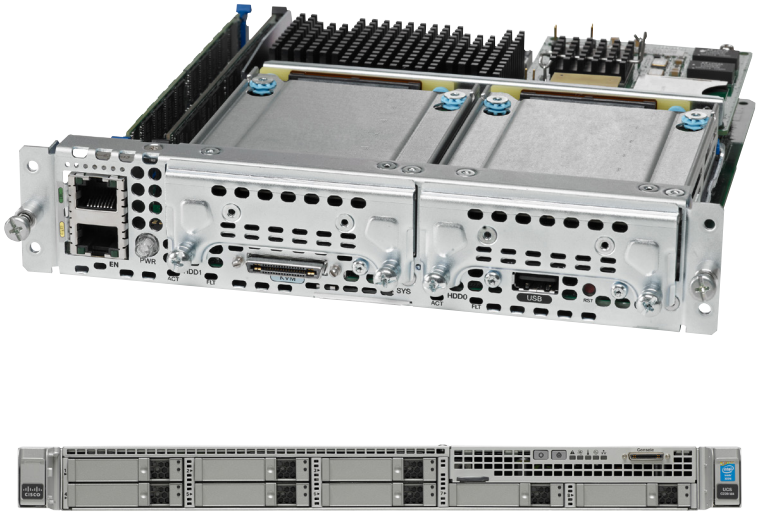
ЧТО УМЕЕТ APPLICATION FIREWALL

Межсетевой экран PT AF отвечает на самые современные вызовы, возникающие при защите веб-порталов, ERP-систем и мобильных приложений. Он блокирует на 30% больше сетевых атак, чем другие экраны, благодаря новым технологиям безопасности:

+ **Быстрая адаптация к вашей системе.** PT AF анализирует сетевой трафик и системные журналы для создания актуальной модели функционирования приложений и на ее основе выявляет аномальное поведение системы. В сочетании с другими защитными механизмами это позволяет блокировать 80% атак нулевого дня без специальной доработки под клиента.
+ **Акцент на основных угрозах.** PT AF отсеивает неактуальные попытки атак, группирует сходные срабатывания и выявляет цепочку развития атаки — от разведки до кражи важных данных или установки закладок.
+ **Мгновенная защита.** Технология виртуального патчинга позволяет защитить приложение до исправления небезопасного кода. Анализатор исходного кода с функцией генерации эксплойтов (P-Code) позволяет автоматически выявлять уязвимости и создавать виртуальные заплатки, а также обеспечивает разработчиков точной информацией об уязвимостях, значительно сокращая расходы на исправление и тестирование.
+ **Защита от техник обхода.** PT AF обрабатывает данные с учетом специфики защищаемого сервера, анализирует XML, JSON и другие протоколы современных порталов и мобильных приложений. Это позволяет противодействовать большинству методов обхода межсетевого экрана (HPC, HPP, Verb Tampering и др.).
+ **Защита от DDoS-атак на прикладном уровне.** Механизмы противодействия автоматизированным атакам включают защиту от подбора паролей, фрода, вовлечения в ботнеты, DDoS-атак и утечек данных.

PT APPLICATION FIREWALL НА ПЛАТФОРМЕ CISCO UCS C- И E-СЕРИЙ: ЭФФЕКТИВНАЯ ЗАЩИТА ПРИЛОЖЕНИЙ

С каждым годом крупный бизнес все активнее использует интернет, включая мобильные сервисы для клиентов и портальные ERP-решения, такие как SAP, для взаимодействия с поставщиками. Широко внедряются порталы массового обслуживания и электронного правительства. Повышая производительность работы и оперативность услуг, эти технологии в то же время дают новые возможности и злоумышленникам. Согласно данным Positive Research, в 2015 году в 47% случаев для получения доступа в корпоративные системы злоумышленники эксплуатировали уязвимости в веб-приложениях.



Обеспечить эффективное и безопасное функционирование бизнес-приложений призван межсетевой экран уровня приложений PT Application Firewall. Специальные версии PT AF разработаны для защиты интернет-банкинга, ERP-систем (SAP и других), веб-сервисов телекоммуникационных компаний, порталов госуслуг и СМИ. Система защиты на основе PT Application Firewall обеспечивает своевременное обнаружение атак на приложения, а также проактивное выявление уязвимостей и устранение угроз до исправления ПО.

Один из лучших вариантов развертывания PT Application Firewall — на платформе Cisco Unified Computing System. Технологии, используемые в Cisco UCS, позволяют оптимизировать IT-инфраструктуру, сократить затраты на приобретение, развертывание и обслуживание оборудования. Серверы Cisco интегрируются в существующий UCS-домен и с помощью Cisco UCS Manager и технологии Cisco SingleConnect настройка оборудования упрощается — благодаря использованию предопределенных политик и шаблонов.

ПРЕИМУЩЕСТВА ДЛЯ СПЕЦИАЛИСТОВ

- Защита от всех распространенных уязвимостей по классификации OWASP и WASC, включая SQLi, XSS и XXE, а также от популярных атак HTTP Request Splitting, Clickjacking и сложных клиентских атак (DOM-based XSS).
- Проактивная защита запросов, данных и cookie-файлов позволяет блокировать такие атаки, как CSRF, даже если противодействие им было упущено разработчиками.
- Выполнение требований РС БР ИББС-2.6-2014, приказов ФСТЭК № 17 и 21 и стандарта PCI DSS.
- Эффективное встраивание в СУИБ организации: интеграция с антивирусами и DLP, анти-DDoS и SIEM, а также со всеми продуктами PT AppSec Ecosystem.
- Механизмы антифрода, помимо защиты об ботов, включают репутационный и профайлинговый сервисы, которые выявляют аномальное поведение клиента (например, вход с необычного адреса).
- Поддержка политики безопасности контента (Content Security Policy, CSP).
- Работа с SSL-трафиком как дополнительный уровень защиты.

КОМПЛЕКС UCS AF: СОКРАЩАЕМ ЗАТРАТЫ НА БЕЗОПАСНОСТЬ

Positive Technologies, Cisco и OCS Distribution подготовили совместное решение — межсетевой экран уровня приложений PT Application Firewall, предустановленный и преднастроенный на оборудовании Cisco UCS.

Используя аппаратное решение на платформе Cisco UCS E-серии, заказчики получают маршрутизатор и защитный экран сетевого и прикладного уровней в одном устройстве, например Cisco 2911, что сокращает затраты на обеспечение безопасности сети и приложений.

PT AF на платформе Cisco UCS E-серии хорошо подходит для небольших местных отделений распределенных организаций, которым требуется недорогое решение для комплексного обеспечения безопасности сетевого трафика.

Cisco UCS C-серии предназначены для работы в центрах обработки данных, защиты высоконагруженных приложений. Оба решения гибко интегрируются в сетевую инфраструктуру на основе Cisco, снижая затраты на оборудование и поддержку.

РЕАЛИЗАЦИЯ

Все решения реализуются через официального дистрибьютора — компанию OCS Distribution, которая с 1997 года занимается продвижением всех технологий Cisco на российском рынке. В компании уже 15 лет действует научно-технический центр, в котором работают сертифицированные специалисты Cisco, в том числе инженеры со статусом экспертов по объединенным сетям Cisco

Cisco — мировой лидер в области технологий, с 1984 года обеспечивающий работу интернета. Наши сотрудники, продукты и партнеры помогают обществу поддерживать надежную связь и уже сегодня использовать цифровые возможности завтрашнего дня. Чистый объем продаж Cisco в 2015 финансовом году составил 49,2 млрд долларов. Информация о решениях, технологиях и текущей деятельности компании публикуется на сайтах cisco.ru и cisco.com.

OCS Distribution работает на российском IT-рынке 21 год. Все это время команда OCS сбалансированно развивает направления вольюмной и проектной дистрибуции, наращивает технологическую базу, разрабатывает программы поддержки партнеров и адаптирует их к переменчивым реалиям и запросам рынка. Компания год от года занимает лидирующие позиции на рынке (рейтинги CRN, @Astera, iXBT, EMEA Channel Academy).

OCS работает по всем продуктовым направлениям IT-рынка и рынка бытовой техники, включая компьютерную технику, телекоммуникационное, периферийное и сетевое оборудование, компоненты, СХД, инфраструктурное ПО, расходные материалы, бытовую технику, аксессуары и товары для интерактивных развлечений, всего порядка 250 линеек ведущих мировых вендоров. Региональная сеть офисов OCS по своей широте не имеет аналогов и включает 28 городов в России и 2 города в Казахстане. Дистрибьютор работает с 11 000 партнеров — как с розничными, так и с корпоративными реселлерами; как с крупными компаниями, так и с небольшими локальными продавцами. Подробнее об OCS Distribution — ocs.ru.

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована «Газпромом» и ФСТЭК. Более 3000 организаций из 30 стран 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 телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности и стала лидером по темпам роста на международном рынке систем управления уязвимостями. В 2015 году Gartner назвал Positive Technologies «визионером» в своем рейтинге Magic Quadrant for Web Application Firewalls.

pt@ptsecurity.com ptsecurity.ru