ПРИМЕНЕНИЕ ПРОТОКОЛА IPSEC ДЛЯ ЗАЩИТЫ СЕТЕВОГО ТРАФИКА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сороко М.В.

Астровский И.И. – к.т.н., доцент

Обеспечение информационной безопасности компьютерных сетей возможно при создании системы защиты не для отдельных классов приложений, а для сети в целом. Применительно к компьютерным сетям это означает, что системы защиты должны действовать на сетевом уровне модели открытых систем. Преимущество такого выбора заключается в том очевидном факте, что в компьютерных сетях именно сетевой уровень отличается наибольшей гомогенностью: независимо от вышележащих протоколов, физической среды передачи и технологии канального уровня, транспортировка данных по сети не может быть произведена в обход протокола IP. Для этих целей в компьютерных сетях принято использовать протокол IPSec. Впервые протокол официально стандартизирован Целевой группой Internet Engineering Task Force (IETF) в 1995 году и по-прежнему используется в корпоративных сетях, благодаря гибкой настройке и управлению политиками.

Благодаря реализации протокола обеспечивается конфиденциальность и целостность информации. IPSec включает протоколы для установления взаимной аутентификации между агентами в начале сеанса и согласование криптографических ключей, которые будут использоваться во время сеанса. IPsec может использоваться для защиты потоков данных между двумя хостами (хост-хост), между двумя шлюзами безопасности (сеть-сеть) или между шлюзом безопасности и хостом (от сети к хосту). IPsec использует криптографические алгоритмы безопасности для защиты соединения по сетям IP, поддерживает аутентификацию источника данных, целостность данных, конфиденциальность данных.

Протокол поддерживает сквозную схему безопасности, работая на сетевом уровне, в то время как другие системы безопасности в Интернете, такие как Transport Layer Security (TLS) и Secure shell (SSH), работают в верхних слоях на транспортном уровне и прикладном уровне соответственно. Следовательно, только IPsec защищает весь трафик приложений по IP-сети [1].

IPSec использует фильтрацию IP для определения того, какой трафик должен быть защищен. Специальный тип действия фильтра указывает на разрешение трафика. IP-фильтры представляют политику безопасности, указывая трафик, требующий шифрования. Фильтры также используются для определения исходящей ассоциации безопасности IPSec и для проверки того, что входящий трафик получен с использованием правильной ассоциации безопасности [2].

Большинство реализаций протокола IPSec имеют несколько компонентов. Основной протокол IPSec реализует протоколы аутентификации (Authentication Header, AH), шифрования (Encapsulated Security Payload, ESP), отвечающим за шифрование содержимого отдельных пакетов, протоколы обмена ключами (Internet Key Exchange, IKE), предназначенные для согласования используемых алгоритмов аутентификации и шифрования, ключей и продолжительности их действия, а также для защищенного обмена ключами [3].

Протоколы AH или ESP передают данные в двух режимах: туннельном, при котором IP-пакеты защищаются целиком, включая их заголовки, и транспортном, обеспечивающим защиту только содержимого IP-пакетов. Основным режимом является туннельный. В туннельном режиме исходный пакет помещается в новый IP-пакет, и передача данных по сети выполняется на основании заголовка нового IP-пакета. При работе в этом режиме каждый обычный IP-пакет помещается целиком в шифрованном виде в конверт IPSec, а тот в свою очередь инкапсулируется в другой защищенный IP-пакет.

Реализация комплекса IPSec в компьютерных сетях необходима в следующих вариациях:

-Обеспечение безопасного подключения к интрасети предприятия через Интернет

-Предоставление возможности удаленного доступа через Интернет

-Установление защищенного соединения с партнерами

-Безопасное проведение транзакций в системах электронной коммерции

-Настройка политик безопасности для соединений клиент-сервер

Главная особенность протокола заключается в том, что IPSec способен поддерживать все приложения и может шифровать или аутентифицировать весь трафик на уровне IP. Это обеспечивает безопасность для всех приложений, которые используются в сети ежедневно.

Список использованных источников:

1. IPSec [Электронный ресурс] – Режим доступа: https://www.opennet.ru/docs/RUS/vpn_ipsec/
2. Информационная безопасность и защита // В. Ф. Шаньгин – 2014
3. IP Security (IPsec) and Internet Key Exchange (IKE) // RFC 6071 – 2011