ВЫБОР ПРОТОКОЛА БЕЗОПАСНОСТИ ДЛЯ ОРГАНИЗАЦИИ VPN

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

Киселёв Д.В.

Астровский И.И. – к.т.н.,доцент

В настоящее время зачастую перед руководителями IT подразделений стоит вопрос: какой из протоколов безопасности выбрать для построения корпоративной сети VPN. Встаёт выбор между использованием протокола безопасности сетевого уровня IPSec и использованием одного из протоколов прикладного уровня SSL/TLS. Ответ не очевиден так как каждый из подходов имеет как плюсы, так и минусы. Проведём анализ и выявим когда необходимо применять IPSec, а когда SSL/TLS.

IPSec (IP Security) – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

SSL (Secure Sockets Layer) / TLS (Transport Layer Security) – криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. Используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Выбор протокола для построения корпоративной сети VPN можно осуществлять по следующим критериям.

1. Тип доступа необходимый для пользователей сети VPN.

1.1. Полнофункциональное постоянное подключение к корпоративной сети. Рекомендуемый выбор – протокол IPSec.

1.2. Временное подключение, например, мобильного пользователя или пользователя использующего публичный компьютер, с целью получения доступа к определенным услугам, например, электронной почте или базе данных. Рекомендуемый выбор – протокол SSL/TLS, который позволяет организовать VPN для каждой отдельной услуги.

2. Является ли пользователь сотрудником компании.

2.1. Если пользователь является сотрудником компании, устройство которым он пользуется для доступа к корпоративной сети через IPSec, может быть сконфигурировано определенным способом.

2.2. Если пользователь не является сотрудником компании к корпоративной сети которой осуществляется доступ, рекомендуется использовать SSL/TLS. Это позволит ограничить гостевой доступ только определенными услугами.

3. Уровень безопасности корпоративной сети.

3.1. Высокий. Рекомендуемый выбор – протокол IPSec. Действительно, уровень безопасности предлагаемый IPSec гораздо выше уровня безопасности предлагаемого протоколом SSL/TLS в силу использования конфигурируемого ПО на стороне пользователя и шлюза безопасности на стороне корпоративной сети.

3.2. Средний. Рекомендуемый выбор – протокол SSL/TLS, позволяющий осуществлять доступ с любых терминалов.

4. Уровень безопасности данных, передаваемых пользователем.

4.1. Высокий, например, менеджмент компании. Рекомендуемый выбор – протокол IPSec.

4.2. Средний, например, партнер. Рекомендуемый выбор – протокол SSL/TLS.

5. Что важнее, быстрое развертывание VPN или масштабируемость решения в будущем.

5.1. Быстрое развертывание сети VPN с минимальными затратами. Рекомендуемый выбор – протокол SSL/TLS. В этом случае нет необходимости реализации специального ПО на стороне пользователя как в случае IPSec.

5.2. Масштабируемость сети VPN – добавление доступа к различным услугам. Рекомендуется протокол IPSec, позволяющий осуществление доступа ко всем услугам и ресурсам корпоративной сети.

5.3. Быстрое развертывание и масштабируемость. Рекомендуемый выбор – комбинация IPSec и SSL/TLS: использование SSL/TLS на первом этапе для осуществления доступа к необходимым услугам с последующим внедрением IPSec.

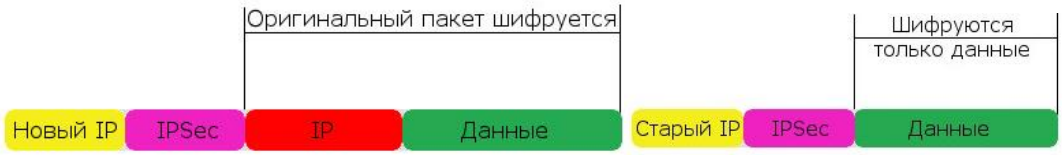

Рис. 1 – Примеры шифрования IP-пакета протоколом IPSec

Как видно из анализа характеристик этих протоколов они не являются взаимозаменяемыми и могут функционировать как отдельно, так и параллельно, определяя функциональные особенности каждой из реализованных VPN.

Список использованных источников:

1. Олифер В. Г.,Олифер Н. П. Глава 24. Сетевая безопасность // Компьютерные сети. Принципы, технологии, протоколы. – 4-е. – СПб: Питер, 2010. – С. 887-902. – 944 с.

2. Stephen Thomas. SSL & TLS Essentials: Securing the Web. – 1-st. – Wiley, February 11, 2000.