McAfee Web Gateway Cloud Service

Облачная технология повсеместной веб-защиты

Защиту от изощренных веб-угроз невозможно организовать без передовых технологий, но это не значит, что такие технологии должны быть дорогими и сложными. Обеспечение веб-защиты из облака дает подразделениям информационной безопасности те же преимущества защиты от сложных угроз, что и локально развернутые аппаратные устройства. Однако при этом вы не несете издержек на покупку аппаратного обеспечения и на ресурсы для его обслуживания. В современных организациях веб-доступ все чаще и чаще осуществляется за пределами сетевого периметра, поэтому для перемещающихся в пространстве устройств и пользователей постоянной точкой контакта становится облако. В такой ситуации систему обеспечения безопасности эффективнее создавать на основе конечных точек, а не на основе трафика, идущего в одно местоположение. Объединение средств контроля доступа и средств защиты от облачных угроз и веб-угроз дает возможность максимально повысить производительность труда персонала и обеспечивает эффективный и систематизированный подход к управлению безопасностью.

Ключевые преимущества

- Самый экономичный способ развертывания веб-защиты, не требующий ни локального оборудования, ни локального программного обеспечения
- Обеспечение не только базового уровня защиты благодаря эмуляции поведения, позволяющей по мере обработки трафика за считанные миллисекунды блокировать вредоносное ПО «нулевого дня»
- Обеспечение защиты пользователей, находящихся за пределами сети — защита из облака упраздняет традиционное понятие сетевого периметра

Экономичная и повсеместная защита

Управление локально развернутыми аппаратными устройствами веб-защиты — дорогостоящая задача, отнимающая ресурсы у зачастую и без того уже урезанных подразделений ИБ. Проведение развертывания веб-защиты в виде облачного сервиса позволит снизить совокупную стоимость владения средствами защиты. При этом отпадет необходимость приобретать, держать в собственности и обслуживать аппаратные устройства. Все те ресурсы, которые ранее использовались для обслуживания оборудования и выполнения таких задач, как установка программных обновлений и исправлений, можно будет перебросить на более стратегически важные направления в области ИТ или ИБ.

Модель гибридного развертывания позволяет параллельно использовать и аппаратные устройства,

Подписаться

и облачный сервис. Большинству организаций эта модель дает, с одной стороны, возможность сохранить за собой право собственности на имеющиеся в сети аппаратные устройства и осуществлять контроль над ними, а, с другой стороны, позволяет с помощью облачных технологий обеспечить защиту небольших удаленных офисов и перемещающихся в пространстве пользователей.

От использования облачных средств веб-защиты сразу выиграют те ИТ-подразделения, которые фильтруют весь трафик на размещенном у себя в сети аппаратном веб-шлюзе и для этого вынуждены передавать трафик из удаленных офисов по каналам многопротокольной коммутации пакетов по меткам (MPLS — MultiProtocol Label Switching). Такая передача трафика не только связана с большими дополнительными расходами, но и повышает уровень сложности сети. Как только удаленные офисы смогут обеспечивать защиту трафика, направляя его прямо в облако, организация сможет сократить количество каналов MPLS и упростить свою сетевую архитектуру.

Наконец, поскольку веб-доступ сотрудников в организациях уже не ограничен периметром сети, пользователи и устройства, покидающие пределы сети, выходят из поля зрения ИТ-подразделения и оказываются незащищенными. Перемещение же веб-защиты в облако выворачивает этот периметр наизнанку. Возможность автоматически перенаправлять веб-трафик находящихся за пределами сети пользователей и устройств с конечных точек в облако позволяет обеспечивать безопасность подключений при работе из дома, в аэропорту, в кафе и в любом другом месте, находящемся за пределами сети. Трафик в пределах физических границ больше не является основным содержанием сети. Теперь сеть повсюду следует за конечными точками.

Глобальная архитектура с высоким уровнем быстродействия

Сервис McAfee® Web Gateway Cloud Service предназначен для корпоративного сегмента. Для многих организаций его использование будет означать более высокий уровень быстродействия, чем тот, который сегодня обеспечивают их локальные решения. Так, например, чтобы увеличить пропускную способность, ИТ-подразделению приходится приобретать и развертывать новое аппаратное устройство, и этот процесс может занимать от нескольких дней до нескольких недель. А в наше облако возможность оперативно увеличивать пропускную способность заложена изначально, поэтому весь процесс занимает около 15 минут.

Вышедшее из строя и нуждающееся в ремонте локальное аппаратное устройство, переставшее фильтровать веб-трафик, может привести к потере подключения к Интернету и к снижению уровня защищенности организации. В случае сбоя в одном из наших центров обработки данных наш облачный сервис автоматически начнет перенаправлять весь веб-трафик в самый близкий и самый быстрый центр обработки данных, мгновенно обеспечивая бесперебойную защиту.

Ключевые преимущества (продолжение)

- Эффективный и систематизированный подход к управлению безопасностью благодаря объединению с консолью McAfee® MVISION Cloud (CASB)
- Проверенная архитектура. McAfee Web Gateway Cloud Service представляет собой многопользовательскую версию McAfee Web Gateway, локального веб-шлюза, который зарекомендовал себя как надежное аппаратное устройство на предприятиях всего мира

Кроме того, архитектура нашего облачного сервиса позволяет осуществлять пиринговое взаимодействие с опорной сетью Интернета в крупнейших точках обмена интернет-трафиком (IXPs). Тем самым из маршрута передачи пакетов исключаются промежуточные интернет-провайдеры (ISP), добавляющие задержку к соединению. Благодаря более коротким маршрутам до таких популярных поставщиков контента, как Microsoft Office 365 и Google, пользователям удается устанавливать через наш облачный сервис более быстрое соединение, чем если бы они подключались непосредственно через открытый Интернет.

Сервис McAfee Web Gateway Cloud Service действует по всему миру. Доставка веб-контента может осуществляться на местном, региональном языке пользователя, поэтому даже если пользователь подключается к ЦОД в другой точке мира, он видит, например, свои локальные результаты поиска Google. Текущее расположение и статус центров обработки данных, работающих с веб-трафиком, можно отслеживать по адресу https://trust.mcafee.com.

Защита от изощренных угроз

Подразделения ИБ зачастую не могут сразу адекватно реагировать на крайне изощренные вредоносные программы и целенаправленные атаки, способные обходить традиционные средства защиты. Такая ситуация приводит к нехватке ресурсов и к непрерывному «пожаротушению» в попытке устранить уязвимости конечных точек. В отличие от традиционных способов предотвращения веб-угроз (путем фильтрации URL-адресов и использования сигнатур) сервис McAfee Web Gateway Cloud Service обеспечивает защиту конечных точек от угроз «нулевого дня» и бесфайловых вредоносных программ посредством встроенной эмуляции файлов, сценариев JavaScript и кода HTML. Это позволяет отлавливать вредоносные программы «нулевого дня» еще до того, как они попадут к пользователю, причем количество блокируемых угроз оказывается примерно на 20 % выше, чем в случае решений, работающих на основе сигнатур и фильтрации URL-адресов. Сокращение общего количества инцидентов, связанных с вредоносными программами, позволяет снизить затраты, лучше распределять ресурсы и, как результат, повысить эффективность операций по обеспечению безопасности. Оставшиеся подозрительные объекты можно направлять в McAfee Cloud Threat Detection, наше облачное решение для анализа сложных угроз, предлагаемое в виде дополнительного интегрированного сервиса вместе с McAfee Web Gateway Cloud Service.

Для доставки веб-угроз нередко используется зашифрованный трафик, позволяющий обходить средства веб-защиты. Зашифрованный трафик по умолчанию используют почти все облачные приложения: облачные хранилища, социальные медиа и т. д. McAfee Web Gateway Cloud Service может полностью расшифровывать и проверять зашифрованный HTTPS-трафик, что позволяет предотвращать попадание вредоносных программ в компьютеры и обеспечивать сбор информации об облачных приложениях внутри зашифрованных каналов.

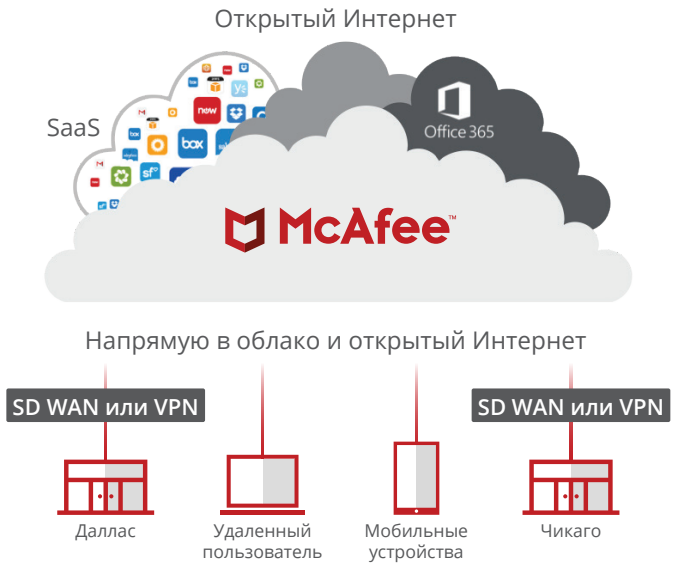

Рис. 1. Облачная архитектура для обеспечения облачной безопасности и веб-защиты.

Объединение средств контроля доступа и средств защиты от облачных угроз и веб-угроз

Облачные сервисы имеют несколько разных уровней риска, и доступ к ним может осуществляться как с управляемых устройств, так и с личных устройств сотрудников. Объединение McAfee Web Gateway Cloud Service и McAfee MVISION Cloud (CASB) позволяет контролировать доступ ко всем облачным сервисам и обеспечивать защиту от возникающих в них угроз посредством одной-единственной консоли. Сочетание политик позволяет получить беспрецедентный уровень контроля за облаком: MVISION Cloud через API и обратный прокси-сервер осуществляет сбор информации и контроль за разрешенными облачными сервисами, а задача McAfee Web Gateway Cloud Service заключается в мониторинге и блокировании неразрешенных облачных сервисов и неразрешенного веб-трафика через прокси-сервер переадресации. Блокирование облачных сервисов, отличающихся высоким уровнем риска, позволяет обезопасить пользователей от случайной потери данных и заражения вредоносным ПО.

В какой точке мира находится McAfee Web Gateway Cloud Service?

На сайте https://trust.mcafee.com вы найдете актуальную информация о местонахождении наших центров обработки данных, их статусе и др.

Дополнительная информация

Для получения подробных сведений посетите наш сайт www.mcafee.com/ru/products/web-gateway-cloud-service.aspx.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru