Welcome to the April 2012 edition of ‘In the Boxing Ring’. In this edition, we focus on Network Box NBRS-5.0 Web Application Firewall.

This month, on pages 2, 3 and 4, we present details on Network Box NBRS-5.0 Web Application Firewall. A state-of-the-art firewall combined with routing, protocol translation, encryption and compression offloading, and DDoS protection. It goes beyond a firewall, which can typically open/close port tcp/80, to providing protection and translation services for web traffic passing over the open port tcp/80.

What makes the Network Box NBRS-5.0 Web Application Firewall (WAF) special? Why choose Network Box over the many competitors in the same field? The basic answer is that just as with the Network Box approach to UTM, adding services and functionality to make UTM+, Network Box has taken all the key security components necessary to protect a web server and put them into one holistically managed device with associated services. WAF+.

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
April 2012
Network Box NBRS-5.0 Web Application Firewall

The Network Box NBRS-5.0 Web Application Firewall is a state-of-the-art firewall combined with routing, protocol translation, encryption and compression offloading, and DDOS protection. It goes beyond a firewall, which can typically open/close port tcp/80, to providing protection and translation services for web traffic passing over the open port tcp/80.

Last month we spoke about Web Application Firewalls in general. This month, we concentrate on Network Box’s approach.

Incoming Network Traffic Flow

Network traffic (connections to tcp/80 usually, for a web application firewall environment) come in on the left side of the diagram, below. The Network Input layer handles, and enforces conformance to, the fundamental IP protocols and deals with common DDOS/DOS style attacks such as synflood, fragmentation attacks and protocol anomalies at the lowest (fastest) level possible. In particular, attacks whereby the source address could be spoofed are dealt with at this level, so that subsequent levels are assured that the source IP address is real.

Acceptable connections are then passed into the Network DDOS protection module. This module maintains a whitelist of IP addresses that are always permitted and never denied access by DDOS protection. The whitelist is commonly used to protect against self-denial of service by listing an organisation’s own addresses, as well as important partner addresses. After passing the whitelist, two blacklists are used for active blocking of connections - (a) a dynamic blacklist is used to temporarily hold source attacking addresses for short periods of time, and (b) a permanent blacklist is used to hold source attacking addresses for longer periods of time. Entries in the dynamic blacklist will typically expire and be automatically removed after just a few minutes, while entries in the permanent blacklist will remain until administratively removed. All three blacklists use hash-based lookups in order to cope with attacks scaling hundreds of thousands of connections a second.

Network Selection

Once an incoming connection has passed the INPUT and DDOS protection modules, it passes into the Network Selection phase. Here, the traffic is classified and a decision made whether to pass it through at network firewall level, or intercept it for more in-depth processing. In the case of web traffic, it would typically be configured to be intercepted, and redirected through the firewall into the Proxy Intercept system.

Proxy Intercept and Web Application Firewallsing

The Proxy Intercept module is a high-performance module capable of proxying network traffic. An incoming connection is accepted and security partitioned from a related, but separate, outbound server connection. This partitioning allows for the request headers, request body, response headers and response body to be individually analysed for policy enforcement.

The incoming traffic (from the web client) is then passed to the Input Translations module which handles high-level protocol translations such as SSL proxying, as well as supporting both IPv4 and IPv6 protocols. SSL connections can be terminated within the Proxy Intercept system, and traffic decrypted for further analysis.
The Web Server Proxy then handles the connection stream in and out of the Web Application Firewall itself, decoding the HTTP protocol (transparently supporting up to HTTP/1.1) into its constituent parts and working with the Web Application Firewall to enforce policy on those parts of the web transaction, in real-time as the traffic passes through the box.

The outgoing traffic (from the web client, having passed successfully through the web application firewall) is then passed to the Output Translations module which handles high-level protocol translations such as SSL client connections, as well as supporting both IPv4 and IPv6 protocols. Connections can be SSL encrypted at this stage (regardless of whether they originally came in SSL encrypted).

**Outgoing Network Traffic Flow**

The final part of the flow is for the traffic to pass back out through the firewall to the Network Source and Destination NAT module. At this stage, the network traffic can have its source address changed (typically used for private many-to-one NAT), destination address changed (for service redirection or load balancing), or just be transparently proxied (without any change to source or destination address).

From there, the traffic passes through the Network Output module on to the protected web server.

**Approach and Benefits of Network Box WAF**

So, what makes the Network Box NBRS-5.0 Web Application Firewall (WAF) special? Why choose Network Box over the many competitors in the same field?

The basic answer is that just as with the Network Box approach to UTM, adding services and functionality to make UTM+, Network Box has taken all the key security components necessary to protect a web server and put them into one holistically managed device with associated services. WAF+.

Let's look at just some of the key points of this approach.

1. **Denial of Service Protection**

   Using DOS/DDOS protection at the lowest possible levels of the network stack, NBRS-5.0 provides for first-level mitigation of both DOS and DDOS style attacks. But, going beyond that, the DDOS system is integrated to the WAF, permitting active response against scanning and other brute-force attacks and undesirable competitive activity such as web-site scraping for theft of intellectual property.

2. **Protocol Translation**

   Supporting IPv4, IPv6 and SSL protocols, the NBRS-5.0 Proxy Intercept system permits translation between all combinations of these protocols. For example, the box can be configured to accept both IPv4 and IPv6 connections both plain-text HTTP (on tcp/80) and SSL HTTPS (on tcp/443), then send those connections as a single IPv4 stream load-balanced across a cluster of IPv4-only web servers. This vastly simplifies the network infrastructure that must be maintained in the web server DMZ.

   NBRS-5.0 can also perform both source and destination NAT between IPv4 and IPv6 protocols, allowing for seamless service migration and incredible flexibility in deployment and maintenance of the system.

3. **Internal and External Load Balancing**

   The NBRS5 WAF hosts a highly multithreaded proxy server implementation that takes advantage of hugely multicore CPUs, including the latest Intel Sandy Bridge architecture. The NBRS5 WAF software architecture is designed to internally balance connection workloads among the multiple CPU cores thus enabling it to perform to the level of multiple WAF installations, all in a single hardware unit. Coupled with advanced networking communication hardware such as the Intel i350 network adapter chipset, that reduces the length of data pathways between the network and system memory, the NBRS5 WAF makes the most of advances in server hardware.

   In addition, the NBRS5 WAF supports the ability to load balance connections across multiple physical server instances.
4. Computational Proxying
The NBRS5 WAF provides means to reduce CPU load on Web Servers by employing a number of strategies to allow it to take responsibility for certain computationally expensive tasks on behalf of the Web Server.

5. Compression Proxying
Content compression is a standard feature of the HTTP protocol, designed to increase perceived bandwidth by compressing, or reversibly shrinking, browser and Web Server communications in real time. For a browser communicating with one Web Server, the CPU cost involved is negligible, but for a Web Server communicating with many many clients, the CPU load costs can negate many of the bandwidth usage optimisation benefits, especially in modern times when bandwidth costs have reduced.

6. Encryption Proxying
Secure web communication or HTTPS is a cornerstone of internet security. Its foremost use is to ensure the privacy of communications between the browser and the Web Server, which is fundamental to online commerce and banking in particular. The drawback is that encryption algorithms are very computationally expensive, and can tax a browser client and Web Server CPU to a high degree. Again, for a Web Server serving numerous clients, the CPU cost of maintaining secure connections is significant.

The NBRS5 WAF, when acting on behalf of the Web Server and directly receiving client browser requests, can perform decryption and encryption of incoming and outgoing traffic travelling over the public internet, while communicating without encryption burden with the Web Server over a secure internal network. Using hardware assisted cryptography, the NBRS5 WAF will be capable of handling significant cryptography workloads on behalf of the protected Web Server.

The benefits don't stop there, as NBRS5 constantly maintains its cryptography software suite, keeping it up to date with the latest security and feature fixes, therefore also keeping the protected Web Server up to date by 'proxy'.

7. Web Application Firewalling
And all the above is done without compromising the effectiveness of the core web application firewall. Supporting protection and policy enforcement at the inbound connection, request headers, request bodies, outbound connection, response headers and response bodies phases, the Network Box NBRS-5.0 WAF can be leveraged to provide vulnerability protection as well as outbound protection, using either of the negative, positive and DDOS security models.

Conclusions

The NBRS-5.0 Proxy Web Server WAF will typically be installed inline between the attack source and the web servers to be protected. Web requests destined for the protected web servers are transparently intercepted and proxied by the the NBRS-5.0 WAF, and subjected to protection rules before being passed on to the web servers. Replies from the protected web servers are similarly intercepted and subjected to protection rules before being returned to the caller.

Released to final beta-testing on Tuesday 3rd April 2012, the Network Box NBRS-5.0 WAF provides comprehensive and effective protection against web application attacks.
April 2012 Features
On Tuesday, 3rd April 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
- Inclusion of Box Type and SLA in Box Office ticket update emails
- Revisions to the GMS health monitoring system improving monitoring of IDPS services
- Performance improvements to the SMTP authentication service
- 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.

Capital Magazine Outstanding Enterprise 2012 Award
Network Box won the Capital Magazine Outstanding Enterprise 2012 Award, for the 'Best Network Security Provider.'

The awards ceremony took place on 13th of March 2012, at the Island Shangri-La Hotel ballroom, Hong Kong.

Capital Magazine is Greater China's Premier Business Magazine. The Capital Outstanding Enterprise Awards aims to recognize the contribution and effort of those enterprises that have outstanding performance and achievements during the year. All winning companies were strictly evaluated by a team of professional judges, the editorial board of Capital Magazine, as well as public online voting.

Public selection criteria included the following: Enterprise's reputation, Marketing strategies, Product's Innovation and Development, Social Responsibility and Environmentally Friendly Projects, Training Programs for Staff, and Customer Service to Business Partners.

Network Box is extremely proud to have won this highly prestigious award. We would like to thank everyone, especially our customers, who voted for us in this competition.