DNSSEC

DNSSEC (DNS Security Extensions) provides mechanisms for authenticating the source of DNS data and ensuring its integrity. It protects DNS data from certain attacks, such as man-in-the-middle attacks and cache poisoning. A man-in-the-middle attack occurs when an attacker intercepts responses to queries and inserts false records. Cache poisoning can occur when a client accepts maliciously created data. DNSSEC helps you avoid such attacks on your networks.

DNSSEC provides changes to the DNS protocol and additional resource records (RRs) as described in the following RFCs:

- RFC 4033, DNS Security Introduction and Requirements
- RFC 4034, Resource Records for the DNS Security Extensions
- RFC 4035, DNSSEC Protocol Modifications
- RFC 4641, DNSSEC Operational Practices
- RFC 4956, DNS Security (DNSSEC) Opt-In
- RFC 4986, Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover
- RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
- RFC 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC

DNSSEC uses public key cryptography to authenticate the source of DNS responses and to ensure that DNS responses were not modified during transit. Public key cryptography uses an asymmetric key algorithm. With asymmetric keys, one key is used to decrypt data that was encrypted using the other key.

In DNSSEC, the primary name server of a zone generates at least one public/private key pair. It "signs" each data set in the zone by running it through a one-way hash, and then encrypting the hash value with the private key. The public key is stored in an RR type introduced by DNSSEC, the DNSKEY RR. Resolvers use the DNSKEY record to decrypt the hash value. If the hash values match, then the resolver is assured of the authenticity of the message.

In addition to the DNSKEY record, DNSSEC also introduces new RRs which DNS servers can use to authenticate the non-existence of servers, zones, or resource records. For information about the DNSSEC resource records, see DNSSEC Resource Records.

DNSSEC uses the EDNSO message extension. Resolvers include the EDNS OPT pseudo-RR with the DO (DNSSEC OK) bit set to indicate that they are requesting DNSSEC records. A DNS client or resolver sets the EDNS DO bit when it sends a query for data in a signed zone. When the DNS server receives such a query, it includes the additional DNSSEC records in its response, according to the DNSSEC standard rules. In addition, because DNSSEC messages are often large, the EDNSO message extension also provides mechanisms for handling larger DNS UDP messages. For information about EDNS0, refer to RFC 2671, Extension Mechanisms for DNS (EDNS0). For information about the DO bit, refer to RFC 3225, Indicating Resolver Support of DNSSEC.

**WARNING:** Note that when you disable EDNS0 on the appliance, all outgoing DNSSEC queries to zones within trusted anchors will fail even if DNSSEC validation is enabled. To ensure that DNSSEC functions properly, do not disable EDNS0 on the appliance. For more information, see Using Extension Mechanisms for DNS (EDNS0).

DNSSEC also supports new data in the packet header, the CD (Checking Disabled) bit and the AD (Authenticated Data) bit. The CD bit is used by resolvers in their DNS queries and the AD bit is used by recursive name servers in their responses to queries.

A resolver can set the CD bit in its query to indicate that the name server should not validate the DNS response and that the resolver takes responsibility for validating the DNS data it receives.

A name server that has successfully validated the data in a DNS response sets the AD (Authenticated Data) bit in the message header to indicate that all resource records in its response have been validated and are authentic. Note that unless the connection between the DNS server and client has been secured, such as through TSIG, the client cannot rely on the AD bit to indicate valid data. The data could have been changed in transit between the server and client. Resolvers can trust a response with the AD bit set only if their communication channel is secure.

You can also configure the NIOS appliance to always apply RPZ policies, DNS blacklists, or NXDOMAIN rules to DNS responses, regardless of whether the queries request DNSSEC data. For more information about how to configure this, see Applying Policies and Rules to DNS Queries at Request DNSSEC Data. For information about RPZ policies, DNS blacklists, and NXDOMAIN rules, see their respective sections in this guide.

Related topic

Configuring DNSSEC