Welcome to the October 2013 edition of In the Boxing Ring

Since the launch of Network Box NBRS-5 WAF+, we’ve received many enquiries asking about the differences between traditional IDS/IPS systems and the Network Box WAF+ offering. Both protect web servers, so which is better? In this month’s feature article, we answer this question.

On pages 5 and 6 we feature the fixes to be released in this month’s NBRS-5.0 patch Tuesday; and cover the key milestones of the NBRS-5.0 platform.

Page 7 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.

Finally, Network Box is pleased to announce that we will be launching the new Network Box 5 hardware at the end of this month. The new hardware will support the Network Box NBRS-5.0 UTM+ and Anti-DDoS WAF+ systems.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
October 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/0/107446804085109324633/posts

IN THIS ISSUE

2-4
IDS/IDP vs WAF
In this month’s feature article, we answer which is better and highlight the IDS/IPS and WAF differences.

5-6
NBRS-5.0 Features and Roadmap
The features and fixes to be released in this month’s patch Tuesday for NBRS-5.0. NBRS-5.0 roadmap, which gives a clear overview of what we have recently released, as well as the final milestones.

7
NBRS-3.0 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).

7
Network Box 5 Launch
At the end of this month we will officially launch the Network Box 5 hardware and systems. If you are interested in attending the launch please contact our marketing team: marketing@network-box.com
IDS/IPS

Under the Hood

Intrusion Detection / Prevention Systems operate at the network level, usually in a transparent manner. They receive network packets, and attempt to recreate the communication sessions that those packets make up. They can then provide advanced higher-layer decoding, for specific protocols, but they always operate at the network layer itself.

At the packet level, let’s see how this works with a typical HTTP session over tcp/80 destined to a web server. Separating out just the one session we are interested in, this is what the IDS/IPS system seems at the network packet layer:

09:35:57.858874 IP 10.8.2.100.65132 > 74.125.128.147: Flags [S], seq 893507093, win 65535, options [mss 1460,nop,wscale 4,nop,nop,TS val 3712851838 ecr 0,sackOK,eol], length 0
09:35:57.862643 IP 74.125.128.147 > 10.8.2.100.65132: Flags [S.], seq 2557492822, ack 893507094, win 42900, options [mss 1430,nop,wscale 6], length 0
09:35:57.862817 IP 10.8.2.100.65132 > 74.125.128.147: Flags [.], ack 1, win 16384, length 0
09:35:57.862873 IP 10.8.2.100.65132 > 74.125.128.147: Flags [P.], seq 1:146, ack 1, win 16384, length 145
09:35:57.866990 IP 74.125.128.147 > 10.8.2.100.65132: Flags [.], seq 146, win 669, length 0
09:35:57.881756 IP 74.125.128.147 > 10.8.2.100.65132: Flags [.], seq 1431, ack 146, win 669, length 1430
09:35:57.881881 IP 74.125.128.147 > 10.8.2.100.65132: Flags [.], seq 1431:2861, ack 146, win 669, length 1430
09:35:57.881883 IP 74.125.128.147 > 10.8.2.100.65132: Flags [.], seq 2861:4291, ack 146, win 669, length 1430
09:35:57.881904 IP 74.125.128.147 > 10.8.2.100.65132: Flags [.], seq 4291:5721, ack 146, win 669, length 1430
09:35:57.882176 IP 74.125.128.147 > 10.8.2.100.65132: Flags [.], seq 1:146, ack 1, win 16384, length 145
09:35:57.882525 IP 74.125.128.147 > 10.8.2.100.65132: Flags [.], seq 7151:8581, ack 146, win 669, length 1430
09:35:57.882271 IP 10.8.2.100.65132 > 74.125.128.147: Flags [.], seq 146, ack 11259, win 16384, length 0
09:35:57.883065 IP 10.8.2.100.65132 > 74.125.128.147: Flags [.], seq 146, ack 11260, win 16384, length 0

WAF

Since the launch of Network Box NBRS-5.0 Anti-DDoS WAF+ we’ve received many enquiries asking about the differences between traditional IDS/IPS systems and the Network Box Anti-DDoS WAF+ offering. Both protect web servers, so which is better? This article answers this question.

IDS/IPS versus WAF

In the Boxing Ring - October 2013
First, it sees a SYN packet going 10.8.2.100 -> 74.125.128.147, followed by a SYN+ACK coming back, followed by an ACK - this is the classic three way handshake and shows a successful TCP/IP connection. Then, it sees TCP/IP data travelling back and forth, along with packet acknowledgements, and possibly re-transmissions, duplicate packets, and all the other mess that occurs at the IP layer. Finally, it sees a FIN packet going 10.8.2.100 -> 74.125.128.147, followed by a FIN+ACK and finally an ACK - this is the TCP/IP connection being closed.

A good IDS/IPS will start at the network layer, and try to re-assemble the packets into streams (TCP/IP streams in this example). Once it has the stream, and has been told the protocol involved, it will attempt to decode the protocol data. Let's have a look at the fourth packet, in detail:

At the start of the packet is the ethernet, IP and TCP encapsulation. The data itself starts at offset 0x0028 and contains the following:

GET / HTTP/1.1
User-Agent: curl/
7.24.0 (x86_64-apple-darwin12.0) libcurl/
7.24.0.OpenSSL/
0.9.8.zlib/1.2.5
Host: 74.125.128.147
Accept: */*

That is an HTTP request, and the request, headers and values can be decoded by high level protocol decoders in the IDS/IPS.

The problem for most IDS/IPS systems start here at the application layer, and that is why most IDS/IPS systems stop here. The encodings, and data transfers, at the application layer become very complicated, so traditional IDS/IPS systems generally decode only up to, but not into, the application layer. An IDS/IPS system can see the application traffic, but can't understand it. IDS/IPS systems just blindly apply pattern marching signature rules against both raw packet and stream re-assembled data, but they do not understand the meaning of the data itself.

WAF
Under the Hood

A WAF, such as Network Box NBR5-5.0 Anti-DDoS WAF+, starts where the IDS/IPS finishes. Web Application Firewalls decode the HTTP web protocol completely, and understand the meaning of requests and responses on that protocol.

Examples of this include:

- A WAF typically takes the stream level data, and correlates streams together (so for example, requests to the same web application from the same web client, are treated together).
- WAF systems can protect both HTTP and HTTPS protocol traffic.
- Web-specific formats such as HTML, JSON and XML have specific protection modules in the WAF.
- Unlike protocols such as SMTP, POP3, FTP, the HTTP protocol is used to deliver applications - and the WAF understands both that delivery process and the applications themselves.
- Web requests can include both headers as well as bodies, and the WAF understands and decodes these completely. As well as decoding headers, the WAF can decode fields and attached files within POSTed forms.
- Requests and bodies can be encoded in a myriad of formats, and the WAF is able to fully decode all these.
- Bodies can be subjected to more in-depth analysis (such as anti-virus scan).

For example, let's examine a web request that recently came in to www.network-box.com from a host in the Netherlands. Here is the request:

```
POST /phppath/php?-d+allow_url_include%3Don+-d+safemode%3Doff+-d+suhosin.simulation%3Don+-d+disable_functions%3D
%d%22+-d+open_basedir%3Dnone+-d+auto_prepend_file%3Dphp%2Finput+-n HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U: Windows NT 6.1; tr-TR) AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4
Safari/533.20.27
Content-Type: application/x-www-form-urlencoded
Host: www.network-box.com
Content-Length: 2634
```

(2,634 byte HTML form provided, but not shown)
The WAF decoded not just the headers, but also the attached form and even the fields within that form. It found the following laundry list of problems:

1. PHP Injection Attack - OWASP_AppSensor/CIE4 OWASP_TOP_10/A1 OWASP_TOP_10/A6 PCI/6.5.2 WASCTC/WASC-15 WASCTC/WASC-25 WEB_ATTACK/HTTP_RESPONSE_SPLITTING WEB_ATTACK/PHP_INJECTION
2. SQL Comment Sequence Detected - OWASP_AppSensor/CIE1 OWASP_TOP_10/A1 PCI/6.5.2 WASCTC/WASC-19 WEB_ATTACK/SQL_INJECTION
3. SQL Hex Encoding Identified - OWASP_AppSensor/CIE1 OWASP_TOP_10/A1 PCI/6.5.2 WASCTC/ WASC-19 WEB_ATTACK/SQL_INJECTION
4. SQL Injection Attack: SQL Operator Detected - OWASP_AppSensor/CIE1 OWASP_TOP_10/A1 PCI/6.5.2 WASCTC/WASC-19 WEB_ATTACK/SQL_INJECTION
5. Blind SQL Injection Attack - OWASP_AppSensor/CIE1 OWASP_TOP_10/A1 PCI/6.5.2 WASCTC/WASC-19 WEB_ATTACK/SQL_INJECTION
6. SQL Character Anomaly Detection Alert - Repetative Non-Word Characters
7. Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded
8. Detects MySQL comment-/space-obfuscated injections and backtick termination - WEB_ATTACK/SQLI
9. Detects SQL benchmark and sleep injection attempts including conditional queries - WEB_ATTACK/SQLI
10. Detects basic SQL authentication bypass attempts 2/3 - WEB_ATTACK/SQLI
11. Detects MySQL comments, conditions and ch(a)r injections - WEB_ATTACK/SQLI
12. Detects classic SQL injection probings 2/2 - WEB_ATTACK/SQLI
13. XSS Attack Detected
14. IE XSS Filters - Attack Detected

A total of 14 suspicious attributes in the web request headers and body.

While an IDS/IPS system blindly blocks/permits based on a single result, the WAF can operate an Anomaly Scoring System - similar to how anti-spam systems work, the WAF assigns each test a score - and the entire transaction is permitted / denied based on the total anomaly score. These tests can be done at each of the four stages of the web transaction (request header, request body, response header and response body).

In the case of the above web request, the anomaly score totalled 158 (54 being SQL injection types, and 25 being XSS cross-site-scripting types), and the request was blocked as it exceeded the default threshold of 10 (by more than 15x).

**Conclusion**

So, what is the difference between IDS/IPS and WAF? Well, simply put the IDS/IPS system operates between the network and application layers, while the WAF operates purely at the application layer. While IDS/IPS systems can provide limited support for application layer protocols, WAF concentrates purely on protection of web protocols and the applications running on those protocols.

An IDS/IPS can provide protection for a large number of protocols, while a WAF provides complete and comprehensive protection for applications running on just one protocol - the HTTP web protocol.
On Tuesday, 1st October 2013, Network Box will release our patch Tuesday set of enhancements and fixes. These enhancements have been primarily made to support the new web client security modules.

**NBRS-5.0 Features**

**October 2013**

Our work this month primarily involves extensions and enhancements to existing security modules, as we prepare for the upcoming release of NBRS-5 UTM+ service packages. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for NBRS-5, these include:

- Box timezone support in my.network-box.com administrative user interface
- Support for detailed record enquiries in on-line reports from my.network-box.com
- Improvements to management of RAID disk systems
- Allow for resync of individual signature packages (as well as all)
- Extension to support entering of an optional administrative comment alongside configuration changes
- Facilities to customize templates for alert pages and messages
- Support for a new unified quarantine arrangement
- Support for tracing system log messages
- Extensions to the network high availability subsystem
- Support for network address translation for connections originating from the box itself, as well as passing through the box
- Base proxy support for bridging configurations
- Extensions to application identification
- Improvements to proxy memory management
- Revisions to the timeout system for high-priority scanning jobs (such as HTTP)

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.
NBR5.0

Roadmap

We are now well into the ramp-up phase of our road-map for NBR5.0. The majority of development work has been completed, and we are now conducting final development, packaging and beta tests for the remaining security modules.

With last July’s patch Tuesday we released our SURF SCAN product, and included anti-malware and content-filtering support for web clients - rounding-out our web content protection offering (both client and server). In August, we released our NBR5.0 application identification framework to public beta test. Last month we released our mail scanning product, and that will be followed by the remaining miscellaneous modules to bring NBR5.0 up to, and beyond, full UTM+ equivalence to NBR3.0. Now that we have reached these milestones, we can start the process of offering NBR5.0 upgrades to our existing NBR3.0 clients.

The NBR5 major releases for Network Box (NBR5.0, NBR5.0, NBR5.0, etc) include long-term support, of 5+ years, so this is just the start of a long journey with NBR5.0. We have some truly exciting new product offerings, taking advantage of the new foundational support architecture of NBR5.0 that will help us to help you to keep your online networks secure.

1. BASE PLATFORM

Back in the summer of 2012, we completed and released the base platform and support infrastructure for NBR5.0. This made up the bulk of the product’s code base, and forms the foundation for all our NBR5.0 product offerings.

2. WAF+

We followed that up with the Anti-DDoS WAP+ service package. This package provide new functionality (not previously available with NBR3.0) to protect DMZ/cloud based web servers from Internet-based attackers. It provides network firewall, web application firewall, DDoS protection, and protocol translation (IPv4-IPv6 / IPv6-IPv4 bridging) functionality, into a single service offering.

3. SURF SCAN

To produce a web application firewall, we had to design and build a proxy capable of understanding the web’s HTTP protocol. We’re now turning that around, and combining it with our advanced scanning technology, to make up our next NBR5.0 offering: SURF SCAN. This will provide for protection of web based clients on the LAN, browsing web servers on the Internet. It will support anti-virus scanning, as well as web site and content classification – for comprehensive policy control. It will also support extensive reporting capabilities.

4. APP SCAN

Following on from that, we will be releasing APP SCAN - the application identification system that we have been working on for some time. This, operating standalone, or combined with SURF SCAN, is capable of identifying applications at the network level, and extracting meta data and content from the data streams. Both anti-virus scanning and policy control technology can then be applied.

5. MAIL SCAN

At that point, we will have comprehensive web server, and LAN client support, so we will be releasing our mail server protection MAIL SCAN. This will provide support for scanning mail traffic using the SMTP, POP3 and IMAP4 protocols.

6. UTM+

Finally, we will round-out the UTM+ equivalence, with the release of a set of security modules implementing such functionality as QoS (Quality of Service), VPNs, Clustering, High Availability, etc. Some of these will actually be released alongside the earlier service offerings, as and when they are ready.
NBRS-3.0 Features
October 2013

On Tuesday, 1st October 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, for NFRS-3.0, these include:

- Fix to my.network-box.com related to display of group name in Web Proxy / Config / Rule
- Extensions to assist NOC configuration of primary and secondary DNS servers
- Performance improvements in the iOS PUSH notification system
- 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.

Network Box 5 Launch

Network Box will be launching a new range of Network Box 5 hardware, at the end of this month to match the new range of NBRS-5.0 UTM+ (Unified Threat Management Plus) and Anti-DDoS WAF+ (Anti-Distributed Denial of Service Web Application Firewall Plus) managed security services. The new range of hardware platforms, offer world class security, stunning levels of performance, as well as proven business continuity.