Научная статья

Original article

УДК 004.424

ИНСТРУМЕНТЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ

OPERATING SYSTEM SECURITY TOOLS

Камбулов Данил Александрович, магистр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kambulov18@yandex.ru

Kambulov Danil Alexandrovich, Master, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kambulov18@yandex.ru

Аннотация: Брандмауэр веб-приложений или WAF - это инструмент безопасности для мониторинга, фильтрации и блокировки входящих и исходящих пакетов данных из веб-приложения или веб-сайта. WAF могут быть хостовыми, сетевыми или облачными и обычно развертываются через обратные прокси-серверы и размещаются перед приложением или веб-сайтом (или несколькими приложениями и сайтами).

WAF могут работать как сетевые устройства, серверные плагины или облачные сервисы, проверяя каждый пакет и анализируя логику прикладного уровня (уровень 7) в соответствии с правилами для фильтрации подозрительного или опасного трафика.

Abstract: Web Application Firewall or WAF is a security tool for monitoring, filtering and blocking incoming and outgoing data packets from a web application or website. WAFs can be hosted, networked, or cloud-based and are typically

deployed through reverse proxies and placed in front of an application or website (or multiple applications and sites).

WAFs can act as network devices, server plugins or cloud services, inspecting each packet and analyzing the application layer logic (layer 7) according to rules to filter suspicious or dangerous traffic.

Ключевые слова: безопасность, мониторинг, фильтрация, блокировка, входящий и исходящий пакет данных

Keywords: security, monitoring, filtering, blocking, incoming and outgoing data packet

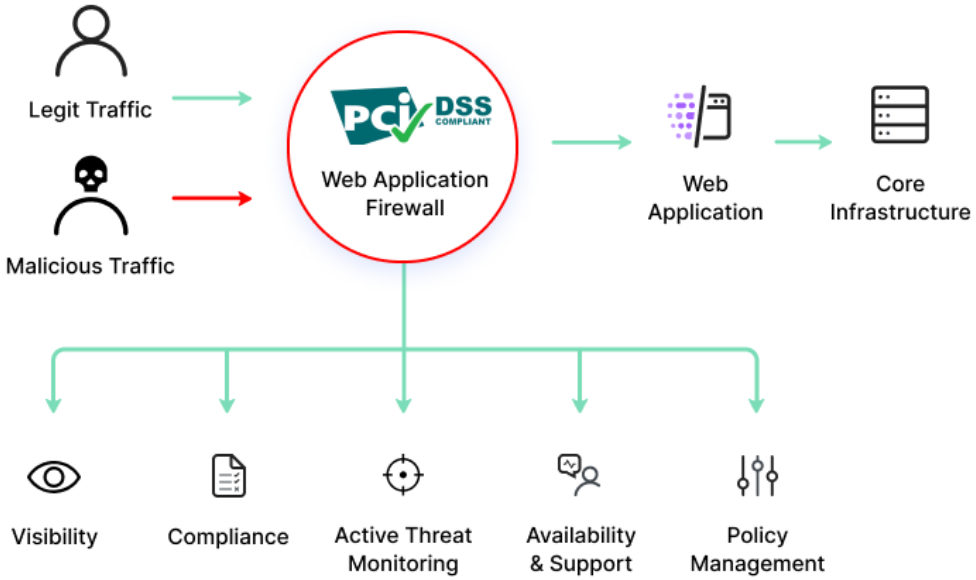
WAF важны для растущего числа организаций, предлагающих продукты или услуги в Интернете, включая разработчиков мобильных приложений, поставщиков социальных сетей и цифровых банкиров. WAF может помочь вам защитить конфиденциальные данные , такие как записи клиентов и данные платежных карт, и предотвратить утечку.

Организации обычно хранят большую часть своих конфиденциальных данных в серверной базе данных, к которой можно получить доступ через веб-приложения. Компании все чаще используют мобильные приложения и устройства IoT для облегчения бизнес-взаимодействия, при этом многие онлайн-транзакции происходят на уровне приложений. Злоумышленники часто нацелены на приложения, чтобы получить доступ к этим данным.

Использование WAF может помочь вам выполнить требования соответствия, такие как PCI DSS (стандарт безопасности данных индустрии платежных карт), который применяется к любой организации, обрабатывающей данные держателей карт, и требует установки брандмауэра. Таким образом, WAF является важным компонентом модели безопасности организации.

Важно иметь WAF, но рекомендуется сочетать его с другими мерами безопасности, такими как системы обнаружения вторжений (IDS), системы

предотвращения вторжений (IPS) и традиционные брандмауэры, чтобы получить модель глубокоэшелонированной защиты. .



Рабочий процесс WAF

Типы брандмауэров веб-приложений

Есть три основных способа реализовать WAF:

- **Сетевой WAF** - обычно аппаратный, он устанавливается локально, чтобы минимизировать задержку. Однако это самый дорогой тип WAF, требующий хранения и обслуживания физического оборудования.
- **WAF на основе хоста** - может быть полностью интегрирован в программное обеспечение приложения. Этот вариант дешевле, чем сетевые WAF, и более настраиваемый, но он требует значительных ресурсов локального сервера, сложен в реализации и может быть дорогим в обслуживании. Машину, используемую для запуска WAF на основе хоста, часто необходимо укрепить и настроить, что может занять время и быть дорогостоящим.
- **Облачный WAF** - доступное, легко реализуемое решение, которое обычно не требует предварительных вложений, при этом пользователи оплачивают ежемесячную или годовую подписку на услугу «Безопасность как услуга». Облачный WAF можно регулярно обновлять без

дополнительных затрат и без каких-либо усилий со стороны пользователя. Однако, поскольку вы полагаетесь на стороннюю организацию для управления своим WAF, важно убедиться, что облачные WAF имеют достаточные параметры настройки для соответствия бизнес-правилам вашей организации.

Функции и возможности WAF

Брандмауэры веб-приложений обычно предлагают следующие функции и возможности:

Базы данных сигнатур атак	Сигнатуры атак - это шаблоны, которые могут указывать на вредоносный трафик, включая типы запросов, аномальные ответы сервера и известные вредоносные IP-адреса. Раньше WAF полагались преимущественно на базы данных шаблонов атак, которые были менее эффективны против новых или неизвестных атак.
Анализ шаблонов трафика на базе искусственного интеллекта	Алгоритмы искусственного интеллекта позволяют проводить поведенческий анализ моделей трафика, используя поведенческие базовые параметры для различных типов трафика, чтобы обнаруживать аномалии, указывающие на атаку. Это позволяет обнаруживать атаки, которые не соответствуют известным вредоносным шаблонам.
Профилирование приложений	Это включает в себя анализ структуры приложения, включая типичные запросы, URL-адреса, значения и разрешенные типы данных. Это позволяет WAF выявлять и блокировать потенциально вредоносные запросы.
Настройка	Операторы могут определять правила безопасности, применяемые к трафику

	приложений. Это позволяет организациям настраивать поведение WAF в соответствии со своими потребностями и предотвращать блокировку легитимного трафика.
Механизмы корреляции	Они анализируют входящий трафик и сортируют его с помощью известных сигнатур атак, профилирования приложений, анализа искусственного интеллекта и настраиваемых правил, чтобы определить, следует ли его блокировать.
Платформы защиты от DDoS-атак	Вы можете интегрировать облачную платформу, которая защищает от распределенных атак типа «отказ в обслуживании» (DDoS). Если WAF обнаруживает DDoS-атаку , он может передавать трафик на платформу защиты от DDoS-атак, которая может обрабатывать большой объем атак.
Сети доставки контента (CDN)	WAF развертываются на границе сети, поэтому облачный WAF может предоставить CDN для кэширования веб-сайта и сокращения времени его загрузки. WAF развертывает CDN в нескольких точках присутствия (PoP), которые распределены по всему миру, поэтому пользователи обслуживаются из ближайшего PoP.

Технология WAF

WAF может быть встроен в программные плагины на стороне сервера или аппаратные устройства, или они могут быть предложены в качестве службы для фильтрации трафика. WAF могут защищать веб-приложения от вредоносных или взломанных конечных точек и функционировать как обратные прокси-серверы (в отличие от прокси-сервера, который защищает пользователей от вредоносных веб-сайтов).

WAF обеспечивают безопасность, перехватывая и исследуя каждый HTTP-запрос. Незаконный трафик можно проверить с помощью различных методов, таких как снятие отпечатков пальцев с устройства, анализ устройства ввода и проверка CAPTCHA , и, если они кажутся незаконными, их можно заблокировать.

В WAF предварительно загружены правила безопасности, которые могут обнаруживать и блокировать многие известные шаблоны атак - обычно к ним относятся основные уязвимости безопасности веб-приложений, поддерживаемые Open Web Application Security Project (OWASP).

Кроме того, организация может определять собственные правила и политики безопасности в соответствии с бизнес-логикой своего приложения. Для настройки и настройки WAF могут потребоваться специальные знания.

Модели безопасности WAF

WAF могут использовать позитивную или негативную модель безопасности или их комбинацию:

- **Модель позитивной безопасности** - позитивная модель безопасности WAF включает в себя белый список, который фильтрует трафик в соответствии со списком разрешенных элементов и действий - все, чего нет в списке, блокируется. Преимущество этой модели в том, что она может блокировать новые или неизвестные атаки, которые разработчик не ожидал.
- **Модель отрицательной безопасности** - отрицательная модель включает черный список (или список запретов), который блокирует только определенные элементы - все, что не входит в список, разрешено. Эту модель проще реализовать, но она не может гарантировать, что будут устранены все угрозы. Это также требует ведения потенциально длинного списка вредоносных сигнатур. Уровень безопасности зависит от количества введенных ограничений.

Литература

1. Толковый словарь по вычислительной технике. – М.: Издательский отдел "Русская редакция" ТОО "Channel trading Ltd", 2005.

2. Материалы сайта "Сервер информационных технологий". WEB: www.citforum.ru.
3. Хомоненко А. Базы данных: Учеб. Для вузов. – 2-е изд. – СПб., 2000.
4. Фёдорова А., Елманова Н. Базы данных для всех. –М.: Компьютер пресс , 2001.
5. Глушаков С.В., Ломотько. Базы данных (2001 год издания). – М.: АСТ, 2001.
6. Карпова Т. Базы данных: модели, разработка, реализация, 2001.
7. Когаловский М.Р. Энциклопедия технологий баз данных. –М.: Финансы и статистика, 2002.
8. Конноли Т., Бегг Л., Страчан А. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – 2-е изд. – Вильямс, 2000.
9. Ханенко В.Н. Информационные системы. – СПб.: Питер, 2001
10. Корнеев В.В., Гареев А.Ф. и др. Базы данных. Интеллектуальная обработка информации. М.: Изд. С.В. Молгачева, 2001.
11. Ребекка М. Райордан Основы реляционных баз данных, 2001.

References

1. Explanatory dictionary of computer technology. - M.: Publishing department "Russian edition" LLP "Channel trading Ltd", 2005.
2. Materials of the site "Information Technology Server". WEB: www.citforum.ru
3. Homonenko A. Databases: Proc. For universities. - 2nd ed. - St. Petersburg, 2000.
4. Fedorova A., Elmanova N. Databases for everyone. –M.: Computer press, 2001.
5. Glushakov S.V., Lomotko. Databases (2001 edition). – M.: AST, 2001.
6. Karpova T. Databases: models, development, implementation, 2001.
7. Kogalovsky M.R. Database Technology Encyclopedia. –M.: Finance and statistics, 2002.

8. Connolly T., Begg L., Strachan A. Databases. Design, implementation and support. Theory and practice. - 2nd ed. - Williams, 2000.
9. Khanenko V.N. Information Systems. - St. Petersburg: Peter, 2001
10. Korneev V.V., Gareev A.F. and other databases. Intelligent information processing. M.: Ed. S.V. Molgacheva, 2001.
11. Rebecca M. Riordan Fundamentals of Relational Databases, 2001.

© Камбулов Д. А., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Камбулов Д. А. ИНСТРУМЕНТЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.