WEB APPLICATION FIREWALL НОВОГО ПОКОЛЕНИЯ

SOLIDWALL

В настоящее время веб-технологии получают все более широкое распространение. Они используются повсеместно для создания самых разнообразных приложений и сервисов – от простых сайтов-«визиток» до сложнейших ресурсов электронной коммерции, систем управления предприятием или систем межведомственного взаимодействия между государственными органами.

При этом веб-технологии на данный момент, к сожалению, являются одним из основных источником рисков, связанных с информационной безопасностью.

По статистике атаки на веб-приложения стоят на первом месте среди «технологичных» причин инцидентов информационной безопасности – после сбоев оборудования, действий инсайдеров, краж или потери устройств – и опережают даже DDoS атаки. При этом ущерб от подобных инцидентов может быть очень значительным.

Решение SolidWall WAF создавалось с учетом богатого опыта разработчиков в области анализа защищенности веб-приложений и настройки различных решений класса WAF. Оно лишено многих недостатков, свойственных современным средствам защиты, способно обеспечить высокий уровень безопасности любых, даже самых сложных приложений, а также обладает гибкими возможностями по настройке и широким дополнительным функционалом для решения индивидуальных задач клиента.

НЕДОСТАТКИ СОВРЕМЕННЫХ РЕШЕНИЙ

Во многих организациях уже имеются межсетевые экраны и системы обнаружения вторжений, способные инспектировать веб-трафик и реагировать на простые и хорошо известные виды атак, однако для защиты сложных веб-приложений индивидуальной разработки эти средства не подходят.

Для защиты таких ресурсов относительно недавно появились специализированные решения – межсетевые экраны уровня приложения (Web Application Firewall), которые способны учитывать особенности работы конкретного приложения и таким образом, противодействовать направленным на него атакам.

Однако решения этого класса, присутствующие в настоящее время на рынке все еще обладают рядом существенных недостатков.

- ***Использование устаревших моделей представления веб-приложений.*** В большинстве WAF моделью клиентской части приложения является концепция "HTML-страница со ссылками и формами", URL, набор исполняемых файлов на стороне сервера. Но с развитием подходов к разработке веб-приложений (MVC, SOA, REST, API-centric) эта концепция устарела. В результате выразительные средства современных WAF не позволяют описывать структуру и нормальное поведение современных приложений ни вручную, ни, тем более, автоматически.

- ***Слабая защита от определенных классов атак.*** При разработке веб-приложений часто применяются распространенные фреймворки, которые реализуют многие механизмы безопасности (защита от CSRF, работа с СУБД через ORM, компонентное построение веб-интерфейсов для защиты от XSS). Однако задачи интеграции компонент и реализация бизнес-логики всегда остаются на разработчике, что делает актуальными атаки на уязвимости авторизации, ошибки в реализации сложных многоступенчатых процессов (OAuth, 3DSecure и т.п.), атаки на исчерпание ресурсов (т.н. "умный" DoS). Современные WAF-решения либо в принципе неспособны бороться с подобными атаками, либо решают эту задачу лишь частично, с использованием Ad-hoc Методов («костылей» и «велосипедов»), имеющих ограниченную применимость и требующих трудоёмкой ручной настройки.

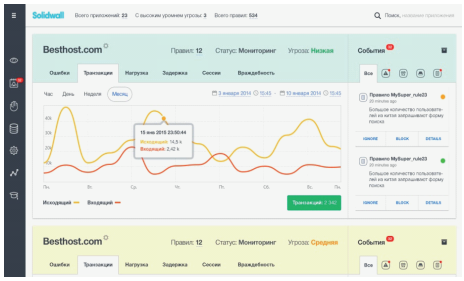
- ***Ограниченная модель угроз.*** Современные WAF изначально разрабатывались для противодействия внешним атакам, поэтому в них как правило отсутствует возможность выявления угроз на бизнес-уровне, не нарушающих общую логику работы приложения – например, несанкционированный доступ к данным или несанкционированные действия легитимных пользователей, утечки конфиденциальной информации, некорректные или подозрительные транзакции, нарушение политики информационной безопасности и т.п.

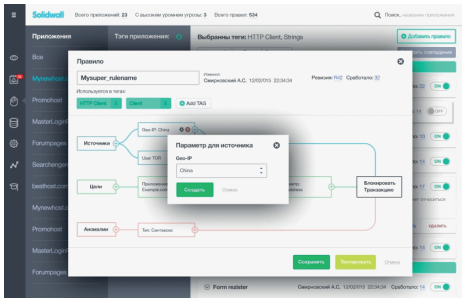
WEB APPLICATION FIREWALL НОВОГО ПОКОЛЕНИЯ

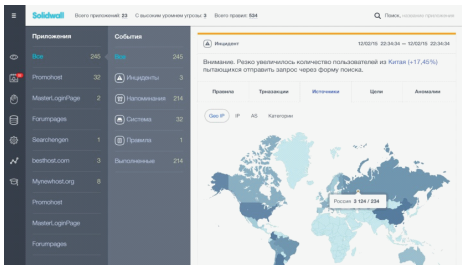
SOLIDWALL

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ РЕШЕНИЯ

- Сочетание двух методов обнаружения: сигнатурного и на основе положительной модели работы приложения дают высокую степень защиты как от широко распространенных видов атак, так и от направленных атак.
- Использование специальных механизмов подавления ложных срабатываний позволяет снизить их количество до минимума
- Разбор HTTP запросов и ответов с любым уровнем сложности, поддержка современных фреймворков, структурных схем передачи параметров для XML, JSON и т.п., в т.ч. вложенных (base64-encoded json в xml), контроль механизмов идентификации и аутентификации, контроль сессий
- Разбор бизнес-логики приложения с использованием механизма Smart Action. Определение пользователей, их действий в приложении, параметров и данных действий. Эта информация может быть использована для подавления ложных срабатываний, создания положительной модели работы приложения или экспортирована в другие системы для дальнейшего анализа.
- Возможность устранения уязвимостей, не только привнесенных на уровне реализации приложения , но также уязвимостей на уровне архитектуры или логики работы приложения (например отсутствующие или неправильно спроектированные механизмы безопасности)
- Гибкие механизмы настройки, дающие возможность адаптировать систему под приложения любой сложности, обслуживающие как внешних, так и внутренних пользователей.
- Профессиональные сервисы от разработчика по внедрению, настройке системы, мониторингу и реагированию на инциденты позволяют получить максимум эффективности от использования системы.





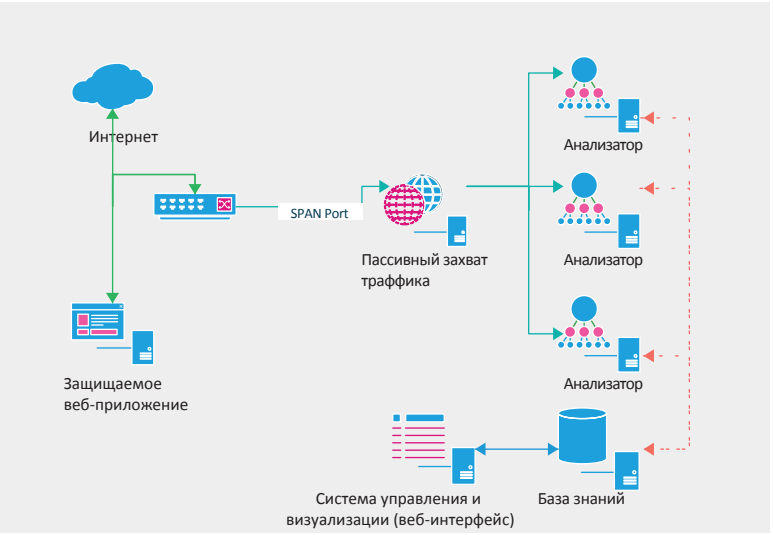


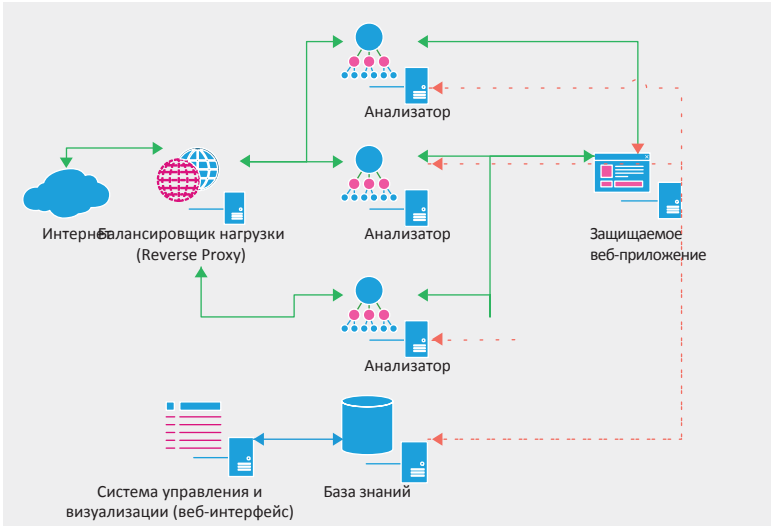
WEB APPLICATION FIREWALL НОВОГО ПОКОЛЕНИЯ

SOLIDWALL

АРХИТЕКТУРНЫЕ ВОЗМОЖНОСТИ РЕШЕНИЯ

- Может поставляться в виде ПО, виртуального аппаратного комплекса Vmware
- Возможность работы как в режиме мониторинга так и в режиме Inline (Reverse proxy, блокировка и модификация запросов/ответов).
- Централизованное управление с ипользованием веб-интерфейса, поддержка распределенных архитектур с несколькими сенсорами. Возможность защиты нескольких веб-приложений на одном сенсоре.
- Интеграция с другими компонентами инфраструктуры доставки приложений – балансировщики нагрузки, SSL концентраторы и т.д.
- Возможность интеграции со сторонними решениями для защиты веб-приложений SIEM, IDM, DLP, BI, Antifraud и т.д.





СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

Защита внешних веб-ресурсов от атак. Системы ДБО, интернет-ритейл, информационные ресурсы, личные кабинеты, торговые площадки, порталы гос.услуг.

Защита корпоративных веб-приложений. Порталы, ERP, CRM, системы ЭДО, BI, B2B-сервисы и т.п. Контроль действий пользователей, защита от НСД, предотвращение утечки конфиденциальной информации.

Безопасность облачных сервисов. Возможность защиты как самих облачных сервисов от внешних атак, так и возможность контроля использования облачных сервисов сотрудниками и контрагентами.

Контроль транзакций, противодействие мошенничеству. Значимые технические данные об HTTP-Запросах, информация о пользователях, выполняемых ими действиях и транзакциях могут передаваться в специализированную систему для дальнейшего анализа.

Защита критичных и фиксированных систем. Использование полной модели представления позволяет полностью зафиксировать протокол взаимодействия с критичным приложением на всех уровнях и запретить любые отклонения от нормы.

Контроль действий привилегированных пользователей. Благодаря механизмам контроля сессий и действий пользователей имеется возможность полностью контролировать доступ привилегированных пользователей к веб-консоли администрирования.

Анализ использования веб-сервисов. Решение позволяет собирать всеобъемлющую статистику работы веб-приложения, находить ошибки и узкие места, возможности для улучшения.

WEB APPLICATION FIREWALL НОВОГО ПОКОЛЕНИЯ

SOLIDWALL

ПРОФЕССИОНАЛЬНЫЕ СЕРВИСЫ

Сервисы оказываются высококвалифицированными российскими специалистами, имеющими богатый опыт в области противодействия интернет-угрозам.

- Анализ уязвимостей веб-приложений и оценка связанных с ними рисков информационной безопасности
- Пилотное тестирование предлагаемого решения для оценки его потенциальной эффективности.
- Техническое проектирование и внедрение системы SolidWall в инфраструктуру Заказчика
- Тонкая настройка системы для защиты конкретных веб-приложений. Адаптация WAF под изменения приложений клиента, подключение дополнительных приложений.
- Мониторинг угроз, реагирование на инциденты. Поддержка клиента при расследовании инцидентов ИБ.
- Разработка процесса реагирования на инциденты информационной безопасности.
- Обучение персонала заказчика навыкам работы с системой, а также основам противодействия угрозам в сети Интернет.
- Техническая и консультационная поддержка
- Доработка системы в случае нестандартных требований со стороны клиента. Изменение функциональности WAF по запросу клиента (формы отчетности, изменение сценариев работы пользовательским интерфейсом).

Российская компания SolidSoft – отечественный разработчик систем по защите веб-приложений.

Российская компания SolidSoft – отечественный разработчик систем по защите веб-приложений.

В 2014 году SolidSoft была выделена в отдельную компанию из лаборатории безопасности SolidLab с целью создания продуктов и решений по информационной безопасности на основе богатого опыта экспертов лаборатории.

Основу команды составляют выпускники, аспиранты и исследователи группы, занимающейся актуальными вопросами практической безопасности на факультете ВМК Московского Государственного университета. С 2009 года команда активно участвует в CTF-соревнованиях под именем «Bushwhackers». По итогам каждого соревнования Bushwhackers стабильно занимает место среди 15 лучших команд мира.

SOLIDWALL

+7 (499) 705-76-57 info@solidlab.ru

www.solidwall.ru / www.solidlab.ru