ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНТЕРНЕТ ВЕЩЕЙ В ПРОМЫШЛЕННОСТИ 4.0 С ИСПОЛЬЗОВАНИЕМ WAF

Muhiddin Shakarov
Nurafshon branch of Tashkent University of Information Technologies
named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Nuriddin Safoev
Tashkent University of Information Technologies named after
Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Nurbek Nasrullaev
Nurafshon branch of Tashkent University of Information Technologies
named after Muhammad al-Khwarizmi
Department of Cybersecurity and criminology
Tashkent, Uzbekistan

Аннотация. Сегодня возрастает необходимость удаленно управлять бытовой техникой, ставить перед ней задачи и получать от нее нужную информацию. Интернет вещей (IoT) — это совокупность объектов, сервисов и устройств, соединенных друг с другом для обмена данными в различных отраслях и приложениях с использованием Интернета. Однако существуют риски и опасности, такие как физические атаки, атаки по сторонним каналам, атаки криптоанализа, программные атаки, сетевые атаки, нацеленные на устройства IoT. Сетевые атаки не требуют физического доступа к сети для создания серьезных сбоев. Брандмауэр делит сеть на две части: доверенную сеть и ненадежную сеть. В этой работе мы рассматриваем безопасность IoT с помощью брандмауэров веб-приложений.

Ключевые слова: Умный дом, Интернет вещей, WAF, атака, OWASP.

1 Введение

Интернет вещей (IoT) относится к сети физических объектов со встроенными датчиками, программным обеспечением и другими технологиями, позволяющими устройствам и системам подключаться и обмениваться данными через Интернет. Эти устройства могут варьироваться от простых бытовых

приборов до сложных промышленных устройств. Однако проблема безопасности становится большой проблемой для IoT. Как правило, успешные атаки происходят на прикладном уровне (модель OSI — Layer 7), так как это все еще самая уязвимая часть.

Почти все веб-приложения имеют уязвимости и ошибки, которые могут привести к множеству различных потенциальных угроз, нацеленных на эту уязвимость. Исследования консорциума Web Security Consortium показывают, что более 49% веб-приложений обнаруживают уязвимости высокого риска во время автоматического сканирования [2].

Аппаратные устройства, которые отделяют корпоративные сети от Интернета путем фильтрации пакетов, считаются первым поколением брандмауэров, и эти типы брандмауэров предотвращают атаки до уровня 3 (сетевого уровня) модели OSI. Принцип работы этих межсетевых экранов заключается в следующем, то есть он проверяет адрес (входящий и исходящий) и порт (входящий и исходящий) пакетов на основе набора правил фильтрации и уничтожает их или пересылает в указанное место назначения на основе по существующим правилам. Этот тип брандмауэра называется брандмауэром без сохранения состояния и не проверяет трафик, а только проверяет, соответствует ли пакет существующим правилам безопасности. Эти типы брандмауэров требуют определенной настройки для достижения соответствующего уровня защиты.

Межсетевые экраны второго поколения могут работать до уровня 4 модели OSI и обеспечивать перечисленные выше функции, а также возможность отслеживать текущие интернет-соединения или разрешать/запрещать трафик в зависимости от состояния этих соединений. Вот почему эти типы брандмауэров обеспечивают больше удобства и безопасности.

Аппаратные брандмауэры в основном использовались в промышленности в 90-х годах для защиты внутренних сетей от более крупных сетей. В начале 90-х стали появляться несколько известных антивирусных программ (panda, Norton, F-Secure). Они стали важными, потому что их можно было легко установить, настроить и, в свою очередь, действовать как брандмауэры на ПК, уменьшая потребность в аппаратных брандмауэрах.

Термин брандмауэр веб-приложений (WAF) появился в 2005 году в результате стремительного развития мира Интернета и на фоне проблемы безопасности. Эти типы брандмауэров считались первыми брандмауэрами, предотвращающими атаки до уровня 7 OSI (уровень приложений). В последние годы в связи с активным ростом количества высокоуровневых угроз и атак

увеличивается спрос компаний на WAF. По данным на 2022 год, выручка мирового рынка WAF составляет 5,8 млрд долларов [1].

Ниже перечислены некоторые категории атак, которые происходят в веб-приложениях:

- Внедрения скриптов, особенно SQL-внедрений;
- Изменение параметров (внедрение скриптов);
- принудительный просмотр;
- Межсайтовый скриптинг;
- Человек в ближней атаке;
- распределенный отказ в обслуживании (DDoS);
- Перехват сеанса и фальсификация файлов cookie;
- переполнение буфера;

Брандмауэры веб-приложений стали решением для защиты приложений от вышеуказанных атак и онлайн-мошенничества [3]. Остальную информацию, связанную с исследованием безопасности, можно получить в [10-22].

2. Основная часть

Инструмент (устройство, серверный подключаемый модуль или фильтр), который применяет набор правил к HTTP-диалогу, называется брандмауэром веб-приложений (WAF), и WAF находится на веб-сервере или промежуточном прокси-сервере, который он защищает. Целью этого инструмента WAF является защита веб-приложений от вредоносного содержимого или злонамеренного поведения, и он отдает приоритет контролю над прикладным уровнем. Таким образом, он отлично справляется с предотвращением атак, которые не могут быть предотвращены системами обнаружения вторжений (IDS) и сетевыми брандмауэрами.

Веб-приложение может изменить поведение веб-приложения, не требуя каких-либо изменений, и именно поэтому брандмауэр веб-приложения является мощным инструментом. Более подробная информация раскрывается путем изучения части данных пакетов. Это называется гранулярностью пакетов [5]. Заголовок HTTP может содержать запрос, который может включать файлы cookie, пользовательские агенты и многое другое. Веб-приложения часто неуязвимы для угроз, исходящих от злоумышленников. Кроме того, исправление известных дыр в системе безопасности может занять гораздо больше времени. Очень важно внедрить WAF на системы, уязвимые для атак.

Принцип работы всех WAF практически одинаков, то есть они выступают промежуточным элементом между приложением сайта и посетителем[10].

Реализация технологий WAF устанавливается в качестве помощника, а не за счет замены других элементов управления.

WAF служит для обеспечения безопасности веб-приложений путем реализации политик или правил безопасности. WAF может использовать положительную или отрицательную модель безопасности [4].

Модель положительной безопасности работает следующим образом, что означает, что принимается решение о том, какие запросы принимаются, а все остальные запросы отклоняются. Эта модель безопасности также известна как белый список, и этот метод считается более эффективным и безопасным. Но эту модель немного сложно применить, потому что на этот процесс влияют частые изменения приложений. Однако в отрицательной модели безопасности он контролирует процесс, запрещая все внешние запросы и разрешая все остальное. Эта модель безопасности также называется черным списком. То есть входящий трафик сравнивается с сигнатурами атак и соответствующие данные блокируются. Эти политики не учитывают производительность приложения.

Существуют разные способы установки инструмента WAF:

Обратный прокси: Обратный прокси-сервер действует от имени вашего веб-сервера, получает внешние запросы (например, от ваших клиентов) и определяет, как их обрабатывать. WAF обрабатывает запрос, либо проверяя, либо блокируя запрос. Веб-ускоритель пытается ответить на запрос кэшированными данными. Обеспечивает безопасность до уровня 7 (прикладной уровень) модели OSI.

Мост: В этом же режиме WAF устанавливается inline и выполняет роль коммутатора, а также дополнительно выполняет расшифровку неактивного SSL-пароля. Он также может блокировать трафик, отбрасывая поврежденные пакеты. Он обеспечивает более высокую производительность, чем обратный прокси-сервер, с устойчивостью к сетевым изменениям. В целом архитектура этого режима аналогична архитектуре обратного прокси WAF.

Внеполосный: Во внешнем режиме существующие правила проверяют HTTP-запросы и ответы через дубликаты трафика, чтобы обеспечить обнаружение WAF.

Резидент сервера: Резидентный или встроенный WAF на сервере — это программное обеспечение, установленное на хосте, работающем в Интернете. Это можно сделать как отдельное приложение или как плагин веб-сервера. Серверные WAF не так функциональны, как их аналоги сетевых устройств, но устраняют дополнительную сетевую точку отказа.

Облако: Это недавно добавленный режим, который использует облачного провайдера для реализации решения WAF. Он работает как вариант обратного

прокси-сервера, при этом система имен общедоступных доменов (DNS) настроена так, чтобы указывать на облачного провайдера, который может создать другое подключение к веб-ресурсу.

3. Обсуждение функций WAF с преимуществами

Чтобы лучше понять структуру WAF, нам необходимо проанализировать наиболее распространенные функции WAF. В таблице ниже описаны важные функции и некоторые расширенные наборы функций различных WAF.

Таблица 1. Функции брандмауэра веб-приложений

Особенность	Основной брандмауэр веб-приложений	Расширенный брандмауэр веб-риложений	Традиционные средства безопасности
Понимание протоколов прикладного уровня (L7)	+		
- протоколов HTTPS	+		
- XML средства		+	
Блокировка IP	+		
- По геолокации		+	
- По репутации		+	
Блокировка (Запрос)	+		
Блокировка (ответ)		+	
Модель (отрицательная безопасность)	+		
Модель (позитивная безопасность)		+	
Свойство для виртуальных исправлений	+		
Функция декодирования символов	+		
Функция смягчения грубой силы	+		
Защитный файл cookie		+	
Функция для ведения журнала	+		
Функция для отчетов		+	
Функция сканирования уязвимостей			+
Функция отладки программного обеспечения			+

Мы можем предоставить эти брандмауэры в качестве эффективного инструмента, защищающего веб-приложение от несанкционированного доступа. Это также полезно для любого онлайн-бизнеса (электронная коммерция,

интернет-магазины), поскольку оно обеспечивает безопасность личной информации пользователя. WAF может автоматически фильтровать вредоносный веб-трафик. А также позволяет вручную решать, кого блокировать на сайте [9].

WAF защищают систему от:

- Автоматическая защита от разнообразных угроз
- DDoS-атаки
- Внедрение SQL, спам в комментариях
- Атаки на конкретные приложения
- XSS
- Отчетность в режиме реального времени и надежное ведение журнала

Сравнивая функции WAF с функциями системы защиты от вторжений (IPS), мы видим, что между этими двумя системами есть некоторые сходства и некоторые различия. IPS рассматривается как внутренний инспектор пакетов, который имеет возможность отклонить пакет или разорвать соединение. То есть он в основном полагается на обнаружение сигнатур, но не понимает веб-приложения, такие как WAF. В таблице ниже мы сравниваем функции IPS и функции WAF [8].

Таблица 2. Сравнение функций WAF и IPS

Функция безопасности	**IPS**	**WAF**
SQL-инъекция и XSS	Существуют, но ограничены	Существовать
Проекция веб-сервисов	Не существует	Существовать
Кодированный трафик	Не существует	Существовать
Проверяйте HTTPS-трафик	Не существует	Существовать
Фальсификация/перехват сеанса	Не существует	Существовать
Защита от кражи данных, маскировка	Не существует	Существовать
Предотвращение CSRF	Не существует	Существовать
Защита от контроля скорости	Не существует	Существовать
Защита от вирусов	Существовать	Существовать
Защита от DOS прикладного уровня	Не существует	Существовать
Подход грубой силы	Не существует	Существовать
Принудительное предотвращение просмотра	Не существует	Существовать
Запрос, ответ переписать	Не существует	Существовать
Ведение журнала доступа к приложениям и контрольные журналы пользователей	Не существует	Существовать

4. Выводы

Наиболее важным аспектом Интернета вещей является возможность подключения к чему угодно, в любое время и в любом месте из любой сети и службы. Но безопасность — это отдельная тема, а это означает, что устройства IoT сыграли важную роль в DDoS-атаках, и мы все еще находимся в начале тенденции IoT. WAF используется для фильтрации вредоносного трафика из веб-трафика. В этой статье мы попытались осветить эффективность инструмента WAF и его роль в безопасности веб-приложений.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Markets & Markets, " Web Application Firewall Market Size and Share," [online]. Available: https://www.marketsandmarkets.com/Market-Reports/web-application-firewall-market-176479811.html [Accessed 18th July 2022].
2. Pałka, Dariusz, and Marek Zachara. "Learning web application firewall-benefits and caveats." International Conference on Availability, Reliability, and Security. Springer, Berlin, Heidelberg, 2011.
3. Hope, Paco, and Ben Walther. Web security testing cookbook: systematic techniques to find problems fast. " O‘Reilly Media, Inc.", 2008.
4. Pubal, Jason. "Web Application Firewalls." SANS Institute Reading Room (2015).
5. Briscoe, Neil. "Understanding the OSI 7-layer model." PC Network Advisor 120.2 (2000): 13-15.
6. Endraca, Alexander, et al. "Web Application Fi rewall (W AF)." International Journal of e-Education, e-Business, e-Management and e-Learning 3.6 (2013): 451.
7. Narayana, Srikar. "Security Analysis of Web Application for Industrial Internet of Things." (2022).
8. Dupont, Benoit. "The cyber security environment to 2022: trends, drivers and implications." Drivers and Implications (2012).
9. Clincy, Victor, and Hossain Shahriar. "Web application firewall: Network security models and configuration." 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 1. IEEE, 2018.
10. Amouei, Mohammadhossein, Mohsen Rezvani, and Mansoor Fateh. "RAT: Reinforcement-Learning-Driven and Adaptive Testing for Vulnerability Discovery in Web Application Firewalls." IEEE Transactions on Dependable and Secure Computing (2021).

11. Safoev, N., & Nasrullaev, N. (2021, November). Low area QCA Demultiplexer Design. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 01-05). IEEE.
12. Rajaboevich, G. S., Baxtiyarovich, N. N., & Salimovna, F. D. (2020, November). Methods and intelligent mechanisms for constructing cyberattack detection components on distance-learning systems. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.
13. Yakubdjanovna, I. D., Bakhtiyarovich, N. N., & Iqbol Ubaydullayevna, X. (2020, November). Implementation of intercorporate correlation of information security messages and audits. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
14. Baxtiyorovich, N. N., & Ubaydullaevna, H. I. (2019, November). Method of analyzing of antivirus errors when audit provides. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-3). IEEE.
15. Bakhodir, Y., Nurbek, N., & Odiljon, Z. (2019). Methods for applying of scheme of packet filtering rules. International Journal of Innovative Technology and Exploring Engineering, 8(11), 1014-1019.
16. Gulomov, S. R., & Bakhtiyorovich, N. N. (2016, November). Method for security monitoring and special filtering traffic mode in info communication systems. In 2016 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.
17. N Akhmedov, H Khujamatov, A Lazarev, M Seidullayev (2021, November). Application of LPWAN technologies for the implementation of iot projects in the Republic of Uzbekistan. In 2021 International Conference on Information Science and Communications Technologies (ICISCT).IEEE.