СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

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

Малько В.С.

Бильдюк Д.М. – старший преподаватель

Важной частью коммуникаций большинства современных компаний стали беспроводные широкополосные сети передачи данных. С их помощью можно организовать городские опорные сети связи, обеспечивающие широкополосный доступ к Интернету для частных компаний и государственных учреждений. Для беспроводных сетей разработан ряд программных и аппаратных средств контроля над трафиком и управления безопасностью. На сегодняшний день сняты все вопросы администрирования, теперь они так же, как и проводные могут быть "прозрачными" для технических специалистов и администраторов.

На производительность радиоустройств влияют многие факторы, поэтому контролировать беспроводные сети и управлять ими сложнее, чем проводными. До недавнего времени было невозможно контролировать потоки данных и проводить мониторинг уровней поступающих радиосигналов, поэтому возникали трудности при выяснении причин того или иного события в сети. При использовании современных программных и аппаратных средств мониторинга и анализа трафика беспроводных сетей эти вопросы успешно решаются.

Следует остановиться на основных задачах, решаемых с помощью современных средств контроля:

- Поскольку средой распространения радиосигналов является окружающее пространство со случайными характеристиками, то заранее неизвестен уровень сигналов, приходящих к границам зоны обслуживания, от этого зависит качество и скорость обслуживания. Современные средства контроля измеряют уровни сигнала в любой точке зоны обслуживания сети.

- Реальная пропускная способность беспроводной сети зависит от количества служебной информации, передаваемой в ней. Следовательно, необходимо фиксировать служебную информацию и данные, фиксировать повторные передачи и определять активные узлы сети (порождающие наибольший трафик). Тогда во время замедления работы с помощью средств контроля, можно будет узнать, какие же узлы "съедают" драгоценную полосу пропускания.

- Для повышения безопасности передачи данных используют защитные механизмы, а если они не используются, то появляется вероятность подключения "не авторизованных" пользователей. С помощью средств контроля можно обеспечить анализ трафика сетей на предмет определения используемых механизмов защиты.

- Для контроля за трафиком нужно декодировать протоколы всех уровней семиуровневой модели взаимодействия открытых систем. Следовательно, для обработки и проведения анализа всего переданного трафика необходимо включить поддержку протоколов, как низкого, так и высокого уровней. Большинство современных средств контроля поддерживают такой режим работы.

Правила политики безопасности усиливаются посредством использования модулей доступа. В межсетевом экране прикладного уровня каждому разрешаемому протоколу должен соответствовать свой собственный модуль доступа. Лучшими модулями доступа считаются те, которые построены специально для разрешаемого протокола. Например, модуль доступа FTP предназначен для протокола FTP и может определять, соответствует ли проходящий трафик этому протоколу и разрешен ли этот трафик правилами политики безопасности.

При использовании межсетевого экрана прикладного уровня все соединения проходят через него. Как показано на рисунке 1, соединение начинается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол и определяет, соответствует ли данный трафик правилам политики безопасности. Если это так, то межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой-сервером.

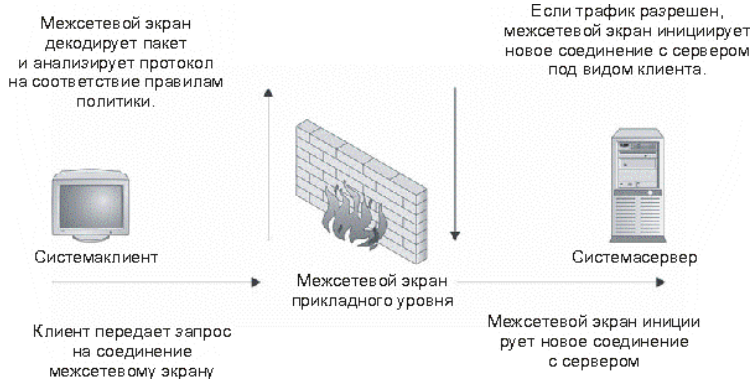

Рис. 1 – Соединения модуля доступа межсетевого экрана прикладного уровня

Межсетевые экраны прикладного уровня используют модули доступа для входящих подключений. Модуль доступа в межсетевом экране принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений.

На сегодняшний день разработано большое количество программных и аппаратных средств, позволяющих осуществлять мониторинг, обработку и анализ трафика сети, построенной на оборудовании семейства стандартов IEEE 802.11 (a, b). Эти средства могут контролировать работающие радиоустройства в диапазонах 2,4-2,5 ГГц, 5,15-5,25 ГГц, 5,25-5,35 ГГц и 5,725-5,825 ГГц.

Основные отличия программного и аппаратного подходов:

Программные средства контроля, работают с драйверами стандартного оборудования, поэтому с выходом новой версии ПО вам не придется менять радиомодуль, это значительно упрощает процедуру обновления средств контроля. Программные средства контроля намного гибче к изменениям и новшествам. Из недостатков можно отметить, что приходится использовать радиомодули с обычными характеристиками, а для проведения анализа сетей диапазонов 2,4 и 5 ГГц необходимо параллельно использовать два радиомодуля, что накладывает определенные требования на производительность компьютера. Программные средства контроля поддерживают радиооборудование ограниченного числа производителей. После завершения мониторинга и анализа трафика высвободившееся оборудование можно использовать как обычные сетевые устройства.

Список использованных источников:

1. Информационная безопасность компьютерных систем и сетей. В. Ф. Шаньгин – Инфра-М, 2008. – 416с
2. Firewalls. Практическое применение межсетевых экранов. Терри Оглтри – ДМК пресс, 2001. – 400с;