

# In The Boxing Ring



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

### Welcome

Welcome to the July 2009 edition of 'In the Boxing Ring'. In this edition, we focus on how to best protect your Virtual Private Network (VPN). Turn to page 2 for details.

We also address the growing concern with website compromise through SQL injection – a threat that can never be 100% blocked at the gateway. We look at what SQL Injection is and what you can do to protect yourself. Page 3 provides further information.

Also on Page 3, we review Bing.com beta, Microsoft's new 'decision' engine, and talk about *safe search*.

In our July features, we also have the usual allotment of updates to the NBRS-3.0 system, enhancements to the

scanning engine, further support for four more new spam signature types, and performance improvements to the system. Turn to Page 4.

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](mailto:nbhq@network-box.com)). Or, drop by our office next time you are in town.

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

***[twitter.com/networkboxhq](https://twitter.com/networkboxhq)***

Mark Webb-Johnson  
CTO, Network Box Corporation

July 2009

### IN THIS ISSUE

#### 2. **NETWORK BOX VIRTUAL PRIVATE NETWORK (VPN)**

What a true SSL VPN is and how to deploy it. With the July 2009 Patch Tuesday firmware update, Network Box has fully integrated our SSL VPN to the Network Box Certificate Authority.

#### 3. **NETWORK BOX SQL INJECTION ADVICE**

Fighting SQL Injection is tough; this article provides some insights.

#### 3. **BING.COM AND SAFE SEARCH**

SafeSearch for Bing.com (beta) appears too good to be true.

#### 4. **JULY 2009 FEATURES**

The ongoing deployment of our recently released features and enhancements.





## Network Box Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a virtual circuit between nodes, carried over some larger network (such as the Internet), as opposed to running across a single private network. The Link Layer protocols of the virtual network are said to be tunneled through the transport network.

VPNs are site-to-site tunnels, and as such operate at the lowest layers of the ISO stack.

There is a misunderstanding (deliberate, or otherwise, depending on how you read it) in the industry that groups together true SSL VPNs with SSL enabled web servers and proxy servers.

The interpretation that SSL can only encrypt traffic at the application layer is also incorrect.

True SSL VPNs encrypt traffic at the lowest layers of the ISO stack, and, as such, can protect all network (and application) traffic transparently. SSL proxies and port forwarders merely encrypt traffic for individual specified applications one-at-a-time. These are not true VPNs and suffer from limitations regarding what they can protect.

As well as support for the PPTP and IPSEC protocols, Network Box includes an Open Source SSL VPN server and client called "Open VPN" (see <http://www.openvpn.org/>).

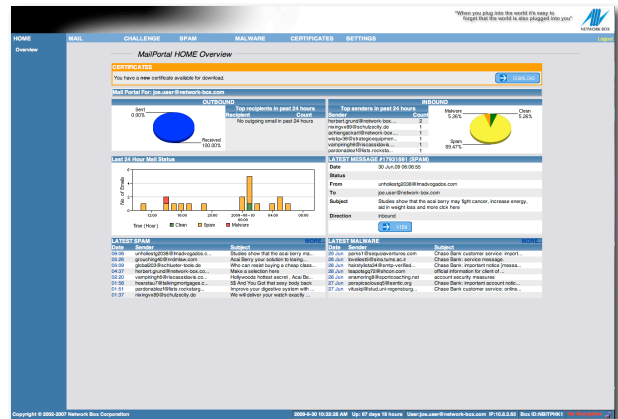
This is a true SSL VPN which establishes a link-level encrypted and authenticated tunnel between two end-points and protects all the traffic passing through it (irrespective of the application). As such, it requires client software to be installed and this client software is currently available for Microsoft Windows, Apple OSX and Unix.

From a security standpoint, the use of SSL certificates (a form of PKI - Public Key Infrastructure) provides the highest level of security. However, managing these SSL certificates, as well as the client software and configuration files, has proven to be administratively intensive and has limited the deployment of this technology.



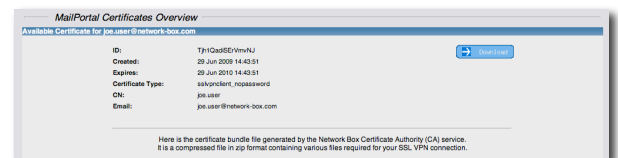
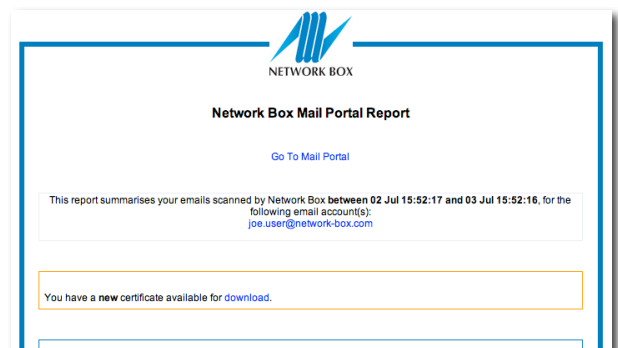
With the July 2009 Patch Tuesday firmware update, Network Box has addressed the problem of management of SSL VPN certificates, client software and configuration files, by fully integrating our SSL VPN to the Network Box Certificate Authority. As such, client certificates (as well as installation instructions, customized configuration files, and other ancillary

documents) can be distributed automatically either via eMail or via the Network Box Mail Portal web based system.



A full Certificate Revocation List (CRL) is maintained by the Network Box to allow instant revocation of client access (on a per-client basis), and a powerful templating system is used for the automatic generation of per-user based configuration files and installation instructions.

To issue a certificate for a SSL VPN client, the authorized administrator uses the MY.NETWORK-BOX.COM administrative portal. Entering the email address of the user, and choosing to distribute either by email or mail portal, the system automatically generates and distributes everything necessary for the end-user to setup his SSL VPN client. Certificate renewals and revocations are handled using the same integrated mechanism.



The optional Mail Portal distribution mechanism highlights (on the home page of Mail Portal and in the email report) the availability of a certificate to be downloaded, and allows downloading of previously issued certificates.

Network Box recommends the use of SSL VPNs for both site-to-site and road-warrior configurations. The protocol operates excellently over NAT devices and supports extremely flexible configuration options.



## Network Box SQL Injection Advice

In the very first In The Boxing Ring newsletter (a year ago, July 2008), we talked about SQL Injection and the problems with web application vulnerabilities. On this anniversary, I think it useful to re-visit this, as we are still seeing a large number of these attacks (both in the news and in the wild).

SQL Injection attacks are extremely hard to stop at the gateway, as the attacks are application dependent and therefore generic IDS/IPS rules can provide only limited defence. While Network Box has a number of IDS and IPS rules in place, application level security (by way of strict input validation) is ultimately the only way to thwart these type of attacks.

Let me give you an example of just such an attack. Let's say a web server runs an application (called news.cgi) that takes a single parameter 'id' to retrieve a news story:

<http://target.com/news.cgi?id=22>

It retrieves the story using a SQL statement of the form:

```
"select article from news where id=" . $id
```

which generates the SQL statement (for example):

```
select article from news where id=22
```

Now, what if an attacker manipulates the 'id' parameter for his own purposes? For example, what if he sends:

<http://target.com/news.cgi?id=22;truncate%20table%20news>

The resulting SQL statement would become:

```
select article from news where id=22;truncate table news
```

with the result being the loss of all news stories.

So, how would you stop this attack? There are three main methods:

- 1) Use parameterized SQL statements (where the above statement becomes "select article from news where id=?" and the 'id' is passed as a parameter).
- 2) Enforce strict parameter validation (for example, validating the 'id' parameter to ensure it is a number).
- 3) Escape parameters before insertion into the SQL statement (to remove problems such as embedded ';' and quote characters – in this case, the SQL statement would then become "select article from news where id='22;truncate table news'").

This is just one example of the many possible vectors for SQL Injection attacks. Such vulnerabilities in web applications (as demonstrated by the above news.cgi application) can wreak havoc and result in a loss or corruption of data.

In the case of common, public, web applications, with known vulnerabilities, gateway perimeter protection (such as Network Box) can apply IDS/IPS rules to detect and block exploit of the known vulnerabilities. But in the case of customized private web applications, this is not generally possible.

All NBR3-3.0 Network Box devices have two IDP modules (named HTTP-S- SQLINJECT and HTTP-S-SQLINJWORM) to provide application-specific and worm-specific protection for SQL Injection, and these new protection modules were released to all our customers back in July 2008. However, as previously stated, generic IDS/IPS rules can provide only limited defence, and application level security (by way of strict input validation) is ultimately the only way to thwart these types of attacks.

We do recommend that customers operating public web servers (in particular those accessible to the Internet) review the scripts and applications on their web servers to ensure that they are up-to-date and patched so as not to be vulnerable to this class of attack.



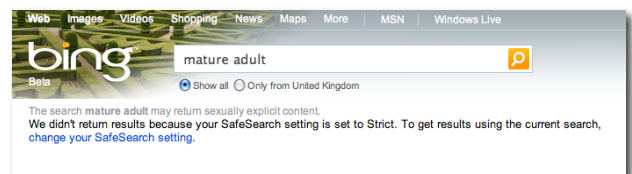
## Bing.com (beta) and Safe Search

In the September 2008 issue of *In the Boxing Ring*, we covered SafeSearch for Google and Yahoo!. A new search engine, Bing.com, has joined the search engine giants. Tagged by creator, Microsoft, as its 'decision engine', Bing.com provides the functionality of a search engine with a simplified presentation of search results. It also provides the SafeSearch functionality:

- Strict – Filter sexually explicit text, images and videos from your search results.
- Moderate – Filter sexually explicit images and videos, but not text, from your research results.
- Off – Don't filter any sexually explicit text, images, or videos from your search results.

Though the standard SafeSearch filtering levels are appreciated, as at writing, Bing.com's SafeSearch functionality seems to go too far on the *Moderate* setting. With searches for various terms that should trigger a warning, despite these terms'

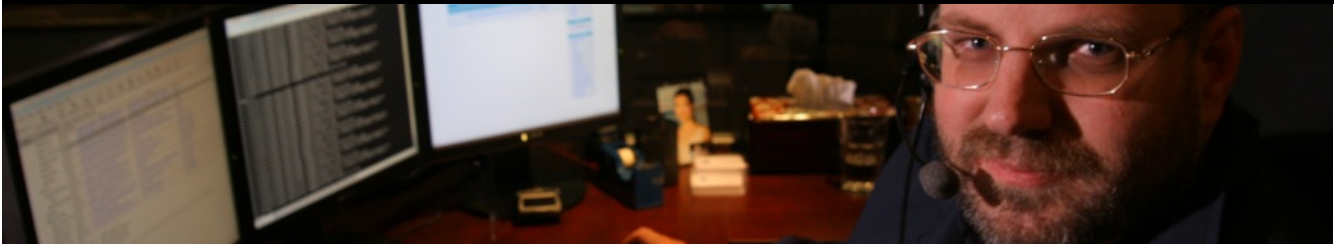
multiple meanings, e.g., "mature adult" (a stage of chronological advancement), Bing.com returns "We didn't return results because your SafeSearch setting is set to Strict."



Rather than removing unsafe results from the search results (as Google and Yahoo do), Bing.com blocks the entire search itself. This is a key difference and severely limits the usefulness of Bing.com as a safe search engine.

However, that said, Network Box has now extended its policy engine-integrated Safe Searching to not only include Google and Yahoo!, but also Bing.com. This enables a policy to be set to enforce a safe search level and enforce the SafeSearch functionality on all three search engines.

But so far, Bing.com's SafeSearch, disappointingly, lacks the practical control of other search engines.



## July 2009 Features

On Tuesday, 7 July 2009, we will be releasing a number of improvements to the mail scanning system, primarily to further improve anti-spam performance. And also new GMS health metrics for the correct operation of envelope verification and the customer LDAP server will be released.

Revisions to the MY.NETWORK-BOX.COM administrative interface and Mail Portal have been made to restrict users from whitelisting themselves, or administrators from whitelisting their own domain, by accident.

Additionally, we also release support for SSL Certificate bundles (including template configurations, instructions and software clients) in the Network Box Certificate Authority, MY.NETWORK-BOX.COM and Mail Portal systems.

And as always, we will be releasing general performance improvements and functionality enhancements.

The above changes will not require any impacting service or device restarts, and should not cause any significant interruption to device operation. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner.

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

## July Hint

For any company seeking clients, information is key. To access this information, particularly in the virtual business world, the web browser is the most widely used tool. But a majority of us are unaware of alternative choices to the default web browser provided. For example; FireFox, Safari and Opera.

All these browsers are free to download and use; each also offers roughly the same set of functionality. More importantly, each browser offers a slightly different user experience, that will appeal to each person in different ways.

To help you expand your business tools, recently Safari 4 and Google Chrome have been made available and the latest FireFox 3 has just been released. These browsers offer significantly greater Javascript performance than IE7 and IE8.

## Conclusions

Thank you for your support of Network Box, and the continued entrustment of your network security to our managed service. I hope you find this communication useful – if you have any suggestions, they are most appreciated, and should be directed towards your local NOC or account manager. Please don't hesitate to contact us for assistance.

Mark Webb-Johnson  
CTO, Network Box Corporation  
July 2009

### JUNE 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,083	+14.7
Signatures Released	204,873	-38.7
Firewall Blocks (/box)	637,305	+3.1
IDP Blocks (/box)	157,576	+13.2
Spams (/box)	73,136	-11.9
Malware (/box)	2,216	+22.8
URL Blocks (/box)	82,445	+17.4
URL Visits (/box)	3,080,726	+11.9

### NEWSLETTER STAFF

**Mark Webb-Johnson**  
Editor

**Pauline Chiu**

**Michael Gazeley**

**Jason Law**

**Nick Jones**

Production Support

**Network Box Australia**

**Network Box Hong Kong**

**Network Box UK**

### SUBSCRIPTION

Network Box Corporation  
[nbhq@network-box.com](mailto: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](http://www.network-box.com)