



NEXT  
GENERATION  
MANAGED SECURITY

# Network Box 5.3

## THE NEXT LEVEL IN SECURITY

# Next Generation Firewalls

Network Box has taken our **Hybrid Firewall** which combined:

- ▶ Packet Filtering
- ▶ Stateful Inspection
- ▶ and Proxying

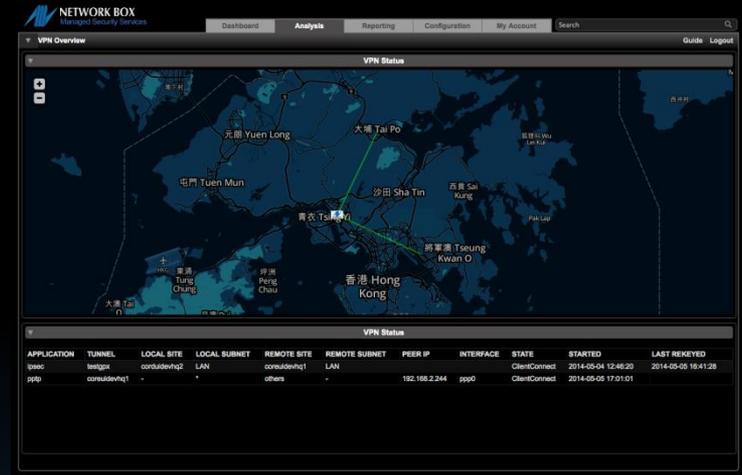
**and added Anti-DDoS as standard, with automatic bridging between IPv4 and IPv6 protocols**



# Visual VPN

All VPN types (IPSEC, SSL, PPTP, etc) have been unified into a single unified framework, and centralized status, reporting and control.

- ▶ Configurability of VPN types
- ▶ Reporting on VPN availability
- ▶ Capability to start/stop/restart VPN tunnels
- ▶ New Global Monitoring Sensor for VPN links



| IPsec |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| IPsec |

# Ruggedized VPN

The Network Box VPN system has been Ruggedized to relieve connectivity issues

- ▶ Bridges non-standard compliant connections
- ▶ Automates the approach for the most common issues
- ▶ Better handling of ISP connectivity issues
- ▶ Logging at three levels:
  - *Connection start/stop events*
  - *Session*
  - *Correlation*



# Enhanced Authentication and Encryption

Elliptical Curve Key Exchange, X.509 Certificate Authentication, and IKE2 Support, have all been added to Network Box 5.3, so that **KV-S@feNet Certification** could be achieved, allowing for official integration with Germany's medical network



# IDP – WAF Augmentation

The Network Box IDP (Intrusion and Detection and Prevention) system can now optionally include WAF (Web Application Firewall)

## **Web Application Firewall**

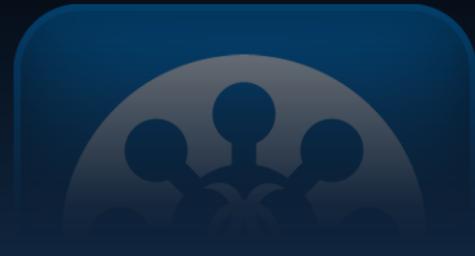
*For protecting web servers with vulnerabilities, usually in the DMZ, from malicious attackers on the Internet*



# Infected LAN

Identifies infected workstations and server in the LAN/DMZ, and isolates them from the network

- ▶ Detection of outbound access to known public BotNet command and control servers
- ▶ Detection of outbound access to known malware update sites
- ▶ Highly-granular detection for highly-prolific malware
- ▶ Optional support for dynamically blacklisting detected infected workstations / servers



# Kiosk Mode

Gives an overview of users activity irrespective of the device they are using, application and IP address

- ▶ Supports user authentication transparently  
*users access the network via a log in screen*
- ▶ Supports iOS, Android and other mobile devices
- ▶ Able to track entity attributes and activities
- ▶ Fully integrated with holistic entities



# SSL support for encrypted traffic

Network Box also blocks malware and other undesirable content arriving via encrypted channels

- ▶ SSL support through all our core protocols
- ▶ STARTTLS support for switching to secure mode
- ▶ SSL offload

**All this includes full scanning and policy enforcement**



# Event Correlation

The system correlates intrusion activity across all the network-frontline, network-ips, network-ids and network-firewall systems

- ▶ Maintains statistical data for each source IP
- ▶ Highly configurable thresholds
- ▶ Dynamically blacklisting the source of the attack
- ▶ Alerts admin (via email) to the source and details of the attack

# Z-Scan+

Enhanced protection with the augmentation of Z-Scan, with additional third-party threat intelligence

- ▶ Extends the number and breadth of signatures available in the cloud
- ▶ Supplements the on the box anti-malware signature set
- ▶ Allows Network Box to be one step ahead of the attackers



# Cloud email backup

Resolves loss of email issues by storing incoming emails in the cloud, and delivering them when the problem has been resolved

- ▶ Backup queuing if the primary MX servers are overloaded and temporarily not accepting new connections/emails
- ▶ 4 geographical locations:  
Asia, America, Europe and the Pacific
- ▶ Once delivered, the emails will be removed and only logs will be retained



# Cloud DNS backup

Allows customers to use Network Box's extensive network of cloud DNS servers to provide backup DNS in the cloud

- ▶ DNS queries are responded to, even if the Internet link to the master DNS server in the LAN/ DMZ is down
- ▶ Full control over which of domains will use the service
- ▶ Full control over which cloud backup servers will be used for which domain



# Enhanced multi-protocol handling

Network Box 5.3 includes an enhanced Protocol Enforcement system, for better handling of non-native use of ports, by applications

- ▶ Supports Next Generation applications such as WhatsApp and Line
- ▶ Allows or denies access for these applications
- ▶ Integrated with the Application Identification and Control system



# HTML-5 Dashboard Enhancements

The Network Box 5.3 Dashboard has been significantly improved:

- ▶ Icons refreshed (clearer, self-explanatory)
- ▶ Improved workflow (spam, holistic, etc)
- ▶ KPIs and Reporting
- ▶ User-focused dashboard layout
- ▶ Single global menu
- ▶ Enhanced search function



# KPI reporting

The monitoring and reporting system, have been enhanced to leverage the concept of KPIs (Key performance Indicators), and is able to show what has been happening both in real-time, as well as over any given period of time

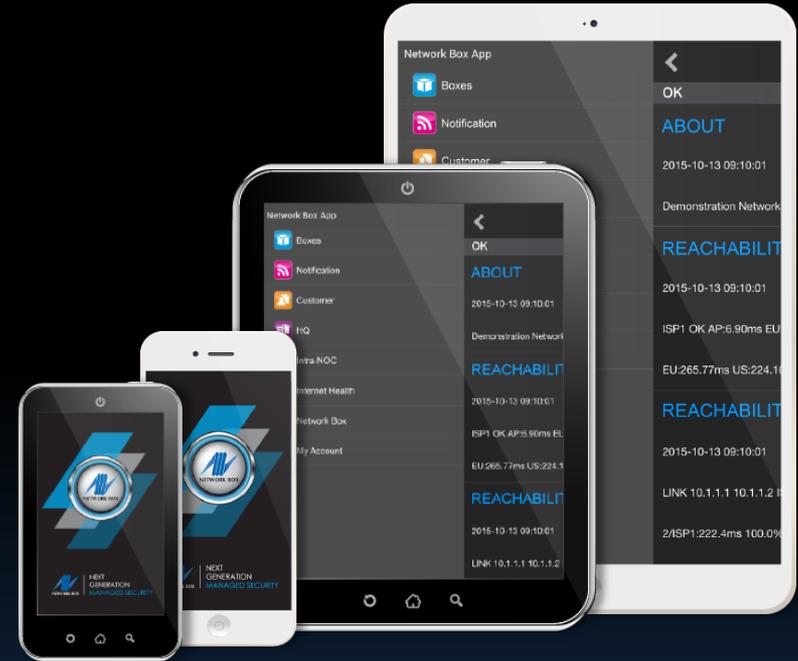
- Network (INTERNET) utilization
- Network (LAN) utilization
- Network (DMZ) utilization
- Network (VPN) utilization
- DISK utilization
- CPU utilization
- Network Firewall connections denied
- Web Client requests made
- Web Client requests denied
- Web Client URL categories
- Web Client Threats
- emails received
- emails denied
- Outgoing emails sent
- Outgoing emails denied
- Incoming emails received
- Incoming emails denied
- email SPAM blocked
- email MALWARE blocked
- email POLICY blocked
- email DLP blocked
- And many more...



# iOS/Android App

New iOS / Android App for mobile devices will be launched

- ▶ iOS APNS support
- ▶ Google GCM support
- ▶ Control for notifications:
  - *Set-up schedules*
  - *Types of notifications*
  - *Group boxes and notifications*



# VPN-5

High performance VPN device for securing connections for your home office or branch office's Virtual Private Network

- ▶ Dual Core 1.6 GHz CPU
- ▶ PPTP, SSL and IPSEC support
- ▶ High performance to handle large bandwidth remote office connections



# S-38i and S-68i

UTM device to offer small offices  
Enterprise-level protection

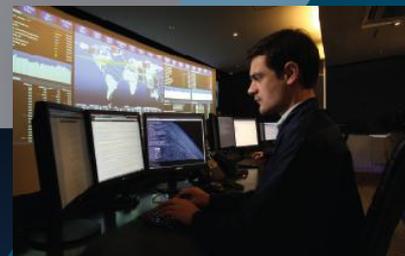
- ▶ Multi-core processor
- ▶ Industrial grade chassis
- ▶ Fanless, with no moving parts





NEXT  
GENERATION  
MANAGED SECURITY

# Thank You



Network Box Corporation Ltd.

