Welcome

Welcome to the October 2011 edition of ‘In the Boxing Ring’. Continuing on from April’s format changes, we have had a new look since June, as we continue the run-up to the release of NBRS-5.0. For the rest of this year, each month we will present one topic on NBRS-5.0 (the upcoming major Network Box firmware release). The monthly hint will go, and is replaced with an entire back page on the updates being released to the existing NBRS-3.0 product. This front page will remain, and summarise what is new and notable.

This month, on pages 2 and 3, we present details on the NBRS-5.0 Intrusion Prevention. The six systems of Network Box Intrusion Prevention co-operate at all layers of the network model to balance performance with protection. This six systems are Network Protocol Validation, Denial of Service Protection, Front-Line IPS, Passive/Active IDS, Inline IPS and Application-Level Protection.

Going beyond tradition network-level-only IDS/IPS systems, the Network Box approach extends this down to layer 2 and up to layer 7 of the OSI model. Both inbound and outbound Intrusion Prevention are supported, and are tightly integrated to the other modules of the NBRS-5.0 system.

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

Mark Webb-Johnson  
CTO, Network Box Corporation  
October 2011
The NBRS-5.0 Intrusion Prevention

If you ask a UTM vendor what is Intrusion Prevention, they will normally answer by talking about network-level scanning of traffic, IDS, IDP, IPS and other such catch words. If you ask the same of a network administrator, they more often than not talk about keeping the bad guys out of their networks (and in some cases keeping their own bad guys from getting out of their own networks!). Here at Network Box, we side with the administrators.

The role of the firewall is to permit traffic on designated ports, protocols or applications to pass, while denying / blocking all other traffic. The Intrusion Prevention System must monitor that permitted traffic to try to differentiate between the good and the bad. Firewalls block specified services, Intrusion Prevention Systems block bad traffic on the services left open by the firewall.

Intrusion Prevention systems which operate at the network level (layers 2 and 3) offer the best performance, while those that operate at the application level (layer 7) offer the best protection. The best solution is thus achieved by a careful balance of the two techniques - and this multi-layered approach is at the core of the Network Box approach to Intrusion Prevention.

Intrusion Prevention in NBRS-5.0 consists of six alternative, but co-operative, systems. The systems co-operate and cover all seven layers of the OSI Network model. They are designed to detect anomalous traffic and block it as early as possible, Let’s look at the six systems, in detail.

1. Network Protocol Validation

Network Protocol Validation occurs in the kernel, for both layer 2 and layer 3 traffic. It involves validation of network traffic, at the core protocol levels, identification of fundamental protocol issues, and resolution as close to the hardware as possible. Examples of attacks detected and blocking at this level include exploits of the IP fragmentation facility, sequence number exploits, scans with invalid IP options or sequences, and invalid sequence scans.

Combined with the connection-tracking of the core firewall (which allows the Network Box to validate the connection sequence and detect connections using invalid states), the technology at this level is designed to protect against intrusions using such very low IP-protocol level detection avoidance techniques.

2. Denial of Service Protection

The NBRS-5.0 Network DDOS Security Module provides support for Denial-of-Service (DOS) and Distributed-Denial-of-Service (DDOS) protection at the network layer. Tightly-integrated to the firewall, this module protects by detecting potentially malicious attackers and blacklisting them from all further access for a defined period.

Spoofed Source Address Mitigation uses three main techniques of (a) total connection rate limiting, (b) total connections limiting, and (c) SYN cookies. The first two provide some level of protection against server overload (e.g., ICMP), and the last protects against SYN flood attacks.

Non-Spoofed Source Address Mitigation uses two main techniques of (a) per-source connections limiting, and (b) per-source connection rate limiting. Sources exceeding either of these two limits can be designated malicious and connections dropped. Such sources can be dynamically added to a real-time blacklist for active blocking of future connection requests from that source.

In co-operation with higher-level modules (such as Proxy Base DDOS), Dynamic Signature Generation involves the use of heuristics that can be applied against incoming traffic to dynamically generate signatures identifying malicious traffic and attack sources. Examples of this include identification of URL patterns in HTTP traffic that uniquely identify an attack, and checking of source IP addresses with real-time reputation lookup. Such dynamic signatures can then be used for identification of malicious traffic in both spoofed and non-spoofed connections.
The NBRS-5.0 Network DDOS security module maintains two whitelists of known good traffic sources: (a) a dynamic list anticipating replies to outgoing connection requests, and (b) a static list of known good sources. These two whitelists are used to avoid blacklisting a known good source.

A time-based blacklist of known attack source addresses is maintained, and is used to blacklist traffic from listed addresses for a defined period of time. This is incredibly fast and particularly useful in DDOS attacks from non-spoofed sources. Once a source of any malicious traffic is identified, the source address can be added to the dynamic blacklist, to block all traffic from that source for a pre-defined time period.

3. Front-Line IPS

The Front-Line IPS system is an extremely light-weight, high-speed service offering zero-latency protection inline with the data stream. It targets network worms, exploits and other such attacks, in combination with the DDOS protection modules. Operating in conjunction with the firewall, at the individual packet level (after fragment reassembly), the Front-Line IPS adds packet content inspection and traffic analysis to the base firewall capabilities.

4. Passive/Active IDS

The Network Box IDS system operates at the network level, side-by-side with the data stream (offering little impact on the performance of the data stream itself). It can be configured either as purely-passive (alerting and logging of traffic, without any active enforcement), or in active-mode (with the ability to actively tear-down connections that it deems to be malicious).

5. Inline IPS

The Network Box IDS system operates at the network level, inline with the data stream. Each packet of each connection passes through the system, with an individual packet verdict (derived from the packet data itself, as well as decoded application-level streams) able to permit or deny the packet to pass. Tightly coupled to the firewall, this is able to drop traffic before the remote system even sees it.

6. Application-Level Protection

Effective application-layer protection requires interception of the connections and full disconnection of the client and server. Once intercepted, high-level protocol-dependent actions can be performed (such as anti-virus, policy enforcement, filtering, etc).

Five security models are supported: (a) vulnerability protection (aka "patch mitigation"), (b) outbound protection, (c) the negative security model, (d) DOS/DDOS security model, and (e) the positive security model. Network Box application-level protection includes request and response analysis, extensive logging, protocol validation and policy, response filtering, client authentication and many more such techniques.

Conclusion

The six systems of Network Box Intrusion Prevention co-operate at all layers of the network model to balance performance with protection. Going beyond tradition network-level-only IDS/IPS systems, the Network Box approach extends this down to layer 2 and up to layer 7 of the OSI model. Both inbound and outbound Intrusion Prevention are supported, and are tightly integrated to the other modules of the NBRS-5.0 system.
**October 2011 Features**

On Tuesday, 6th September 2011, 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
- Support for GMS monitoring of boxes behind multiple ADSL links using dynamic IP addressing.
- Improvements to active-response mode of the NBIDPS system.
- Support for contractual arrangements on virtual in-the-cloud network boxes.
- Various (mostly internal) enhancements to Box Office and support systems.
- Revisions to support for daylight savings time in various time zones.

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 Security Response**

As you may know, in addition to Network Box’s main website, we also have a Security Response website, which is updated with the latest firewall, intrusion, malware and spam attack information, all in real-time.

If you click on [http://response.network-box.com/internet-health](http://response.network-box.com/internet-health), for example, you will see a live world map showing global Internet Health, which not only shows all of the attack sources, but also gives Top Ten lists of where the attacks are actually coming from. Two sections of our Security Response website have been updated recently.

The first is the Protection page, which now shows an overview of Network Box’s live protection statistics. At this moment in time, Network Box systems can run up to 78 protection engines, which include a total of 45,818,940 signatures.

The second is the Services page, which now shows Spam Trap Accuracy. This is a particularly compelling statistic, which many of our clients around the world have requested. Currently, our Spam Detection Accuracy is 99.47% and our Email Detection Accuracy is 99.81%. Both are industry leading figures, and both are achieved with no customization, no anti-spam training, and no usage of any intrusive anti-spam techniques such as ‘Challenge Response’; indeed these results are obtained using only default settings.

If you go to the Network Box Security Response website, you will notice that on the left hand side of the page, there is an option to LIKE us on Facebook. Please do so, so you can receive timely security news updates via Facebook, alerting you to any particularly important security issues that you should be aware of. ([http://www.facebook.com/networkboxresponse](http://www.facebook.com/networkboxresponse))