

In The Boxing Ring



IN THIS ISSUE

2.

ROOT ZONE DNSSEC

We present the timeline for the migration of the DNS Root Zone to DNSSEC. The Domain Name System (DNS) provides one of the core foundational services on today's Internet, but is susceptible to cache poisoning and man-in-the-middle attacks. The solution to this is the deployment of DNSSEC technology, and that deployment is happening now.

3.

DNSSEC SUPPORT TESTS

Four simple tests (published by Mark Andrews, of ISC) that you can conduct to check your compatibility and readiness for the upcoming DNSSEC changes to the DNS Root Zone servers.

3.

NEW MODELS AND MULTI-LINGUAL BOX OFFICE

The launch and availability of the S-25, S-35, S-55, M-255 and M-285 models, as well as Korean support in Box Office.

4.

MARCH 2010 FEATURES

As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features to all NBR3.0 customers.

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

Welcome

Welcome to the March 2010 edition of 'In the Boxing Ring'. In this edition, I'll be concentrating on some very important upcoming changes to the Domain Name System that we must all plan and check support for. I'm also excited to confirm the release and availability of the five new box models I outlined last month.

On page 2, we present the timeline for the migration of the DNS Root Zone to DNSSEC. The Domain Name System (DNS) provides one of the core foundational services on today's Internet, but is susceptible to cache poisoning and man-in-the-middle attacks. The solution to this is the deployment of DNSSEC technology, and that deployment (to the Root Zone servers, as well as other sub-zone servers) is happening now. We must all take steps to prepare for this, and to ensure that our networks are not adversely affected by this change.

On page 3, we present you with four simple tests (published by Mark Andrews, of ISC) that you can conduct to check your compatibility and readiness for the upcoming DNSSEC changes to the DNS Root Zone servers. Here, we also confirm the launch and availability of the five new

models of Network Box (S-25, S-35, S-85, M-255 and M-285) that I presented last month, and announce Korean language support in the Network Box Office system.

On page 4, we present the usual monthly hint, 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

March 2010



The Root Zone will be DNSSEC Signed in July 2010

The Domain Name System (DNS) provides one of the core foundational services on today's Internet. It is primarily responsible for converting names (e.g.; google.com) to IP addresses (e.g.; 64.233.189.104) and vice-versa. The serving of the 'root zone' (i.e.; the root of the DNS tree) is a critical part of this infrastructure delivered by a collection of hundreds of servers distributed across the globe, all seen as one highly reliable network.

However, DNS has a problem. Like most unencrypted Internet services, it is vulnerable to man-in-the-middle attacks. A malicious hacker, with the ability to position equipment between the DNS client (i.e.; you) and DNS server (i.e.; a server on the Internet) can alter DNS replies and redirect you to an address of his own choice (rather than the correct address you required).

The Root Zone acts as the central index for the DNS system, and is particularly susceptible to this type of attack. An attacker able to alter replies from the Root Zone has the ability to change any DNS name on the Internet.

The solution is DNSSEC. Wikipedia defines this nicely as a suite of [Internet Engineering Task Force \(IETF\) specifications for securing certain kinds of information provided by the Domain Name System \(DNS\) as used on Internet Protocol \(IP\) networks. It is a set of extensions to DNS which provide to DNS clients \(resolvers\) origin authentication of DNS data, data integrity, but not availability or confidentiality, and authenticated denial of existence.](#)

DNSSEC allows DNS server replies to be digitally signed using public key cryptography. While protecting IP addresses is our primary concern, DNSSEC can protect any information stored in the DNS system (including those used for email, making it possible to use DNSSEC as a worldwide public key infrastructure for email).

DNSSEC does not provide for the protection of confidentiality of data; DNSSEC responses are authenticated but not encrypted.



Global Network of Root DNS Servers

As the first, critical, step on the path to full deployment of DNSSEC, the authorities responsible for the management of the Root Zone have announced a high-level timeline for deployment of DNSSEC to the Root Zone servers. This started in December 2009 and is planned to complete full deployment by July 2010.

While some zones (such as .gov and .org) have historically been signed for some time now, once the Root Zone has completed full deployment of DNSSEC, it is anticipated that more sub-zones (such as .com, etc) will follow suite.

One issue is that historically DNS servers have been restricted to 512 byte UDP packets, and DNSSEC requires longer packets for its replies. When the root is signed, many of the responses will be larger than 512 bytes and some outdated firewalls will no longer accept them. Your domain name lookups may still work through such firewalls, but not as fast or as efficiently as they should. With the Root Zone now being signed, all recursive name servers will potentially be impacted.

Each NBR3-3.0 Network Box includes a full recursive name server, fully compatible with DNSSEC, responses bigger than 512 bytes, and the new signed Root Zones. We recommend that all customers use this on-the-box name server as their primary name server, to gain the compatibility, speed and robustness required for this essential service. Please discuss with your local support NOC for more information.

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

Mark Andrews, of ISC, has published some useful tests that you can run to see if your network is compatible and ready for DNSSEC on the Root Zones. These tests rely on the fact that the L.ROOT-SERVERS.NET servers have already switched to a signed copy of the root zone, and use the 'dig' tool common with Unix-like operating systems. The tests should be valid for the next few months, and we recommend you run these (or something like them) before July 2010.

```

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
    
```

Should all the above tests pass, you can be reasonably confident that your network is ready for DNSSEC and the coming migration of the Root Zone servers.

Note that over the coming months, Network Box operation centres will, as part of our managed service for you, be conducting these tests from the Network Box itself (to ensure that the ISP and upstream devices are not interfering with this traffic, and your Network Box and gateways will be compatible with the upcoming changes).

However, we recommend that you should still conduct these (or similar) tests from your own network (servers and/or workstations), to ensure that you don't have any internal problems with this new arrangement.

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.

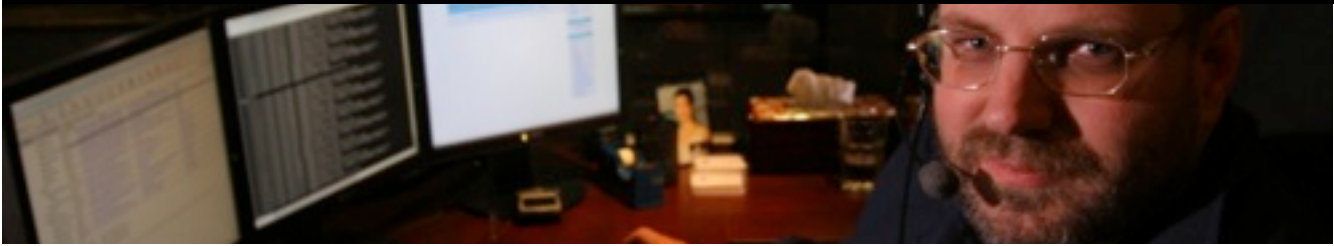


Multi-Lingual Box Office and my.network-box.com

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.





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

As the new year settles in, we're seeing threats up this month across the board. Spams +22.8%, Firewall probes +4.1%, Intrusions +7.1%, Malware +84.8%, URL blocks +3.5%, and last month we PUSHed out almost twice as many signature updates as we did the month before. This continues the trend that we've seen in past years.

In light of this continually worsening threat landscape, we suggest our customers periodically conduct a policy review. Some examples of things to think about:

- Do you really need to accept EXE files as mail attachments?
- Can you be more restrictive against 'core' category sites (such as hacking, criminal, malware)?
- Are you using all the features of the system available to you (such as Google Safe Browsing, etc)?

You can always see your current policy in the my.network-box.com web interface, under Mail / Status / Policy Summary for eMail and Web Proxy / Config for the web. Please remember that this is your policy - Network Box is merely enforcing it for you, and our NOCs are there to help you configure the gateway to effectively perform that enforcement.

As always, if you have any questions, please contact your local NOC for clarification.

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