JUL 2014

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the July 2014 edition of In the Boxing Ring

This month, we are launching a new Key Performance Indicators (KPI) menu item on the ANALYSIS tab of the admin web portal. This will show a summary of all the KPIs in the system, comparing two period (current and previous) and show the percentage change previous to current.

In the business world, organizations worldwide have come to rely on KPI, which have become the standard method for measuring progress towards predefined and measurable goals. The Network Box 5 monitoring and reporting systems, have been enhanced to leverage the concept of KPI, for use in Managed Cyber Security. This is highlighted further on pages 2-4.

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 a partnership agreement with Jardine OneSolution (JOS), where JOS will become an authorized reseller of Network Box product and services in Hong Kong. By partnering with JOS, it will gives us an opportunity to bring world-class security solutions to an even greater range of customers.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
July 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

Key Performance Indicators

Peter Drucker, the renowned management consultant who invented the concept known as, 'management by objectives,' once famously said, "What gets measured, gets managed." In other words, it is those things which we can quantify and monitor objectively, that we can most easily supervise and control. Without clear data, gathered impartially, one is left with little choice by to manage by guesswork. Guessing is obviously far from ideal, even at the best of times, and hardly a reliable foundation for any form of reporting or management.

In the business world, organizations worldwide have therefore come to rely Key Performance Indicators (KPI), which have become the standard method for measuring progress towards predefined and measurable goals. By using KPI throughout an organization, one can (for example) ensure sales are really up, costs are really down, quality is really increasing, and success is both real, and most importantly, repeatable. Without KPI in the workplace, it's almost impossible to know what is going well, and what is not.

For all of these reasons, the Network Box 5 monitoring and reporting systems, have been enhanced to leverage the concept of KPI, for use in Managed Cyber Security.

By using KPI, each Network Box hardware appliance (or virtual device), is able to much better communicate what has been happening both in real-time, as well as over any given period of time. This spectrum of empirical information covers both the Network Box system itself, as well as the protected client gateway and computer systems in general.

NETWORK BOX

Everything from network utilization, to how many web client requests have been made, to how many emails have been denied, to the average and peak CPU utilization, are carefully monitored and logged, to allow for detailed, fully customizable, real-time HTML-5 dashboards, and Adobe PDF format reports.

It is also possible to output this data to centralized organizational syslog servers, or to save it in various industry standard formats, such as comma-separated values (CSV).

In order to remove any initial learning curve, each Network Box 5 device (physical or virtual), comes with pre-defined KPI weekly reports, which closely mirror the weekly reports which have always been part of the Network Box 3 managed security services. The inclusion of a default report will allow any Network Box 3 client to upgrade to Network Box 5, without immediately needing to lean about the new KPI systems built into Network Box 5.

Once upgraded to Network Box 5, a standard (default) Network Box KPI weekly report will be delivered, in place of the old Network Box 3 weekly report.

However, given the enormous power and flexibility of the new Network Box 5 monitoring and reporting systems, it is obviously well worth utilizing the new built-in KPI capabilities to produce bespoke real-time HTML-5 dashboards and periodic Adobe PDF format reports.

Key Performance Indicators are usually long-term considerations, and therefore the definition of what they are, and how they are measured, do not change very often. This means that even a small amount of time and effort invested in creating such real-time dashboards and reports, will see substantial returns over the long term, as it will not be necessary to keep making changes to these dashboards and reports very often.

It is also worth noting that once an HTML-5 dashboard has been created by an IT Manager on his or her desktop computer, the same HTML-5 dashboard will automatically be available across all the devices he or she uses. This means that IT Managers do not have to be at their desks to see what is happening at their Internet gateways; they can just use their laptop, tablet, or even smart phone, to monitor their systems from almost anywhere on earth.

For far too long Unified Threat Management has been far from unified, and far too difficult to monitor and manage. Network Box 5 not only unifies cyber security, but its monitoring and reporting tools, leverage the concept of KPI, to allow for the very best kind of management possible – informed management.

Peter Drucker also famously said, "Trying to predict the future is like trying to drive down a country road at night with no lights while looking out the back window."

The objective of Key Performance Indicators in general, and the new Network Box 5 KPI monitoring and reporting systems in practice, is to at least allow IT Managers to turn the car headlights back on, and allow them to look out of the front windscreen.

There are twenty one initial Key Performance Indicators offered by the new Network Box 5 KPI monitoring and reporting systems.

1. Network (INTERNET) utilization
2. Network (LAN) utilization
3. Network (DMZ) utilization
4. Network (VPN) utilization
5. DISK utilization
6. CPU utilization
7. Network Firewall connections denied
8. Web Client requests made
9. Web Client requests denied
10. Web Client URL categories
11. Web Client Threats
12. eMails received
13. eMails denied
14. Outgoing eMails sent
15. Outgoing eMails denied
16. Incoming eMails received
17. Incoming eMails denied
18. eMail SPAM blocked
19. eMail MALWARE blocked
20. eMail POLICY blocked
21. eMail DLP blocked

For each of those, there are six variants:

1. 24hour average
2. 24hour peak
3. Peak-hours average
4. Peak-hours peak
5. Offpeak-hours average
6. Offpeak-hours peak

These allow for a total of one hundred and twenty six KPI which can be monitored and reported on as required right now.

In the near future we also plan to release the following KPI types.

1. VPN SSL site-to-site connections made
2. VPN SSL client connections made to the server
3. VPN SSL site-to-site percentage uptime
4. VPN PPTP connections made
5. VPN IPSEC connections made
6. VPN IPSEC percentage uptime
7. Frontline IPS attacks denied
8. IPS attacks denied
9. IDS attacks detected
10. WORKLOAD utilization
11. MEMORY utilization

This will bring the total number of KPI to one hundred and ninety two, as all of the KPI types will be available in six variants.

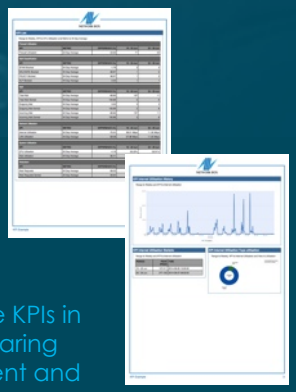
For each KPI, as an overview, it is also possible to make a comparison between any two defined time periods. This facility is very useful to see if workloads are increasing over time, for example, to see how many more emails are being scanned by the system this week, than in the same week last year.

1. Current time period (day, week, month, etc)
2. Previous time period (previous day, week, month, etc)
3. Percentage change from previous to current

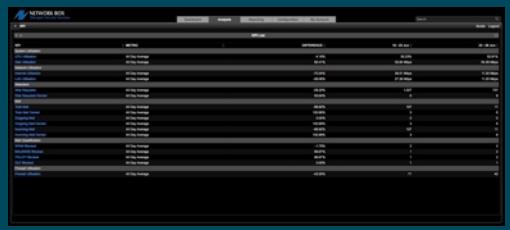
For each KPI, in detailed view, provision is also made to show:

1. KPI history over time (chart/table of KPI over time, to see historical trends)
2. KPI Statistics (for each time period, the average of the KPI)
3. KPI Tops (depending on the KPI, but things like Top Users, Top Senders, Top Recipients, etc)

Network Box 5 now has a new 'KPI' menu item on the ANALYSIS tab of the admin web portal.



This will show a summary of all the KPIs in the system, comparing two periods (current and previous) and show the percentage change previous to current.



Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 1st July 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
July 2014

This month, for Network Box 5, these include:

- Support for custom local rules in network IDS and IPS security modules
- Enhanced support for editing of filters from inside the administrative reporting module
- New "Emergency Mode" support in front-panel
- Support for multiple server SSL vpns on a single network box appliance
- UTF-8 international encoding support in LDAP synchronization
- New 'random100' term to support statistical randomization of rule results
- Support for IPSec ID Extension in network-vpn-ipsec
- Change to default block page for WAF+ to be an anonymized version
- Include recordID in mail alert default template
- Change to use 'warn' logging result (instead of 'audit') when an HTTP client/server transaction response is 4xx or 5xx
- Add support for POP3 'AUTH' login mechanism
- Improvements to DHCP server logging when provided clientname is blank/missing
- Improvements to M-285i and M-385i front-panel display drivers
- New 'gateways' Global Monitoring System sensor, including multi-gateway support
- Addition of monitoring and status commands for network-highavailability security module
- Support for new GMS 'CLOCK' sensor, and control of configuration changes when system time has not been set
- Support for new GMS 'DNSCLIENT' sensor, testing DNS resolution as a client
- Support for base 'conditions' in GMS
- Performance and stability improvements to GMS
- Change to the calculation of overall confidence figure logging - it is now the maximum, not the average
- Extensions to authentication, URL and file scanning, to permit improvements in scanning and content classification
- Improvements to web client logging related to CONNECT HTTPS method
- Improvements to threat cache for web client security module
- Add support for ADSL boxes running PPTP servers
- Extensions to pop3 client, to allow rules based on categorization to be realized
- Introduction of log target 'syslog' support for export of logs to remote syslog server
- Improvements to hardware RMA process to allow replacement of system maintenance password
- Improvements to smtp mail client and server logging
- Security update addressing CVE-2014-3470: Anonymous ECDH denial of service
- Security update addressing CVE-2010-5298: SSL_MODE_RELEASE_BUFFERS session injection or denial of service
- Security update addressing CVE-2014-0198: SSL_MODE_RELEASE_BUFFERS NULL pointer dereference
- Security update addressing CVE-2014-0195: DTLS invalid fragment vulnerability
- Security update addressing CVE-2014-0221: DTLS recursion flaw
- Security update addressing CVE-2014-0224: SSL/TLS MITM vulnerability
- Enhancement to support mail quarantine release to multiple recipients
- Enhancement to introduce new Key Performance Indicators (KPI) system
- KPI screens in administrative web portal
- NETWORK utilization KPIs
- DISK utilization KPIs
- CPU utilization KPIs
- WEBCLIENT classification and utilization KPIs
- EMAIL classification and utilization KPIs
- FIREWALL utilization KPIs

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 July 2014

On Tuesday, 1st July 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:

- Various (mostly internal) enhancements to several internal support systems
- Anti-spam engine improvements

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

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2078
Fax: +852 2736-2778

www.network-box.com

Network Box Partnership
Jardine OneSolution

Network Box signed a strategic partnership agreement where Jardine OneSolution (JOS) will become an authorized reseller of Network Box in Hong Kong. With more than 60 years of solid experience, JOS is one of the region's leading IT products and distribution services companies.

Network Box – ComputerWorld HK
The Vulnerability of Everything

Network Box's Managing Director, Michael Gazeley, had his article, "The Vulnerability of Everything", published in ComputerWorld this month.

Link:
http://cw.com.hk/opinion/vulnerability-everything

Network Box USA –
The Price of Business

Network Box USA's CTO, Pierluigi Stella, was interviewed on, *'The Price of Business,'* hosted by multi-award winning broadcast journalist, Kevin Price. During the interview Stella discussed issues of Cyber Security and the need for comprehensive protection for all businesses.

Link: https://www.youtube.com/watch?v=Oo7MsjO4w8M&feature=youtu.be