Устройство Cisco Web Security Appliance

В чем состоит ценность устройства Cisco® Web Security Appliance?

Устройства Cisco Web Security Appliance, использующие функциональные возможности службы Cisco Security Intelligence Operations (SIO), – это лучшие в своем классе, надежные веб-шлюзы, которым нет равных в обеспечении безопасности и контроля интернет-трафика, а также в формировании отчетов по нему для организаций любого масштаба. При помощи мобильного клиента Cisco AnyConnect® Secure Mobility Client они также обеспечивают интернет-безопасность удаленным и мобильным пользователям (в том числе пользователям планшетов и смартфонов).

Какие проблемы помогает решать Cisco Web Security Appliance?

Используя Интернет, организации сталкиваются с ощутимыми рисками, такими как:

- нарушение текущей деятельности компании и снижение ее производительности вследствие проникновения из Интернета быстродействующих и хорошо маскирующихся вредоносных программ;
- ущерб бренду и потеря данных вследствие ненадлежащего или бесконтрольного использования веб-приложений.

Решая вопросы интернет-безопасности, организации сталкиваются с дополнительными препятствиями, такими как:

- необходимость обеспечивать интернет-безопасность в новых подходах к бизнесу, которые не укладываются в традиционные модели развертывания и обеспечения безопасности, например использование личных устройств на рабочем месте или работа мобильных пользователей.

Высокая интернет-безопасность – в одном устройстве

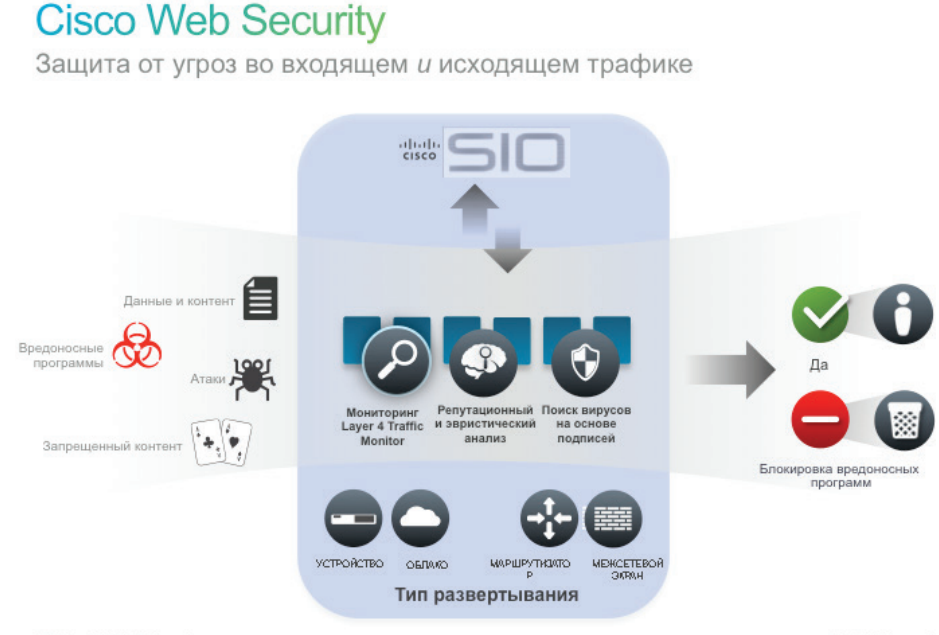
Устройства Cisco Web Security Appliance – это первый и единственный в отрасли надежный веб-шлюз, который сочетает на единой платформе продвинутую защиту от вредоносных программ, систему идентификации и контроля приложений (AVC), контроль за допустимым использованием Интернета, формирование информативных отчетов и мобильную безопасность. Благодаря сочетанию инновационных технологий, устройства Cisco Web Security Appliance помогают организациям успешно справляться с растущими проблемами защиты и контроля интернет-трафика независимо от того, работают ли сотрудники в офисе, в корпоративной локальной сети или на ноутбуке, смартфоне или планшете, ожидая своего рейса в аэропорту.

Продвинутая защита от вредоносных программ

Применение многоуровневых технологий защиты от вредоносных программ позволяет устройствам Cisco Web Security Appliance надежно защищать вас от вредоносных программ и изощренных APT-атак. Все продукты компании Cisco в области безопасности, включая и устройства Cisco Web Security Appliance, реализованы на основе службы Cisco SIO. Пользуясь знаниями, полученными от Cisco SIO, репутационные фильтры Cisco Web Reputation Filters анализируют интернет- и внутрисетевой трафик по более чем 200 разным параметрам, обеспечивая мощную защиту от вредоносных программ на внешнем уровне и блокируя большую их часть.

Cisco Web Security Appliance – это первое на рынке решение, где в рамках одного устройства предлагается сразу несколько модулей для поиска вредоносных программ. Для повышения защиты от вредоносных программ администратор может запускать все эти модули сканирования одновременно.

Рис. 1. Как работает Cisco Web Security



Полный контроль интернет-трафика

Технология идентификации и контроля приложений (AVC), используемая в устройстве Cisco Web Security Appliance, позволяет администраторам точечно контролировать сотни тысяч «микроприложений» на Фейсбуке и в Твиттере, а также на многих других популярных платформах и в мультимедийных потоках. Не блокируя сайт целиком, администратор может разрешить или запретить выполнение определенных функций, таких как чат, отправка сообщений, видео или звук. Встроенная фильтрация URL-адресов обеспечивает максимальный на сегодняшний день охват сайтов, использующих категории URL. Благодаря тому, что с облака на устройства оперативно, в динамическом режиме, поступают обновления подписей и баз данных, организации могут пользоваться разрешенными приложениями и контентом, лишаясь доступа лишь к тем из них, которые повышают риски, снижают производительность или потенциально могут привести к утечке конфиденциальной информации.

Защита данных

Устройство Cisco Web Security Appliance можно интегрировать с другими DLP-серверами для более глубокой проверки контента и реализации стратегий предотвращения потери данных (DLP). Организации могут разрешать или блокировать контент в зависимости от требований регулирующих органов и в целях соблюдения прав на интеллектуальную собственность.

Важная информация

Благодаря встроенному формированию отчетов можно получить ценные сведения об использовании Интернета в корпоративных сетях, а также о выявленных и предотвращенных угрозах. В такие отчеты в реальном времени попадают актуальные данные, а также информация о тенденциях и инцидентах. Усовершенствованная система формирования отчетов позволяет предприятиям выявлять нарушения стратегий и правил безопасности.

Повсеместная защита для всех пользователей

При помощи мобильного клиента Cisco AnyConnect Secure Mobility Client устройство Cisco Web Security Appliance обеспечивает безопасность удаленных и мобильных пользователей, работающих, в числе прочего, на ноутбуках, смартфонах и планшетах.

Как максимально использовать вашу сеть Cisco

Лучший способ повысить отдачу от инвестиций в оборудование Cisco для центров обработки данных, сетей и филиалов – интегрировать их с устройствами Cisco Web Security Appliance. Cisco Web Security Appliance – эта лучшая в своем классе защита от самых разных интернет-угроз, и консалтинговая компания Gartner в своем докладе за 2012 год в третий раз подряд поместила этот продукт в число лидеров в категории Secure Web Gateway.

Каковы преимущества Cisco Web Security Appliance?

Cisco Web Security Appliance – решение, в котором в рамках одного устройства предлагается контроль и защита сразу от трех основных видов рисков, угрожающих интернет-трафику в корпоративной сети. Это риски, связанные с обеспечением безопасности, с сохранением ресурсов и с выполнением информационной политики. Cisco Web Security Appliance – наиболее эффективная защита от вредоносных программ, поступающих из Интернета, а также:

- самая надежная среди аналогов система обеспечения интернет-безопасности, интегрированная в одно устройство;
- продвинутая защита от вредоносных программ и широчайшего спектра интернет-угроз;
- насыщенный, гибкий и эффективный контроль за стратегиями для веб-приложений и социальных сетей;
- недопущение утечки конфиденциальной информации и личных данных из вашей сети, будь то преднамеренная акция или случайность;
- интеграция с другими продуктами компании Cisco в сфере безопасности, повышающая отдачу от уже сделанных инвестиций в оборудование Cisco и обеспечивающая не имеющую аналогов защиту всем пользователям – как подключенным к корпоративной сети, так и удаленным.

Почему Cisco?

Сегодня проблема безопасности сетей стоит так остро, как никогда ранее. В обстановке постоянных угроз и рисков обеспечение безопасности необходимо для бесперебойного ведения бизнеса, защиты ценной информации, поддержания репутации бренда и внедрения новых технологий. Безопасная сеть – залог мобильности ваших сотрудников и их защищенного доступа к нужной им информации. Это также облегчает ведение бизнеса с клиентами и партнерами.

Никакая другая организация не понимает проблему сетевой безопасности так хорошо, как компания Cisco. Наше лидерство на рынке, наш многолетний опыт работы и непревзойденная компетентность в сфере предотвращения угроз и защиты от них делают нас именно тем поставщиком инновационных решений для обеспечения безопасности, который вам нужен.

Где можно получить дополнительную информацию?

Более подробную информацию можно найти по адресу: http://www.cisco.com/go/websecurity

Cisco Web Security Appliance: наиболее часто задаваемые вопросы

В. Как работает устройство Cisco Web Security Appliance?

О. Cisco Web Security Appliance – это прокси-сервер переадресации, который может работать либо в режиме Explicit (файлы PAC, WPAD, настройки браузера), либо в режиме Transparent (WCCP, PBR, подсистемы балансировки нагрузки). Он может проксировать HTTP-, HTTPs-, SOCKS- и собственный FTP-трафик для выполнения дополнительных функций, таких как предотвращение потери данных (DLP), обеспечение безопасности мобильных пользователей или идентификация и контроль приложений (AVC).

В. Как осуществляется управление такими устройствами?

О. Устройство Web Security Appliance управляется преимущественно веб-приложением, но часть команд можно задавать через интерфейс командной строки. Централизованное управление сразу несколькими устройствами, установленными в разных местах, осуществляется при помощи устройств Content Security Management Appliance M-серии.

В. Как устроена система предотвращения потери данных (DLP)?

О. Реализация стратегий обеспечения безопасности данных осуществляется через встроенный механизм простых понятных стратегий путем блокирования POST-запросов в протоколе HTTP на основе метаданных контента. В интеграции предотвращения потери данных (DLP) используется стандартный ICAP-протокол для передачи контента на отдельный DLP-сервер, где производится дополнительное сканирование и более точечная реализация выбранной стратегии. Так, устройство Cisco Web Security Appliance может взять все вложения из исходящей веб-почты и передать их по ICAP DLP-решениям от компаний Symantec или RSA, которые проведут сканирование самого содержимого файлов, вместо сканирования метаданных файлов.

В. Какие типы отчетов можно получить от устройства Cisco Web Security Appliance?

О. Отчеты по всему трафику, проходящему через устройство Cisco Web Security Appliance, можно получить непосредственно с устройства, благодаря встроенной в него функции формирования отчетов. Централизованное формирование отчетов сразу по нескольким устройствам Cisco Web Security Appliances осуществляется при помощи устройств Content Security Management Appliance. Мы также добавили специальное приложение, разработанное компанией Splunk, внешне похожее на встроенную систему формирования отчетов, но обеспечивающее выполнение дополнительных функций, масштабируемость и гибкость.

C45-716641-00 09/12