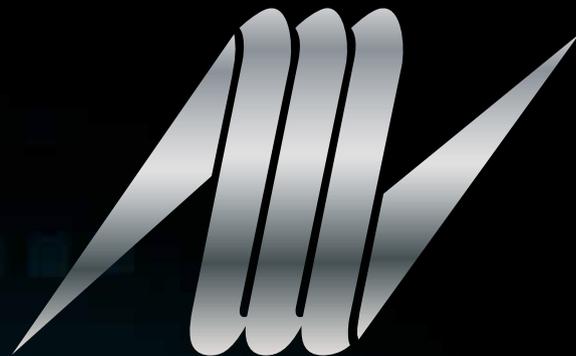


DDoS
Mitigation

Web Application
Protection

IPv4 to IPv6 /
IPv6 to IPv4
Bridging



NETWORK BOX
www.network-box.com

Anti-DDoS

WAF+

Anti-Distributed Denial of Service
Web Application Firewall Plus

IPv6

IPv6 Ready Core
Phase-2 certified



Triple ISO

ISO 9001:2008
ISO/IEC 20000-1:2011
ISO/IEC 27001:2005

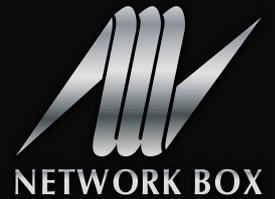


Real-time automated
fingerprinting

Up to 15,000 fully
analyzed transactions
per second

Millisecond response to
Brute Force Attacks

A New Dawn in Network Security



WAF SCAN

Today, the key cyber security technologies protecting most organizations are: *Anti-Virus, Anti-Spam, Firewalling, Intrusion Detection and Prevention, Web Content Filtering, Data Leakage Protection and Company Policy Enforcement*. However, whilst these are all vital security solutions, in the last few years there has been a new type of threat that is affecting organizations world-wide: the combination of DDoS and Web-based attacks.

BACKGROUND

These types of attacks have increased in frequency and sophistication with recent cyber attacks on Sony Online Entertainment and Play Station Network, the CIA and NBC. There is a distinct need for organizations to protect themselves from such threats.

In addition to these cyber threats, the last block of IPv4 web addresses were assigned in February 2011. As IPv4 addresses will soon become unavailable, organizations everywhere will soon be faced with the very real need to migrate over to IPv6.

THE SOLUTION

Network Box saw the need for an urgent solution to these security and connectivity issues and developed *Anti-DDoS WAF+*. The system, is a highly customizable managed security platform, available as a physical appliance or alternatively as a virtual/cloud based device. It protects against the *violence* of brute force DDoS attacks, the *stealth* of web-based attacks which target applications running on web servers, and offers the *adaptability* of IPv4 to IPv6 and IPv6 to IPv4 cross protocol bridging.

SYSTEM OVERVIEW

As standard each Network Box Anti-DDoS WAF+ system is pre-configured with rules to protect against the *OWASP* (Open Web Application Security Project) top ten security risks. It is also possible to customize each Anti-DDoS WAF+ system, with rules to protect against attacks that target specific web applications.

Over time, as each protected web application is modified and updated, the Anti-DDoS WAF+ system can also be similarly modified and updated, to ensure *effective* on-going protection.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.



System Design, Features and Objectives

One of the key design goals of the Network Box Anti-DDoS WAF+ system has been to allow companies and organizations to implement effective Anti-DDoS technology, on an affordable basis. Layer 3 (network) protocol enforcement, including connection rate, data transfer volume and connection slowness can be handled; and a wide range of Layer 7 (application) properties, including URL pattern, user agent and request header contents are taken into account.

SYSTEM DESIGN

Network Box utilizes the **OWASP** top ten as a minimum set of guidelines which need to be adhered to.

Popular web server and application software packages such as Apache, IIS, Joomla, Drupal, Mediawiki and Wordpress are supported as standard. False positives are kept **as low as possible**, with the goal of never disallowing any authorized requests.

This highly flexible system, allows for load balanced, high availability and clustered configurations, to maximize both **performance** and **business continuity**.

The defensive strength of the default settings are maximized, and augmented by the power and accuracy of a state-of-the art **real-time automated threat fingerprinting** engine. This ensures as many incoming threats can be blocked as possible, using the minimum of effort; brute force protection is built-in as standard.

IPv6 / IPv4 compatibility has been a fundamental design consideration from the beginning. The system has the ability to recognize IPv6 addresses and all network configuration scenarios and is able to transparently bridge traffic between networks of the two Internet standards.

FEATURES

Unlike many dedicated Web Application Firewall systems on the market, the Anti-DDoS WAF+ system includes a wide range of capabilities to allow for the mitigation of Distributed Denial of Service attacks.

Administrators have a wide range of options for blocking and logging traffic as it passes through the WAF rules system. The rules system offers the possibility to define both **positive** and **negative** security models.

Cyber attacks can be monitored in **real-time**, using an easy to understand, highly customizable **HTML-5 GUI**. In addition, Adobe PDF format reports can be generated to meet organizational reporting requirements.

In the event of a newly discovered web application vulnerability being revealed, or an actual attack taking place, the Network Box Anti-DDoS WAF+ system allows for the real-time installation of emergency **virtual patches at the gateway**, in the form of specific WAF rules, to immediately detect and prevent any specific security issues.

Security Models

The Anti-DDoS WAF+ supports **five** security models. Individual servers, web sites within those servers, URL paths and applications can be **protected** with a combination of any of these security models:



DDoS/DoS Model

The DDoS/DoS model works in co-operation with the Proxy Base DDoS and Network DDoS models to track usage patterns and identify attack sources for suppression/mitigation and blacklisting. Examples of techniques used include:

- connection rate limiting
- request rate limiting
- negative response rate limiting
- repeat request limiting
- request duration limiting



Negative Security Model

Scans inbound requests and applies protection criteria (signatures, rules and heuristics) to detect:

- protocol anomalies
- unusual behavior
- exploits and other common attacks

Sources of attacks can be integrated with other security modules to react to such malicious traffic, or the traffic itself can simply be logged, dropped or sanitized.



Vulnerability Protection

The Anti-DDoS WAF+ uses powerful rules language to protect against the latest known vulnerabilities and exploit techniques. This is kept up-to-date, from a network of over **70** security partners including Microsoft's **MAPP** program. Protected systems can be **virtually patched** at the gateway without having to install the patches on the affected systems themselves; keeping protected systems secure.



Outbound Protection

The Anti-DDoS WAF+ can enforce policy on outbound traffic. This is commonly used for:

- data leakage prevention (DLP)
- detection of defacement
- 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.



Positive Security Model

The Positive Security Model requires the definition of a set of rules to define:

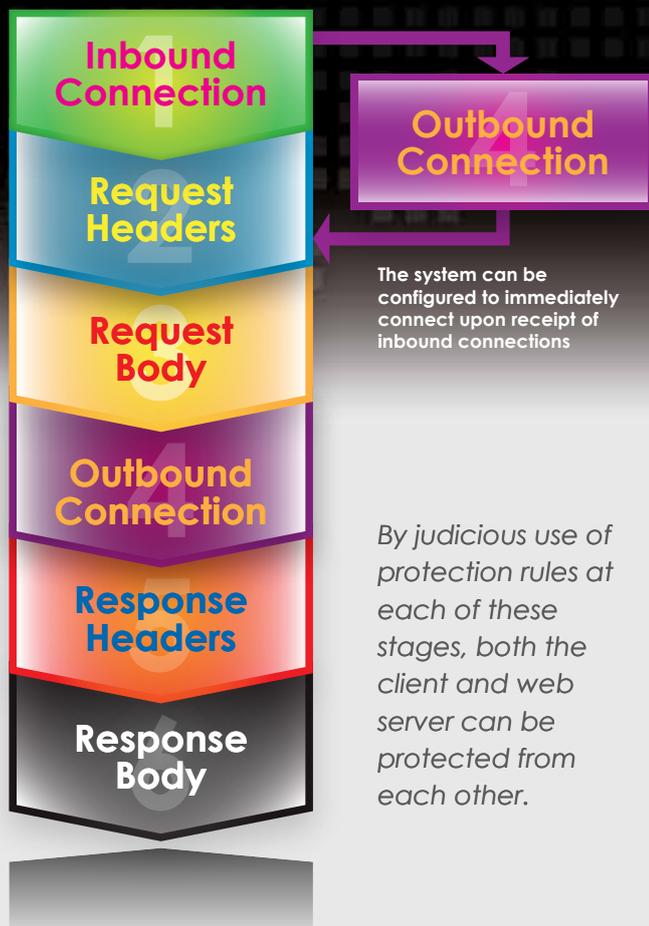
- what applications will be permitted
- what traffic will be permitted

All other non-conforming traffic is rejected.



Request and Response Analysis

The Anti-DDoS WAF+ conducts extensive **decoding** and **analysis** of the web server traffic. This analysis is conducted early on, and in **six** stages:



The rule database currently contains approximately **6,300** rules combined with a signature database to identify several million threat sources. All signatures and rules are updated in real-time by the Network Box PUSH update system.

1. Inbound Connection

The inbound connection details are known at this stage (such as source and target IP addresses). This can be correlated with the statistical history of that source and a decision is made whether to permit the source to send a request or to reject the connection.

2. Request Headers

The request from the source is received and decoded/analyzed. The contents of these headers can be analyzed and subjected to protection rules and a decision is made whether or not 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/analyzed. The contents of the request body can be analyzed and subjected to protection rules and a decision is made whether or not to permit the source to continue with connection to the server.

4. Outbound Connection

The Anti-DDoS WAF+ can be configured to make outgoing connections immediately after the inbound connection is made (stage 4 occurs immediately after stage 1 and before stage 2), in cases where performance and response time is critical; or to delay outbound connection until after reception of request headers and body. Giving administrators a greater amount of flexibility for traffic redirection and rule enforcement.

5. Response Headers

The protected web server will respond to the request headers and body with response headers. These headers are decoded/analyzed, and protection rules are applied so that a decision can be made whether or not to permit the server to transmit these headers on to the client.

6. Response Body

The protected web server will follow up the response headers with a response body. This body can be decoded/analyzed, and protection rules are applied so that a decision can be made whether or not to permit the server to transmit this body on to the client.

Protocol Validation and Policy Restriction

The Anti-DDoS WAF+ has extensive support for **protocol validation** and **policy restriction** of the HTTP protocol requests and responses:

The Network Box Access Control List (ACL) system is used so that restrictions can be placed at a very granular level (eg; user, protected server, URL, path, parameter, etc).

The proxy can integrate to the Scan Anti-malware module for further in-depth request filtering.

- Request Method Validation
- Request Protocol Version
- Request URL Encoding Validation
- Request Unicode Encoding Validation
- Request Directory Traversal Validation
- Response Protocol Version
- Request Protocol Policy
- Request Element Content Policy
- Request Element Length Policy
- Request Element Byte Range Policy
- Response Protocol Policy
- Request Method Length Policy
- Request Line Length Policy
- Request URI Length Policy
- Request Query String Length Policy
- Request Protocol Length Policy
- Request Number of Headers Policy
- Request Header Name Length Policy
- Request Header Value Length Policy
- Request Body Length Policy
- Request Number of Cookies Policy
- Request Cookie Name Length Policy
- Request Cookie Value Length Policy
- Request Number of Parameters Policy
- Request Parameter Name Length Policy
- Request Parameter Value Length Policy
- Request URI Protocol Part Length Policy
- Request URI Host Part Length Policy
- Request URI Path Part Length Policy
- Request URI Parameter Part Length Policy
- Request URI Bookmark Part Length Policy
- Request POST/PUT Number of Files Policy
- Request POST/PUT File Length Policy
- Request POST/PUT Total File Lengths Policy

Response Filtering

The system can be integrated with **Scan DLP** and **Anti-Malware** modules for further in-depth response filtering.

Policy rules can be defined to filter the responses from the protected server:

Response Header removal/change/addition

Response Result Filter

Response Body Filter

The Anti-DDoS 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 Anti-DDoS 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 sender.

DDoS Mitigation

The Anti-DDoS WAF+ uses **real-time automated fingerprinting** to identify and blacklist attacks. The system takes **milliseconds** to respond to brute force attacks that typically come from thousands of sources.

The Anti-DDoS WAF+ offers DoS/DDoS mitigation facilities. In particular:

- Total connections limiting
- Total connection rate limiting
- Per-source connections limiting
- Per-source connection rate limiting
- Per-source-per-method rate limiting
- SYN cookies for SYN flood protection
- Outbound connection postponement

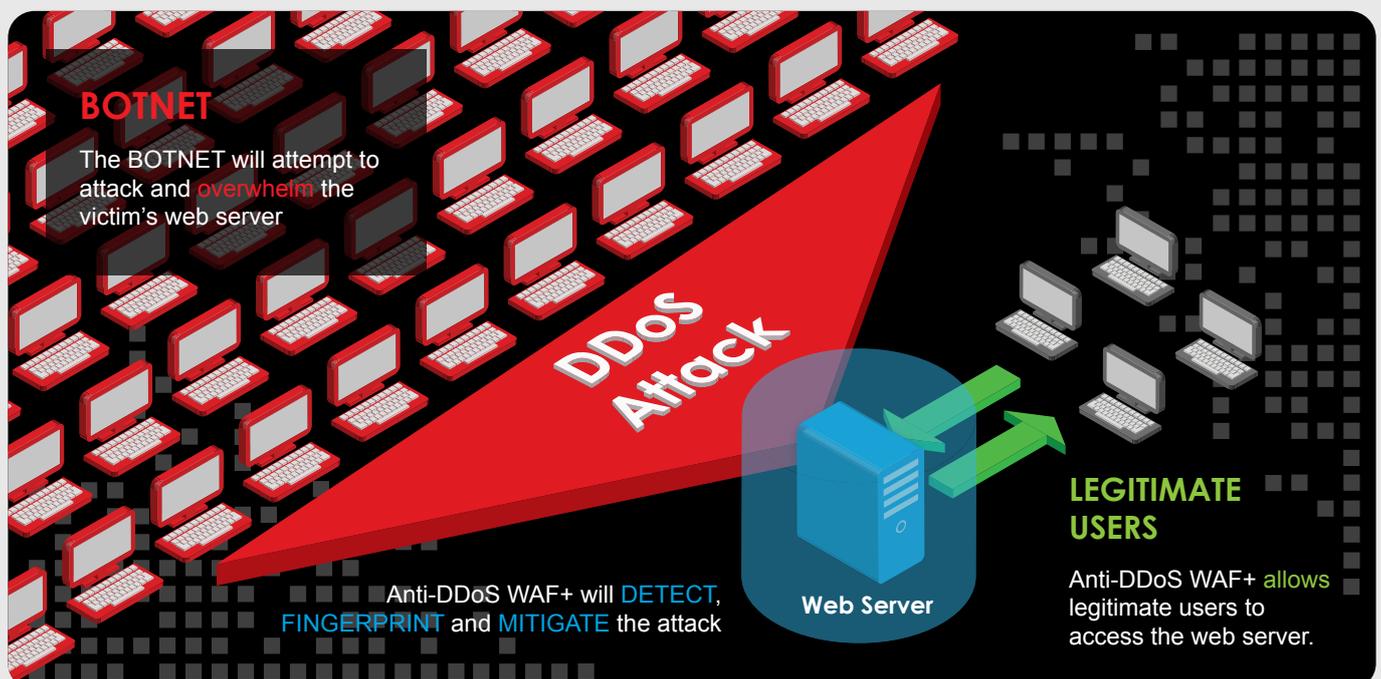
Features

Real-Time Automated fingerprinting

Slows down attacks by a factor of up to 1,000

Millisecond response to brute force attacks

The system keeps track of DDoS information on a per-source basis (which it periodically maintains and prunes), and imposes limits on reasonable behavior. Sources which exceed those limits are deemed to be DoS/DDoS attack sources and mitigated.



Transaction Analysis

Comprehensive web protocol analysis, extracts **hundreds** of web transaction properties for use in the **rules engine**.



Features

High performance rules engine capable of millions of rule-checks per second

Up to 15,000 fully analyzed transactions per second

Support for major Content Management Systems including: Joomla, Drupal, and Wordpress

Default rule sets contain protection for commonly used web application frameworks. New threats to the application frameworks can be quickly identified and mitigated by the Anti-DDoS WAF+ avoiding the need to perform a costly upgrade to the web application itself.

ATTACKER

Exploiting a new security vulnerability, the attacker sends malicious requests such as:

- SQL Injection
- XSS Injection
- Insufficient Input Validation

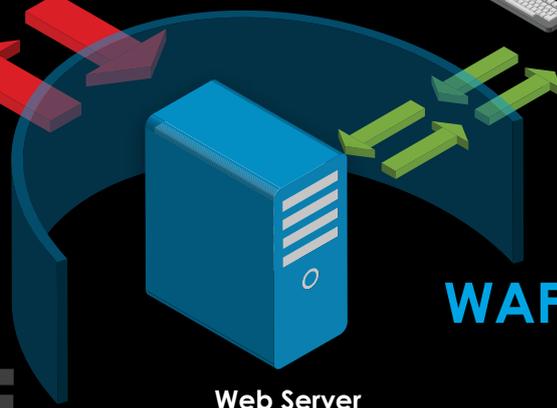


The WAF detects that it is a malicious request and **blocks** the request.



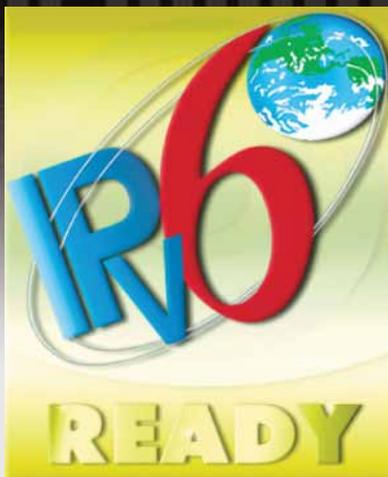
LEGITIMATE USERS

The WAF detects that the data is a normal request and **allows** it to pass.



IPv4 to IPv6 Bridging

The Anti-DDoS WAF+ supports **bi-directional translation** between IPv4 and IPv6; allowing IPv4 clients to connect to IPv6 servers, and vice-versa.



Features

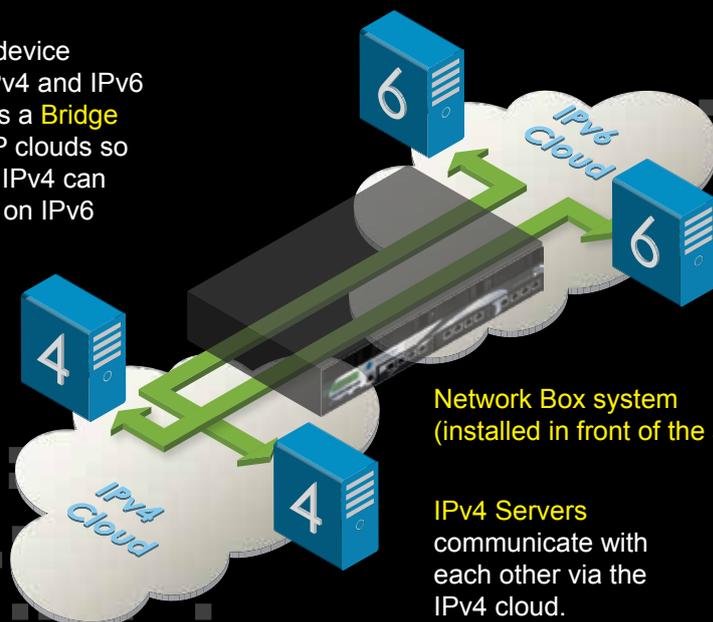
Certified to globally recognized IPv6 Ready Core Phase-2 Protocol standard

Automatic dual-stack interception mechanism combined with outgoing protocol translation

IPv6 Border Gateway Protocol offered as a service for customers

The system is fully dual-stack, with all middleware services developed from the ground up to be IPv6 capable. Network Box also offers an IPv6 Border Gateway Protocol solution that can be installed along-side the IPv4 to IPv6 bridging service for customers.

The Network Box device recognizes both IPv4 and IPv6 protocols. It acts as a **Bridge** between the two IP clouds so that computers on IPv4 can access computers on IPv6 and vice versa.



IPv6 Servers communicate with each other via the IPv6 cloud.

Network Box system (installed in front of the servers)

IPv4 Servers communicate with each other via the IPv4 cloud.

Intelligence Gathering

The Anti-DDoS WAF+ system makes use of Network Box's global security collection network, that gathers the latest information on vulnerabilities and threats from over 70 sources; such as international URL Blacklists and business partnerships including Microsoft Active Protections Program (MAPP) and Kaspersky Labs.

Data is also collected from over 250,000 in-the-cloud virtual sensors, which are exposed to real and current cyber threats. In addition, information is also sourced from existing Network Box customers' devices. Lists of source addresses of all types of malicious activity are processed in real-time at Network Box headquarters and updated lists are actively sent to customers using patented PUSH technology.

Features

70+ Global security sources including Microsoft Active Protections Program (MAPP)

Attack statistics from all customers processed at Headquarters in Real-Time

Information gathered from over 250,000 virtual honey pots



SSL Offload and Upgrade

The Anti-DDoS WAF+ can be configured as a terminator for SSL traffic, offloading cryptographic computation workload onto the Anti-DDoS WAF+ system therefore relieving web content servers of significant CPU stress.

In addition to the standard SSL Offload feature, Network Box middleware software uses an up-to-date and actively maintained SSL software infrastructure, effectively upgrading a customer's secure website to the latest, most secure SSL protocols.

Features

Reduces CPU workload

Up-to-date and actively maintained SSL protocols

Administrative control over SSL connection properties



HTML-5

Graphical User Interface

The Anti-DDoS WAF+ system can be **monitored** using almost any mobile device. This gives vital **real-time** information to IT Managers, allowing them to constantly monitor their network's status, even when they are away from their workstations.



Features

Real-Time
Attack Monitoring

Supports almost any
Mobile Device

Customizable
Dashboards



Probably the most impressive, clearest, and highly customizable Graphical User Interface on the market today

Anti-DDoS WAF+ Features (i)

Features	Comments
General Features	
<p>Concurrent Connections</p> <p>Traffic Throughput</p> <p>Transaction/sec</p> <p>Granular Role-Based Administration</p> <p>Integration with approved enterprise SIEM.</p>	<p>Supports 60,000+ concurrent connections.</p> <p>Throughput up to 800 Mbps for basic WAF rule sets.</p> <p>15,000 fully analyzed transactions per second.</p> <p>Policy rules may be applied to clients identified by a number of connection and transaction properties.</p> <p>Network Box proprietary logging system can output system and event messages in a number of formats.</p>
Deployment	
<p>Inline - Transparent Edge</p> <p>Inline - Reverse Proxy</p> <p>High Availability</p>	<p>Supports in-line transparent data interception. Original client addresses are preserved.</p> <p>Supports in-line connection termination as a reverse proxy. Original client address forwarded to target site in http headers.</p> <p>Using dynamic inter-device status notifications (VRRP) or with a load balancing/forwarding device installed in front.</p>
Protection	
<p>Protected Protocols</p> <p>Supported Application</p>	<p>HTTP, HTTPS (SSL), XML, Web services, SOAP and AJAX supported using baseline protection rule sets. Special protection rule sets available for known web application frameworks such as Drupal, Joomla, many more. For SSL support, it is recommended that the device perform SSL termination using the optional SSL Protocol Upgrade module.</p> <p>Anti-DDoS WAF+ is deployed as a standalone inline solution, so is agnostic to the web server backend. Some custom protection rule sets are available that provide protection not only for web application frameworks, but also for web server vulnerabilities, for example: Apache Range header vulnerability: CVE-2011-3192, Internet Information Server.</p>

Anti-DDoS WAF+ Features(ii)

Features	Comments
<p>OWASP Top 10 Protection PCI DSS Compliance</p> <p>Rule Writing, and Administrative Flexibility</p> <p>Multiple Rule Actions</p> <p>Secure Management</p> <p>Change Management / Auditing</p> <p>White Listed & Black Listed source addresses</p>	<p>Brute Force Login Attack, Buffer Overflow, Command Injection, Cookie Poisoning, Cross-site Request Forgery (CSRF), Cross-site Scripting, Denial Of Service, Directory Traversal, Parameter Manipulation, Phishing, Remote File Inclusion Attacks, Session Hijacking and SQL Injection protection is provided as part of the standard baseline protection rule set.</p> <p>Flexible rule language in the Network Box ACL system can block access based on many properties of both client and target, from the network layer up to protocol layer, as well as external properties such as time of day.</p> <p>allow/alert/debug/permit/deny/alertonly/log/nolog options available.</p> <p>Management performed by Network Box Security Operations Centre engineers.</p> <p>Full history of configuration options saved internally on device, and optionally mirrored back to Security Operations Centre, for purposes of audit.</p> <p>Anti-DDoS WAF+ maintains a system wide black list of addresses and blocks all traffic from these sources. It performs blocking at the network layer, causing very little stress on the device. In addition, built-in DDoS technology can automatically detect sources of denial of service and update system blacklists.</p>
<h2>Correlation and Application Support</h2>	
<p>Bi-directional Web Traffic Analysis</p> <p>Application Performance Metrics</p> <p>Application Source Code Leak Detection</p>	<p>Outgoing responses can have their own set of WAF rules applied to them.</p> <p>HTML-5 web based graphical user interface to query real time and historical event log data and create reports.</p> <p>Available through optional protection rule sets.</p>

Technical Specifications

Key Features

WEB APPLICATION SECURITY

- OWASP Top-Ten Protection
- Protection against common attacks
- Form field meta data validation
- Adaptive security
- Response control
 - + Block client
 - + Reset connection
 - + Redirect
 - + Log as suspicious
- Outbound data theft protection
 - + Credit card numbers
 - + Social Security numbers
 - + Custom pattern matching (regular expression)
- Granular policies for HTML/HTTP elements
- Protocol limit checks
- File upload control
- Blocking based on Client IP Reputation

DoS/DDoS MITIGATION

- Total connection count limiting
- Total connection rate limiting
- Per-source connections limiting
- Per-source connection rate limiting
- Connection rate statistical anomalies
- Data throughput/bandwidth consumption limiting
- SYN cookies for SYN flood protection
- Outbound connection postponement

LOGGING

- Remote log forwarding
- System log (TCP/UDP)

MONITORING AND REPORTING

- HTML-5 GUI
- Adobe PDF reporting
- Secure remote administration

XML FIREWALL

- XML DoS protection
- Schema / WSDL enforcement

APPLICATION DELIVERY AND ACCELERATION

- High availability
- Load balancing
- SSL offloading

SUPPORTED WEB PROTOCOLS

- HTTP/S 0.9/1.0/1.1
- XML
- IPv6 Ready

SUPPORTED WEB APPLICATIONS

- Apache
- IIS
- Joomla
- Drupal
- Mediawiki
- Wordpress

Key Metrics

	M-385i	M-395i	E-1000i	E-2000i	E-4000i	E-8000i
Malicious Web Traffic Blocks (per second)	450,000	450,000	600,000	1,000,000	1,000,000	1,000,000
WAF Throughput (requests per second)	2,900	4,390	4,510	8,600	9,300	12,400
WAF Throughput (Mb per second)	900	1,000	1,060	1,680	1,800	2,000

The trademarks, including but not limited to "Network Box" and the curly "N" device, are either trademarks or registered trademarks of Network Box Corporation Limited. Other trademarks and product names used in this publication are for identification purposes only, and may be the trademarks of their respective companies. Features and specifications are subject to change without notice. Benchmarking is performed with representative data, on a function by function basis. Weights and measurements are approximate only. Actual models may vary in appearance to the illustration and photographs provided. Copyright © Network Box Corporation Limited 2015.

