БРАНДМАУЭРЫ: ИССЛЕДОВАНИЕ МЕТОДОВ БЕЗОПАСНОСТИ И УГРОЗ

Сеидова И.
кандидат технических наук
Азербайджанский Государственный Университет Нефти и Промышленности, Азербайджан, г. Баку
Каратова Д.
Мастер
Азербайджанский Государственный Университет Нефти и Промышленности, Азербайджан, г. Баку

FIREWALLS: SECURITY AND THREAT RESEARCH

Seyidova I.,
Candidate of Technical Sciences
Azerbaijan State Oil and Industry University, Azerbaijan
Karatova D.
Master
State Oil and Industry University, Azerbaijan, Baku

АННОТАЦИЯ

Веб-безопасность превратилась в заслуживающую внимания проблему в нынешнем порядке вещей. И это похоже на зло, которое, если его оставить распространяться, в считанные секунды будет иметь последствия для каждого из нас. Таким образом, в этой статье анализируется веб-безопасность с учетом брандмауэра и того, как он может помочь защитить систему и Интернет. Брандмауэр — это часть компьютерной или сетевой системы, настроенная на предотвращение обмена данными с неавторизованными источниками и разрешение доступа из авторизованных источников. Дополнительно обсуждаются методы и виды брандмауэров. Далее в документе рассматривается брандмауэр и то, как он может помочь в веб-безопасности, безопасности бизнеса и безопасности отдельных систем. Далее обсуждались новые решения по направление развитие брандмауэров- Firewall as a Service (FWaaS).

ABSTRACT

Web security has become a noteworthy issue in the current state of affairs. And it looks like an evil that, if left to spread, will have repercussions for all of us in a matter of seconds. Thus, this article analyzes web security with a firewall in mind and how it can help protect the system and the Internet. A firewall is a part of a computer or network system configured to prevent communications from unauthorized sources and allow access from authorized sources. Additionally, methods and types of firewalls are discussed. The remainder of the paper looks at the firewall and how it can help with web security, business security, and individual system security. Further, new solutions were discussed in the direction of the development of firewalls - Firewall as a Service (FWaaS).

Ключевые слова: интернет, брандмауэр, безопасность, компьютерный трафик, пакетные фильтры, список контроля доступа, угрозы.

Keywords: internet, firewall, security, computer traffic, packet filters, access control list, threats.

ВВЕДЕНИЕ

Безопасность является наиболее важным аспектом в системе. Есть масса идей для системной безопасности. Брандмауэр является выдающимся среди наиболее важных идей, связанных с безопасностью системы. Брандмауэр может быть реализован в виде программного обеспечения или может быть аппаратным обеспечением, которое в основном блокирует несанкционированный обмен данными, исходящий или входящий в сеть. Доступно множество программ для обеспечения безопасности на системном или сетевом уровне.[1] Таким же образом устройства брандмауэра также используются для обеспечения безопасности системы.

Структура безопасности сети.

Основная цель информационной безопасности акцент на защите данных или информации, которая сохраняется в компьютерных системах, особенно на серверах. Серверы обычно имеют несколько уровней безопасности, чтобы обеспечить безопасность информации и данных (рис. 1) [8]. Внутренним уровнем сетевой безопасности является уровень прав доступа. Целью разработки этого уровня является управление активами (данными) и правами (правами клиента на доступ к активам). Этот слой имеет дело с выделениями, организаторами и записями. Следующий за этим уровнем (второй) ограничивает учетную запись, позволяя подсчитывать информацию об именах пользователей и паролях (пароль/логин). Это обычно используемый метод уверенности из-за его простоты, прямоты, эффективности и очень сильного воздействия. Администратор обязан контролировать и обрабатывать операции различных пользователей. Третий внешний уровень использовал метод шифрования информации, называемый шифрованием данных. Информация шифруется с использованием определенного алгоритма, так что даже если кто-то попытается получить доступ к информации, он не сможет проверить ее без ключа шифрования. Внешний или перифе-

рийный уровень, называемый брандмауэром, предотвращает вторжения и фильтрует нежелательные исходящие или входящие информационные пакеты [2].

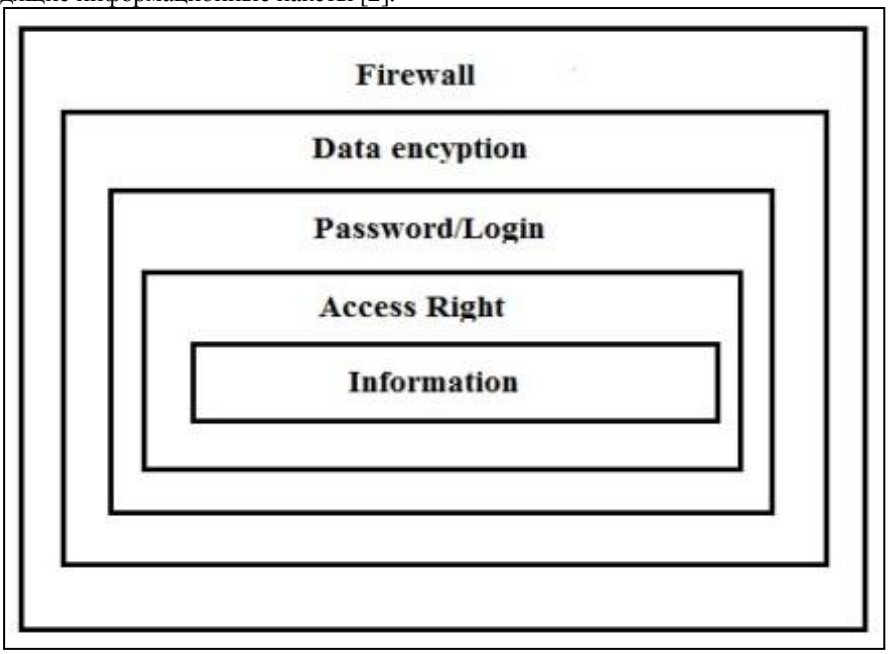

Рис 1. Уровни безопасности сети [8]

Основные характеристики брандмауэра

Прежде чем узнать, как работает брандмауэр, мы должны понять, что он может и чего не может делать. Широкий спектр брандмауэров имеет некоторые общие особенности и возможности, чтобы различать, что может делать брандмауэр[3]. На самом деле брандмауэр должен иметь следующие основные возможности:

• Контролируйте и организуйте трафик
• Доступ для аутентификации
• Защитить активы организации
• Работа в качестве посредника
• Защитите сетевые ресурсы от вредоносных действий при доступе в Интернет.
• Обеспечьте защищенный и безопасный доступ к вашим внутренним ресурсам внешним пользователям.

Брандмауэр — это только внешний уровень защиты, поэтому он не может делать все. Это всего лишь искусственная машина, поэтому она не может классифицировать информацию как лучшую или худшую. Он может просто квадратить трафик с простыми атрибутами. Кроме того, брандмауэр не может предотвратить атаку, если она не проходит через него[4]. Подводя итог, брандмауэр не может играть роль антивирусного сканера из-за его скорости обработки, регулярного появления вирусов и шифрования данных для маскировки вируса. Несмотря на это, на сегодняшний день он считается одним из наиболее часто используемых методов защиты. [3]

Типы брандмауэров

Существует несколько процедур брандмауэра, и каждый брандмауэр может использовать по крайней мере два из двух показанных методов[9]. Одной из серьезных проблем, с которой сталкивается любая организация при попытке проверить свою конфиденциальную информацию, является поиск правильных аппаратов для этой деятельности. Даже для типичного инструмента, например брандмауэра, многие организации, вероятно, не будут иметь четкого представления о том, как найти правильный брандмауэр для своих требований, как спроектировать эти брандмауэры или почему такие брандмауэры могут быть жизненно важны[10]. Начальный этап поиска правильных брандмауэров для обеспечения информации вашей организации заключается в том, чтобы понять, какие существуют брандмауэры. [6] На данный момент существует пять различных типов моделей брандмауэров:

Брандмауэр с фильтрацией пакетов

Этот метод основан на наиболее фундаментальном и самом старом типе модели брандмауэра. [3] Брандмауэры с фильтрацией пакетов, принцип процесса фильтрации, по сути, создают контрольную точку на коммутаторе трафика или маршрутизаторе. Брандмауэр напрямую проверяет информационные пакеты, проходящие через маршрутизатор или коммутатор, например, IP-адрес источника и получателя, номер пакета, номер порта и другие данные, не открывая пакет для изучения его информации. Он работает на сетевом уровне сетевой модели. Этот метод применяет множество принципов (с учетом содержимого полей IP и транспортных заголовков) для каждого пакета и, в зависимости от результата, выбирает либо передачу, либо уничтожение пакета.

Брандмауэры с контролем состояния

Межсетевые экраны с проверкой состояния: этот метод также называется «динамической фильтрацией пакетов» [3]. Брандмауэр с отслеживанием состояния в основном отслеживает состояние активных ссылок и использует эту информацию, чтобы решить, какой пакет следует пропустить через него. При таком подходе брандмауэр ведет запись динамической информации о сеансах TCP и UDP в табличной форме, включая IP-адрес отправителя и получателя сеанса,

номера портов, а также порядковый номер TCP. Записи делаются только для тех соединений UDP или TCP, которые соответствуют установленным критериям безопасности; пакеты, связанные с этими сеансами, могут проходить через брандмауэр. Сеансы, которые не согласуются с какой-либо политикой, отклоняются, как и любые полученные пакеты, которые не согласуются с текущим разделом таблицы [4].

Шлюзы на уровне цепи

Межсетевые экраны шлюза на уровне цепи. Брандмауэры на уровне цепи работают на сеансовом уровне сетевой модели и отслеживают TCP-соединение (трехстороннее рукопожатие), чтобы убедиться, что запрошенное соединение аутентифицировано или нет. Это происходит как виртуальная ассоциация между удаленным хостом и внутренними клиентами путем создания другой ассоциации между собой и удаленным хостом. Кроме того, он изменяет исходный IP-адрес в пакете и ставит свое собственное местоположение на место исходного IP-адреса пакета от конечных клиентов [3]. Таким образом, IP-адреса внутренних клиентов скрываются и проверяются от внешнего мира.

Брандмауэры шлюзов прокси или уровня приложений

Шлюзы приложений: брандмауэры приложений проверяют сетевые пакеты, чтобы проверить, являются ли данные действительными (на прикладном уровне), прежде чем разрешать установление соединения. Он исследует данные, инкапсулированные во всех пакетах, проходящих через сеть, и после этого предоставляет полное состояние соединения. Эти брандмауэры также проверяют другую информацию о безопасности, такую как пароли пользователей и запросы на обслуживание.

Межсетевые экраны нового поколения

Брандмауэр нового поколения(NGFW) — это устройство сетевой безопасности, предоставляющее возможности отслеживания состояния, которое выходит за рамки возможностей традиционных межсетевых экранов [4]. Стандарные функции для архитектуры брандмауэра следующего поколения является осведомленность о приложениях и контроль с глубокой проверкой пакетов (проверку содержимого пакета данных), проверки установления связи TCP и интегрированное предотвращение вторжений, которое автоматически останавливает атаки на вашу сеть[4].

Облачные брандмауэры

Брандмауэр как услуга (FWaaS) — это решение для обеспечения безопасности, основанное на облачном брандмауэре, которое предоставляет расширенные возможности брандмауэра уровня 7/следующего поколения (NGFW), включая средства управления доступом, такие как фильтрация URL-адресов, расширенное предотвращение угроз, системы предотвращения вторжений (IPS), и безопасность DNS[7].

Концепция FWaaS заключается не только в виртуализации сетевого брандмауэра. FWaaS позволяет организациям отказаться от брандмауэров, упростить свою ИТ-инфраструктуру и повысить кибербезопасность в целом. С помощью FWaaS управление централизовано с единой консоли, что позволяет организациям преодолевать проблемы контроля изменений, управления исправлениями, координации периодов простоя и управления политиками, связанными с устройствами NGFW, обеспечивая при этом согласованные политики во всей организации, где бы ни подключались пользователи. Сегодня все больше и больше организаций используют облачные сервисы, такие как SaaS, а с конечными точками повсюду и возникающими новыми угрозами брандмауэры больше не могут находиться в центре обработки данных. Они должны жить в облаке и масштабироваться, чтобы защищать ресурсы и сотрудников повсюду.

Литература

1. Гасымов В.А. Информация защита современный технологии, Баку, 2011,112 с.
2. Коломойцев В.С. Эффективность поэтапного применения средств защиты с пересечением областей обнаружения угроз, выпуск журнала № 3, 2018 год. 557-564с.
3. Как брандмауэр работает Комодо Безопасность Решения, https://ru.comodo.com/software/internet_security/firewall.php
4. Официальная страница CISCO https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/at-a-glance-c45-736624.html
5. Крис Сандерс и Джейсон Смит, Прикладной мониторинг сетевой безопасности. 2014, 101 с
6. Вэньлян Ду Интернет-безопасность - практический подход. 2019, 98-101 с
7. Белая книга Сети центров кибербезопасности ECHO Европейская сеть центров кибербезопасности (ECHO) Белая книга 1,
8. Чендлер Р., Гросс мл., Канетти Д. Хрупкое общественное предпочтение использованию кибератак: данные опросов, проведенных в Соединенных Штатах, Соединенном Королевстве и Израиле. Политика защиты от неуважения. 2021;42:135-62 с.
9. Кодекс этики IEEE. https://www.ieee.org/about/corporate/governance/p7-8.html
10. Платонов В. Программно-аппаратные средства защиты информации. М.: Академия, 2013.334 с.