DNSSEC

DNSSEC is a suite of extensions that add security to the DNS protocol by enabling DNS responses to be validated. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks.

How DNSSEC works

If supported by an authoritative DNS server, a DNS zone can be secured with DNSSEC using a process called zone signing. Signing a zone with DNSSEC adds validation support to a zone without changing the basic mechanism of a DNS query and response.

Validation of DNS responses occurs through the use of digital signatures that are included with DNS responses. These digital signatures are contained in new, DNSSEC-related resource records that are generated and added to the zone during zone signing

When a DNSSEC-aware recursive or forwarding DNS server receives a query from a DNS client for a DNSSEC-signed zone, it will request that the authoritative DNS server also send DNSSEC records, and then attempt to validate the DNS response using these records. A recursive or forwarding DNS server knows that the zone supports DNSSEC if it has a DNSKEY (also called a trust anchor) for that zone

DNSSEC validation

A recursive DNS server uses the DNSKEY resource record to validate responses from the authoritative DNS server by decrypting digital signatures contained in DNSSEC-related resource records and then computing and comparing hash values. If hash values are the same, it provides a reply to the DNS client with the DNS data it requested (such as an A record). If hash values are not the same, it replies with a SERVFAIL message. Additionally, if the DNS client is DNSSEC-aware, the recursive DNS server will indicate that DNSSEC validation was performed, which can be required by the client

DNSKEYs are used to compute hash values and decrypt RRSIG records. The figure does not display all validation processes that are performed. Additional validation is also carried out to ensure the DNSKEYs are valid, and that DS records are valid, if they exist

DNSSEC-related resource records

Table 1: New resource record types used with DNSSEC:

Record Type	Description
Resource Record Signature (RRSIG)	Signatures that are generated with DNSSEC are contained in RRSIG records. Each RRSIG record is matched to another record in the zone for which it provides a digital signature. When a resolver issues a query for a name, one or more RRSIG records are returned in the response.
Next Secure (NSEC)	An NSEC record is used to prove non-existence of a DNS name. NSEC records prevent spoofing attacks intended to fool a DNS client into believing that a DNS name does not exist.
Next Secure 3 (NSEC3)	NSEC3 is a replacement or alternative to NSEC that has the additional benefit of preventing "zone walking" which is the process of repeating NSEC queries in order to retrieve all the names in a zone. A DNS server running Windows Server 2012 or a later operating system supports both NSEC and NSEC3. A zone can be signed with either NSEC or NSEC3, but not both.
Next Secure 3 Parameter (NSEC3PARAM)	The NSEC3PARAM record is used to determine which NSEC3 records to include in responses for non-existing DNS names.
DNS Key (DNSKEY)	A DNSKEY resource record stores a public cryptographic key that is used to verify a signature. The DNSKEY record is used by a DNS server during the validation process. DNSKEY records can store public keys for a zone signing key (ZSK) or a key signing key (KSK).
Delegation Signer (DS)	A DS record is a DNSSEC record type used to secure a delegation. DS records are used to build authentication chains to child zones.

Addition of DNSSEC-related resource records

With the exception of the DS record, all of these records are added to a zone automatically when it is signed with DNSSEC. The DS record is a special record that can be manually added to a parent zone to create a secure delegation for a child zone. For example, the .com zone can contain a DS record for contoso.com; however this record must either be created in the parent zone, or created in a child zone and then propagated to the parent zone. The DS record is not automatically created when you sign a zone.

NSEC or NSEC3 records are automatically added to a zone during zone signing. However, a signed zone cannot have both NSEC and NSEC3 records. The type of record (NSEC or NSEC3) added to the zone depends on how zone signing is configured. In the previous example, the zone is signed using NSEC3.

Trust anchors

DNSKEY and DS record are also called **trust anchors** or **trust points**. A trust anchor must be distributed to all non-authoritative DNS servers that will perform DNSSEC validation of DNS responses for a signed zone. If the DNS server is running on a domain controller, trust anchors are stored in the forest directory partition in Active Directory Domain Services (AD DS) and can be replicated to all domain controllers in the forest. On standalone DNS servers, trust anchors are stored in a file named **TrustAnchors.dns**. A DNS server running Windows Server 2012 or a later operating system also displays configured trust anchors in the DNS Manager console tree in the **Trust Points** container. You can also use Windows PowerShell or dnscmd.exe to view trust anchors (note: dnscmd.exe is deprecated and might be removed in a future version of Windows Server).

An example of the Windows PowerShell cmdlet **Get-DnsServerTrustAnchor** is shown below:

```
PS C:\> Get-DnsServerTrustAnchor -Name secure.contoso.com
```