**DNSSEC - защищенный dns, назначение и основные характеристики.**

Протокол DNSSEC – набор расширений IETF (Инженерный совет Интернета, ответственный за стандарты протокола DNS) протокола DNS, позволяющих минимизировать атаки, связанные с подменой DNS-адреса при разрешении доменных имён.

Протокол DNSSEC позволяет повысить надёжность проверки подлинности в DNS при помощи цифровых подписей, основанных на криптографии открытого ключа. При использовании DNSSEC не запросы и ответы DNS подписываются криптографически, а сами данные DNS подписываются владельцем этих данных.

У каждой зоны DNS есть пара открытых/закрытых ключей. Владелец зоны использует её закрытый ключ для подписания данных DNS в этой зоне и генерирования цифровых подписей для этих данных. Как следует из названия «закрытый ключ», сведения о нём держатся владельцем зоны в секрете. А вот открытый ключ зоны публикуется в ней свободно, и получить его может каждый. Любой рекурсивный резолвер, производящий поиск данных в зоне, также получает открытый ключ этой зоны и использует его для проверки подлинности данных DNS. Резолвер проверяет подлинность цифровой подписи полученных им данных DNS. Если подлинность подтверждается, то данные DNS считаются настоящими и возвращаются пользователю. Если подпись не проходит проверку подлинности, то резолвер предполагает, что произошла атака, избавляется от данных и сообщает пользователю об ошибке.

Применение DNSSEC позволяет обеспечить две важные функции в DNS:

1. Проверка подлинности источника данных позволяет резолверу криптографически проверить, действительно ли полученные данные поступили из той зоны, откуда, как он считает, они произошли;
2. Проверка целостности данных позволяет резолверу проверить, не были ли эти данные изменены при передаче, после того как владелец зоны подписал их закрытым ключом этой зоны.

**Взаимодействие почтовых серверов.**

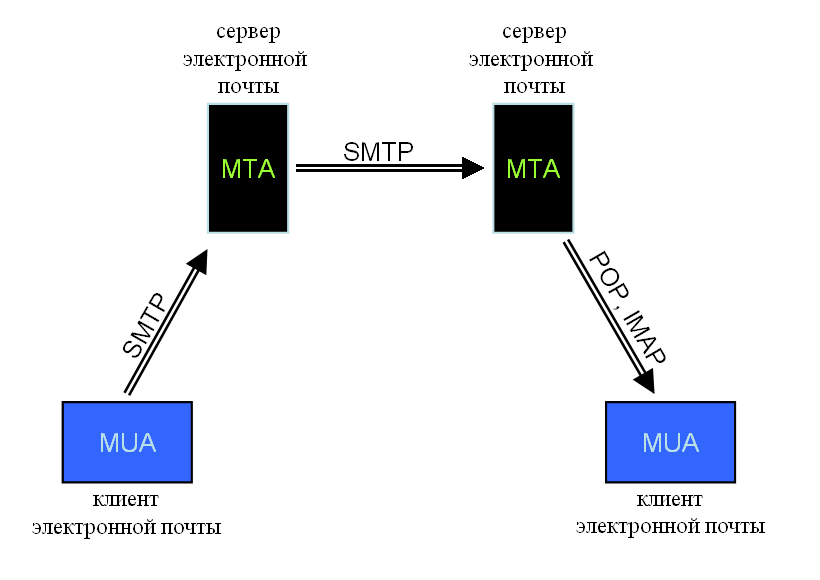


Схема взаимодействия

**MIME формат. (Boundary).**

MIME (многоцелевые расширения интернет-почты) – стандарт, описывающий передачу различных типов данных по электронной почте, а также, в общем случае, спецификация для кодирования информации и форматирования сообщений таким образом, чтобы их можно было пересылать по Интернету.

MIME определяет механизмы для передачи разного рода информации внутри текстовых данных (в частности, с помощью электронной почты), а именно: текст на языках, для которых используются кодировки, отличные от ASCII, и нетекстовые данные, такие, как картинки, музыка, фильмы и программы.

Формат MIME поддерживает передачу нескольких сущностей в пределах одного сообщения. Для передачи множественного сообщения в заголовок добавляется параметр **boundary** (граница), который обозначает последовательность символов, разделяющих части сообщения. Граница может состоять из цифр, букв и символов.

**Протокол IMAP.**

IMAP – протокол прикладного уровня для доступа к электронной почте. Базируется на транспортном протоколе TCP и использует порт 143. IMAP работает только с сообщениями и не требует каких-либо пакетов со специальными заголовками. Протокол IMAP представляет собой альтернативу POP с зачаточными способностями по отправке.

IMAP предоставляет пользователю широкие возможности для работы с почтовыми ящиками, находящимися на почтовом сервере. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя. Электронными письмами можно манипулировать с компьютера пользователя (клиента) без постоянной пересылки с сервера и обратно полного содержания писем.

Для отправки писем используется обычно протокол SMTP, так как собственная команда отправки протокола IMAP не содержит в себе механизма передачи служебной информации.

**Команда nslookup.**

nslookup (поиск на сервере имён) – утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе DNS (проще говоря, DNS-клиент).

Позволяет задавать различные типы запросов и опрашивать произвольно указываемые сервера. Используется для диагностики и проверки DNS-серверов и записей, и выявления проблем с разрешением имен в подсистеме DNS.

Утилита портирована на Windows непосредственно фирмой Microsoft и поставляется вместе с операционной системой.