In The Boxing Ring

IN THIS ISSUE

Network Box Technical News from Mark Webb-Johnson, CTO Network Box

Welcome

Welcome to the August 2010 edition of 'In the Boxing Ring'. We continue to work behind-the-scenes on the new Box Office and NOC support systems (ready for new product feature launches in 2010Q3). There will be more news on this in the upcoming Q3 newsletters.

In the past month there has been more 'Snake Oil' peddled on the Internet than ever before, so on page 2 I'd like to spend some time presenting our viewpoint on the core goals and advantages of the UTM approach to network security (and in particular, the Network Box managed UTM+ system for effective network security). UTM is not a single security function, but an amalgamation of multiple security functions into a single integrated appliance (or cluster of appliances). The true power of UTM comes both from the coverage of the threat landscape (achieved by utilising multiple protection methodologies) and the synergy between the protection (whereby different components co-operate and inter-operate to leverage each others protection capabilities) - and anything else is, quite simply, Snake Oil.

On page 3, we present the usual monthly hint (this month regarding deployment of the Network Box IDPS system), and outline the software updates delivered as part of this month's software release.

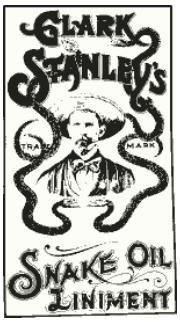
As usual, if you have any feedback, or comments, they are always appreciated. You can contact us here at HQ via eMail (nbhq@network-box.com). Or, drop by our office next time you are in town.

You can also keep in touch by following our Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
August 2010

NETWORK BOX



Security Snake Oil

In the wild days of the American west, snake oil peddlers plied their trade - selling dubious remedies for real (or imagined) ailments. The practice continues today (albeit with updated marketing techniques), and is particularly troublesome in the network security industry.

As we've seen an increase in this practice, over the past month or two, we thought it worthwhile spending some time letting you know our viewpoint on the core goals and advantages of the UTM approach to network security (and in particular, the Network Box managed UTM+ system for effective network security).

So, what is UTM? Simply put, Unified Threat Management (UTM) is the amalgamation of multiple security functions into a single integrated appliance (or cluster of appliances). There is disagreement over what (or how many) functions should be included to make an appliance UTM, but in general it is agreed that at a minimum this should include Firewall, VPN, Intrusion Prevention and Anti-Virus functionality.

Network Box takes UTM as a starting point, and builds dozens of extra functions on top of it. For example, in addition to the core UTM functions listed above, we also provide quality-of-service, policy enforcement, anti-spam, content filtering, web caching, routing, address translation, multiple link aggregation, network traffic analysis, mail portal, as well as many others.

The core benefit of UTM is the application of multiple protection technologies to the problem of providing effective network security. Time and time again, it has been shown that the primary reason security breaches occur is simply because the required protection technology has not been deployed. You get a virus because you have no anti-virus system. You get spam because you have no anti-spam system. You get breached by a worm because you have no network-level Intrusion Prevention. Your bandwidth is saturated because you have no outbound control. etc etc. Only by deploying a collection of technologies covering the entire threat landscape, can the protection be effective against all the different types of threat. The alternative of deploying individual devices (or software packages) to protect against each type of threat is just not possible - as it is prohibitively expensive, and too hard to manage the disparate systems. This is the core benefit of Unified Threat Management.

The reason that UTM works so well is not only the comprehensive coverage of the threat landscape that it provides, but also that the different protection technologies are integrated and unified under the same protection umbrella. This synergy of protection functionality (whereby different components co-operate and inter-operate to leverage each others protection capabilities) is a core reason why UTM works so well (and an effective counter-argument to the 'Jack of all trades, master of none' complaint against UTM).

The importance of maintenance. As previously explained, the primary reason for security breaches is lack of protection technology,. The second most common reason is improperly configured or out-of-date protection. In other words, you get a virus either because you have no anti-virus system or because it hasn't been properly turned on or kept up-to-date.

The Network Box approach (which we call UTM+) takes our core technology and applies a management layer (to ensure that the protection is expertly configured and maintained) and PUSH update systems (to keep the protection up-to-date in real-time). This effectively addresses the fundamental causes of security problems, and provides the most comprehensive UTM offering in the market today.

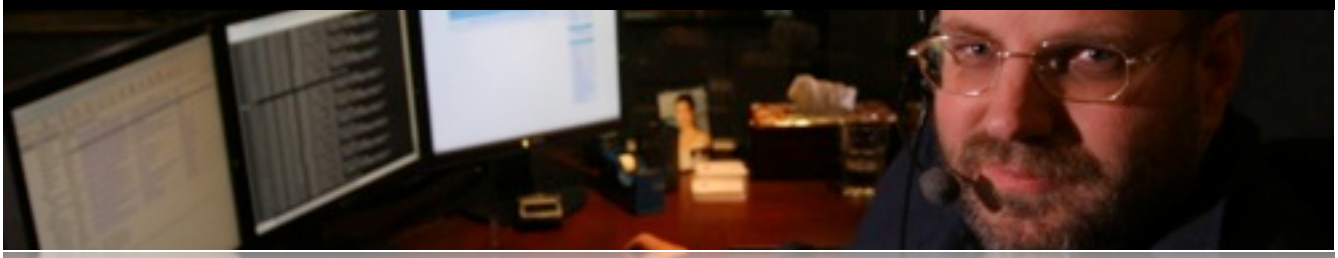
Differentiation of products. In an attempt to differentiate their products, marketers apply 'catchy' phrases to their offerings.

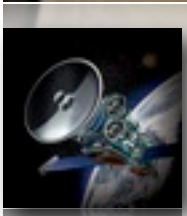
- They say "we're an application-layer firewall". Well, anything that scans for malware in an application-level protocol (such as mail or web protocols) is an application-layer firewall. What's the difference?
- They say "we're a next generation firewall". Yes, but what is the difference?
- They say "we're using application identification rather than port numbers". Yes, but that is 5% of the problem (ie; outbound application identification), but does nothing to address the remaining 95% of the threat landscape. It is not going to help you with a network worm or email virus.
- They say "we use heuristics, so don't rely on signatures". Well, so does pretty much every anti-virus vendor in the market today (and it does little good when the malware writers have access to the same engines so can test to ensure their new malware is not heuristically detected before release).
- They fail to give figures for the size of their signature database (one vendor even has the gall to suggest that 'less is more'). For the record, Network Box today has 4.7 million anti-malware signatures. With that many known malwares, how can a system using just a few thousand signatures be affective?

Just as in the wild west, these Snake Oil salesmen will continue to peddle their 'remedies' to your ailments. The key is to look at the facts, and ensure you follow best recommendations for security practices.

If you want to see the threat landscape, you can refer to the CSI/FBI Computer Crime and Security Survey (or google for 'CSI/FBI Security Survey') - they've been doing this for fourteen years now and provide a fair and unbiased survey on the current state of computer crime and security. That will provide you with an independent overview of the threat landscape. It is then just common sense to look at the major threats and make sure that your chosen computer security solution has them covered. Sometimes when somethings sounds 'too good to be true', it quite simply is.

P.S. If you want to learn all about Snake Oil, the Wikipedia article provides a good starting point. I particularly like the explanation that *"to increase sales, an accomplice in the crowd (a shill) would often attest the value of the product in an effort to provoke buying enthusiasm"* - a practice we still see effectively used today in the peddling of security snake oil.





August 2010 Features

This month, we are glad to say that there are no known vulnerabilities to be addressed by package update (as all the vulnerabilities have been able to be addressed by signature update) so we will not be releasing any software packages to customer Network Boxes in August 2010. We do have a number of enhancements to our internal systems, to be deployed, including:

- Further enhancements to the Box Office portal, related to service contracts and their visibility on customer views. We are conducting a phased deployment of our new customer contracts system, over the next two months, which will improve this further.
- Enhancements to the NOC PUSH update systems, to improve speed of update deployment.
- Enhancements to the NOC device management systems, to provide for improved management functions and capabilities.

The above changes are internal only and will not impact running services or require a device restart. The enhancement work will be handled by the regional NOCs and will not require any action on your part. No service interruption is expected to be required.

We do, however, have a data centre re-organisation which may require firewall rule changes to your devices. Again, the regional NOCs will be handling this for you, and will contact you to arrange this as necessary.

August Hint: Deploy IDPS

The Network Box IDPS system has been available for some time now, and has been successfully deployed protecting tens of thousands of networks, and millions of computers, around the globe.

Network Box is a member of Microsoft's exclusive MAPP program, and we release the majority of our MAPP signatures using our IDPS network-level protection system. When MAPP partners receive vulnerability information early, they can provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. Only by deploying the IDPS protection engine can you benefit from this protection.

This month, Microsoft and Adobe have announced that they are collaborating to share Adobe vulnerability information with Microsoft's MAPP partners. Network Box will benefit from this information and use this to be able to pro-actively release protection for Adobe vulnerabilities as well as Microsoft's. Better protection, earlier - a win-win situation for Network Box and our customers, and even more reason to deploy IDPS.

The IDPS engine does require additional compute resource to deploy, so may not be suitable for everyone (without hardware upgrade). With more than 6,000 protection signatures (growing every day), this is a major protection engine for us.

Please talk to your local support NOC to discuss how this can best be done for your organisation and how we can best serve your network Intrusion Detection and Prevention requirements.

JULY 2010 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	965	+39.0
Signatures Released	131,364	-29.3
Firewall Blocks (/box)	690,756	-2.5
IDP Blocks (/box)	154,221	+4.4
Spams (/box)	48,545	-9.8
Malware (/box)	795	-42.8
URL Blocks (/box)	81,518	-10.7
URL Visits (/box)	3,318,084	-7.5

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jason Law
Nick Jones
Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK
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