



**No IP. No Network.
No Mission.**

DNSSEC

Secure DNS for Government

DNSSEC - Secure DNS for Government BlueCat Networks' Public Sector Practice



Why DNSSEC?

DNS resolution assumes that answers received from remote DNS servers are always valid. As a result of the Kaminsky exploit in 2008, organizations are now realizing that this is not always true. DNS is susceptible to a number of attacks including cache poisoning that can be used to misdirect users to malicious sites. To help provide added security, the DNS Security Extensions (DNSSEC) were created to provide a method for validating DNS information. Organizations need to begin implementing DNSSEC to safeguard against DNS threats.

DNSSEC - How it works

DNSSEC is designed to protect DNS resolvers (clients) from forged DNS data, which occurs as the result of a DNS attack. DNSSEC secures DNS by signing all records hosted on the authoritative server using a cryptographic key to produce a digital signature. When a DNS resolver requests a DNS record, it also receives a digital signature of the record that was created by the cryptographic key. The resolver decrypts the signature using the associated public key to verify that the record it received is identical to the record on the authoritative server.

For example, as the administrator of the example.com domain, you have implemented DNSSEC and signed the resource records in example.com using your private key. When a client makes a request for www.example.com, it receives the signed DNS record. Using example.com's public key, the client's caching server (and by extension, the client) is able to verify that www.example.com was signed by its owner and is therefore valid.

Should someone attempt to compromise an organization's DNS server that was secured using DNSSEC, the client would receive an error. This prevents users from receiving poisoned DNS and increases the reliability that the records they receive from the DNS servers are authentic.

Why BlueCat?

BlueCat Networks has been providing secure DNS solutions since 2001. As a trusted advisor in DNS security, organizations look to BlueCat to help address their security concerns. As part of BlueCat Networks' dedication to security, BlueCat Networks added DNSSEC to its award winning Proteus and Adonis appliances. Through its support of DNSSEC, BlueCat provides organizations with the ability to easily deploy and maintain DNSSEC records and keys.

NOTE: DNSSEC does not provide confidentiality of data. It provides a means to authenticate DNS responses, but does not encrypt the information.



BlueCat Networks' DNSSEC Solutions

DNSSEC Resolution

DNSSEC Validation

BlueCat's appliances provide the ability to properly validate signed records from other DNSSEC enabled servers when configured to answer recursive queries for clients.

Trust Anchors

BlueCat provides the ability to configure Trust Anchors, which are used to validate responses from other authoritative name servers running DNSSEC signed zones.

BlueCat also supports the configuration of DLVs (Designated-Lookaside-Validators), allowing administrators to configure a single address of a server which contains many Trust Anchors, simplifying recursive configuration when chains of trust are not available.

DNSSEC Hosting

DNSSEC Resource Records

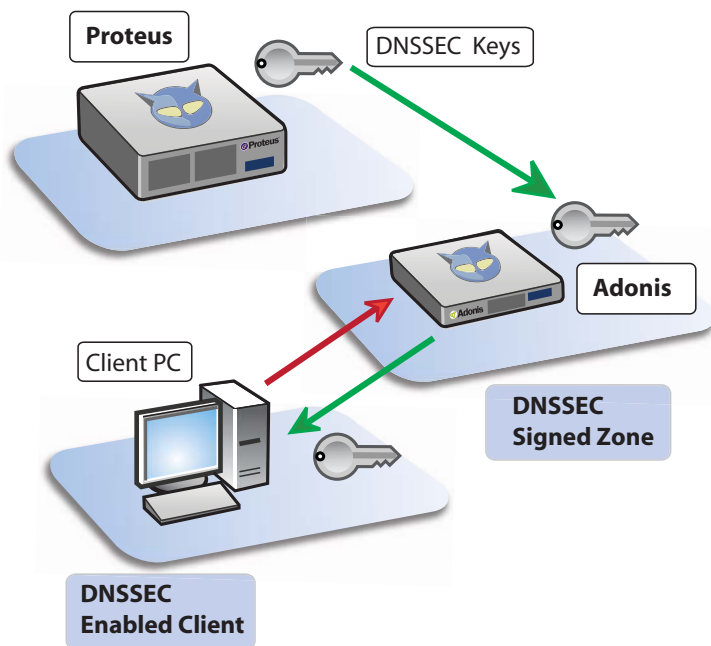
BlueCat supports all the required resource records needed to provide DNSSEC functionality for hosted authoritative domains including Resource Record Signatures (RRSIGs), DNSKEY, Next Secure (NSEC) Records, and Next Secure 3 Records (NSEC3).

Signing the Zone

BlueCat provides full support for DNSSEC Signed Zones using Zone Signing Keys (ZSK) and Key Signing Keys (KSK). Zone Signing Keys are used to sign the record within a zone – for example, the www host in the zone bluecatnetworks.com. Key Signing Keys are used to sign the keys themselves typically used outside the zone as the Trust Anchor. Within Proteus, both ZSKs and KSKs are generated automatically using zone policies.

Zone Signing Policies

BlueCat introduced one-click automatic zone signing in the Proteus 3.0 product, allowing administrators to configure a zone signing policy and apply it to any number of DNS zones. These policies allow the administrator to use Industry Standard National Institute of Standards and Technology (NIST) defaults for zone signing, or choose their own schedules to automate KSK and ZSK re-signing, and key rollover settings. Automated zone signing ensures that the zones are always signed and valid, eliminating the complexity and administrative overhead involved with manual DNSSEC maintenance.



DNSSEC Resolution with Adonis and Proteus