Version 2.1

NETWORK BOX

Next Generation Managed Security

Key Technologies Overview

- Firewall
- Virtual Private Network (VPN)
- Intrusion Detection and Prevention (IDP)
  - + Front-Line IPS
  - + Passive IDS
  - + Active IDS
  - + Inline IPS
- Anti-Malware (M-Scan)
- Zero-Day Anti-Malware (Z-Scan)
- Anti-Spam
- Data Leakage Prevention (DLP)
- Web Content Filtering (S-Scan)
  - + S-Scan *Core*
  - + S-Scan *Extended*
- Application Identification and Control
- SSL Proxying
- Anti-DDoS
- Web Application Firewalling (WAF-Scan)
  - + Standard Applications
  - + Custom Applications
- Entity Management
- Network Monitoring and Reporting
- Cloud Mail Backup
- Cloud DNS Backup
- IPv4 to IPv6 Bridging
- PUSH Technology

www.network-box.com

PUSH Update Technology

Gateway Protection Engines

Anti-Malware Engine

Zero-Day Anti-Malware Engine

Web Content Filtering Engine

Web Application Firewall Engine

Network Box
Key Technologies Overview (i)

HYBRID FIREWALL

The Network Box Hybrid Firewall protects servers and workstations from a host of network-level attacks, including protocol anomalies, connection flooding, SYN flooding, denial-of-service, as well as packet fragmentation evasion techniques. Black hole, finger-print obfuscation and decoy technologies further shield protected networks from malicious probes.

Features:

- 18 Engines.
- Hybrid firewall design for the best of all worlds.
- Application-Level Packet Filtering, both secure and efficient.
- Proxy-ARP Transparency isolates internal systems from attack.
- Policy-based routing for efficient use of dual network connections.
- Multiple redundant / balanced Internet links for fail-safe operation.
- Traffic shaping and QOS control for priority services.
- Multiple Network Boxes configured as a single fault tolerant virtual router.
- Address translation and port / address forwarding hides the internal network.

VIRTUAL PRIVATE NETWORK (VPN)

The Network Box VPN secures out-of-office connections with specific access control policies for groups and individual users. Authenticated user sessions from outside the office, ensure data remains confidential during internet transit. Most major VPN servers (such as Microsoft, Cisco, Checkpoint and Symantec) can be connected to Network Box.

Network Box provides support for three core VPN technologies:

- PPTP
- IPSEC
- SSL VPN

All three VPN options are fully integrated to the Network Box firewall and router and provide for excellent policy control (allowing different firewall policies to be applied to encrypted vs non-encrypted traffic and to specific end-points). The VPNs are also inter-routable (so traffic can be translated between VPN technologies by a single Network Box appliance.

INTRUSION DETECTION AND PREVENTION (IDP)

The Network Box IDP scans network traffic at the application level, and seamlessly blocks malicious behavior with zero latency. Protection against newly emerging threats is provided by a database of vulnerability-class based behavior anomalies and heuristic (expert system) anomaly-based behavioral analysis. This is updated in real-time, using Network Box's patented PUSH Technology.

Features:

- 16,000+ Signatures.
- Zero latency, hybrid, multi-level, tightly integrated with Firewall.
- Active (blocks network traffic) and / or Passive (logs intrusion attempts).
- Real time (on demand), and periodic (summary) by SMTP e-mail.
- Blocks uncharacterized attacks before they have a signature.
- Types of intrusion detected: ICMP / IP, DoS, ports-cans, protocol level, application level.

There are four IDP modes offered by Network Box:

Front-Line IPS

Extremely light-weight, high-speed service, offering zero-latency protection, inline with the data-stream, against network worms, exploits and other such attacks. Operating in conjunc-tion with the firewall, at the individual packet level (after fragment reassembly), the front-line IPS adds packet content inspection, rate limiting and traffic analysis to the base firewall capabilities.

Passive IDS

Alerting and logging of traffic, side-by-side with the data stream – useful for policy enforcement and more aggressive rules.

Active IDS

Alerting and logging of traffic, side-by-side with the data stream, but with the ability to actively teardown connections once malicious traffic has been identified.

Inline IPS

Alerting and logging of traffic, inline with the data stream; tightly coupled to the firewall, this is able to drop traffic before the remote system even sees it.

Network Box
Key Technologies Overview (ii)

ANTI-MALWARE (M-Scan)

The Network Box anti-malware solution provides 16 anti-malware engines, supporting over 700 encoding and packing formats, combining several different anti-malware techniques and is backed by a database of over 11 million signatures. It provides true defense in a single managed gateway appliance.

Features:

- 16 Anti-malware Engines.
- 11 Million+ Signatures.
- Triple 100% Tolly rating for detection of malware over HTTP, SMTP and POP3 protocols.
- email malware protection.
- Updated in real-time using PUSH technology.
- Open-relay protection prevents spread and significantly limits damage.
- Mobile malware protection.

ZERO-DAY ANTI-MALWARE (Z-Scan)

Z-Scan is an in-the-cloud defence shield that provides zero-day anti-malware protection against the latest zero-day threats. Z-Scan operates by continually analysing all the threat information obtained in real time from more than 250,000 traps in the cloud, poised 24/7 for attacks to occur; and releasing its own signatures to protect against emerging malware within seconds. Z-Scan provides the fastest protection against emerging new threats.

Features:

- Industry best response times of just 3 seconds.
- Performs 4,200 times faster than typical gateway anti-malware systems.
- 250,000+ virtual honey pots already deployed.
- Multi-Award Winning Technology:
  - + Info Security Global Excellence Awards *(published out of Silicon Valley)*
  - + ITPro Corporate Choice Awards
  - + Asia Pacific ICT Alliance Awards
  - + PC3 Corporate Choice Awards
  - + Hong Kong Awards for Industries: *Technological Achievement Grand Award*
- Real-time malware gathering.
- In-the-cloud Update Technology.

MULTI-LAYERED ANTI-SPAM

The Network Box anti-spam system is the most comprehensive and effective gateway anti-spam solution in the market today. It provides 25 anti-spam engines, combining several different techniques and is backed by a database of over 30 million signatures. The Network Box anti-spam email gateway achieves an industry-record detection rate of at least 98% with almost zero false-positives values.

Features:

- 25 Anti-Spam Engines.
- 30 million+ Signatures.
- 99.49% Detection Accuracy.
- 0.01% False-Positive Rate.
- Co-operative Spam Checksums.
- Signatures and Spam Scoring.
- White lists and Black lists.
- Heuristics.
- Real-Time IP Blacklists.
- Real-Time URL Blacklists.
- URL to IP Mapping and Blacklists.
- URL Categorization.
- Domain Age.
- Bayesian Filtering.
- Challenge / Response Systems.

DATA LEAKAGE PREVENTION (DLP)

The Network Box DLP engine uses a complex 'dlp_rules' and 'dlp_policy' engine to scan and block outbound SMTP mail that may contain sensitive materials. This can include client info, account details, designs, commercial secrets, medical records as well document files, credit card numbers or social security numbers. The rules and policies can be customized thus ensuring effective prevention.

Features:

- Customizable rules and policies.
- Complex Pattern Matching.
- Content Analysis.
- Heuristics.
- Boolean and Arithmetic logic.
- Optical Image Recognition.

Network Box
Key Technologies Overview (iii)

WEB CONTENT FILTERING(S-Scan)

S-Scan is a high speed web content filtering system, designed to help organizations block undesirable web content from reaching their users. It uses high performance signature based technology, rather than a simple URL database, to identify web content more efficiently and effectively. Thus certain categories of new undesirable websites, can be identified in real-time, without the need to update a URL database. As a result, S-Scan offers excellent performance, in terms of speed, coverage, and accuracy.

Features:

- 16 Content Filtering Engines.
- 33 Million+ Signatures.
- Uses high performance signatures to identify web content.
- Real-time identification and classification of websites.
- 98.7% detection rate of the top 100,000 global websites.
- Customizable access privileges for different individuals or user groups.
- Policy violation reporting which is logged and audited by triple ISO certified security analysts.

There are two S-Scan versions offered by Network Box:

S-Scan *Core*

Covers the basic 14 categories of web content:
Adult / Sexually Explicit, Criminal Activity, Gambling, Hacking, Illegal Drugs, Intolerance & Hate, Phishing & Fraud, Spam URLs, Spyware, Suspicious URL, Tasteless & Offensive, Violence, Virus / Malware Infected, Weapons

S-Scan *Extended*

57 categories for more granular control:
Adult/Sexually Explicit, Advertisements & Popups, Alcohol & Tobacco, Arts, Blogs & Forums, Business, Chat, Computing & Internet, Criminal Activity, Downloads, Education, Entertainment, Fashion & Beauty, Finance & Investment, Food & Dining, Gambling, Games, Government, Hacking, Health & Medicine, Hobbies & Recreation, Hosting Sites, Illegal Drugs, Infrastructure, Intimate Apparel & Swimwear, Intolerance & Hate, Jobs Search & Career Development, Kids Sites, Motor Vehicles, News, Peer-to-Peer, Personal & Dating, Philanthropic & Professional Orgs., Phishing & Fraud, Photo Searches, Politics, Proxies & Translators, Real Estate, Reference, Religion, Ringtones/Mobile Phone Downloads, Search Engines, Sex Education, Shopping, Society & Culture, Spam URLs, Sports, Spyware, Streaming Media, Suspicious URL, Tasteless & Offensive, Travel,Violence, Virus/Malware Infected, Weapons, Web-based email, Uncategorized.

APPLICATION IDENTIFICATION AND CONTROL

The Network Box Application Identification and Control engine analyzes web traffic up to and including layer 7, to identify the application responsible for that traffic. Applications such as Skype, Dropbox, BitTorrent, Gnutella, Facebook, YouTube, Limewire, ICQ Messenger, and more than 1,300 others are supported. Identification is based on the traffic itself and not just the network port / address it is on. Once identified, policy control can be applied to that. For enhanced control, the system also allows traffic to be analyzed both in terms of 'productivity' and 'potential risk.'

Features:

- Supports over 1,300 applications.
- 15 categories and 20 tags for identification.
- Customisable policy rules for enhanced control of internet access.
- Allows granular control of applications.
- Encrypted SSL traffic can also be identified and controlled.

SSL PROXYING

Network Box SSL Proxy secures communication between two internet endpoints by decrypting secure connections on the way in, performing security analysis, then re-encrypting data on the way out. Incoming and outgoing SSL connections over the internet, are upgraded to use as secure settings as possible, following the approach of highest common denominator security, rather than the lowest. The engine also moves the choice of bypassing failed SSL server certificate validation away from the end-user, to the IT Manager.

Features:

- Identification, decryption, encryption, certificate validation and protection of SSL network traffic.
- Uses lowest denominator of security internally, but highest common denominator externally.
- Denies end-users from bypassing failed SSL certificates.
- Allows encrypted SSL traffic to be scanned for malicious and undesirable content.

Network Box
Key Technologies Overview (iv)

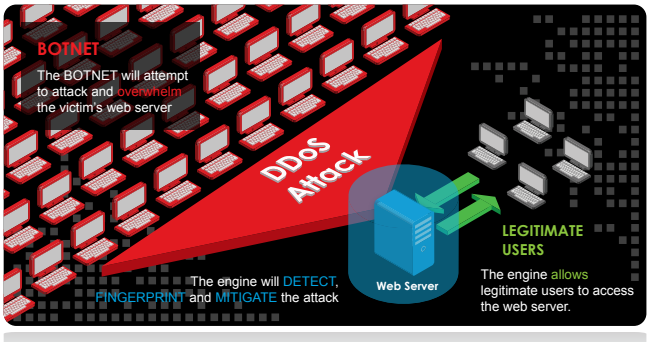
ANTI-DISTRIBUTED DENIAL OF SERVICE (DDoS)

The Network Box Anti-DDoS engine was created to provide Distributed Denial of Service (DDoS) Attack mitigation, so that 'bad traffic' is kept at bay, while 'good traffic' is allowed through to secured web facing servers, ensuring business continuity during ongoing attacks. It uses real-time automated finger-printing to identify and blacklist attacks. The system takes milliseconds to respond to brute force attacks that typically come from thousands of sources.

Features:

- 250,000+ malicious HTTP/HTTPS traffic blocks/sec.
- 95,000+ HTTP traffic classifications/sec.
- 7,000+ accepted HTTP transactions/sec.
- 6,500+ accepted HTTPS (SSL) transactions/sec.
- Real-Time Automated fingerprinting.
- Slows down attacks by a factor of up to 1,000.
- Millisecond response to brute force attacks.
- 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 .
- 70+ global security sources including Microsoft Active Protections Program and Kaspersky Labs.
- Attack statistics from all customers processed at Headquarters in real-time.
- Information gathered from over 250,000 virtual honey pots.

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.



WEB APPLICATION FIREWALL (WAF-Scan)

WAF-Scan protects web servers against web application based attacks including SQL and XSS injections. It allows IT 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. The engine also allows for the real-time installation of emergency virtual patches at the gateway, to immediately detect and prevent any specific security issues.

Features:

- High performance rules engine capable of millions of rule-checks per second.
- Database of 6,000+ rules combined with a signature database to identify several million threats.
- Rules updated in real-time using PUSH technology.
- Up to 15,000 fully analyzed transactions per second.
- 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

WAF-Scan can offer protection for two application models:

Standard Applications
Apache, IIS, Joomla, Drupal, Mediawiki, Wordpress

Custom Applications
Tailor made software that has been specially developed for a specific organization or specific user.

Network Box
Key Technologies Overview (v)

ENTITY MANAGEMENT

The Entity Management system allows IT Managers to group all users' devices (such as iPad, iPhone, Laptop, Desktop, VOIP Phone, etc) into a single entity and provide effective monitoring, management and protection. The system tracks their attributes, the network resources which they utilize and presents a single holistic view of the activity of each of the entities in your network.

Features:

- All 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.

NETWORK MONITORING AND REPORTING

The HTML-5 based Network Box Dashboard is the most intuitive and clearest User Interface available on the market today. The highly customizable dashboard gives the IT Manager real-time statistical data of their network, offering visual feedback of both cyber attacks and system usage.

Features:

- HTML-5 Customizable Dashboard.
- Customized Reports: Adobe PDF, CSV and other formats.
- Real-time portable monitoring.

CLOUD MAIL BACKUP

The Network Box Cloud Mail Backup system allows email deliveries to be backed up in the cloud, so if there is a problem with your ISP, your internal network, or your email server, incoming mail will be stored in the cloud, and delivered when the problem is resolved.

CLOUD DNS BACKUP

The Network Box 5 Cloud DNS Backup allows customers to use Network Box's extensive network of cloud DNS servers to provide backup DNS in the cloud. By using this, service reliability can be improved and DNS queries can be responded to, even if the Internet link to the master DNS server in the LAN/ DMZ is down.

IPv4 / IPv6 BRIDGING

The Network Box IPv4/IPv6 Bridging engine supports bi-directional translation between IPv4 and IPv6, allowing IPv4 clients to connect to IPv6 servers, and vice-versa. As IPv4 addresses will soon become unavailable, organizations everywhere will soon be faced with the very real need to migrate over to IPv6.

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 customer.

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.

PUSH TECHNOLOGY

Network Box's key technologies are all supported by patented PUSH Technology. The engine proactively pushes out and installs updates in an average time of less than 45 seconds. Standard security systems usually pull updates from a server once a day, or at best once an hour. In contrast, Network Box pushes out updates as soon as they become available.