УДК 004.67

Брандмауэры, как один из способов защиты информации

Хамидуллова Динара Рамильевна
Мордовский государственный университет им. Н. П. Огарева
студент

Фадеева Ксения Андреевна
Мордовский государственный университет им. Н. П. Огарева
студент

Макаров Вячеслав Эдуардович
Мордовский государственный университет им. Н. П. Огарева
преподаватель

Аннотация
Данная статья посвящена такой программе, как брандмауэр, которая осуществляет защиту информации отдельных компьютеров и локальных сетей от несанкционированного доступа.
Ключевые слова: Брандмауэр, защита информации, локальная сеть, несанкционированный доступ, вредоносные программы.

Firewalls, as one of the ways to protect information

Khamidullova Dinara Ramilyevna
Ogarev Mordovia State University
student

Fadeeva Ksenia Andreevna
Ogarev Mordovia State University
student

Makarov Vyacheslav Eduardovich
Ogarev Mordovia State University
Lecturer

Abstract
This article is devoted to a program such as a firewall that protects the information of individual computers and local networks from unauthorized access.
Keywords: Firewall, data protection, local network, unauthorized access, malicious programs.

Любой современный пользователь компьютера наверняка встречал термин «брандмауэр» и знает, что он имеет какое-то отношение к обеспечению безопасности. Но для полной защиты ресурсов требуется более глубокое понимание того, как работают брандмауэры и где их размещать.

Термин «брандмауэр» изначально использовался в строительстве и означал кирпичную стену из огнеупорного материала между двумя структурами, предотвращающую пожар. Отсюда следует и главное предназначение брандмауэра в компьютерной безопасности: он осуществляет контроль сетевых пакетов или установленных программ, защищает систему от компьютерных атак, управляет сетевым трафиком как в сети Интернет, так и вне её, или между разными сегментами внутренней сети.

Internet Connection Firewall (предшественник нынешнего брандмауэра) изначально был включен по умолчанию в Windows XP, но вскоре был исключен в связи с проблемами совместимости. Главной причиной всего этого стало то, что настройки данной программы находились в конфигурации сети и пользователи не могли найти их. В середине 2003 года компьютер червь Blaster подверг атаке множество компьютеров под управлением операционной системы Windows, а через несколько месяцев еще один червь Sasser также провел аналогичную атаку. В 2004 году такие атаки распространялись все больше и больше, в результате чего незащищенные компьютеры заражались за считанные минуты. Все эти атаки были результатом отключения Internet Connection Firewall [1]. В связи с этим компания Microsoft приняла решение усовершенствовать функциональность и интерфейс Internet Connection Firewall и назвать его «Брандмауэр Windows».

С тех пор и по сей день в компьютерах брандмауэр идет как встроенное программное обеспечение, а также входит в состав платных антивирусов. Как правило, брандмауэр имеет два сетевых интерфейса: один для внешней стороны сети, один для внутренней стороны. Его цель - контролировать, какой трафик разрешён для перехода с одной стороны на другую.

Существует несколько типов брандмауэров:

1) пакетные фильтры (packet filter);
2) сервера прикладного уровня (application gateways);
3) сервера уровня соединения (circuit gateways).

Все эти типы могут встретиться в одном брандмауэре.

На базовом уровне брандмауэры могут блокировать трафик, предназначенный для определенных IP-адресов или портов сервера. Как правило, компании настраивают свои брандмауэры, чтобы обеспечить входящие подключения к порту 80, который является стандартным портом для использования веб-серверами. Это позволяет, например, посещать web-сайт, но «ненадёжный» трафик, предназначенный для другого порта, будет лишён доступа[2-3]. Сотрудникам компании, у которых есть соответствующие учетные данные, такие как имя пользователя и пароль, будет разрешён доступ через безопасное соединение, обычно это виртуальная частная сеть.

При правильной настройке брандмауэры также обеспечивают защиту от угроз, включая атаки на отказ в обслуживании (DOS). Атаки DOS происходят, когда злоумышленник пытается загрузить корпоративный веб-сайт с потоком трафика, настолько, что он сбрасывает web-сервер и позволяет злоумышленнику проникнуть в него. Оттуда злоумышленник может иметь доступ к другим сетевым ресурсам.

Более сложные брандмауэры поддерживают методы «проверки состояния», когда брандмауэр рассматривает шаблоны в потоках трафика для выявления аномалий, которые предполагают, что какая-либо форма атаки продолжается, например атаки DOS или атаки spoof, когда злоумышленник пытается маскироваться как разрешенный ресурс.

На практике большинство компаний используют два брандмауэра для создания DMZ или демилитаризованной зоны[5]. Один брандмауэр подключается к Интернету, а другой подключается к внутренней сети. В промежутке между ними находится DMZ, где компании размещают свои публичные web-серверы. Идея состоит в том, что даже если злоумышленнику удастся взломать web-сервер, например, посредством атаки DOS, второй брандмауэр не позволит ему получить доступ к частной корпоративной сети.

Аналогичным образом компании могут настраивать несколько брандмауэров внутри своей корпоративной сети, чтобы существенно разделить сеть на несколько сегментов. Это помогает уменьшить ущерб, если какая-либо форма червя или другого вредоносного программного обеспечения будет выпущена в любом сегменте.

На сегодняшний день на рынке существует множество программных и аппаратных средств для защиты информации локальной сети или персональных компьютеров от несанкционированного доступа, но большинство пользователей привыкли обращаться к стандартным, проверенным программам, как брандмауэры.

Библиографический список

1. Хамидуллова Д.Р., Фадеева К.А., Ладанова Е.О. Есть ли перспективы у Pascal? История создания и дальнейшее использование языка// Постулат. 2018. № 1 (2018).
2. Хамидуллова Д.Р., Фадеева К.А., Ладанова Е.О. Язык Assembler: структура и применение// Постулат. 2018. № 5 (2018).
3. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности. СПб.:Питер. 2017.
4. Галатенко В. А. Основы информационной безопасности. Интернет-университет информационных технологий. ИНТУИТ.ру, 2008.
5. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. Серия: безопасность человека и общества. М.:2000. 428с.
6. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. 544с.