



DNSX SECURE RESOLVER
DNSSEC MANAGEMENT SOLUTION



What is DNSX Secure Resolver?

Xelerance DNSX Secure Resolver is a DNSSEC caching and resolving nameserver with full support for DNSSEC Lookaside Verification (DLV).

It features the latest in hardening and security measures for DNS and provides an intuitive web management interface, making configuration and key management easy.

Advanced DNS features

In addition to performing basic DNS resolving and DNSSEC validation, DNSX Secure Resolver protects against cache poisoning and DNS spoofing attacks, as seen with the now infamous Kaminsky Attack.

It protects against DNS rebinding and Domain Fast Flux attacks and includes countermeasures to prevent abuse in a DNS amplification or DNS reflection attack.

In the fast paced world of the internet it is important to not only be current, but to look ahead. DNSX Secure Resolver includes support for several internet drafts which have not yet turned into RFC standards, such as draft-vixie-dnsextdns-0x20-00 and draft-wijngaards-dnsextdns-resolver-side-mitigation-01 in addition to recently published DNS resilience recommendations from RFC-5452.

DNSSEC Options	
Enable DNSSEC Validation	<input checked="" type="checkbox"/>
Enable DNSSEC Lookaside Validation (DLV)	<input checked="" type="checkbox"/>
DLV Registry	<input type="text" value="dlv.isc.org."/>
Kaminsky Attack Protection	
Additional infrastructure DNS verification	<input checked="" type="checkbox"/>
Remove unsigned additional data from signed data	<input checked="" type="checkbox"/>
Enable 0x20 Bit protection (draft-vixie-dnsextdns)	<input checked="" type="checkbox"/>
Cache Poisoning Protection	
Clear cache after excessive bogus replies	<input checked="" type="checkbox"/>
Number of bogus packets until clearing cache	<input type="text" value="10000000"/>
Number of randomised source ports to use	<input type="text" value="1024"/>
Denial of Service Protection	
Drop excessively small and large packets	<input checked="" type="checkbox"/>
<input type="button" value="Save"/>	

DNS and DNSSEC configuration made easy

DNSSEC Features

DNSX Secure Resolver is designed to work with a signed or unsigned root and supports the ICANN (IANA) "Interim Trust Anchor Repository" for TLD's. It supports a customizable DLV Registry which defaults to the Internet Software Consortium DLV Registry.

It implements RFC-5011 for Trust Anchor rollover procedures used for updating DNSSEC keys. In addition, custom or company DNSSEC keys can be maintained according to local policy.

Network features

IPv4 and IPv6 are fully supported on the DNSX Secure Resolver. Multiple Ethernet links can be used to multiple uplink providers, enabling automatic failover and providing additional cache poisoning protection.

An unlimited number of IP addresses can be specified to add further protection against cache poisoning. Individual domains can be blacklisted using a DNS override, or redirected at the requests of Law Enforcement Agencies. Local corporate zones can be transparently forwarded to corporate Authorative Nameservers.

Cache Inspection

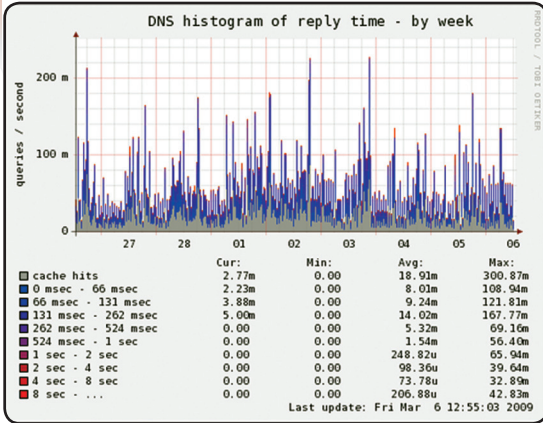
The entire DNS cache can be downloaded for inspection and debugging. The web interface allows for easy testing of an individual query to determine why a certain DNS query has given a particular result.



"DNSSEC needs to be far more automated than it is today. The Xelerance DNSX appliances address this issue"
-- Dan Kaminsky

Monitoring

Statistics on memory usage, types of queries, errors, cache hits, and response times are updated every minute and available via the web interface.



DNSSEC without a signed Root

DNSX Secure Resolver supports updating TLD keys for DNSSEC via its automatic update service in addition to the RFC-5011 Trust Anchor update protocol.

To facilitate these updates, Xelerance monitors the worldwide DNSSEC deployment using real time DNS tracking and third party Trust Anchor Repository verification.

Status	Zone	Key id	Type	Revoked	Alg	Public Key
<input type="checkbox"/>	bg.	61993	KSK	-	RSASHA1	AwEAAcHs [...]+8hrbDO3
<input checked="" type="checkbox"/>	br.	18457	KSK	-	RSASHA1	AwEAAAdo [...]+Npy6AM=
<input checked="" type="checkbox"/>	cz.	7978	KSK	-	RSASHA1	AwEAAAdo9 [...]+MnktuM=
<input checked="" type="checkbox"/>	dnsops.biz.	53377	KSK	-	RSASHA1	AwEAAAd20 [...]+EYHmwak=
<input checked="" type="checkbox"/>	dnsx.xelerance.com.	38478	KSK	-	RSASHA1	BQEAAAAB [...]+Wkw8+Q==
<input checked="" type="checkbox"/>	gov.	28079	KSK	-	[unknown]	AwEAAAZ10 [...]+4Hf2aM8=
<input checked="" type="checkbox"/>	museum.	39226	KSK	-	RSASHA1	AwEAAAd4F [...]+2Cwm2E=
<input checked="" type="checkbox"/>	pr.	62704	KSK	-	RSASHA1	AwEAAAc6S [...]+xuMuDOSr
<input checked="" type="checkbox"/>	se.	6166	KSK	-	RSASHA1	AwEAAAb6x [...]+9ELFN6k=
<input checked="" type="checkbox"/>	se.	8779	KSK	-	RSASHA1	AwEAAeeG [...]+yQgsTlc=
<input checked="" type="checkbox"/>	se.	49678	KSK	-	RSASHA1	AwEAAAdKc [...]+UKNB8Qc=
<input checked="" type="checkbox"/>	0.4.1.0.0.2.jp6.arpa.	17191	KSK	-	RSASHA1	AwEAAAcxA [...]+c1bFA8=

DNSSEC keys for TLDs can be listed and modified

Cryptographic Acceleration

DNSSEC validation consists of performing chains of cryptographic operations. These operations are offloaded to an onboard hardware cryptographic accelerator.

Deployment in existing organizations:

DNSX Secure Resolver is designed to operate in both stand-alone or forwarding mode. In forwarding mode, it provides protection to your currently deployed non-DNSSEC resolvers.

This versatility makes DNSX Secure Resolver a perfect fit for any type of network, ranging from small sized WANs and LANs to large scale ISP deployments.



Corporate DNSSEC keys

DNSX Secure Resolver supports several methods of loading corporate DNSSEC keys. Keys can be obtained via DNS, web management uploads or trusted URL.

Add DNSKEY from DNS

Add DNSKEY for Zone:

Optional nameserver to use:

Add DNSKEY(s) from URL

Specify URL:

Add DNSKEY via File Upload

Select local file:

Three easy ways to add DNSSEC resolver keys

DNSX Secure Resolver allows you to handle the increased DNSSEC administration without the cost of additional staff.

Partial DNSSEC deployment in TLD's

Support for partial DNSSEC deployment within unsigned TLD's, such as .com or .org, is accomplished through DNSSEC Lookaside Verification (DLV). DNSX Secure Resolver supports an easy configurable DLV, with the Internet Software Consortium (ISC) DLV as default.



Hardware Specification

CPU 1.5ghz VIA C7 Padlock/ACE
Hardware RNG On-Die Quantum Random Generator
Hardware Crypto VIA Padlock ACE (AES, RSA, SHA-1, SHA-256)
RAM 1 Gbyte

Storage

DNSX System 2Gbyte Solid State Disk

Peripherals

Ethernet 2x 10/100/1000
Display 2 line B/W with backlight and warning sounds

Implemented RFCs

DNSSEC RFCs 3225, 3226, 3597, 4025, 4033, 4034, 4035, 4509, 4956, 5155, [2535]
DLV RFCs 4431, 5074
Trust Anchor RFCs 4986, 5011
DNSSEC Records DNSKEY, RRSIG, NSEC, NSEC3, DS, DLV
Related Records SSHFP, IPSECKEY, CERT

Software Specification

OS Xelerance Linux Centos5 based
App Xelerance DNSX Secure Resolver 1.4

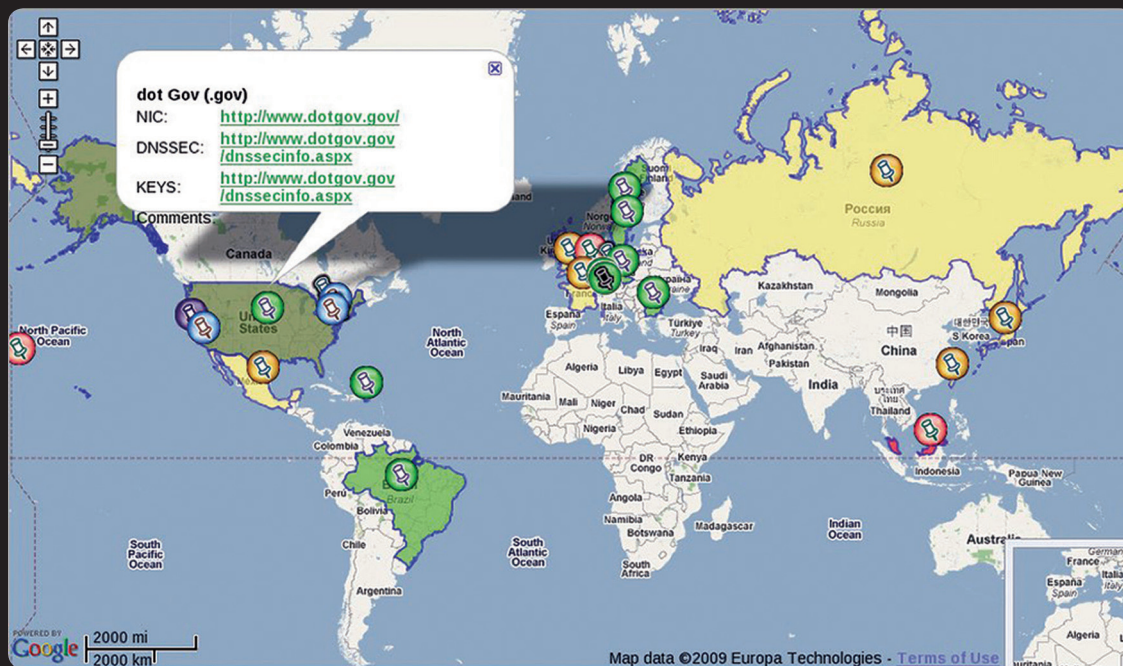
Only peer-reviewed open source cryptographic algorithm and cipher implementations are used in this product.

Cryptographic applications include IETF RFC compliant and NIST conforming cryptographic software from:

Xelerance Corporation	www.xelerance.com
Internet Software Consortium	www.isc.org
NLnetlabs	www.nlnetlabs.nl
Linux kernel CryptoAPI	www.linux.org
The Apache Foundation	www.apache.org
GNUPG	www.gnupg.org

Software license

Source code to all Free and Opensource Software is available for customers at <http://dnsx.xelerance.com/>



- TLD Production
- Reverse Production
- ccTLD Testbeds
- gTLD Testbeds
- DLV Registry
- Unofficial Projects
- Discontinued

Regulatory Compliance

UL Canada and the United States
NIST SP800-81 Secure Domain Name System (DNS) Deployment Guide
NIST SP800-53-R1 Recommended Security Controls for Federal Information Systems.
SP800-53-R2 (SC-21) Secure Name/Address Resolution Service (Recursive or Caching Service)

Trademarks

The product names used are for identification purposes only. All trademarks and registered trademarks are the property of their respective owners.