ЗАЩИТА ИНФОРМАЦИИ В IP-СЕТЯХ

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

Сергеев Н.Н., Белятко А.Л.

Астровский И.И. – к.т.н.,доцент

Организация системы защиты информации сейчас, во время стремительного развития информационных технологий и вхождение их практически во все сферы жизни, стала неотъемлемой частью этого развития. Для создания системы защиты информации необходимо произвести анализ всевозможных информационных угроз. Самыми опасными для инфраструктуры предприятия являются атаки без физического доступа к сети предприятия. Данные атаки направлены на анализ и перехват сетевого трафика, поэтому защита каналов связи является самой приоритетной задачей.

Шифрование трафика – один из наиболее эффективных методов защиты каналов связи.

IP Security (IPSec) – это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов. В его состав входят около 20 предложений по стандартам. IPsec включает в себя 3 алгоритмонезависимые базовые спецификации:

5) архитектура безопасности IP[1];
6) аутентифицирующий заголовок (AH);
7) инкапсуляция зашифрованных данных (ESP) [2].

Архитектура IPSec представлена на рисунке 1:

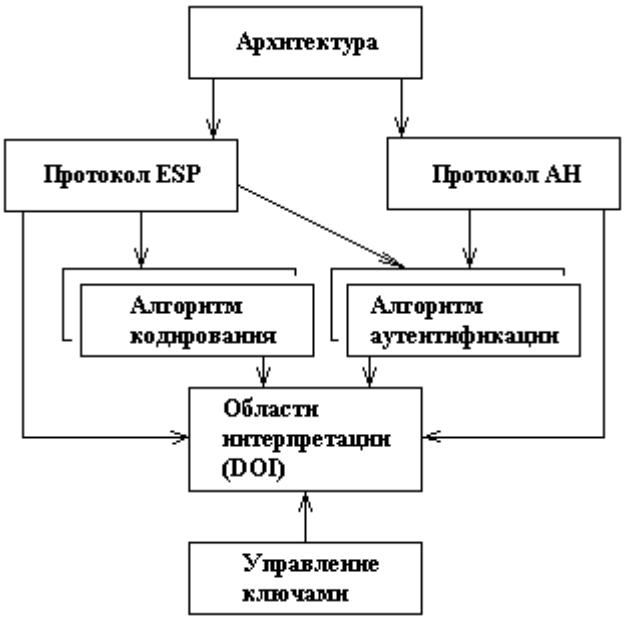

Рис. 1 – Архитектура IPSec

Аутентифицирующий заголовок (AH) является обычным опциональным заголовком. Он располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основное и единственное назначение AH — обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня.

Основная цель заголовка ESP — обеспечение конфиденциальности данных. Формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов.

Гарантия целостности и конфиденциальности данных в спецификации IPSec обеспечивается за счет использования механизмов аутентификации и шифрования. Спецификация IPSec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей. При этом результатом согласования контекста безопасности является установление индекса параметров безопасности, представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности.

IPSec работает на сетевом уровне модели OSI. В результате передаваемые IP-пакеты защищены прозрачным для сетевых приложений и инфраструктуры образом.

Основные преимущества IPSec:

– обеспечивает гибкость при выборе алгоритмов шифрования и длины ключей;

– обеспечивает соединение пакетов по безопасному туннелю, что гарантирует качественную работу приложений с малым временем отклика;

– хорошо подходит для связывания узлов по надежным (безопасным) сетям;

– не IP-протоколы не поддерживаются по умолчанию.

Основные недостатки IPSec — требуется постоянный IP-адрес и не всё клиентское ПО одинаково качественное. Поэтому целесообразно использовать IPSec совместно с AuthIP[3].

Сочетание новых опций проверки подлинности пользователя, возможности использования нескольких учетных данных, более гибкого взаимодействия аутентификации и возможности каждой стороны использовать разные способы аутентификации, позволяет IPSec создать надежные и мощные политики без лишней сложности.

Список использованных источников:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы, 3-е изд.: – СПб., Питер, 2006.

2. Домарев В.В. Защита информации и безопасность компьютерных систем, 2007.

3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах, 2008.