



**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 information received from remote DNS servers is always valid. As a result of the Kaminsky exploit from mid-2008, organizations are now realizing that this is not always true. DNS is susceptible to cache poisoning attacks 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, such as cache poisoning. DNSSEC secures DNS by signing all records hosted on the authoritative server, using a digital signature. When a DNS resolver requests a DNS record, it also downloads the DNSSEC key to verify that the record it received is identical to the record on the authoritative server.

For example, BlueCat Networks has implemented DNSSEC and signed all hosts for the bluecatnetworks.com domain using the private key of an asymmetric key pair. When a client makes a request for www.bluecatnetworks.com, they will receive the signed DNS record. Using BlueCat Networks' public key, they will be able to verify that the www.bluecatnetworks.com was signed by BlueCat and is therefore valid.

Should someone exploit an organization's DNS server that is using DNSSEC, any record that they alter will not have been signed using the company's private key. When a client receives the altered record and attempts to verify the record integrity, an error will be received indicating that the record is invalid and has been tampered with. This prevents users from receiving poisoned DNS and increased the reliability of records they receive from DNSSEC-enabled DNS servers.

Why BlueCat?

BlueCat Networks has been providing secure DNS solutions since 2001, and as a trusted advisor in DNS security, organizations have looked to BlueCat to help address their security concerns. As part of BlueCat Networks' dedication to security, the DNS Security Extensions have been added to BlueCat's award winning Proteus and Adonis appliances. Through the addition 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

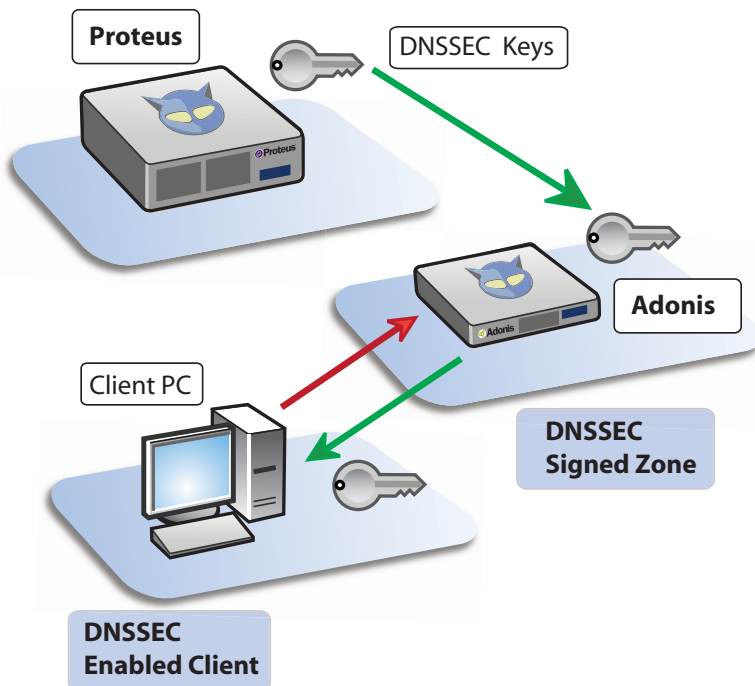
DNSSEC Resolution

DNSSEC Validation

BlueCat's Adonis appliances are able to properly validate signed records from other DNSSEC enabled servers.

Trust Anchors

BlueCat provides the ability to configure Trust Anchors, which are used to validate responses from other authoritative name servers. Trust Anchors will be configurable at a server level using DNS options, where multiple trust anchors can be configured using their zone name and public KSK..



DNSSEC Hosting

DNSSEC Resource Records

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

Signing the Zone

BlueCat provides full support for DNSSEC Signed Zones in using Zone Signing Keys (ZSK) and Key Signing Keys (KSK). Zone Signing Keys are used to sign the records within a zone – for example, the www host in the zone bluecatnetworks.com. Key Signing Keys are used to sign the keys and are typically used outside the zone as the trust anchor. Within Proteus, both ZSKs and KSKs can be automatically generated on a per zone basis.

Schedule Zone Signing

BlueCat provides customers with a simplified way to manage the changing of keys. Before a key is set to expire, Proteus will notify the administrator through email, that their key is nearing its expiration date. These emails will be sent out at user-configured times before the expiration date to ensure that administrators are kept up to date.

Once an administrator receives the expiration message, they can log into the management interface and generate/add a new set of keys. This can be done at any point before the old keys are set to expire. Once this is done, an additional set of keys will be generated. Both sets of keys (old and new) will be used until the old set of keys expires. This provides a mechanism for rolling over keys to ensure that DNSSEC keys never unduly expire.

DNSSEC Resolution with Adonis and Proteus