NETWORK BOX
www.network-box.com

Network Box 5

Unified Threat Management + Anti-DDoS WAF +

Triple ISO

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

Triple Tolly

100% Extended WildList Malware detection over **HTTP**, **POP3** and **SMTP** protocols

IPv6

IPv6 Ready Core Phase-2 certified

Firewall, Intrusion Detection and Prevention (IDP), Virtual Private Networking (VPN), Anti-Malware, Anti-Spam, Anti-Spyware, Web Proxy, Content Filtering, Data Loss Prevention (DLP), Company Policy Enforcement / Compliance, Real-Time updates with PUSH Technology, Secure 24 x 7 x 365 Monitoring, ISO 9001 / 20000 / 27001 Certified Management, IPv6 Ready Core Phase-2 Certified, In-the-Cloud Protection, Comprehensive Adobe PDF Format Reporting, Apple iPhone / iPad HD Management Platform, Anti-Distributed Denial of Service, Web Application Firewall, IPv4-IPv6 / IPv6-IPv4 Bridging, Multiple Internet Connections, High Availability / Load Balancing, Internet Acceleration, Secure VoIP (Voice over Internet Protocol) Gatekeeper, Secure Video Conferencing Gatekeeper, Quality of Service Control, Traffic Policing, Denial of Service Protection, Threshold Limiting, Hardware Fault Tolerance, clustering possible, Live Watch Real-Time Monitoring, Adobe PDF Report Generation, SSL (Secure Socket Layer) Virtual Private Networking, Anti-SPAM Pre-Scanning, bandwidth protection, Enhanced Image SPAM protection, including Optical Character Recognition technology, Mail Portal System, End User email management including SPAM release and white / black listing, Enhanced GUI (Graphical User Interface), Secure Socket Layer (SSL) Proxy, Application Identification, Entity Management, HTML-5 Dashboard

Network Box 5

Next Generation Managed Security

BACKGROUND

Network Box 5 is Next Generation Managed Security. It takes our core foundational UTM+ (Unified Threat Management) appliance and services, along with ten years of Intellectual Property and experience, into a new enhanced platform, which expands beyond traditional UTM+ capabilities.

In addition to Firewall, IDP (Intrusion Detection and Prevention), VPN (Virtual Private Networking), Anti-Malware, Anti-SPAM, Data Leakage Prevention, and Content Filtering, we have added Entity Management, SSL (Secure Socket Layer) Proxy, Application Identification, Anti-DDoS (Anti-Distributed Denial of Service), WAF+ (Web Application Firewall), and IPv4-IPv6 Bridging technologies.

HIGHLIGHTS

The state-of-the-art Network Box 5 software platform, consists of more than one-point-one million lines of code; representing more than one hundred and thirty eight thousand hours of highly dedicated research and development.

A truly enormous amount of hard work has gone into optimizing this code, the algorithms, and technologies used. All this dedication and effort, has resulted in the new Network Box 5 software platform, being up to 8 times faster, than the previous Network Box 3 software platform.

The Network Box 5 code base, from the underlying platform, to the individual modules and security engines, support multi-core technology throughout.

The new software platform is dual 32bit and 64bit, supporting both architectures for backwards compatibility, but all Network Box 5 hardware is 64bit.

SYSTEM OVERVIEW

Every aspect of the new system's design; security, speed, granularity, transparency, functionality, scalability, monitoring, control, customization, and reporting, have all been enormously improved in almost every way possible.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.

Intelligence Gathering

Network Box 5 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

Entity Management

Network Box 5 offers a revolutionary Entity Management system, which completely redefines how users and machines are monitored and protected.

Entities are Users and Devices that are parts of your network. Network Box 5 tracks these entities, their attributes (such as MAC addresses, IP addresses, email addresses, etc.), and the network resources which they utilize.

Features

All the users' devices can be grouped into individual entities

Presents a single holistic view of the activity, of each of the entities in the network

Allows IT Managers to monitor, manage, and protect, their users and networks

Rather than presenting a set of disparate screens, showing firewall blocks by IP address, URL access by authenticated user, and email by email address, the Network Box 5 platform presents a single holistic view of the activity, of each of the entities in your network. For example; calling up user "Joe," will show all his firewall blocks, web accesses, network usage, email, etc.; across his desktop, laptop, phone, tablet, and remote VPN.

The entity model itself is built and maintained by automated systems, and is an extremely efficient, and effective, technology, for helping IT Managers to monitor, manage, and protect, their users and networks.

Secure Socket Layer (SSL) Proxy

SSL is the technology used to provide security to web browser and web application communications. However, as with any modern technology, SSL can suffer from security issues of its own, because of problems with its design, or flaws in its implementation.

Regardless, the very fact that SSL data steams are encrypted, means that without SSL-Proxy technology, it is all but impossible to scan such data streams for viruses, worms, spyware, and other undesirable content.

Features

Provides security to web browser and web application communications

Allows certificate validation policy to be performed and enforced at the gateway

SSL traffic is identified, decrypted and then subjected to security functions

The SSL-Proxy has therefore been developed with two goals in mind:

1 To enhance security, by allowing connections to secure servers on the Internet to be made with the highest common denominator security, rather than the lowest. For example, even if the certificate installed on an internal computer is known to be compromised, when a connection is made from that computer out to the Internet, a secure certificate is used in its place for the external connection.

2 To allow the scanning of encrypted protocols, so that anti-malware protection, content filtering, and organizational policy enforcement, can take place, despite the data stream being encrypted.

Application Identification (i)

While traditional firewalls block protocols, and ports, Application Identification looks at the traffic up to and including layer 7 to identify the application responsible for that traffic.

Once identified, policy control can be applied to that traffic. The traffic can also be 'promote' - for example HTTP traffic detected on ports other than tcp/80 can be promoted to be handled by the web client scanning modules for anti-malware and policy control. Integrated to the SSL proxy, even traffic inside encrypted SSL sessions can be identified and controlled.

Features

Encrypted SSL sessions can be identified and controlled

Layer 7 traffic analysis

Policy control can be applied to traffic

The Network Box 5 application identification engine, comes in both Lite and Full versions. The Lite version is included as standard with every UTM+ system; while the optional Full version is available as an upgrade. The new Application Identification system allows connections to be appropriately labelled for reporting and policy control.

In this way, one can detect traffic such as Skype, QQ, FTP, HTTP, Facebook, and more than 1,390 other recognised applications; all based on the traffic itself and not just the network port / address it is on. For enhanced control, the new system also allows data streams to be analyzed both in terms of 'productivity' and 'potential risk.'

Application Identification (ii)

The productivity index ranks application usage from 1 (Recreation) to 5 (Business).

1. Primary use is recreation.
2. Main use is recreation.
3. Equally used for business and recreation.
4. Main use is business.
5. Primarily used for business.

The risk index ranks application usage from 1 (No Risk) to 5 (Very High Risk).

1. No risk.
2. Minimal risk.
3. Some risk. Possible misuse.
4. High Risk. Possible Data Leaks / Malware.
5. Very High Risk. Evades Detection / Bypasses Firewalls

The system supports over 1,300 applications such as Skype, Dropbox, BitTorrent, Gnutella, Facebook, YouTube, Limewire, ICQ Messenger, etc; split over 15 categories and 20 tags.

15 Categories

Collaboration
Database
File Transfer
Games
Mail
Messaging
Network Monitoring
Networking
Proxy
Remote Access
Social Networking
Streaming Media
Unknown
VPN and Tunneling
Web Services

20 Tags

Advertisements
Encryption
Facebook App
Instant Messaging
Internet Search
Logs Communication
Media Share
Mobile
Peer 2 Peer
Phones Home
Proxy
Remote Control
Screen Sharing
Uses Stealth
Video Conferencing
Voice Conferencing
Excessive Bandwidth
Potential Data Leak
Prone To Misuse
Used By Malware

IPv4 to IPv6 Bridging

Network Box 5 supports bi-directional translation between IPv4 and IPv6; allowing IPv4 clients to connect to IPv6 servers, and vice-versa.

Features

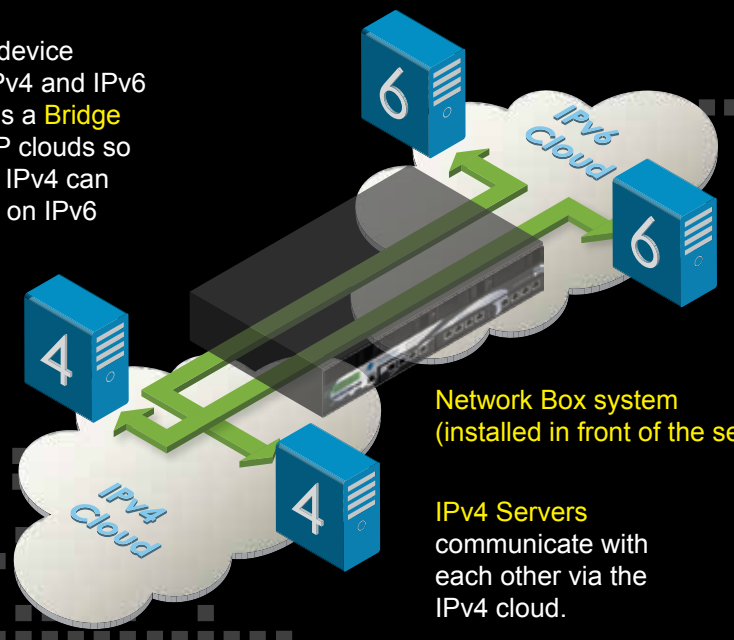
Certified to globally recognized IPv6 Ready Core Phase-2 Protocol standard

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.

HTML-5 Dashboard

Networks 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

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

Anti-DDoS WAF+

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.

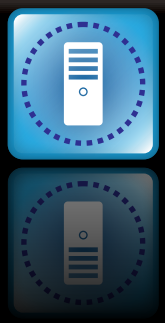
Administrators have a wide range of options for blocking and logging traffic as it passes through the WAF rules system. The rules system offers the possibility to define both positive and negative security models.

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:



Vulnerability Protection

The Anti-DDoS WAF+ uses a 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.

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

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.

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.

Positive Security Model

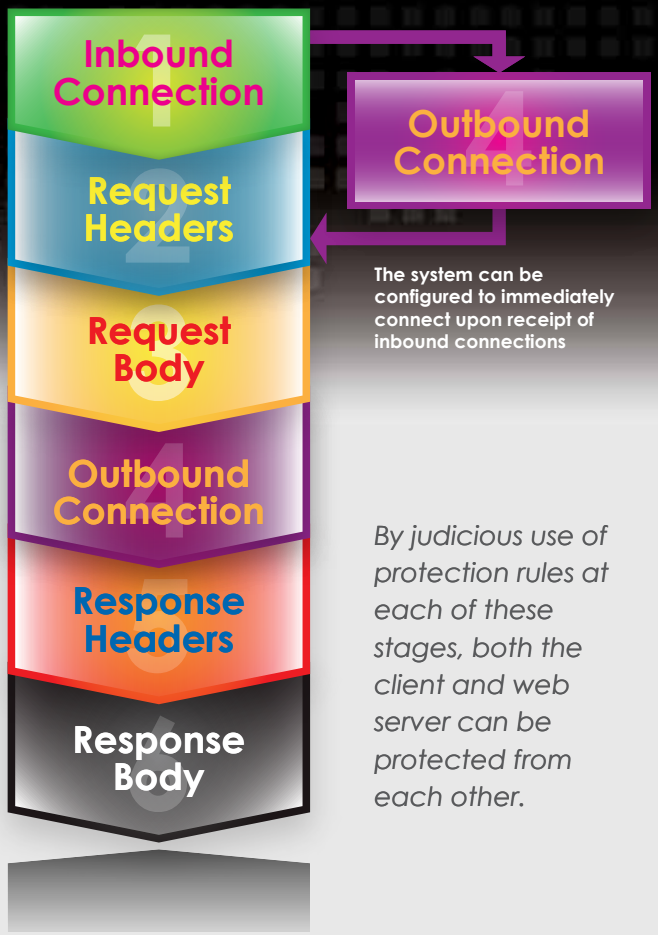
The Positive Security Model requires the definition of a set of rules to define:

- 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:



By judicious use of protection rules at each of these stages, both the client and web server can be protected from each other.

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

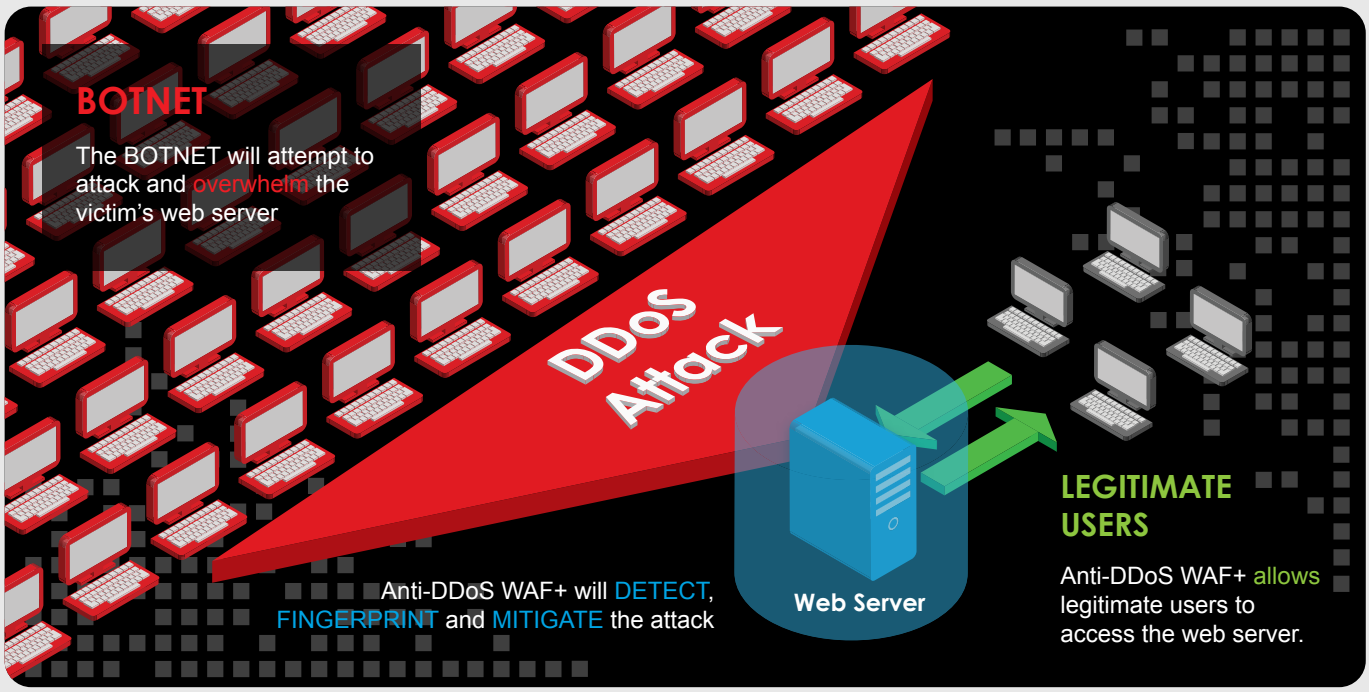
Features

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.

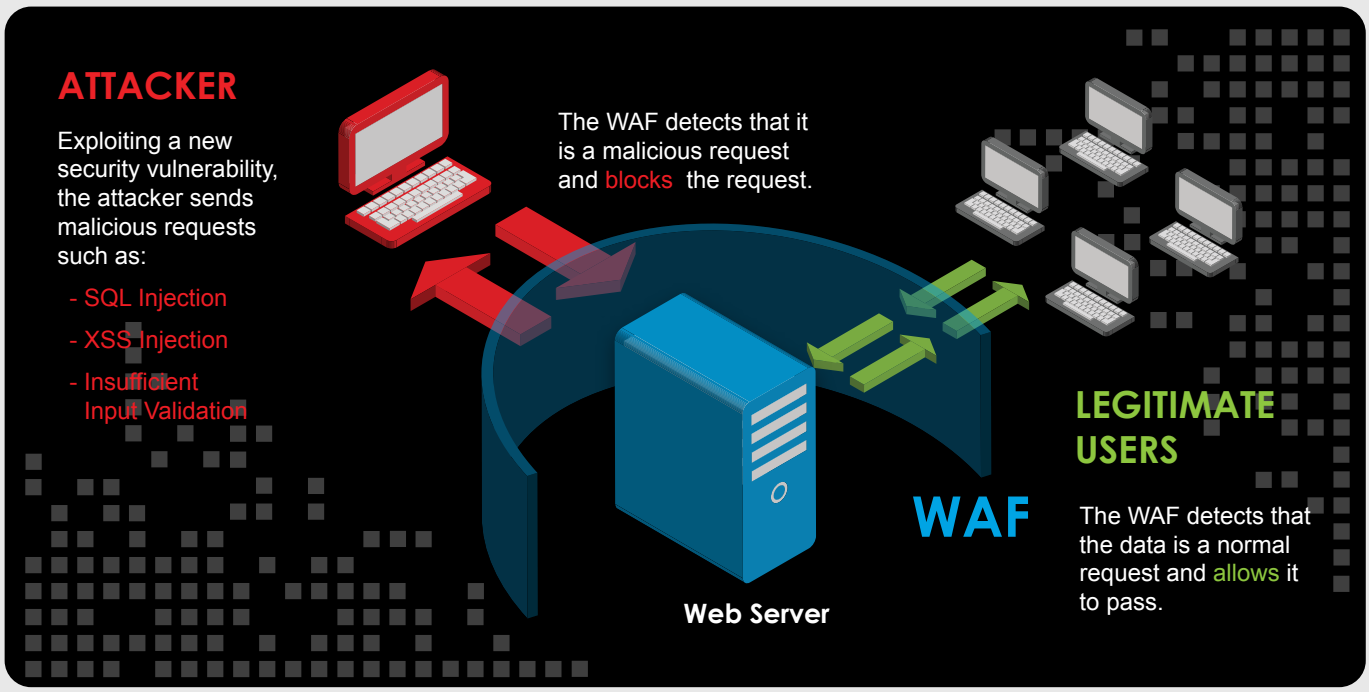
Features

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.



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

Anti-DDoS WAF+ Features (i)

Features	Comments
General Features	
Concurrent Connections	Supports 60,000+ concurrent connections.
Traffic Throughput	Throughput up to 800 Mbps for basic WAF rule sets.
Transaction/sec	15,000 fully analyzed transactions per second.
Granular Role-Based Administration	Policy rules may be applied to clients identified by a number of connection and transaction properties.
Integration with approved enterprise SEIM.	Network Box proprietary logging system can output system and event messages in a number of formats.
Deployment	
Inline - Transparent Edge	Supports in-line transparent data interception. Original client addresses are preserved.
Inline - Reverse Proxy	Supports in-line connection termination as a reverse proxy. Original client address forwarded to target site in http headers.
High Availability	Using dynamic inter-device status notifications (VRRP) or with a load balancing/forwarding device installed in front.
Protection	
Protected Protocols	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.
Supported Application	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.

Anti-DDoS WAF+ Features(ii)

Features	Comments
OWASP Top 10 Protection PCI DSS Compliance	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.
Rule Writing, and Administrative Flexibility	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.
Multiple Rule Actions	allow/alert/debug/permit/deny/alertonly/log/nolog options available.
Secure Management	Management performed by Network Box Security Operations Centre engineers.
Change Management / Auditing	Full history of configuration options saved internally on device, and optionally mirrored back to Security Operations Centre, for purposes of audit.
White Listed & Black Listed source addresses	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.
Correlation and Application Support	
Bi-directional Web Traffic Analysis	Outgoing responses can have their own set of WAF rules applied to them.
Application Performance Metrics	HTML-5 web based graphical user interface to query real time and historical event log data and create reports.
Application Source Code Leak Detection	Available through optional protection rule sets.

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