Методы обеспечения безопасности в сетях общего пользования

Медведев Алексей Владимирович

УО "Брестский государственный университет имени А.С. Пушкина"

В наше время найти кафе или гостиницу с бесплатной сетью Wi-Fi не трудная задача. Но не стоит забывать и о методах защиты от хакерских атак и кибер-хулиганов. Любая неизвестная вам сеть может стать причиной потери пользовательских данных: логины и пароли от почтовых ящиков, социальных сетей, данные банковских карт и т.д.

Есть несколько способов обеспечить безопасность пользовательских данных. На стороне пользователя – установка и настройка антивирусного ПО, включение и настройка брандмауэра, а так же использование VPN тоннелей. На стороне сервера – настройка NAT (разделение адресного пространства), настройка Firewall или IPtables, а так же использование сервера проксификации.

NAT позволяет спрятать пользователей публичной (и не только) сети от пользователей в глобальной сети, или, как часто делают на крупных предприятиях, отделить пользователей внутренней сети предприятия от пользователей общественной сети того же предприятия.

Firewall (межсетевой экран) – это защита сети компьютеров от внешних угроз, а именно незаконного проникновения, доступа к вашим персональным данным, операционной системе и файлам извне. Можно сказать – это, своего рода, антивирус и фильтр входящих подключений. Зачастую функции NAT и Firewall присутствуют в предоставляемых провайдерами модемах, однако их функционал не полный и отсутствует гибкость настройки данных систем обеспечения безопасности. Поэтому системные администраторы предпочитают устанавливать и настраивать их самостоятельно на своих серверах.

IPtables – утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) Netfilter для ядер Linux. С её помощью создаются и изменяются правила, управляющие фильтрацией и перенаправлением пакетов. Для работы с семейством протоколов IPv6 существует отдельная версия утилиты – Ip6tables.

Прокси-сервер – (комплекс программ) в компьютерных сетях, позволяющий клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс расположенный на другом сервере. Затем прокси-сервер подключается к указанному серверу и получает ресурс у него. Прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента.

СПИСОК ЛИТЕРАТУРЫ

1. Прокси-сервер (Википедия) [Электронный ресурс] – Режим доступа: https://goo.gl/qgU0uK. – Дата доступа: 05.03.2017.