WATCHGUARD NEXT-GENERATION FIREWALL

На сегодняшний день многие компании нуждаются в более совершенных решениях обеспечения информационной безопасности, чем традиционные межсетевые экраны. Компаниям необходимы более широкие технические возможности, которые помогут обеспечить надежную защиту деловых активов. Поскольку объемы интеграции различных приложений в бизнес среду постоянно увеличиваются, а сотрудники компаний пользуются все большим количеством разнообразных бизнес инструментов, защита конфиденциальной информации и соответствие всем необходимым законодательным требованиям становятся все более сложными. Специалисты выбирают наиболее быстрые, простые и понятные решения, которые позволят работать как в офисе, так в дороге, в аэропорту или дома. Приложения, которые разрабатывались не для использования в бизнес среде, могут обходить защиту традиционных межсетевых экранов независимо от того, каким образом системные администраторы пытаются заблокировать использование этих приложений. Это означает, что компаниям необходимо использовать решения обеспечения сетевой и информационной безопасности, которые смогут обеспечить высокий уровень защиты в современных информационных средах.

На данный момент возможностей традиционных межсетевых экранов явно недостаточно для того, чтобы противостоять атакам злоумышленников, представляющих серьезную угрозу для деловых активов компании. Сегодня компаниям необходимо уделять большое внимание вопросам защиты корпоративных ресурсов от несанкционированного доступа, предотвращению утечек данных, защиты каналов связи, соблюдения политик информационной безопасности, предотвращения сетевых атак. Помимо этого, необходимо постоянно быть в курсе того, что происходит внутри корпоративной сети.

ЧТО ЖЕ НЕОБХОДИМО ДЕЛАТЬ ДЛЯ ОБЕСПЕЧЕНИЯ ВЫСОКОГО УРОВНЯ БЕЗОПАСНОСТИ?

Межсетевые экраны нового поколения (Next Generation Firewalls - NGFW) анализируют сетевой трафик в режиме реального времени, что обеспечивает надежную защиту против злоумышленников, вредоносного программного обеспечения, сетевых атак, попыток сетевого вторжения, краж данных, а также других видов сетевых угроз. Межсетевые экраны WatchGuard нового поколения обеспечивают надежные каналы связи между филиалами компании и сотрудниками, работающими удаленно, а также позволяют в режиме реального времени следить за состоянием сети, соблюдением пользователями политик безопасности.

Межсетевые экраны WatchGuard NGFW обеспечивают высокую скорость обработки и фильтрации трафика. Кроме того, решения WatchGuard NGFW позволяют управлять приложениями, создавать VPN туннели методом «Drag & Drop», создавать клиентские SSL и IPSec VPN подключения, а также предоставляют обширнейшие возможности по наблюдению за трафиком пользователей в режиме реального времени, за состоянием сети и соблюдением политик безопасности.

С решениями WatchGuard NGFW компании могут с высокой точностью контролировать соблюдение политик сетевой безопасности, что способствует уменьшению рисков, связанных с кражами интеллектуальной собственности или конфиденциальных данных.

ОСНОВНЫЕ ОСОБЕННОСТИ WATCHGUARD NEXT GENERETION FIREWALL

- Высокая скорость обработки сетевого трафика позволяет блокировать атаки и нежелательный трафик
- Основные возможности межсетевого экранирования:
  - Пакетная фильтрация
  - NAT (Network Address Translation)
  - Инспектирование трафика с запоминанием состояния пакета данных (Stateful Inspection)
  - Создание виртуальных сетей (VPN)
- Интегрированный сервис предотвращения сетевых атак (IPS)
- Управление приложениями (Application Control)
- Дополнительные возможности:
  - Интеграция с Active Directory позволяет связывать учетные записи пользователей и групп пользователей с установленными политиками безопасности
  - Основанный на «облачных» технологиях сервис оценки репутации Web-ресурсов блокирует трафик из небезопасных источников
  - Возможность наблюдать в режиме реального времени за пользовательскими событиями, состоянием сети и соблюдением политик безопасности

ПРЕИМУЩЕСТВА СЕРВИСА WATCHGUARD APPLICATION CONTROL

ДЕТАЛИЗИРОВАННОЕ УПРАВЛЕНИЕ ПРИЛОЖЕНИЯМИ

Пользователи используют большое количество самых разнообразных приложений, и компаниям важно иметь инструменты, позволяющие полноценно управлять разными параметрами приложений. Используя сервис WatchGuard Application Control можно, например, разрешить использовать приложение Windows Live Messenger для обмена сообщениями, но запретить передачу файлов с использованием функционала этого приложения. С помощью сервиса WatchGuard Application Control также, например, можно разрешить доступ к социальной сети Facebook, но запретить доступ к играм в Facebook.

СПИСОК ПОДДЕРЖИВАЕМЫХ ПРИЛОЖЕНИЙ

Сервис WatchGuard Application Control позволяет управлять огромным количеством приложений, список которых постоянно обновляется и актуализируется. Список сигнатур приложений обновляется автоматически, а при обновлении не требуется полное обновление программного обеспечения устройства WatchGuard NGFW.

СПОСОБНОСТЬ ИДЕНТИФИЦИРОВАТЬ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЮЩИЕ ШИФРОВАНИЕ ДАННЫХ

Сервис WatchGuard Application Control имеет уникальную функцию анализа поведения приложений, которая помогает обнаруживать даже хорошо «замаскированные» приложения, способные обойти политики безопасности межсетевого экрана путем шифрования трафика и передаваемых данных.

ДЕТАЛИЗИРОВАННОЕ УПРАВЛЕНИЕ ПРИЛОЖЕНИЯМИ

Интернет ресурсы являются основным источником угроз для информационной безопасности компаний, а Web-приложения часто являются основным инструментом для организации сетевых атак. Часто для организации атак с использованием методов социальной инженерии хакеры используют социальные сети. Учитывая, что интернет трафик и Web-приложения являются источником множества угроз, IT-администраторы могут блокировать вредоносное воздействие, разграничивая права доступа пользователей к приложениям, разрешая использовать только те приложения или функции приложений которые действительно необходимы для бизнес деятельности.

Сервис WatchGuard Application Control предоставляет системным администраторам средства управления и детализированного контроля сотнями приложений, а также возможность составлять отчеты, содержащие информацию о сетевой активности пользователей и используемых ими приложениях. Системные администраторы могут устанавливать политики безопасности, как для отдельных пользователей, так и для групп пользователей, разграничивая права пользователей относительно отдельных приложений, относительно категорий приложений и относительно отдельных функций приложений. Например, IT-администраторы могут установить политику безопасности, которая откроет сотрудникам отдела маркетинга доступ к социальной сети Facebook, но закроет доступ к играм сети Facebook.

СЕРВИС ПРЕДОТВРАЩЕНИЯ СЕТЕВЫХ АТАК (INTRUSION PREVENTION SYSTEM) ПОЗВОЛЯЕТ ПОВЫСИТЬ НАДЕЖНОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ СЕТИ

Если сетевой трафик и системные события внутри корпоративной сети не контролируются с должной тщательностью, то велика вероятность возникновения резкого увеличения вредоносных действий со стороны злоумышленников. Сервис WatchGuard IPS позволяет предотвращать сетевые атаки и работает совместно с другими сервисами безопасности, реализованными в операционной системе WatchGuard Fireware XTM OS. Подобная интеграция позволяет в режиме реального времени обеспечивать постоянную и всеобъемлющую защиту от сетевых угроз, таких как шпионское ПО, атак типа «SQL-инъекции», межсайтовый скриптинг (XSS) и атаки типа «Переполнение буфера». Сервис WatchGuard IPS сканирует сетевой трафик по всем протоколам, и использует постоянно обновляемую базу данных сигнатур, что позволяет обнаружить и заблокировать все современные типы угроз.

ПРЕИМУЩЕСТВА

БЛОКИРОВАНИЕ СЕТЕВЫХ УГРОЗ

- Постоянно обновляемая база данных сигнатур сетевых угроз позволяет защищать сеть от новых видов угроз

ГИБКОСТЬ

- Идентификация вредоносного программного обеспечения позволяет регистрировать и блокировать весь сомнительный сетевой трафик

ВЫСОКОЭФФЕКТИВНОЕ СКАНИРОВАНИЕ

- Сканирование сетевого трафика, проходящего по протоколам HTTP, HTTPS, FTP, TCP, UDP, DNS, SMTP и POP3, позволяет блокировать сетевые атаки и атаки, использующие уязвимости в протоколах и пользовательских приложениях.