In The Boxing Ring

Network Box Technical News from
Mark Webb-Johnson, CTO Network Box

Welcome
Welcome to the March 2012 edition of ‘In the Boxing Ring’. In this edition, we focus on the Web Application Firewall.

This month, on pages 2 and 3, we present details on Web Application Firewall. Web Application Firewall can be thought of as a very specific sort of Intrusion Prevention System and/or Firewall, targeted purely at protecting web servers and applications running on them, accessed through the HTTP protocol.

It works by examining traffic travelling between untrusted (dirty) web clients and trusted (clean) web servers. It does this by completely decoding the six stages of the HTTP transaction, and enforcing protection rules at each stage: Inbound connection, Request headers, Request body (applicable to some requests only), Outbound connection, Response headers, Response body.

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
March 2012

IN THIS ISSUE

2-3. Firewalling Web Applications
Web Application Firewall can be thought of as a very specific sort of Intrusion Prevention System and/or Firewall, targeted purely at protecting web servers and applications running on them, accessed through the HTTP protocol.

Network Box won the ‘Security Products and Solutions for Finance and Banking’ category, at the 8th Annual 2012 Info Security’s Global Excellence Awards, for our Z-Scan zero day anti-virus system.

4. March 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.
Firewalling Web Applications

It seems like every week, prospects and customers approach Network Box with concerns about the applications running on their Internet-facing web servers. Often, a security scan or PCI vulnerability assessment has highlighted a problem with legacy applications, and fixing the issue in the application themselves is just too hard and costly.

While NBIDPS Intrusion Prevention systems can do wonders for protecting the web servers themselves, it (and other similar technology) is limited in its ability to protect custom applications running on those servers. While generic attack types can be detected and blocked, custom attacks against custom applications are beyond the scope of most Intrusion Prevention Systems.

There is, however, another class of protection nowadays becoming available - Web Application Firewalls. In this two part article, I’ll be talking about this technology and how it can be applied in the real world. This month, I’ll present an overview of the technology itself, while next month I’ll get into specifics.

What is a Web Application Firewall?

A Web Application Firewall can be thought of as a very specific sort of Intrusion Prevention System and/or Firewall, targeted purely at protecting web servers and applications running on them, accessed through the HTTP protocol.

While a Firewall can be told to open/close port tcp/80 for web access, and an Intrusion Prevention System can look at the traffic going by on port tcp/80 and check for common vulnerabilities and exploits, a Web Application Firewall goes beyond both by completely decoding the HTTP protocol and applying rules to requests and responses using that protocol.

Can’t I just turn on HTTP Anti-Virus Inbound?

This is one of the most common requests that get asked. In particular, for scanning files being uploaded to the web server. Protecting ‘clean’ web clients (typically on the LAN/DMZ) against ‘dirty’ malicious web servers in the Internet is what the Network Box HTTP Anti-Virus proxy is designed to do, and it does an impressive job doing it. Protecting ‘dirty’ web clients on the NET from attacking your ‘clean’ web servers in the LAN/DMZ, while using the same basic HTTP protocol, brings with it a completely different set of challenges. Technically, this is called a ‘reverse proxy’, and unfortunately, is not so easy to implement as it is to request.

Even if we could overcome the forward-proxy vs reverse-proxy issue, Anti-Virus is really just one tiny portion of the problem.

So, how does a Web Application Firewall work?

A web application firewall works by examining traffic travelling between untrusted (dirty) web clients and trusted (clean) web servers. It does this by completely decoding the six stages of the HTTP transaction, and enforcing protection rules at each stage:

1. **Inbound connection**
   The connection from the web client arrives and is to be routed to a web server. At this stage, the inbound connection details are known (such as source and target IP addresses), and this can be correlated with the statistical history of that source and a decision made as to whether to permit the source to send a request or to reject the connection.

2. **Request headers**
   At this stage, the request from the web client is received and decoded/analysed. The contents of these headers can be analysed and subject to protection rules, and a decision made as to whether to permit the source to send the request body (if required).

3. **Request body (applicable to some requests only)**
   At this stage, the entire request has been received and decoded/analysed. The contents of the headers and body can be analysed and subject to protection rules, and a decision made as to whether to permit the source to continue with connection to the web server.

4. **Outbound connection**
   At this stage, the connection details are known and subject to protection rules, so that a decision can be made as to whether to permit the source to connect to the target server and to continue with sending the request headers and body to the target server. Some Web Application Firewalls can be configured to delay outbound connection stage until reception of request headers and body, or to immediately connect upon receipt of the inbound connection (so this stage 4 occurs immediately after stage 1 and before stage 2).
5. **Response headers**
The protected web server will respond to the request headers and body with response headers. These headers are decoded/analysed, and protection rules are applied so that a decision can be made as to whether to permit the server to transmit these headers on to the client.

6. **Response body (applicable to some responses only)**
The protected web server will follow up the response headers with a response body. This body can be decoded/analysed, and protection rules are applied so that a decision can be made as to whether to permit the server to transmit this body on to the client.

**Security Models**

Web Application Firewalls typically offer a variety of security modules to choose from. Here are five of the most popular:

1. **Vulnerability Protection**
Web Application Firewalls have powerful rules languages, kept up to date to protect against the latest known vulnerabilities and exploit techniques, to provide for vulnerability mitigation and support the customer’s internal patch release cycle. Protected systems can be virtually patched at the firewall without having to install the patches on the affected systems themselves; keeping protected systems secure until the manufacturer’s patches can be applied.

2. **Outbound Protection**
The Web Application Firewall can enforce policy on outbound traffic. This is commonly used for data leakage prevention, detection of defacement, and other such capabilities. When combined with other modules (such as Web Server Anti-Virus and Network Infected LAN), an effective outbound defence can be defined.

3. **Negative security model**
The Negative security model is an approach to scanning inbound requests and applying protection criteria (signatures, rules and heuristics) to detect protocol anomalies, unusual behaviour, exploits and other common attacks. Sources of attacks can be integrated with other security modules (such as Network DDOS protection) to react to such malicious traffic, or the traffic itself can simply be logged, dropped or sanitised.

4. **DDOS/DOS model**
The DDOS/DOS model typically tracks usage patterns to identify attack sources for suppression and blacklisting. Examples of techniques used include connection rate limiting, request rate limiting, negative response rate limiting, repeat request limiting, and request duration limiting.

5. **Positive security model**
The Positive security model requires the definition of a set of rules to define what applications and traffic will be permitted, and all other non-conforming traffic is rejected.

**Logging**
The logging capabilities of most modern web servers are primarily concerned with logging sufficient information for statistical analysis purposes only. In particular the headers and bodies of POST requests are commonly not logged, and this makes forensic analysis of attacker behaviour impossible.

Web Application Firewalls includes extensive, configurable, logging capabilities. They are usually capable of logging full request and response headers, as well as request and response bodies.

**Protocol Validation and Policy**
Web Application Firewalls often have technology to validate and enforce the HTTP protocol, as well as help the administrator define comprehensive policies on that protocol. Examples include numbers of parameters, length of parameters, size limits, cookie limits, etc.

While a network firewall can allow/deny tcp/80, a Web Application Firewall can allow/deny requests and responses based on a deep understanding of the HTTP protocol, and a rich configuration language.

**Conclusions**
I hope the above has given you a good overview of what a Web Application Firewall is, and what it can do for you. Next month, we’ll get into the specifics of the Network Box Web Application Firewall available in NBRS-5.0, and how it can help you solve your real-world security issues.
March 2012 Features

On Tuesday, 6th March 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
- Improvements to the my.network-box.com validation of email addresses for personal whitelists and blacklists
- A fix to an issue affecting some virus email quarantine release in the mail trace message screen of my.network-box.com
- SSL certificate renewed in my.network-box.com
- Security patch to the domain name lookup service
- Further support for NBRS-3.0 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.

Info Security Global Excellence Awards 2012

Network Box won the 'Security Products and Solutions for Finance and Banking' category, at the 8th Annual 2012 Info Security’s Global Excellence Awards, for our Z-Scan zero day anti-virus system.

Many of the world’s leading professionals from the security industry celebrated the finalists and winners of the 8th Annual 2012 Info Security's Global Excellence Awards on February 29th, 2012. This is the security industry’s leading global excellence program, honoring achievements in every facet of the security industry.

Info Security Products Guide sponsors leading conferences and expos worldwide and plays a vital role in keeping end-users informed of the choices they can make when it comes to protecting their digital resources. It is written expressly for those who are adamant on staying informed of security threats and the preventive measure they can take. You will discover a wealth of information in this guide including tomorrow’s technology today, best deployment scenarios, people and technologies shaping info security and independent product evaluations that facilitate in making the most pertinent security decisions. The Info Security Products Guide Awards recognize and honor excellence in all areas of information security.