Positive Technologies
Application Firewall

ОПИСАНИЕ ПРОДУКТА

POSITIVE TECHNOLOGIES

С каждым годом организации все активнее используют интернет, включая мобильные и ERP-приложения, тем самым повышая производительность своей работы и оперативность услуг. Но с увеличением числа приложений растет и количество уязвимостей, которыми могут воспользоваться злоумышленники.

По данным компании Verizon, в 2016 году от кибератак чаще всего страдали именно веб-приложения. В отчете также сообщается, что веб-атаки составляют 40% всех атак, хотя в 2015 году эта цифра составляла лишь 9,4%.

1. БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ: КЛЮЧЕВЫЕ ЗАДАЧИ

Какие уязвимости в приложениях используют злоумышленники? Согласно проведенному Positive Technologies исследованию корпоративных приложений для финансовых учреждений, только треть возникающих проблем связана с недостатками конфигурации и отсутствием актуальных обновлений безопасности. Большинство угроз связаны с уязвимостями, возникающими вследствие ошибок разработчиков, и не всегда могут быть выявлены обычными сканерами, системами обнаружения вторжений и межсетевыми экранами.

Типы уязвимостей

Как результат, за последние годы средний уровень защищенности корпоративных систем заметно снизился. Ниже приведены основные проблемы, с которыми сталкиваются современные системы обеспечения безопасности приложений:

- Применение методов безопасной разработки (secure software development lifecycle, SSDL) значительно снижает издержки, связанные с ошибками в коде, при условии их быстрого обнаружения и исправления на ранних стадиях разработки. Однако найти эффективные автоматизированные решения для анализа кода — сложная задача.
- Современные корпоративные приложения используют разные языки программирования, протоколы и технологии, а также различные сторонние компоненты. Защита таких приложений требует всестороннего анализа их структуры, контекста использования и схем взаимодействия с пользователями.
- Злоумышленники активно используют уязвимости нулевого дня, что делает сигнатурные методы анализа бесполезными. В настоящий момент назрела необходимость в новых решениях, способных к адаптации, самообучению и поведенческому анализу.
- В современных реалиях операторам сетевых экранов приходится анализировать тысячи подозрительных событий, что превращается в практически невыполнимую задачу без продвинутых технологий автоматической сортировки, ранжирования и интеллектуальной предобработки информации.
- Даже известные уязвимости невозможно устранить сразу: патчинг ERP-систем или АБС может занимать месяцы. Система безопасности приложений должна обладать механизмами защиты от потенциальных атак, на время пока разработчики вносят исправления в код.

2. PT APPLICATION FIREWALL: КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

Система Positive Technologies Application Firewall (PT AF) — это мощный ответ на современные вызовы, возникающие при защите веб-порталов, ERP-систем и мобильных приложений. Благодаря комбинации инновационных технологий и уникальных механизмов PT AF обеспечивает непрерывную проактивную защиту веб-приложений от большинства атак, включая OWASP Top 10, автоматизированные атаки, атаки на стороне клиента и атаки нулевого дня.

Ключевые возможности PT AF:

- **Автоматическое блокирование атак нулевого дня.** PT Application Firewall анализирует сетевой трафик, системные журналы и действия пользователей для создания актуальной статистической модели функционирования приложения. Такой подход позволяет перейти от сигнатурного анализа к интеллектуальному, при котором выявляются аномальные запросы и поведение. В сочетании с другими защитными механизмами это позволяет блокировать атаки нулевого дня без дополнительной настройки профиля безопасности.
- **Быстрое и точное выявление основных угроз.** PT Application Firewall может отсеивать незначительные события безопасности, группировать сходные срабатывания и выстраивать цепочки развития атак — от шпионажа до хищения данных или установки закладок. Вместо списка из тысяч потенциальных атак ИБ-специалисты получают несколько десятков действительно важных сообщений.
- **P-Code: мгновенная целевая защита.** Технология виртуального патчинга позволяет защитить приложение до исправления небезопасного кода. Однако в большинстве WAF создание патчей происходит вручную. Уникальный анализатор исходного кода с функцией генерации эксплойтов (P-Code) позволяет автоматически выявлять уязвимости и создавать виртуальные патчи для PT Application Firewall, а также обеспечивает разработчиков точной информацией об уязвимостях, значительно сокращая расходы на исправление и тестирование.
- **Расширенная защита от DDoS-атак уровня приложений.** С помощью алгоритмов машинного обучения продукт автоматически выполняет непрерывное профилирование поведения пользователей. В результате можно отслеживать активности, отличающиеся от нормального пользовательского поведения, включая попытки совершить DDoS-атаки уровня приложений. Информация о подозрительных активностях поступает заблаговременно, чтобы специалисты по безопасности могли принять меры по защите и предотвратить сбои в работе приложения. Расширенные возможности PT AF устраняют необходимость использования сторонних средств мониторинга DDoS-атак уровня приложений.
- **Защита от программ-роботов (bot mitigation).** Автоматическое профилирование поведения пользователей также позволяет оперативно обнаруживать автоматизированные атаки, осуществляемые с целью кражи уникального контента или размещения несанкционированного контента на защищаемом сайте. При этом PT AF не блокирует поисковые боты, тем самым не нарушая индексацию сайта.
- **Предотвращение утечки данных (DLP).** Весь исходящий трафик находится под контролем, и любая чувствительная информация блокируется автоматически, не требуя внимания администратора.
- **Маскирование данных.** Администратор может создавать правила определения чувствительных данных, к примеру паспортных данных или номеров банковских карт. Эти правила можно применять для маскировки такой информации от третьих лиц или даже от администраторов PT Application Firewall. Это позволяет добиваться максимального уровня конфиденциальности данных конечных пользователей.

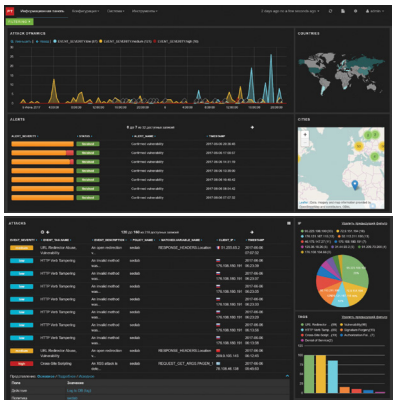
Компания Positive Technologies в третий раз подряд стала визионером магического квадранта Gartner по безопасности веб-приложений (Gartner Magic Quadrant for Web Application Firewalls 2017).

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ:

- **Проактивная защита** запросов, данных и файлов cookies позволяет блокировать такие атаки, как межсайтовая подделка запроса (CSRF), даже если разработчики не реализовали соответствующих механизмов защиты в самом приложении.
- **Эффективное встраивание в СУИБ организации:** интеграция с антивирусами, DLP-, анти-DDoS- и SIEM-системами, а также со сторонними решениями (Check Point, Arbor) — для многоуровневой защиты.
- **Защита от обхода.** PT AF обрабатывает данные с учетом специфики защищаемого сервера, анализирует XML, JSON и другие форматы данных современных порталов и мобильных приложений. Это позволяет противодействовать большинству методов обхода межсетевого экрана, включая HTTP Parameter Contamination и HTTP Parameter Pollution.
- **Помощь в выполнении требований PCI DSS** и других международных, государственных и корпоративных стандартов безопасности.

PT Application Firewall сертифицирован по новым требованиям ФСТЭК России.

3. ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ



Каждая отрасль обладает уникальным набором особенностей и требований к практической безопасности. Имея за плечами более 15 лет исследований и огромную базу знаний, эксперты Positive Technologies понимают, как защитить бизнес любого масштаба и профиля. Каждое внедрение PT Application Firewall осуществляется с учетом специфики инфраструктуры заказчика.

Банки и финансовые учреждения

Особенности:

- Критически важные приложения зачастую используются как самими банками, так и их партнерами: ДБО, CRM, приложения для трейдинга.
- Существует множество сторонних приложений, в которых банки сами не могут устранить уязвимости.
- Непрерывная работа практически не оставляет возможности для установки актуальных обновлений безопасности.
- Часто используются системы, обладающие малой (или нулевой) степенью защищенности.
- Повышенные риски атак (ручных и автоматизированных) на клиентов банковских приложений.
- Необходимость соблюдения стандарта безопасности данных индустрии платежных карт PCI DSS и требований регулирующих органов.

РЕШЕНИЯ POSITIVE TECHNOLOGIES:

- Обнаружение бэкдоров и уязвимостей, представляющих угрозу для конфиденциальной информации и незашифрованных данных
- Самообучающиеся механизмы
- Мониторинг и идентификация пользователей, обнаружение мошенничества
- Виртуальный патчинг
- Возможность замаскировать персональные данные пользователя (номера банковских карт, номер паспорта и т. п.)
- Возможность поддерживать нормальную работу приложения в случае незначительных дефектов

Медиа

Особенности:

- Приложения доступны для всех интернет-пользователей.
- Часто обновляемый контент и интеграция с большим числом сайтов (рекламные и партнерские сайты, социальные сети).
- Онлайн-вещание и XML-шлюзы для передачи данных.
- Атаки хактивистов, конкурентов и преступников.

- Автоматическое обучение с использованием параметров приложения
- Защита от DDoS-атак уровня приложений
- Обнаружение компрометации сайта и утечки данных
- Поведенческий анализ: обнаружение подозрительной активности, в частности программ-роботов

Телеком-операторы

Особенности:

- Множество различных приложений, включая порталы самообслуживания, VAS/MMS-порталы для клиентов, мобильные и облачные приложения.
- Конвергенция и тесная интеграция приводят к эффекту домино, когда отказ одного элемента приводит к возникновению проблем во всех других.
- Интеграция систем массового обслуживания с платежными шлюзами увеличивает угрозу мошенничества.

- Поддержка VAS/MMS-модели: защита клиентских приложений
- Поведенческий анализ: обнаружение подозрительной активности и программ-роботов
- Защита от DDoS-атак на уровне приложений
- Защита мобильных версий приложений

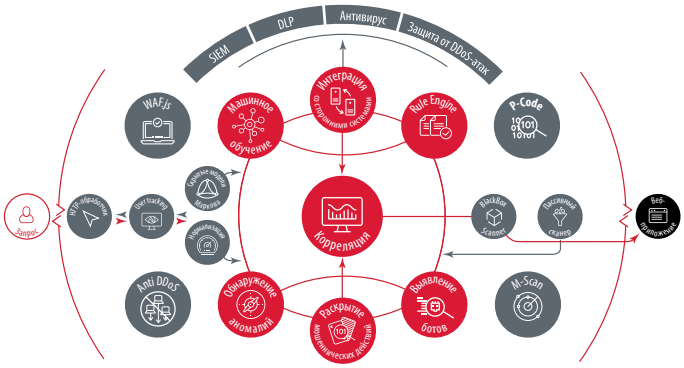
Инженерные сети и коммуникации

Особенности:

- В основе любого современного предприятия лежит ERP-система, при помощи которой осуществляются бухгалтерский учет, управление, контроль поставок и многие другие процессы. Такие системы часто имеют доступ в интернет (например, SRM, CRM и HCM) и связаны через интеграционные шлюзы.
- Системы часто обслуживаются компаниями-посредниками и контролируются удаленно, а механизмы их защиты ослаблены для упрощения эксплуатации.
- Разработчики кода бизнес-приложений больше заботятся о функциональности, чем о безопасности.
- Такие системы часто подвергаются специфической модификации и адаптации к нуждам заказчика.
- Требования к непрерывности работы практически не оставляют возможности для разработки и установки актуальных обновлений безопасности.

- Предварительно обученные модули для порталов SAP-решений
- Защита от XML-атак
- Виртуальный патчинг

4. КАК ЭТО РАБОТАЕТ: МОДУЛИ И МЕХАНИЗМЫ



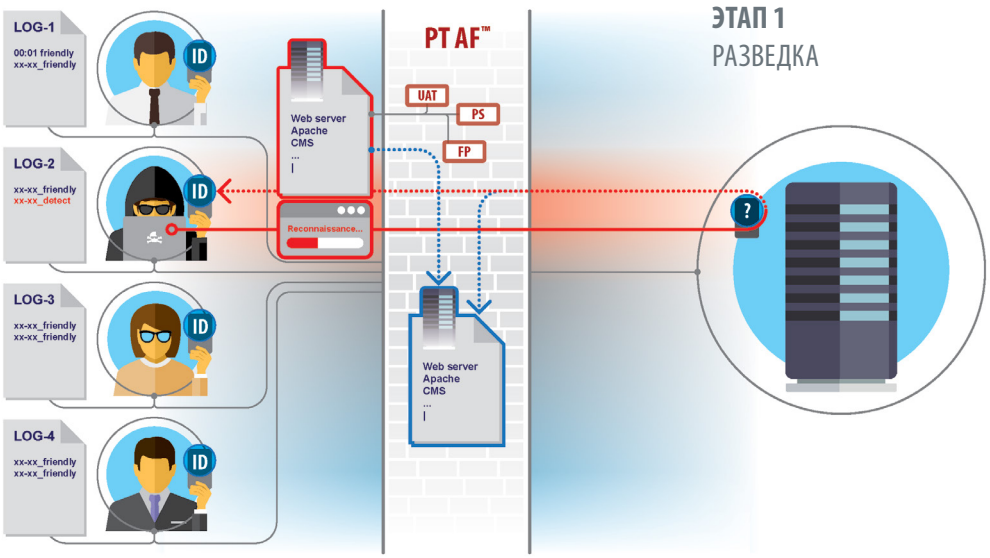
Чтобы обеспечить высокий уровень безопасности веб-, ERP- и мобильных приложений, PT Application Firewall использует многослойную схему защиты со множеством специализированных модулей:

Модуль P-Code выявляет уязвимости исходного кода приложения и автоматически формирует правила блокировки атак на эти уязвимости (виртуальные патчи).

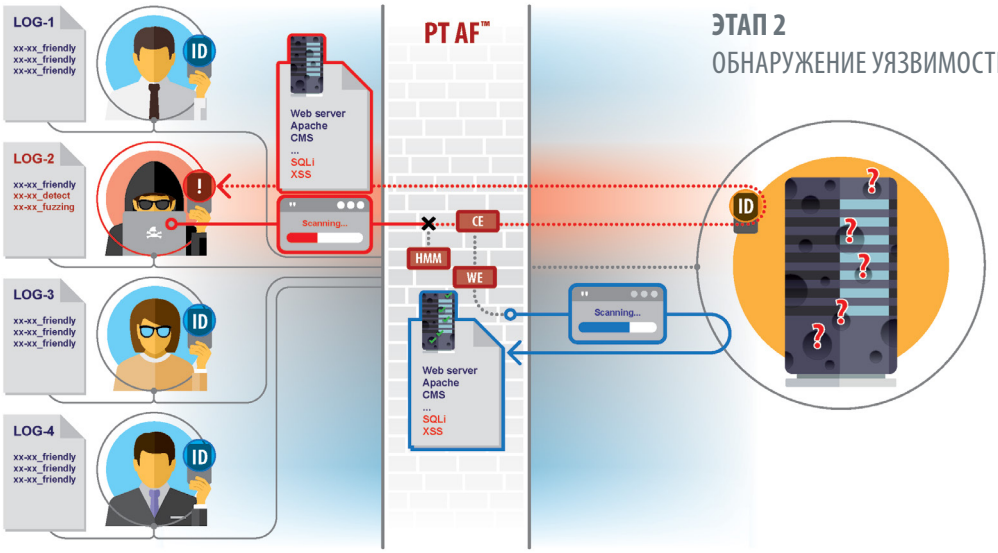
- **Отслеживание активности пользователей (user tracking)** позволяет администраторам анализировать данные сессии, включая геолокацию учетной записи пользователя, которая используется для доступа к защищенному приложению. Это позволяет администратору PT AF добавлять правила блокировки для каждого пользователя или группы пользователей и управлять доступом через списки контроля доступа. В случае подозрительной активности правила также могут идентифицировать инциденты безопасности, чтобы предотвратить веб-мошенничество. Кроме того, PT AF может обнаруживать несколько неудачных попыток входа в систему и связывать такие инциденты вместе, чтобы быстро идентифицировать и блокировать попытки взлома пароля.
- **Web Engine:** встроенный модуль динамического тестирования безопасности приложений (dynamic application security testing, DAST), предназначенный для активной идентификации компонентов приложений (CMS, фреймворка, библиотек), подготовки самообучающегося ядра и обнаружения уязвимостей в приложении. Он может работать в режиме реального времени для быстрой проверки уязвимостей, которые «прощупывают» злоумышленники.
- **Пассивное сканирование** идентифицирует компоненты приложений (CMS, фреймворки, библиотеки) для настройки модуля нормализации и обнаружения утечки данных, а также известных уязвимостей на базе словаря CVE.
- **Механизм нормализации** переписывает данные и заголовки HTTP-запросов так, чтобы они соответствовали формату защищаемых веб-приложений и их компонентов (веб-сервера, языка, фреймворка), для того чтобы предотвратить обход защиты при помощи HPP, HPC и других атак, связанных с манипуляцией данными.
- **Интеграция со сторонними решениями:** PT AF использует встроенное антивирусное ядро и правила обнаружения конфиденциальной информации, но может быть при необходимости интегрирован со сторонним антивирусом и DLP-решением. Для борьбы с DDoS-атаками PT AF может сообщать задействованные в атаке IP-адреса специализированным программам, например решениям Arbor Networks.
- **Механизм Rule Engine** позволяет создавать пользовательские правила, в том числе для всех известных уязвимостей CVE. Дополнительная настройка геолокации поддерживает создание правил блокировки и исключений на основе конкретного географического положения, обеспечивая целенаправленную защиту от атак из определенных регионов.
- **WAF.js** — модуль JavaScript, который обеспечивает защиту от атак на стороне клиента (XSS, DOM XSS, DOM Clobbering, CSRF) каждый раз, когда защищаемая страница открыта. WAF.js также обеспечивает защиту от программ-роботов разной степени сложности, даже от тех, которые способны исполнять JavaScript, эмулируя браузер. Модуль также обнаруживает инструменты взлома, которые запущены у клиентов в момент обращения к защищаемому приложению.
- **Эвристика:** при помощи самообучающихся алгоритмов искусственного интеллекта PT AF постоянно отслеживает структуру и параметры приложений для обнаружения известных атак и атак нулевого дня.
- **Корреляция** позволяет уменьшить количество срабатываний и приоритизировать важные инциденты на основе идентифицированных особенностей приложений и уязвимостей, отслеживания пользователей и истории атак. Выстраивает цепочки атак для упрощения расследования инцидентов.
- **Маскирование данных** обеспечивает конфиденциальность данных конечного пользователя, таких как номера платежных карт, паспортные данные, страховые реквизиты. С помощью данной функции можно также поддерживать веб-приложения для продолжения нормальной работы до тех пор, пока не будут устранены обнаруженные в них незначительные дефекты.

5. СЦЕНАРИИ АТАКИ И ЗАЩИТЫ

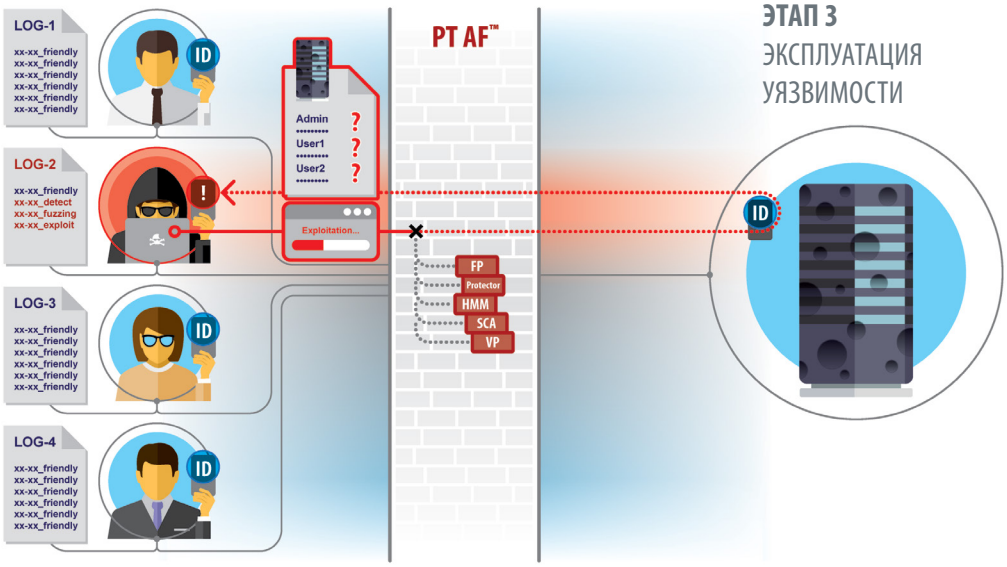
Обычно атаки состоят из нескольких этапов. Посмотрим, какие шаги предпринимает PT Application Firewall для защиты приложения в режиме реального времени на каждой стадии проведения атаки злоумышленником.



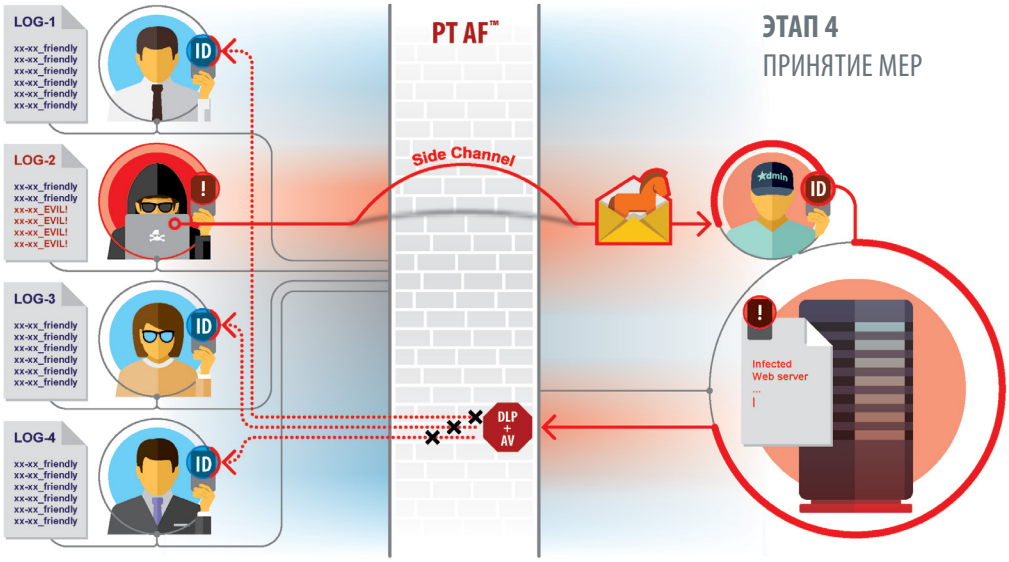
Этап 1. Разведка. Злоумышленник изучает архитектуру и логику приложения и узнает, какие типы служб, компонентов программного обеспечения и среды разработки используются. PT Application Firewall идентифицирует компоненты приложений при помощи своего модуля пассивного сканирования и настраивает ядро нормализации и защиты с учетом особенностей поведения системы и ее уязвимостей. Это позволяет PT Application Firewall значительно повысить показатели обнаружения потенциальных угроз и предотвратить возможный обход системы безопасности.



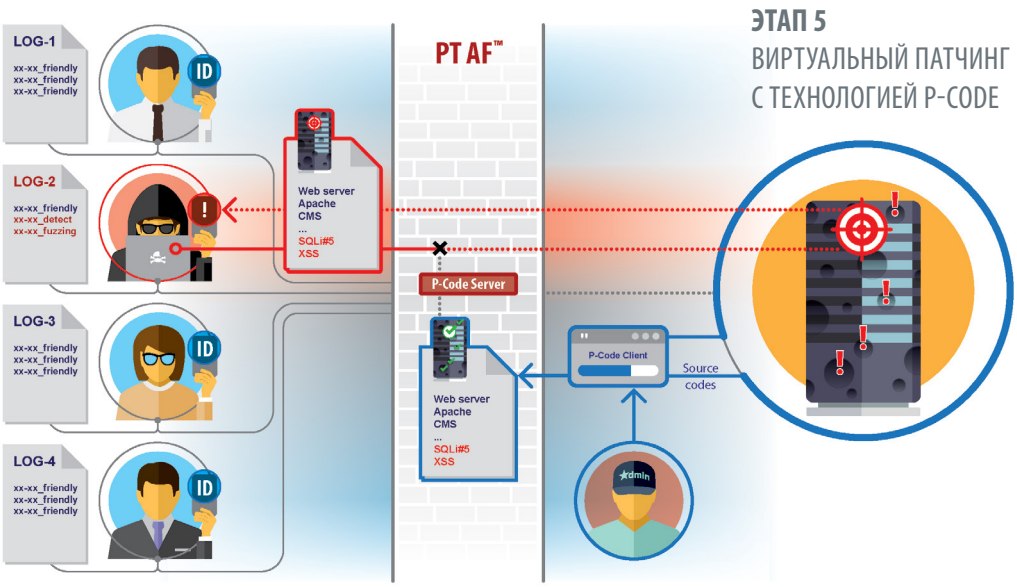
Этап 2. Обнаружение уязвимости. Пока злоумышленник предпринимает попытки обнаружить уязвимость, PT Application Firewall использует встроенный DAST-модуль Web Engine, чтобы удостовериться в ее актуальности. Если уязвимость актуальна, всем целенаправленным атакам с ее участием будет присвоен высший приоритет. Модуль самообучения на основе скрытых моделей Маркова может обнаружить (и при необходимости заблокировать) атаку на самых ранних ее стадиях.



Этап 3. Эксплуатация уязвимости. Как только злоумышленник обнаружил уязвимости в приложении, он попытается воспользоваться ими, чтобы нарушить работу системы или получить доступ к конфиденциальной информации. PT Application Firewall блокирует подобные атаки благодаря обучаемым алгоритмам, которые обнаруживают аномалии в структуре данных и в поведении пользователя.



Этап 4. Принятие мер. Если в систему вторглись через сторонние каналы (трояны, недобросовестные пользователи с доступом к конфиденциальной информации, физическое вторжение), PT Application Firewall позволит обнаружить и заблокировать атаки, использующие зараженный сервер для кражи информации или внедрения вредоносного программного обеспечения. Встроенные механизмы контроля данных и защиты от вирусов могут дополняться уже имеющимся антивирусом или DLP-решением благодаря гибкому API.

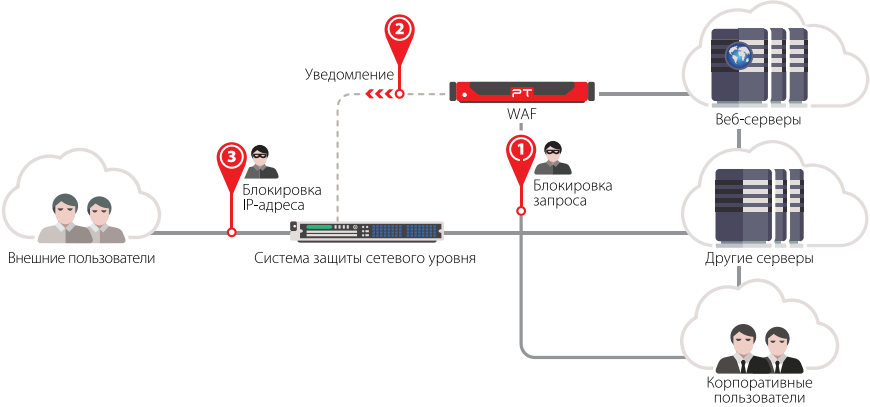


Этап 5. Виртуальный патчинг с технологией P-Code. Современные WAF позволяют создавать собственные правила блокировки для защиты уязвимого кода, исправление которого невозможно или требует времени. Однако анализировать приложения и создавать виртуальные патчи в большинстве WAF приходится вручную. Использование сторонних динамических сканеров позволяет выявить далеко не все уязвимости из-за невозможности анализа исходного кода.

В случае использования PT Application Firewall можно подключить уникальный модуль P-Code, который объединяет преимущества статического, динамического и интерактивного анализа кода (SAST, DAST, IAST) для автоматизации виртуального патчинга. Для каждой найденной уязвимости P-Code вычисляет конкретный набор «опасных» параметров и их значений и генерирует эксплойт, на основе которого моментально создается правило блокировки без дополнительного участия ИБ-специалистов. Таким образом значительно снижаются расходы на ручное обслуживание защитной системы. Та же технология позволяет обеспечить разработчиков точной информацией об уязвимостях (эксплойты с конкретными параметрами вызова) для исправления небезопасного кода.

6. МНОГОУРОВНЕВАЯ ЗАЩИТА

PT AF — гибкое решение, которое может быть интегрировано со сторонними системами, предназначенными для защиты на сетевом уровне (например, Check Point, Arbor). В интегрированном решении PT AF обнаруживает подозрительный запрос, блокирует его и сразу же уведомляет сетевую систему защиты о подозрительном IP-адресе. После этого система сетевой защиты блокирует источник угрозы во всей организации.

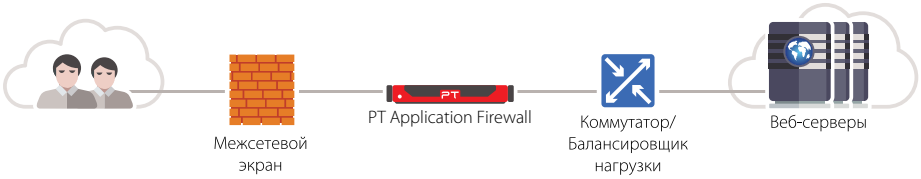


7. МОДЕЛИ РАЗВЕРТЫВАНИЯ

PT Application Firewall может быть развернут как аппаратное или виртуальное решение. Также возможно распространение по модели SaaS. Кроме того, PT AF доступен в публичной облачной среде (Microsoft Azure).

PT Application Firewall может работать в одном из трех режимов:

1



Работа «в разрыв»

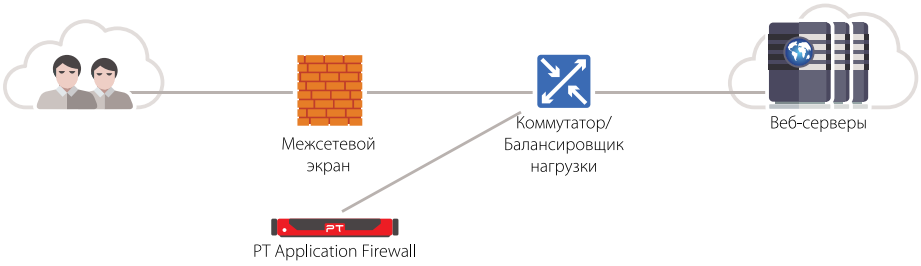
Трафик проходит через PT Application Firewall, который активно обнаруживает и предотвращает атаки.

Доступны следующие модели:

- обратный прокси-сервер,
- прозрачный прокси-сервер,
- сетевой мост L2 (только режим обнаружения).

Администраторы могут легко переключиться с прозрачного прокси-сервера на сетевой мост L2 прямо из интерфейса продукта.

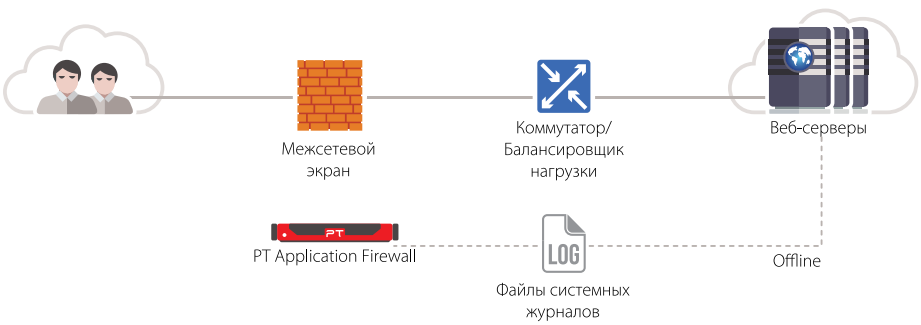
2



Режим мониторинга

Маршрутизатор создает копию трафика для PT Application Firewall, который обнаруживает потенциальные угрозы и предупреждает о них системы безопасности.

3



Автономный режим

PT Application Firewall изучает системные журналы на предмет наличия в них следов атак, что может быть использовано при расследовании инцидентов.

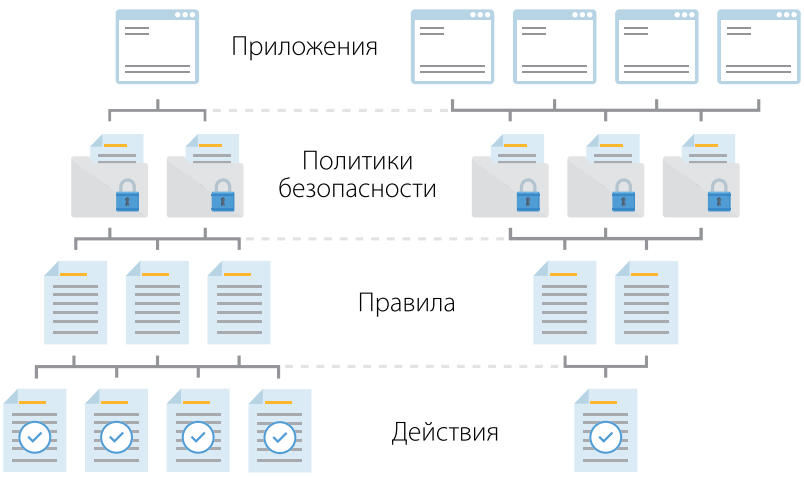
8. НАСТРОЙКА И КОНФИГУРАЦИЯ

PT AF требует минимум времени для настройки и конфигурации благодаря следующим возможностям:

- **Консольная утилита WSC CLI и удобный интерфейс.** Первичная настройка происходит в мастере настройки системы. Затем администратор переключается в удобный и понятный веб-интерфейс для последующей настройки и конфигурации продукта.
- **Автоматическое определение защищаемых ресурсов.** При использовании режимов прозрачного прокси-севера, сетевого моста L2 и режима мониторинга продукт автоматически определяет защищаемые ресурсы, то есть администраторам не нужно специально их запоминать. Как только защищаемые ресурсы определены, ими можно легко управлять в зависимости от задачи — фильтровать, сортировать, удалять и т. п.
- **Гибкие настройки политик безопасности.** PT AF содержит готовые шаблоны политик безопасности. Администраторы могут гибко настраивать их в самых разных модификациях в зависимости от задач:
  - **по уровню безопасности** (высокий, средний, низкий);
  - **по иерархии** (например, одна политика для нескольких приложений или несколько политик для одного приложения);
  - **по функциям** (различные политики для различных составляющих приложения — например, для учетной записи пользователя или для интерфейса администрирования).

Созданные настройки можно сохранять и повторно использовать для новых приложений, что существенно сокращает время активации защиты для новых ресурсов.

Гибкие настройки внутри политик безопасности. PT AF включает единую базу правил, которая автоматически применяется ко всем политикам безопасности. Поэтому нет необходимости создавать отдельные правила для каждой политики. Администраторы могут также применять различные действия, такие как блокировка или журналирование, для каждого правила, в зависимости от значимости защищаемого приложения. При этом не требуется изменять политику безопасности. Это означает, что администраторы могут гибко и тонко настраивать защиту, не затрачивая на это много времени и усилий, что особенно важно при работе с большим количеством приложений.



ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ:

- **Автоматическое восстановление конфигурации системы.** В случае сбоя конфигурации системы ранее сохраненные настройки автоматически восстанавливаются. Это избавляет от необходимости восстанавливать конфигурацию вручную, что особенно важно в тех случаях, если PT AF установлен удаленно от администратора.
- **Возможность регулировать объем сохраняемых данных.** Нет необходимости сохранять все данные (заголовки запроса или ответа и т. п.), если они не нужны. В каждом случае администраторы могут решать, какие именно части они хотят сохранить. Это снижает риск перегрузки базы данных и ускоряет поиск по ней.

PT AF позволяет гибко и тонко настраивать защиту под любые сценарии:

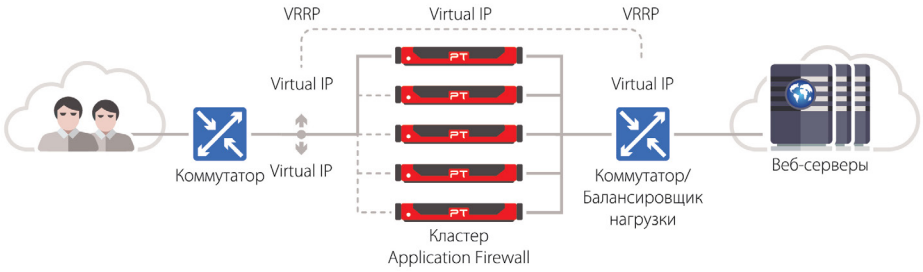
- К каждому приложению или набору приложений могут быть применены одна или несколько политик безопасности.
- К каждой политике или набору политик могут быть применены одно или несколько правил.
- К каждому правилу или набору правил может быть применено одно или несколько действий.

Все настройки могут быть сохранены и повторно использованы, что избавляет от необходимости каждый раз выполнять настройки защиты для новых ресурсов с нуля.

9. ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ И ДОСТУПНОСТЬ

PT AF отвечает требованиям к высокой степени доступности. Он может быть развернут в конфигурациях «активный — активный» и «активный — пассивный». Организации могут пользоваться как встроенной в ядро PT AF функцией балансировки нагрузки, так и внешним балансировщиком.

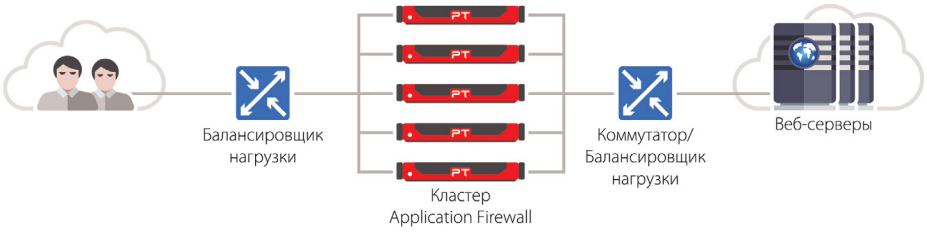
1



Активный — активный

Встроенная балансировка нагрузки, кэширование и кластер в конфигурации «активный — активный» обеспечивают высокую производительность и надежность приложения

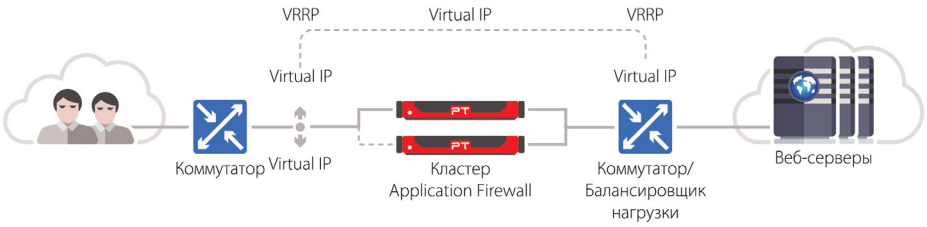
2



Активный — активный

Кластер «активный — активный» может быть интегрирован с внешними балансировщиками нагрузки

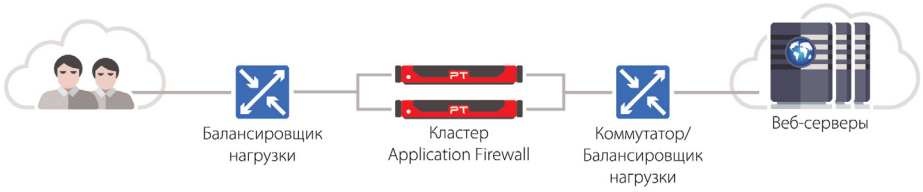
3



Активный — пассивный

Кластер «активный — пассивный» поддерживает 2-узловые операции со встроенной балансировкой нагрузки

4



Активный — пассивный

Кластер «активный — пассивный» Может быть интегрирован с внешними балансировщиками нагрузки

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays