MAR 2014

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the March 2014 edition of In the Boxing Ring

This month, we discuss in detail the Network Box 5 **Security Modules and Security Packages**. Previously, we only offered a choice of four simple service packages: FW+, CF+, AV+ and UTM+. These equated to firewall protection, content protection, anti-virus, and 'all three'. Network Box 5 offers additional 'application based' service packages, to add further flexibility by as well as the option to choose individual security modules. These are highlighted further on pages 2-3.

A breakdown of the different features and the security modules are illustrated in the Network Box 5 Security Modules Matrix on page 4.

On pages 5-6, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally we are pleased to announce the launch of our new Security Operations Centre in Cologne, Germany; lead by our team at Network Box Germany. If you want to contact Network Box Germany, please feel free to contact us, we will be more than happy to put you in touch with them directly.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 2014

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 with us by several social networks:

twitter http://twitter.com/networkbox

facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

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

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

Security Modules & Service Packages

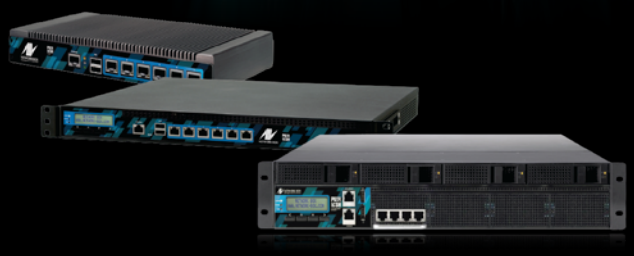
Network Box 3 delivered a choice of four simple service packages: **FW+**, **CF+**, **AV+** and **UTM+**. Based around the concept of 'scanning technologies', these equated to firewall protection, content protection, anti-virus, and 'all three'. While Network Box 5 provides an option for these same 4 services packages, we've also added further flexibility by offering 'application based' service packages, as well as the option to choose individual security modules.

Network Box 5 Security Modules

The Network Box 5 product is delivered as a set of security modules building upon a single base module. The base module consists of a kernel, user space toolchain, logging and configuration – essentially an extremely sophisticated router – and it is these security modules that provide the security functionality.

The security modules are inter-related and communicate amongst themselves, but each individual security module is targeted towards a single security problem. Examples of such modules include:

- Web Client protection
- Web Server protection
- SMTP Mail Server Protection
- Anti-Virus scanning
- Intrusion Detection
- Quality of Service



As you can see, some of these modules provide specific security functionality (such as anti-virus scanning) and are used as tools by other higher-level modules. Other modules provide specific protection (such as web client protection). An important distinction is drawn between client and server protection – even if the core protocol (e.g.; http for web) is the same, the threat landscape and protection requirements are completely different.

Network Box 5
Service Packages

Service packages are bundles of security modules. In general, it is more cost-effective to choose a service package, than a group of individual security modules, as bundle pricing is available for service packages.

The core four Network Box service packages based on "scanning technology" are still available and offered in Network 5:

FW+
Firewall Plus

AV+
Anti-Virus Plus

CF+
Content Filtering Plus

UTM+
Unified Threat Management Plus

And in addition, a fifth such package is now also offered to provide for Web Application Firewall protection for web servers:

WAF+
Web Application Firewall Plus

But, now we also offer the option for application-based service packages:

- **EMP+**
  eMail protection
- **WBP+**
  Web Browsing protection
- **FWAF**
  Firewall+ and WAF protection bundle
- **UTMW**
  UTM+ and WAF protection bundle

For example; if your goal is to protect web clients, you may find the WBP+ package more suitable than CF+, as it includes both anti-virus and content filtering protection for web clients.

Network Box 5
Optional Security Modules

Network Box 5 also includes a number of optional security modules. These can be chosen either to add on specific optional security technologies, or to supplement a service package with additional functionality. Examples include:

- NAVL Application Identification (1,000+ applications identified)
- Data Leakage Prevention
- Clustered Scanning

Conclusion

Network Box 5 takes the four core service packages of Network Box 3 and provides alternative choices for application-based service packages and optional security modules. Each security module is targeted towards a single specific security problem.

NETWORK BOX

Network Box 5

Security Modules Matrix

Security Modules	Service Packages									
	BASE	FW+	CF+	AV+	UTM+	WAF+	EMP+	WBP+	FWAF	UTMW
Base	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network-Firewall		✓	✓	✓	✓	✓	✓	✓	✓	✓
Network-NAT		✓	✓	✓	✓	✓	✓	✓	✓	✓
Network-DDoS		✓	✓	✓	✓	✓	✓	✓	✓	✓
Network-IDS		✓	✓	✓	✓		✓	✓	✓	✓
Network-IPS		✓	✓	✓	✓		✓	✓	✓	✓
Network-Frontline		✓	✓	✓	✓		✓	✓	✓	✓
Network-QOS		✓	✓	✓	✓		✓	✓	✓	✓
Network-DHCP-Server		✓	✓	✓	✓		✓	✓	✓	✓
Network-DNS-Server		✓	✓	✓	✓		✓	✓	✓	✓
Network-HighAvailability		✓	✓	✓	✓	✓	✓	✓	✓	✓
Network-LoadBalancing		✓	✓	✓	✓	✓	✓	✓	✓	✓
Network-InfectedLAN		✓	✓	✓	✓		✓	✓	✓	✓
Network-VPN-Base		✓	✓	✓	✓		✓	✓	✓	✓
Network-VPN-IPSEC		✓	✓	✓	✓		✓	✓	✓	✓
Network-VPN-PPTP		✓	✓	✓	✓		✓	✓	✓	✓
Network-VPN-SSL		✓	✓	✓	✓		✓	✓	✓	✓
Proxy-Base		✓	✓	✓	✓	✓	✓	✓	✓	✓
Proxy-DDoS-Base		✓	✓	✓	✓	✓	✓	✓	✓	✓
Proxy-SSL-Base						✓			✓	✓
Proxy-Base-LoadBalancing										
Proxy-Auth			✓	✓	✓			✓		✓
Proxy-QOS			✓	✓	✓		✓	✓		✓
Proxy-Web-Base			✓	✓	✓	✓		✓		✓
Proxy-Web-Client			✓	✓	✓			✓		✓
Proxy-Web-Client-Accel										
Proxy-Web-Client-Quota										
Proxy-Web-Server-Base						✓			✓	✓
Proxy-Web-Server-WAF						✓			✓	✓
Proxy-Web-Server-Gateway						✓			✓	✓
Proxy-FTP-Base				✓	✓					✓
Proxy-FTP-Client				✓	✓					✓
Proxy-FTP-Server				✓	✓					✓
Proxy-InfectedLAN		✓	✓	✓	✓		✓	✓	✓	✓
Proxy-Mail-Base				✓	✓		✓			✓
Proxy-Mail-SMTP-Base				✓	✓		✓			✓
Proxy-Mail-SMTP-Client				✓	✓		✓			✓
Proxy-Mail-SMTP-Server				✓	✓		✓			✓
Proxy-Mail-IMAP-Client				✓	✓		✓			✓
Proxy-Mail-POP-Client				✓	✓		✓			✓
Proxy-AppID-Base		✓	✓	✓	✓		✓	✓	✓	✓
Proxy-AppID-NAVLite		✓	✓	✓	✓		✓	✓	✓	✓
Proxy-AppID-NAVL										
Portal-Base		✓	✓	✓	✓	✓	✓	✓	✓	✓
Portal-Admin		✓	✓	✓	✓	✓	✓	✓	✓	✓
Portal-User										
Reporting-Base		✓	✓	✓	✓	✓	✓	✓	✓	✓
Scan-Base			✓	✓	✓		✓	✓		✓
Scan-File				✓	✓			✓		✓
Scan-URL			✓		✓			✓		✓
Scan-Auth			✓	✓	✓		✓	✓		✓
Scan-Mail				✓	✓		✓			✓
Scan-Clustering										
Scan-Provider-AntiMalware-NB				✓	✓		✓	✓		✓
Scan-Provider-AntiMalware-Kaspersky				✓	✓		✓	✓		✓
Scan-Provider-AntiMalware-CLAM				✓	✓		✓	✓		✓
Scan-Provider-URL-NB			✓		✓			✓		✓
Scan-Provider-URL-SSCAN			✓		✓			✓		✓
Scan-Provider-URL-NBCP			✓		✓			✓		✓
Scan-Provider-AntiSpam-NB				✓	✓		✓			✓
Scan-Provider-AntiSpam-ChallengeResponse				✓	✓		✓			✓
Scan-Provider-AntiSpam-Reputation				✓	✓		✓			✓
Scan-Provider-DLP-NB										
Scan-Provider-Policy-NB			✓	✓	✓		✓	✓		✓
NOC-Provisioning										
NOC-SigPush										
NOC-ConfigSync										

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 4th March 2014, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days.

Network Box 5 Features
March 2014

This month, for Network Box 5, our patch Tuesday set of enhancements and fixes include:

- Security fixes to address CVE-2013-6467 in IPSEC
- Enhancement to accept numeric digits in IPSEC tunnel names
- Various enhancements and improvements to SSL VPN configurations
- Support for new service- Global Monitoring System sensors
- Improvements to web policy block page
- Improvements to map zoom levels on Administrative Portal
- Colorization of the mail status on Administrative Portal
- Support for international encodings in mail subjects
- Various revisions and enhancements to RBL scanning of email messages and envelopes
- Improvements to Administrative Guide for network-dhcp-server security module
- Support for new entity attribute types for SSH authorized keys
- Improvements to mail delivery detail reports
- Standardization and enhancement of range selection for reporting
- Support for multi-box selection in Network Box 5 SOCs
- Improvements to registry caching system (for performance and reliability)
- Improve GMS reporting reliability if server unreachable
- Performance improvements to the web Administrative Portal
- Support for new regional SOCs and their public IP addresses
- Support for sessions, background jobs and background connections in administrative console client

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 SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

NETWORK BOX

Network Box 3 Features March 2014

On Tuesday, 4th March 2014, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Extensions to Global Monitoring System
- Speed-ups and improvements to Box Office
- Various (mostly internal) enhancements to several internal support systems

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 SOC will contact you to arrange this if necessary.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor	Network Box Corporation nbhq@network-box.com or via mail at:
Michael Gazeley **Nick Jones** **Kevin Hla** Production Support	**Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong
Network Box HQ **Network Box UK** **Network Box USA** Contributors	Tel: +852 2736-2078 Fax: +852 2736-2778 www.network-box.com

Network Box Germany
New Security Operations Centre

Network Box is extremely pleased to announce that Network Box Germany's Security Operations Centre was launched last month in Cologne, Germany. Lead by **Jacqueline Voss** and her dedicated team, Network Box Germany will be providing world class Managed Security Service to new and existing Network Box customers in Central Europe.

The Changing Face of Advanced Malware Detection

David Strom, one of the leading global experts in the field of network and communications technologies, recently wrote an article titled, "The changing face of advanced malware detection", which outlines the latest anti-malware technologies. In the article, he highlighted Network Box's Z-Scan and its advanced capabilities and near instant response times.

LINK: http://searchsecurity.techtarget.com/feature/The-changing-face-of-advanced-malware-detection

Apple iOS Secure Transport connection validation failure

Last month, Apple announced a security vulnerability in their iOS operating system as well as their Safari web browser. **However, customers using Network BOX 5 SSL Proxy were protected by default from exploit of this vulnerability even before patches were available from Apple.**