McAfee Web Gateway Cloud Service

Повсеместная веб-защита из облака

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
- Использование платформы McAfee® ePolicy Orchestrator® (McAfee ePO™) Cloud в качестве единой консоли управления всеми защитными облачными службами Intel Security, позволяющее обеспечить беспрецедентно высокую эффективность управления

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, что и локально развернутые аппаратные устройства для защиты от сложных угроз, но только без необходимости платить за аппаратное обеспечение и его обслуживание. 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. Подключение конечных точек и даже целых местоположений к облаку позволяет обеспечить повсеместную защиту в пределах нового периметра, не ограниченного физическими границами сети.

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 облачной службы 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, и облачную службу. 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.

intel Security

Ключевые преимущества (продолжение)

- Проверенная архитектура: McAfee® Web Gateway Cloud Service представляет собой многопользовательскую версию McAfee Web Gateway — надежного аппаратного веб-шлюза, пользующегося доверием крупных компаний по всему миру

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 отказаться от 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

Служба McAfee Web Gateway Cloud Service предназначена для корпоративного сегмента. Для многих организаций ее использование будет означать более высокий уровень быстродействия, чем тот, который обеспечивают их локальные решения на данный момент. Так, например, при необходимости 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.

Рис. 1. Развертывание McAfee Web Gateway Cloud Service

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 наша облачная служба автоматически начнет перенаправлять весь веб-трафик в самый близкий и самый быстрый центр обработки данных, мгновенно обеспечивая бесперебойную защиту.

Кроме того, архитектура нашей облачной службы позволяет осуществлять пиринговое взаимодействие с опорной сетью Интернета в крупнейших точках обмена интернет-трафиком (IXP). 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 нередко удается устанавливать через нашу облачную службу более быстрое соединение, чем если бы они подключались непосредственно через открытый Интернет.

Служба McAfee Web Gateway Cloud Service действует по всему миру. Текущее расположение и статус центров обработки данных, работающих с веб-трафиком, можно отслеживать по адресу **https://trust.mcafee.com**. 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.

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) служба 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.

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 блокировать вредоносные программы и обеспечивать видимость облачных приложений внутри зашифрованных каналов.

Перед большинством ИТ-подразделений стоит непростая задача контроля за распространением облачных приложений, особенно в том, что касается «теневых информационных технологий» и риска, связанного с предоставленной пользователям свободой выбора служб и сервисов. Полная прозрачность всего веб-трафика, включая HTTPS-трафик, дает возможность генерировать типовые отчеты с информацией о посещенных веб-сайтах, используемых облачных приложениях и соответствующих данных для оценки риска. «Теневые информационные технологии» легко выявляются путем сравнения того, что на самом деле используется, с тем, на что имеется разрешение ИТ-подразделения. Другой проблемой являются облачные приложения, особенно облачные хранилища, которые в последнее время все чаще используются в качестве механизма доставки вредоносных программ. Возможность выявлять приложения, послужившие инструментом доставки вредоносных программ, помогает правильно задавать политики, а наличие полной информации об используемых облачных службах позволяет минимизировать риск с помощью более 1 600 способов осуществления контроля над облачными приложениями (запрет выгрузки файлов, запрет обмена сообщениями, полное блокирование приложений и др.).

Эффективное управление безопасностью

При наличии нескольких разных консолей и политик управление безопасностью представляет собой довольно обременительную задачу, особенно если управление локальными и облачными средствами веб-защиты осуществляется раздельно. В гибридной среде управление локальными и облачными развертываниями осуществляется с помощью одной консоли управления, одного набора политик и одного интерфейса для генерирования отчетов.

В какой точке мира находится McAfee Web Gateway Cloud Service?
На сайте **https://trust.mcafee.com** приведена актуальная информация о местонахождении наших центров обработки данных, их статусе и др.

Если служба McAfee Web Gateway Cloud Service развернута без использования локального аппаратного или программного обеспечения, то управление ею осуществляется с помощью McAfee ePO Cloud — единой консоли управления всеми защитными облачными службами Intel Security и средствами защиты конечных точек, позволяющей управлять безопасностью на беспрецедентно высоком уровне эффективности.

Развертывание средств веб-защиты для конечных устройств — задача не из простых, особенно в том, что касается маршрутизации и проверки подлинности. Развертываемый дополнительно клиент для конечных точек McAfee Client Proxy автоматизирует маршрутизацию трафика и проверку подлинности пользователей в нашей облачной службе, обеспечивая подключение к облаку из любой точки мира и согласованное применение политик. В случае гибридной модели с использованием локальных аппаратных устройств клиент McAfee Client Proxy обеспечивает интеллектуальную маршрутизацию пакетов, направляя их внутри сети в аппаратное устройство, а вне сети — в облачную службу. При необходимости организация может воспользоваться имеющимися в McAfee Client Proxy дополнительными параметрами маршрутизации трафика и проверки подлинности пользователей.

Дополнительная информация

Для получения более подробных сведений посетите наш сайт **www.mcafee.com/ru/products/web-protection.aspx**.

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com

Intel, логотипы Intel и McAfee, ePolicy Orchestrator и McAfee ePO являются товарными знаками Intel Corporation или McAfee, Inc. в США и/или других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Copyright © 2016 Intel Corporation. 1764_0916 Сентябрь 2016 г.