Infoblox
CONTROL YOUR NETWORK

WHITE PAPER

Best Practices DNSSEC Zone Management on the Infoblox Grid

What Is DNSSEC, and What Problem Does It Solve?

DNSSEC is a suite of Request for Comments (RFC) compliant specifications developed by the Internet Engineering Task Force (IETF) for securing information provided by DNS. These extensions provide DNS resolvers with:

- Origin authentication of data
- Authenticated denial of existence
- Data integrity for responses

DNSSEC is just one of a number of key DNS security tools that should be used in combination to handle today's various cyberattacks. Defense-in-depth approaches now include DNS infrastructure, and DNSSEC is one crucial part in securing DNS.

Malicious tactics such as social engineering, DNS hijacking, and cache poisoning can be used to cause Internet users to load websites that aren't the ones they asked for. This is detrimental to the brand and potentially costly for the owners of legitimate websites to which requests are misdirected. It primarily serves as a way to direct web users to malicious sites that distribute malware.

But DNS does more than simply tell web browsers where to go. It is used for many other Internet protocols too, including data published in DNS for security systems that reference cryptographic certificates such as certificate records (CERT records, SSH fingerprints, IPSec public keys, and TLS trust anchors). Even email has a significant dependency on DNS as it utilizes mail exchange (MX) records to determine how to deliver email for a given address. Being able to modify DNS responses makes it possible to control all of these parameters, including where mail is sent.

To protect against having your email hijacked, at the client level you can use end-to-end encryption using PGP or S/MIME. This doesn't guarantee delivery to the intended recipient, but does mean that no one else can read the content of the email. At the server level, the issue is solved by DNSSEC, which guarantees integrity of the DNS responses.

What DNSSEC Does and Doesn't Do

The Internet is a broad communications architecture for clients to access server applications. DNSSEC protects applications and DNS caching resolvers from using forged or manipulated DNS data, like that created by DNS cache poisoning. By design, all responses from a DNSSEC protected zone are digitally signed, using public-key cryptography. When a client or requestor receives the digitally signed zone from the owner of domain DNS, the client can rest assured that a chain of trust has been established at the top level down to the client, and the application or web page that is now presented is authenticated at its origin, is registered at the top-level domain (TLD), and the individual DNS record response is guaranteed to be accurate and true. Simply put, DNSSEC makes DNS responses more trustworthy and secure.

It is also important to mention what DNSSEC does not do. DNSSEC does not provide DDoS protection, availability, data encryption, or confidentiality. Using general Internet traffic as an example, where a client has requested an A record from a company, the DNS response is still visible by a "man in the middle." The difference is when DNSSEC is enabled and checks the digital signature, a DNS resolver is able to determine whether the information is identical (unmodified and complete) to the information published by the zone owner and served on the domain DNS server.

How It Works

DNSSEC works by digitally signing records for DNS lookup using public-key cryptography. The correct DNSKEY record is authenticated via a chain of trust, starting with a set of verified public keys for the DNS root zone, which is the trusted third party. Domain owners generate their own keys, and upload them using their DNS control panel at their domain-name registrar, which in turn pushes the keys to the zone operator (for example, DotGov for .gov, and Verisign for .com) who signs and publishes them in DNS.

There are two key pairs (private/public) that are important for the chain of trust. One is the Key-Signing Key (KSK), which zone operators upload to their registrars. The other is the Zone-Signing Key (ZSK), which is maintained on the domain owner's primary and secondary name servers.

The Unique Infoblox DNSSEC Implementation

Infoblox's focus on management, automation, and control has greatly simplified the process of using DNSSEC so that lower-level DNS administrators can enable and deploy quickly and more securely than they were able to do using command-line interfaces (CLIs). Infoblox has reduced much of the complexity of DNSSEC down to 3 key steps:

1. Enable DNSSEC in the GUI once (in the DNS Grid Properties).
2. Initially sign DNS zones to generate private and public keys.
3. Export and upload signed keys to a trusted TLD registrar.

This is a stark contrast to the 16+ steps required on a general-purpose server running DNS—such as Microsoft Windows or LINUX/BIND—where multiple root-level scripts are required to enable DNSSEC and then again every time a zone or record changes. Management is simplified with the Infoblox Grid™, enabling administrators to manage multiple appliances from a central console, eliminating the need to bounce from one server to another. Filters and Smart Folders aid in grouping DNSSEC signed zones to check status and key rollover dates.

Automation is built in so that initial National Institute of Standards and Technology (NIST) settings are pre-configured and changes can be made using a few check box controls with drop-down menus. Instead of running root-level scripts for both KSKs and ZSKs, Infoblox automates the processing of signing the keys and placing them in the appropriate location for use. Infoblox also automates the storage of keys onto your hidden primary DNS server (Grid Master) or off the Grid to a hardware security module (HSM).

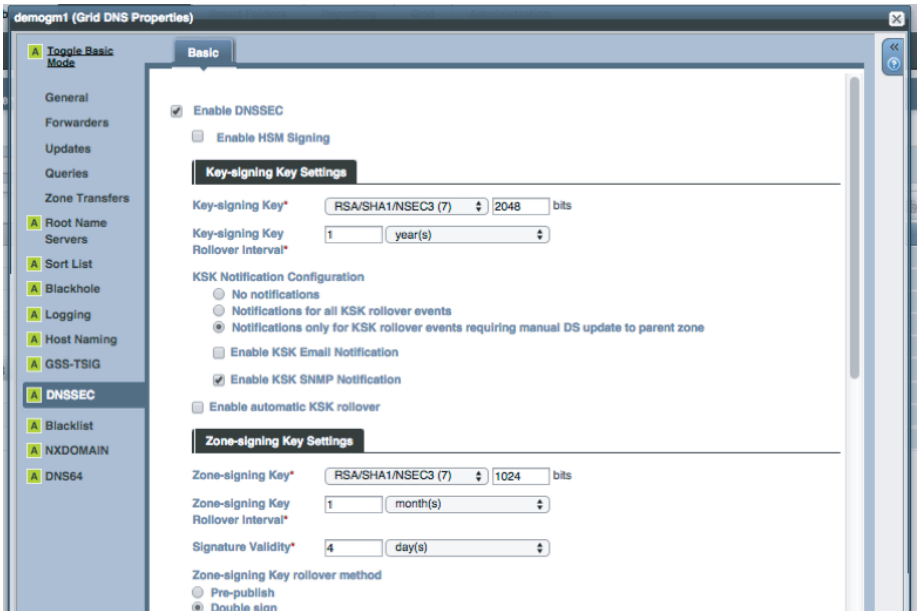

Figure 1. Properties such as key settings and notifications are easily assigned.

A wizard makes it possible to initially sign zones one at a time or in batches. Trust anchors and KSKs can be exported by zone and uploaded to a TLD registrar. After keys have been uploaded to the TLD registrar, DNS administrators can renew them once a year. Administrators need little training to implement Infoblox DNSSEC because the process of managing DNS zones and records stays the same for DNSSEC zone management as it does for DNS.

Architectural Considerations

DNSSEC uses an additional set of record types (RRSIG, DNSKEY, DS, NSEC, NSEC3, NSEC3PARAM) that all hold digital key signatures. The following is a general set of considerations when deploying DNSSEC:

- Zone size will increase significantly when signed.
- Memory and CPU usage increase.
- DNSSEC answers are large.
- Interference may be caused by firewalls, proxies, and other middleware.
- Fallback to TCP is greater for DNSSEC than it is for UDP for DNS alone.
- Modern resolvers already ask for DNSSEC by default, but older clients and resolvers have to be identified and may need to have settings turned on to handle DNSSEC.

Setup and Maintenance

Infoblox first released full DNSSEC support in NIOS version 4.3r6 in October 2009. All subsequent versions of NIOS 5.x and NIOS 6.x fully support DNSSEC. In NIOS 6.11 Infoblox enhanced the feature set for DNSSEC, adding new automation, testing, and notification features. It is recommend that customers using, or planning to use DNSSEC, upgrade to NIOS 6.11.x to take advantage of new automation and security features.

Relationship with the TLD Registrar

Getting signed up

Domain administrators need to know the point of contact (POC) and the POC's login to access the TLD registrar site and manage the company's account. Registrars provide a place for uploading DNSSEC keys per zone into their sites. This is where DS (or trust anchors) are uploaded in the requested format.

Ongoing Relationship with the TLD

When administrators sign zones in DNSSEC, they are required to roll over KSKs on a regular basis (NIST standard recommends once a year.). Depending on the registrar, this is either a regular yearly manual process to upload new keys or an automated key monitoring service to pull the newly rolled over KSKs from appliances on a certain day every year before the old ones expire. If a company does not use this service, then it is the administrators' responsibility to remember and manually upload rolledover KSKs every year, per zone.

The registrar will hold and publish both keys (old and new) for a defined transition period (about two weeks), so that any caching resolvers will have time to update their caches. Having two keys is not a problem: the old one will be removed automatically by the registrar.

Securing Keys

KSKs and ZSKs are required to be stored in a secure place. If these keys are stolen or lost, administrators must re-sign DNSSEC zones immediately to ensure that the chain of trust is not jeopardized. Infoblox Grid technology automates keys stored centrally on the Grid Master, which we recommend to be the hidden or stealth primary DNS. This allows for the DNSSEC private keys to be concealed with no access (root or otherwise) inside the Grid Master. This meets the FIPS-140-1 standard compliance. For a higher level of compliance such as FIPS-140-2, Infoblox supports integration with HSMs so that the DNSSEC keys can be stored off the Grid serving DNSSEC. Today Infoblox supports HSM vendors SafeNet and Thales.

Enabling DNSSEC in the Infoblox Grid

DNSSEC is enabled one time for the entire Grid of appliances. If new appliances are connected to the Grid, they will automatically have DNSSEC enabled by default on the top-level Grid DNS Properties screen. Follow this path to navigate to DNSSEC within the UI.

Data Management > DNS > Grid DNS Properties > DNSSEC

On this screen default NIST Standard Best Practice settings are preconfigured in Infoblox. Most users other than government organizations can keep these default settings and just enable DNSSEC with a single check box.

Government agencies have an additional requirement defined by the registrar DotGov.gov to use a specific DNSSEC record type called "NSEC3." NSEC3 protects against hackers by preventing them from reading other zone files to learn about other records.

NSEC3 is enabled by choosing it from the drop-down boxes for KSKs and ZSKs. It comes in four algorithms for the DNSKEY record. Users can choose the security level policies for their agencies.

Users can choose the security level policies for their agencies.
Users select the algorithm of the DNSKEY record with NSEC3:

DSA/NSEC3,
RSA/SHA1/NSEC3,
RSA/SHA-256/NSEC3
RSA/SHA-512/NSEC3

Then DNSSEC validation is enabled. If an appliance is allowed to respond to recursive queries, this check box can be used to enable the appliance to validate responses to recursive queries for specified zones. The DNSKEY RR of each zone specified in the trust anchors shown in Figure 2 must be configured. Once DNSSEC is enabled, DNS service needs to restart.

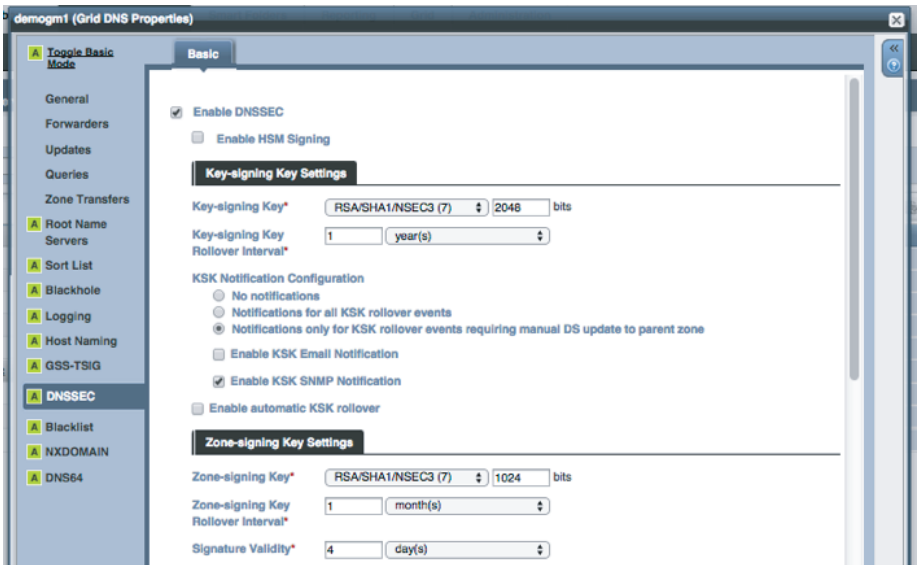

Figure 2. Configuring DNSKEY RR

Initial Signing Zones

Next each zone needs to be signed. To do this, go to:

Data Management > DNS > DNSSEC > Sign Zone

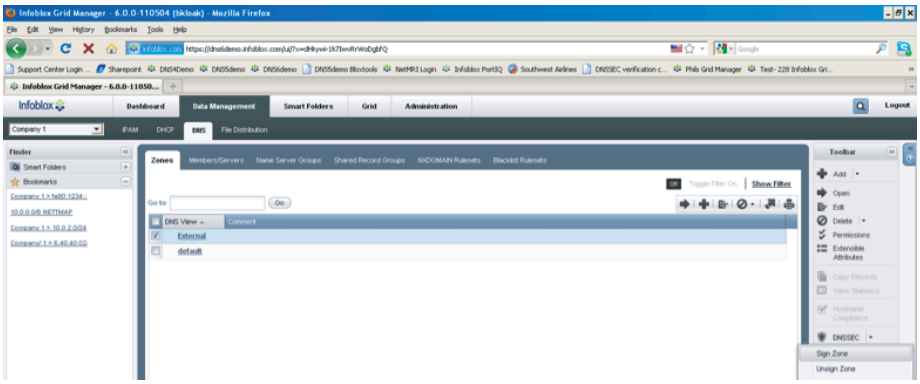

Figure 3. DNS zone view

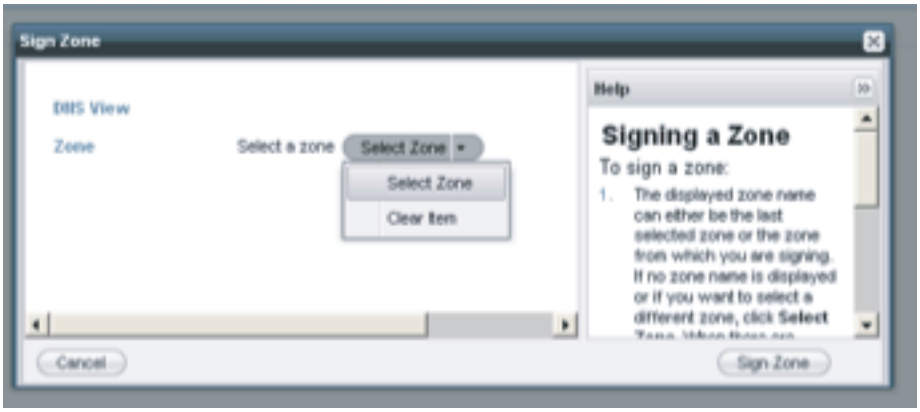

Figure 4. Zone selection view

When Sign Zone is selected, Infoblox will start a DNSSEC Signing Zone Wizard to help in the one-click zone signing process. Select a zone from the predefined DNS zone list already imported or configured in the appliance.

Once a zone is signed, it is not necessary to un-sign it during the course of its life. It stays signed and it is rolled over to keep the keys from getting stale.

DNSSEC Delegated Zone

To add a delegated zone, do the following:

Under **Data Management > DNS > DNS View > Zones**, click into the zone to create the delegated zone.

On the Toolbar, Click Add (with the drop-down arrow). Select Zone > Delegation

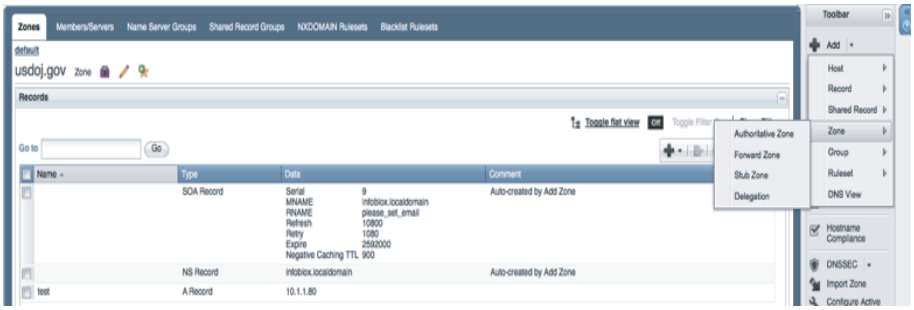

Figure 5. Zone delegation

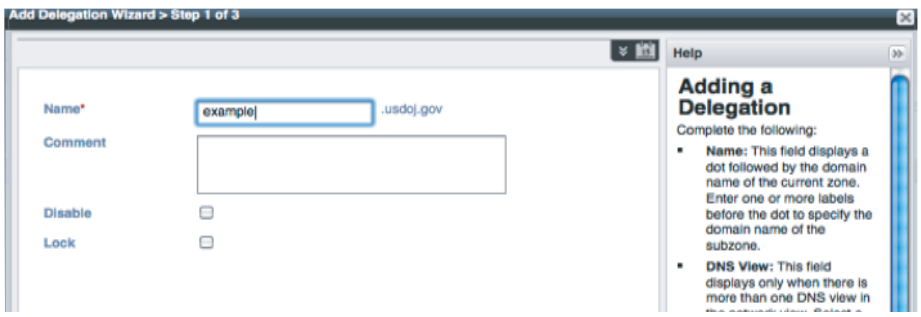

Figure 6. Zone naming

In the wizard, type in the name of the zone, and then click Next.
Click the + Sign to add the Delegated Name Server. Enter the Name and the IP address of the Delegated Zone Name Server. Then click Save & Close.

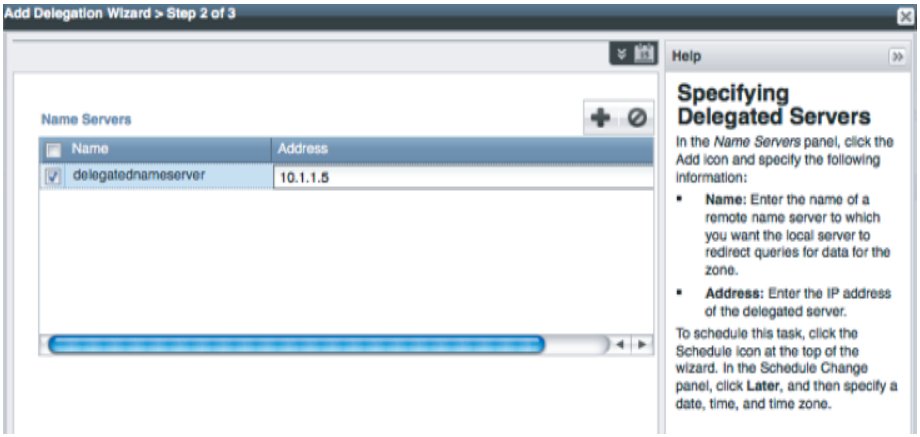

Figure 7. Zone management is a simple GUI-based process.

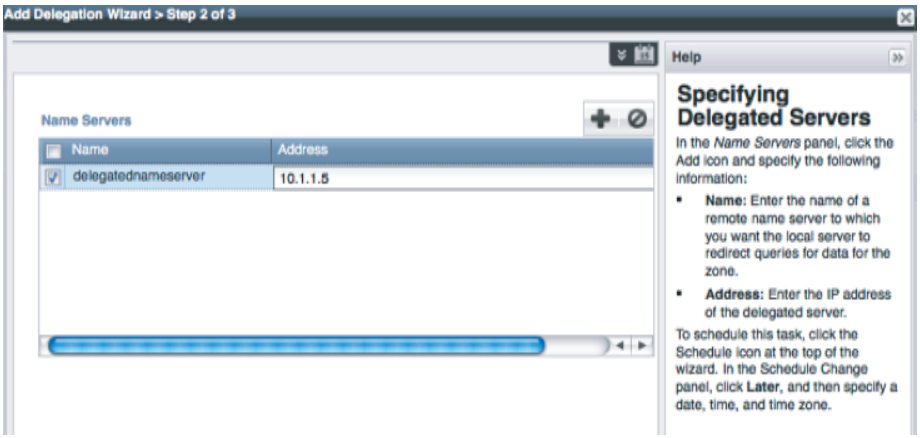

Figure 8. Importing keysets

On the Toolbar, Click DNSSEC (on the drop-down arrow) and select Import Keyset.
In the white box, paste the keyset or DSset received.
Click Import, and then restart DNS service.

Day-to-day DNSSEC Zone Management

After you sign a zone you will see the creation of many new resource records (called RRsets) that DNSSEC uses (RRSIG, DNSKEY, NSEC3), mixed in with your existing DNS records. You do not need to modify or edit these new DNSSEC records directly; they are maintained in Infoblox automatically for you.

Just continue to work with DNS records (A, PTR, MX, NS, TXT, etc.) as you have in the past. A change to an A record will automatically update the corresponding DNSSEC RRSIG RRset for you.

Yearly KSK Rollover(s) of DNSSEC Zones with the TLD

The KSK rollover period is set on the GRID DNS Properties > DNSSEC enable screen. Once you establish the rollover period and sign your initial zone, the clock will start counting down.

Two weeks before your KSK is set to expire, Infoblox will send an email to the administrator that your KSK key needs to be rolled over. If you have signed up for the DotGov.gov "Key Monitoring Service," all you will need to do then is roll over the KSK in the Infoblox GUI. To rollover your key go to:

Data Management > DNS > DNSSEC > Roll Over Key-Signing Key

Once you do this, the Key Monitoring Service will pull the KSK key from your Infoblox appliance automatically on the date you set up with the service.

Summary

DNSSEC is an important security element that can help prevent a number of DNS related issues. DNSSEC is just one of a number of key DNS security tools that should be used in combination to handle today's various cyber-attacks. Defense-in-depth approaches now include DNS infrastructure, and DNSSEC is one crucial part in securing DNS. The Infoblox implementation makes it simple to:

- Enable DNSSEC
- Initially sign DNS zones and generate private and public keys
- Export and upload signed keys to a trusted TLD registrar

The process is aided by simple-to-use wizards that walk the user through the steps and automation to be more efficient and accurate. To learn more about Infoblox solutions visit our website at www.Infoblox.com.

CORPORATE HEADQUARTERS
+1.408.986.4000
+1.866.463.6256
(toll-free, U.S. and Canada)
info@infoblox.com
www.infoblox.com

EMEA HEADQUARTERS
+32.3.259.04.30
info-emea@infoblox.com

APAC HEADQUARTERS
+852.3793.3428
sales-apac@infoblox.com