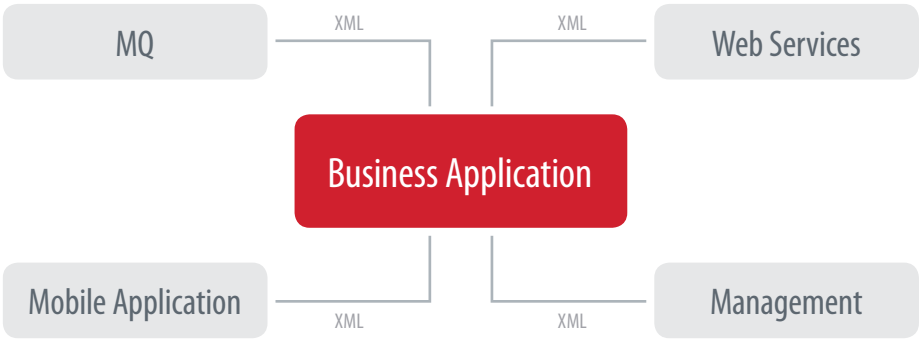
КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- **Защита на уровне XML/SOAP.** Фильтрация запросов путем проверки валидности XML-документа: проверка на соответствие RFC, анализ на соответствие XSD- и WSDL-схемам (valid XML).
- **Самообучение для блокирования неизвестных атак:** обучение модуля HMM на XML-запросах позволяет составить позитивную модель приложения и блокировать аномальные запросы.
- **Поведенческий анализ против роботов** (сканнеры, подбор паролей, фрод, ботнеты) благодаря выявлению аномалий в действиях пользователей.
- **Защита от DDoS и XML DoS:** проверка внешних сущностей в тегах <!ENTITY> и проверка сущностей в тегах <!DOCTYPE>.
- **Защита от типовых веб-атак:** поиск в ключах и значениях XML-документа сигнатур таких атак, как SQLi, XSS, Path Traversal, Remote Code Execution, Local/Remote File Inclusion.
- **Предотвращение утечек:** анализ ответов сервера на наличие чувствительной информации.
- **Защита от внутренних угроз:** разграничение прав доступа в соответствии с политиками безопасности, блокировка нелегитимных запросов сотрудников, контроль доступа к конфиденциальным документам и верификация контента.

PT SOA FIREWALL: ЗАЩИТА ВАШЕГО ВНУТРЕННЕГО И ВНЕШНЕГО XML-ТРАФИКА

Протоколы на основе языка XML используются сегодня в самых различных отраслях: в банках, телекомах, промышленности, здравоохранении и на транспорте. Благодаря универсальности и гибкости сервис-ориентированные платформы (SOA) позволяют связывать самые разнородные бизнес-приложения в критически важных инфраструктурах, включая ERP, АСУ ТП, АБС, порталы госуслуг и СМЭВ.



Распространенность XML делает особенно опасными уязвимости, связанные с возможностями этого языка. В 2014 году в 46% систем онлайн-банкинга обнаружена критическая уязвимость «Внедрение внешних сущностей XML», которая позволяет злоумышленнику получить содержимое файлов на атакуемом сервере. А благодаря технике атак XXE OOB эксперты Positive Technologies обнаружили уязвимости в продуктах Microsoft, Oracle, ModSecurity и в компонентах SCADA-систем Siemens. При этом классические межсетевые экраны пакетного уровня не ориентированы на выявление таких угроз.

Защитный экран уровня приложений PT Application Firewall с новым модулем анализа XML (SOA Firewall) позволяет противодействовать атакам на распределенные веб-сервисы любого уровня сложности, выявляя и блокируя не только типовые угрозы, но и попытки взлома с использованием специфических уязвимостей XML.

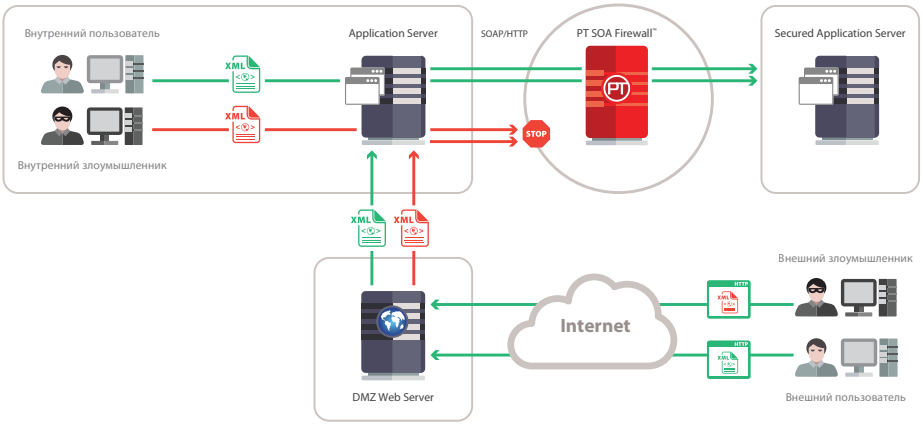
ДОПОЛНИТЕЛЬНЫЕ ПРЕИМУЩЕСТВА

- **Гибкие модели развертывания:** программно-аппаратный комплекс или виртуальная машина.
- **Высокая производительность и доступность:** трафик до 100 000 HTTP-запросов в секунду, кластеризация, возможность использования встроенного или внешнего балансировщика нагрузки.
- **Эффективное встраивание в СУИБ:** интеграция с DLP, антивирусами, анти-DDoS, SIEM.
- **Выполнение требований** ФСБ, ФСТЭК, а также отраслевых и международных стандартов (в частности, PCI DSS).

МОДЕЛИ ИСПОЛЬЗОВАНИЯ PT SOA FIREWALL

Каждый бизнес обладает уникальным набором требований к практической безопасности. Имея за плечами более 10 лет исследований безопасности в таких ключевых отраслях, как промышленные системы управления, финансовые институты, телекомы и государственные онлайн-сервисы, эксперты Positive Technologies осуществляют каждое внедрение защитного экрана PT SOA Firewall с учетом специфики инфраструктуры заказчика. Возможные сферы применения XML-версии защитного экрана:

- Системы интеграции бизнес-приложений крупных компаний (ERP, SAP, CRM), обмен данными как внутри одной распределенной компании, так и между разными организациями.
- СМЭВ: взаимодействие между министерствами, ситуационными центрами и государственными сервисами, а также между подразделениями внутри ведомств.
- Банки: взаимодействие между автоматизированной банковской системой и веб-серверами.
- СМИ и массовые веб-приложения: взаимодействие с рекламными и файлообменными сетями.
- Страховые компании и электронные полисы: взаимодействие с базами данных.
- Ритейловые сети: обмен данными с поставщиками.



О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована ФСТЭК и «Газпромом». 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.

POSITIVE TECHNOLOGIES

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