and memory burden of decryption from their internal Web Servers, as it will be carried out on their behalf by the Anti-DDoS WAF+ device. It must be noted however that communications between the Anti-DDoS WAF+ device and the internal Web Servers must be as direct as possible and over a trusted internal network, to reduce the amount of time that the previously encrypted transaction spends in plaintext form.

Secondly, customers who utilize the Anti-DDoS WAF+ for SSL Termination will enjoy the protection of the most up to date SSL transport protocols, currently up to TLS version 1.2, and automatically be a part of the ongoing Network Box SSL Security Strategy.

This program is part of a long term Security strategy that Network Box is undertaking, to provide customers with a range of products and services based on SSL, executed at the Network Gateway. We’ll go into more detail about the Network Box SSL Security Strategy in future editions of ‘In the Boxing Ring’!
Anti-DDoS WAF+ Global Launch

30 November 2012

Network Box officially launched its new Anti-DDoS WAF+ (Anti-Distributed Denial of Service Web Application Firewall Plus) system, WAF-SCAN. This is the first of a number of Network Box Version Five (NBRS-5.0) based systems which will be launched over the next few months. Thank you to all those who supported and attended the event.

During the event, Managing Director, Michael Gazeley, gave a brief overview of Network Box’s key milestones. This was followed by an introduction and live demonstration by CTO Mark Webb-Johnson and Head of R&D Nick Jones.
December 2012 Features
On Tuesday, 4th December 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 my.network-box.com administrative web interface
- Minor layout fixes to the weekly report PDF
- 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 | Anti-DDoS WAF+ Global Launch

Network Box’s Anti-DDoS WAF+ (Anti-Distributed Denial of Service Web Application Firewall Plus) system, WAF-SCAN, is a highly customizable managed security appliance (or alternatively virtual / cloud based device), which can apply a strict set of pre-configured rules to an HTTP / HTTPS conversation, in order to protect web facing servers against attack.

Key features include: Anti-DDoS Mitigation, Web Application Protection and IPv4 to IPv6 / IPv6 to IPv4 Cross-Protocol Bridging. This is the first of a number of Network Box Version Five (NBRS-5.0) based systems which will be launched over the next few months.