# In The Boxing Ring

## IN THIS ISSUE

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

### Welcome

歡迎您來閱讀2010年3月版“ In The Boxing Ring ”期刊。在這一版，我們將關注即將到來的非常重要的關于DNS域名服務系統的變更，我們需要早做計劃和檢查是否支持。另外，我也非常高興地確認在上個月提出的五款新產品得以正式地發布，並且開始供貨。

在第2頁，我們將展示DNS根區域遷移至域名系統安全擴展DNSSEC的具體時間表。網域名稱系統（DNS）提供了今天互聯網核心的基礎架構服務之一，但是卻容易受到“ 緩存投毒 ”和 “ 中間人 ”等各類攻擊。對這一問題的解決方案是部署域名系統安全擴展DNSSEC技術，而且這項部署工作（到根區的服務器，以及其他分區服務器）現在正在進行之中。所以我們都必須采取措施，作好准備，並確保我們的網絡不會受到此更改的影響。

在第3頁，我們將展示四個（由ISC的Mark Andrews發表）簡單的測試，你可以進行檢查您的兼容性，看它是否已經准備好應對即將到來的DNS根服務器應用DNSSEC的變化。在這裏，我們也證實五款新型號Network Box (S-25，S-35，S-85，M-255 和 M-285)得已成功發布和上市，正如我在上個月提出的那樣。此外，還將宣布Network Box Office系統對韓國語的支持。

打開第4頁，按照慣例將提供月度使用技巧的小提示，和關于本月軟件更新之一的周二補丁的簡單總結。

和以往一樣，如果您有任何的反饋，意見或者建議，我們都歡迎您隨時提出來。您也可以通過發送郵件到我們的郵件列表：

nbhq@network-box.com

聯系我們。或者當您下次在香港市區的話來隨時來我公司辦公室進行參觀指導。

您也可以通過加入或訂閱我們的安全響應Twitter 和我們保持聯系，網址是：

**twitter.com/networkboxhq**

Mark Webb-Johnson
CTO, Network Box Corporation
March 2010

NETWORK BOX

## The Root Zone will be DNSSEC Signed in July 2010

域名系統DNS（Domain Name System）是互聯網的重要組成部分，它負責提供將域名(如Google.com)解析成IP地址（如64.233.189.104)和資源定位服務。根區域的服務（即DNS樹的根）是由分布在全球各地的數百台服務器共同提供，這是互聯網基礎架構設施的重要組成部分，整體看來好似一個高度可靠的網絡。

但是，DNS也存在一些問題。像大多數未加密的互聯網服務一樣，它很容易受到中間人攻擊。不懷好意的黑客可以在DNS客戶端（比如說就是你）和DNS服務器（例如，互聯網上的服務器）之間改變DNS查詢的回複，並重定向到自己想要的地址（而不是您需要的正確的地址）。

根區域提供DNS系統的中心指數，所以特別容易受到這種類型的攻擊。攻擊者可以改變根區域回複的能力允許它改變互聯網上的任何DNS名稱。

該解決方案是DNSSEC。維基百科給了它很好的定義：由互聯網工程任務組（IETF）定義的確保基于互聯網協議（IP）網絡中使用的域名系統（DNS）提供特定類型信息的一整套安全規則。它是對DNS提供的DNS客戶端（解析器）的（1）域名系統(DNS)數據的原生認證、（2）數據完整性驗證，但非可用性或機密性和（3）拒絕存在認證的擴展集。

域名系統安全擴展允許DNS服務器的答複使用公共密鑰加密進行數字簽名。然而保護IP地址是我們的首要關注，DNSSEC可以保護在域名系統中存儲的任何資料（包括給電子郵件使用的，從而有可能以此DNSSEC作為電子郵件的世界性公鑰基礎設施）。

域名系統安全擴展不提供數據保密功能；DNSSEC的回複經過了認證過程，但是沒有得到加密。

Map
Satellite
Hybrid
Legend
Multiple instances
Single instance
Google

Global Network of Root DNS Servers

首先，DNSSEC的全面部署最關鍵的一步，就是負責管理根區域的當局已經宣布了DNSSEC部署到一級根區服務器的時間表。它開始于2009年12月，計劃于2010年7月完成全面部署。

雖然一些區域（如.GOV和.ORG）的頂級域名已經開始采用域名系統安全協議有一段時間，一旦根區域完成了DNSSEC的全面部署，預計有更多的二級子區域（如.com等）將遵循這套規則。

一個曆史遺留問題是，DNS服務器已被限制為512字節長的UDP數據包，而DNSSEC要求數據包的字節數更大一些。當根區域被簽署之後，許多答複數據包將大于512字節，這將不被一些過時的防火牆接受。您的域名查找仍可能通過這種防火牆繼續工作，但是卻並不能像它們應該提供的那麼足夠快速和高效。在根區域逐漸被簽署的過程中，所有的遞歸域名服務器將有可能受到影響。

每台NBRS-3.0 Network Box都包括一個完整的遞歸域名服務器，完全兼容DNSSEC，響應大于512字節和新簽署的根區域。我們建議所有客戶使用箱子上的域名服務器作為首要域名服務器，這樣可以獲得兼容性好、快速和穩健的服務，以滿足關鍵需要。請和您本地的NOC取得聯系獲取更多詳細信息。

**Planned High Level Timeline**
**(tentative and subject to change)**

| | |
|---|---|
| 1st Dec 2009 | Root zone signed for internal use by VeriSign and ICANN. ICANN and VeriSign exercise interaction protocols for signing the ZSK with the KSK. |
| Jan 2010 | The first root server begins serving the signed root in the form of the DURZ (deliberately unvalidatable root zone). The DURZ contains unusable keys in place of the root KSK and ZSK to prevent these keys being used for validation. |
| Early May 2010 | All root servers are now serving the DURZ. The effects of the larger responses from the signed root, if any, would now be encountered. |
| May & Jun 2010 | The deployment results are studied and a final decision to deploy DNSSEC in the root zone is made. |
| 1st Jul 2010 | ICANN publishes the root zone trust anchor and root operators begin to serve the signed root zone with actual keys – The signed root zone is available. |

## Testing for DNSSEC Compatibility

來自ISC的Mark Andrews發表了一些有用的測試，您可以運行它來看看你的網絡是否同根區域DNSSEC相兼容並且有無准備好。這些測試依賴于L.ROOT- SERVERS.NET服務器，它們已經切換到根區簽署的副本，並且在類UNIX操作系統上使用'dig'通用工具。這些測試的有效期為未來數個月，所以我們建議您在2010年7月之前運行它們（或類似的測試）。

1. You should first test that a basic DNS lookup works:

```
$ dig +nodnssec +norec +ignore ns . @L.ROOT-SERVERS.NET

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9367
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 15
```

2. If that works, you can then test for answers greater than 512 bytes (notice the RRSIG response containing the new DNSSEC digital signature):

```
$ dig +dnssec +norec +ignore ns . @L.ROOT-SERVERS.NET

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60117
;; flags: qr aa; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 21
. 518400 IN RRSIG NS 8 0 518400 20100307080000 20100228070000 23763...
```

3. If that works, you can then test for responses greater than 1500 bytes (notice the additional DNSKEY and NSEC records in the response):

```
$ dig +dnssec +norec +ignore any . @L.ROOT-SERVERS.NET

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61647
;; flags: qr aa; QUERY: 1, ANSWER: 21, AUTHORITY: 0, ADDITIONAL: 21
. 518400 IN RRSIG NS 8 0 518400 20100307080000 20100228070000 23763...
. 86400 IN DNSKEY 256 3 8 ...THIS/IS/AN/INVALID/KEY/...
...
. 86400 IN NSEC ac. NS SOA RRSIG NSEC DNSKEY
```

4. If that works, you can then test for outbound TCP/IP DNS requests:

```
$ dig +dnssec +norec +vc any . @L.ROOT-SERVERS.NET

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5409
;; flags: qr aa; QUERY: 1, ANSWER: 21, AUTHORITY: 0, ADDITIONAL: 21
. 518400 IN RRSIG NS 8 0 518400 20100307080000 20100228070000 23763...
. 86400 IN DNSKEY 256 3 8 ...THIS/IS/AN/INVALID/KEY/...
...
. 86400 IN NSEC ac. NS SOA RRSIG NSEC DNSKEY
```

For each of the above tests, the 'dig' command will return a footer showing query time and response message size. You can verify these to ensure they make sense and that the query response time is acceptable.

```
;; Query time: 384 msec
;; SERVER: 199.7.83.42#53(199.7.83.42)
;; WHEN: Mon Mar  1 09:56:36 2010
;; MSG SIZE  rcvd: 1906
```

如果上述所有測試都通過了，你可以有理由相信，您的網絡對DNSSEC已有准備，只等根區域的服務器進行遷移了。

請注意，在今後幾個月，作為我們為您提供的管理服務的一部分，Network Box營運中心將從Network Box本身上進行這些測試（以確保電信供應商和上遊設備不幹擾這個流量，而且你的Network Box和網關將兼容即將到來的變化）。

不過，我們建議您還是應該從您自己的內部網絡（服務器和/或工作站）進行這些（或類似的）測試，以確保對這個新安排你沒有任何內部問題。

## S-25, S-35, S-85, M-255 and M-285 Now Available

With zero moving parts, Gigabit ethernet ports, and blindingly fast Intel processors, the S-series models set the yardstick for performance and reliability in this class of device. Offering a truly unique design, the usual CPU/motherboard layout is inverted - turning the top of the case into a heat sink and requiring no fan).

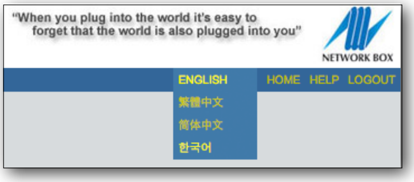
The M-255 and M-285 models utilise low power and low heat technology to deliver outstanding performance. Utilising Intel Celeron and Pentium Mobile technology, coupled with intelligent fan control, these models minimise noise and heat, while maximising performance.

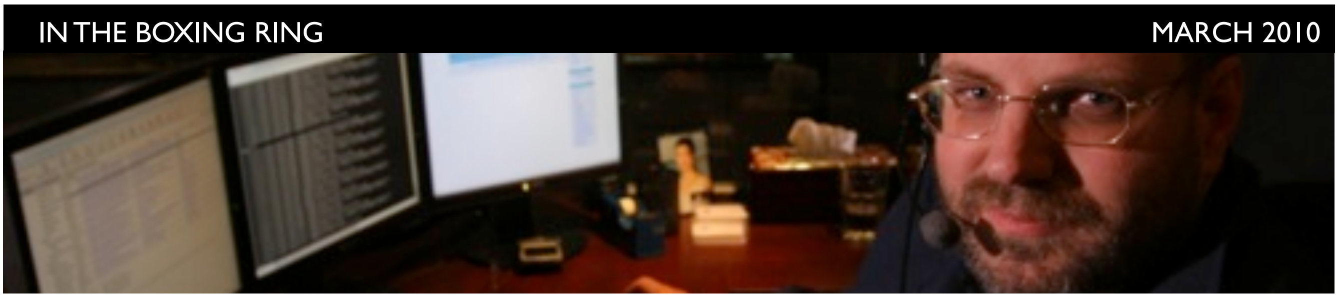
All five models are now available.

## Multi-Lingual Box Office and my.network-box.com

We are pleased to announce that this month we have extended Korean language support to the Box Office support portal. This means that we now support English, Simplified Chinese, Traditional Chinese and Korean in both Box Office and my.network-box.com interfaces.

We continue to work on native foreign language support in all our systems, to allow our customers to work in the languages they feel most comfortable in. Our approach is to provide local regional NOCs for support in the local timezone and local language (rather than a centralised English-only support centre), but with centralised policy control and oversight.


"When you plug into the world it's easy to forget that the world is also plugged into you"
NETWORK BOX
ENGLISH
繁體中文
簡体中文
한국어
HOME
HELP
LOGOUT



## March 2010 Features

On Tuesday, 2nd March 2010, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Finalisation of the firmware support for the new S-25, S-35, S-85, M-255 and M-285 models.
- Enhancements to my.network-box.com to better support some date ranges and better validate entry of invalid date ranges.
- Enhancements to my.network-box.com to improve the display of NTP status where the Network Box is an NTP server for some versions of Microsoft windows used on servers and workstations in the LAN/DMZ.
- Renewal of the SSL certificate used for my.network-box.com and improvements in the handling of client certificate requests in the Mail Portal interface (when accessed over encrypted SSL sessions).
- Improvements to the automatic housekeeping of the database by periodic optimisation of data storage.
- Minor fixes to the logging system, when configured to send log events externally via email and syslog protocols.

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 NOC will contact you to arrange this if necessary.

## March Hint: Policy Review

新年伊始，我們在顯示板上看到本月的威脅有了不少上漲。其中垃圾郵件上升22.8%，防火牆探測上升4.1%，入侵企圖上升7.1%，惡意代碼上升 84.8%，URL訪問阻斷上升3.5%，而且在上個月，我們推進更新了幾乎兩倍于前一個月的簽名更新。這在延續我們已經在過去幾年看到的趨勢。

在這種不斷惡化的威脅環境下，我們建議我們的客戶定期進行政策審查。一些值得思考的事情例子如下：

* 您真的需要在郵件附件中接受EXE文件嗎？

* 能否更嚴格地執行安全策略以限制不良網站（如黑客、暴力和惡意代碼）的訪問？

* 您有使用系統可用的所有功能（如谷哥安全浏覽等）嗎？

您可以隨時從my.network-box.com網絡界面看到你目前的安全政策，在郵件/狀態/政策綜述中了解電子郵件的安全策略，在Web代理/配置中了解內容過濾策略。請記住，這是你的策略 - Network Box只是給你執行這些策略，我們的安全運維中心在那裏幫助您配置網關，以便能更有效地執行該策略。

和以往一樣，如果你對此有任何疑問，請與您當地的NOC取得聯系尋求幫助。

Mark Webb-Johnson,  
CTO, Network Box Corporation

## FEBRUARY 2010 NUMBERS

| Key Metric) | # | % difference (since last month) |
|---|---|---|
| PUSH Updates | 1,339 | -9.8 |
| Signatures Released | 251,291 | +87.3 |
| Firewall Blocks (/box) | 665,742 | +4.1 |
| IDP Blocks (/box) | 202,114 | +7.1 |
| Spams (/box) | 53,753 | +22.8 |
| Malware (/box) | 2,472 | +84.8 |
| URL Blocks (/box) | 80,328 | +3.5 |
| URL Visits (/box) | 3,401,814 | +30.7 |

## 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